ViPNet Coordinator HW 4

Справочник команд и конфигурационных файлов

Версия продукта: 4.5.8

ViPNet Coordinator HW10
ViPNet Coordinator HW50
ViPNet Coordinator HW100
ViPNet Coordinator HW1000
ViPNet Coordinator HW2000
ViPNet Coordinator HW5000
ViPNet Coordinator VA

infotecs

ФРКЕ.00130-03 90 06

Версия продукта 4.5.8, документ обновлен 04.06.2025.

АО «ИнфоТеКС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

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

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

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

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

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую
Меню > Команда	Последовательность элементов или действий
`Код`	Имя файла, путь, фрагмент кода или команда в командной строке

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

Обозначения при описании команд в документе:

- Команды, которые участвуют в сценарии администратора, обозначены символом `#`

  ```
  hostname# admin config list
  ```

- Команды, которые участвуют в сценарии пользователя, обозначены символом `>`

  ```
  hostname> firewall local show
  ```

  Все команды, которые доступны пользователю, доступны и администратору.

- Параметры заключены в угловые скобки:

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

- Необязательные параметры или ключевые слова заключены в квадратные скобки:

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

- Допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:

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

Обратная связь

Контактная информация

- Единый многоканальный телефон:

  +7 (495) 737-6192,

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

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телеграм-канал поддержки: t.me/vhd21

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

- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

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

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

1

Справочник команд

Команды группы admin

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

admin add spare keys

Добавить файл с резервным набором персональных ключей (РНПК) на ViPNet Coordinator HW.

Синтаксис

```
admin add spare keys
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда автоматически выполняет поиск всех имеющихся на выбранном USB-носителе файлов с РНПК (`*.pk`). Для каждого найденного файла `*.pk` проверяется целостность и соответствие идентификатора пользователя идентификатору пользователя ViPNet Coordinator HW. Если файл не поврежден и идентификатор в нем совпал с идентификатором на узле, то он становится доступным для добавления.
- При выполнении команды у пользователя запрашивается пароль, которым защищен файл с РНПК. Файл с РНПК защищен паролем пользователя ViPNet Coordinator HW, который задан администратором сети ViPNet в программе ViPNet Administrator. Обычно он совпадает с текущим паролем пользователя, который используется для доступа к ViPNet Coordinator HW. Однако в процессе использования ViPNet Coordinator HW пароль пользователя мог изменяться (см. admin passwd). В этом случае пароль, на котором защищен РНПК будет отличаться от текущего пароля пользователя. Если вы не помните пароль, заданный в программе ViPNet Administrator, запросите его у администратора сети.

Пример использования

```
hostname# admin add spare keys
Please select the type of the media containing the pk-file:
       USB stick (u) or CD/DVD disc (c) [u/c] :
Insert the media containing the pk-file and press <Enter> to continue
Try to mount /dev/sdc1 as vfat
sdc1 - /tmp/pk-import/0001.pk
```

```
Please enter the password for decrypting the pk-file and press <Enter> to continue
The spare key set successfully imported
```

admin authentication-type-token

Изменить способ аутентификации пользователя ViPNet Coordinator HW.

Синтаксис

```
admin authentication-type-token
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Изменить способ аутентификации можно только на «Устройство». Изменение способа аутентификации с «Устройство» на «Пароль» запрещено по требованиям безопасности.
- Способ аутентификации «Устройство» поддерживается только при использовании ViPNet ЦУС в качестве управляющего ПО.
- При подключении по SSH команда недоступна.
- При работе ViPNet Coordinator HW в режиме кластера горячего резервирования изменение способа аутентификации достаточно выполнить на активном узле кластера. Изменения будут автоматически переданы на пассивный узел кластера при следующей синхронизации.
- При изменении способа аутентификации на «Устройство» в наличии должно быть внешнее устройство, на которое администратор сети ViPNet сохранил персональный ключ пользователя в процессе смены способа аутентификации в ViPNet ЦУС.

Внимание! В текущей версии ViPNet Coordinator HW могут использоваться только внешние устройства Рутокен Lite производства компании «Актив».

- Если при изменении способа аутентификации не будет подключено внешнее устройство, или оно будет извлечено раньше времени, команда не будет выполнена. Способ аутентификации не будет изменен. Информация о неудачном изменении способа аутентификации будет записана в системный журнал.

Пример использования

Чтобы изменить способ аутентификации:

```
hostname# admin authentication-type-token
```

```
In version 4.2, you can enhance security by two-factor authentication. As you switch to
the two-factor authentication, you will not be able to return to the previous settings
[Yes/No] Yes

Enter PIN code:
```

admin config delete

Удалить копию конфигурации VPN.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе имени копии работает автозаполнение с именами из списка сохраненных копий.
- В имени можно указать символ «*» для обозначения любого количества символов. Это позволит удалить сразу нескольких копий конфигурации VPN.
- Если версия не указана и при этом имеется несколько копий конфигурации VPN с совпадающими именами, но различными версиями, то выводится список таких копий конфигурации VPN с предложением указать версию для удаления.

Пример использования

```
hostname# admin config delete Config_*

Configuration 'Config_2024123' (version 2.0.0) deleted
```

admin config list

Просмотреть список сохраненных копий конфигурации VPN.

Синтаксис

```
admin config list
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Список сохраненных копий конфигурации VPN отображается в следующем формате:

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

где:

- `Name` — имя копии конфигурации VPN. Имя автоматически сохраненной копии начинается со слова `autosave`.
- `Version` — версия ПО ViPNet Coordinator HW, в которой была создана копия конфигурации VPN (может отсутствовать).
- `Type` — вид копии конфигурации VPN: `full` (полная) или `part` (частичная).
- `Date`, `Time` — дата и время создания копии конфигурации VPN.
- `Date-load`, `Time-load` — дата и время загрузки копии конфигурации VPN. Если копия конфигурации VPN никогда не загружалась, вместо даты и времени загрузки отображается `never loaded`.

Пример использования

```
hostname# admin config list
"Config_1", version 4.5.8, full, saved on 13.03.2024 at 20:06, never loaded
```

admin config load

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды остановите службы `failoverd`, `iplircfg`, `mftpd`. После выполнения запустите их.
- При вводе имени работает 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 введите имя, под которым будет сохранена копия текущей конфигурации.
- Если текущая версия ПО ViPNet Coordinator HW ниже версии, указанной в команде, дополнительно подтвердите загрузку настроек из копии конфигурации VPN.

Пример использования

Чтобы загрузить настройки из копии конфигурации VPN с именем `Rollback_config`, которая относится к версии `4.5.8`:

```
hostname# admin config load Rollback_config 4.5.8
```

admin config save

Сохранить копию текущей конфигурации VPN.

Синтаксис

```
admin config save <имя>
```

Параметры и ключевые слова

`<имя>` — имя копии конфигурации VPN.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

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

Пример использования

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

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

admin escape

Выйти в системную командную оболочку.

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

Синтаксис

```
admin escape
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе команды автодополнение не работает.
- После выполнения команды требуется ввести пароль администратора ViPNet Coordinator HW.

- Для возвращения в командный интерпретатор ViPNet Coordinator HW введите команду `exit`. После чего командный интерпретатор продолжит свою работу с того момента, в котором он находился перед выходом в системную оболочку.

Пример использования

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

admin export diagnostics

Экспортировать файлы конфигурации на компьютер по протоколу TFTP или на USB-носитель.

Синтаксис

```
admin export diagnostics {tftp | usb}
```

Параметры и ключевые слова

- `tftp` — экспорт на компьютер по протоколу TFTP.
- `usb` — экспорт на USB-носитель.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу служб `iplircfg` (см. iplir stop) и `mftpd` (см. mftp stop).

  При экспорте по TFTP остановите также работу службы `failoverd`.
- При экспорте по TFTP внешний IP-адрес интерфейса `eth1` изменится на 169.254.241.1, остальные сетевые интерфейсы будут отключены.
- Экспорт по протоколу TFTP в удаленной SSH-сессии запрещен.
- Имя файла экспорта формируется по шаблону `logs-<название ViPNet Coordinator HW>-%Y-%m-%d-%H-%M-%S.tar.gz`. По умолчанию `<название ViPNet Coordinator HW>` включает `<платформа ViPNet Coordinator HW>-<идентификатор узла>`.

- Если ViPNet Coordinator HW работает в составе кластера, экспортировать файлы конфигурации можно только на USB-носитель.
- При просмотре архива журнала в Windows время создания архива может отличаться от реального времени. При этом время событий в журналах будет правильным. Это связано с особенностями работы разных ОС с системным временем.

Пример использования

```
hostname# admin export diagnostics usb
```

admin export keys binary-encrypted

Экспортировать справочники, ключи и настройки ViPNet Coordinator HW на компьютер по протоколу TFTP или на USB-носитель.

Синтаксис

```
admin export keys binary-encrypted {tftp | usb}
```

Параметры и ключевые слова

- `tftp` — экспорт на компьютер по протоколу TFTP.
- `usb` — экспорт на USB-носитель.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Экспортировать справочники, ключи и настройки по протоколу TFTP в удаленной SSH-сессии запрещено.
- Имя файла экспорта формируется по шаблону `<название ViPNet Coordinator HW>-%Y-%m-%d-%H-%M-%S.vbe`. По умолчанию `<название ViPNet Coordinator HW>` включает `<платформа ViPNet Coordinator HW>-<идентификатор узла>`.
- Во избежание получения неработоспособного файла экспорта рекомендуем предварительно провести регламентное тестирование ViPNet Coordinator HW.
- В случае экспорта на USB-носитель перед выполнением команды завершите работу служб `iplircfg` (iplir stop) и `mftpd` (mftp stop).
- В случае экспорта на ноутбук по протоколу TFTP перед выполнением команды выгрузите драйверы и завершите работу всех служб ViPNet Coordinator HW (vpn stop).

- Экспорт на ноутбук по протоколу TFTP возможен только с сетевых интерфейсов с классом `access`. Интерфейсы, обрабатывающие трафик из сетей VLAN, и агрегированные интерфейсы не поддерживают функцию экспорта по TFTP.
- Если до начала экспорта на ноутбук по протоколу TFTP на ViPNet Coordinator HW запущен DHCP-сервер, то его работа будет автоматически завершена, а после окончания экспорта — автоматически восстановлена.

Пример использования

```
hostname# admin export keys binary-encrypted usb
Configuration file will be saved to /tmp/vipnet/hw1000-15ea000b-2024-02-09-12-12-12.vbe
Put hw1000-15ea000b-2024-02-09-12-12-12.vbe file onto USB drive.
Insert USB drive with at least 64KB free space and press Enter
1) General USB Flash Drive partition 3839Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc1 as vfat
Partition /dev/ was successfully mounted on /usb.
Copying files hw1000-15ea000b-2024-02-09-12-12-12.vbe to /dev/sdc1. Press ^+C to abort.
File hw1000-15ea000b-2024-02-09-12-12-12.vbe was successfully copied onto the USB drive.
You may remove the USB drive.
```

admin export logs

Экспортировать системный журнал ViPNet Coordinator HW и файлы конфигурации на компьютер по протоколу TFTP или на USB-носитель.

Чтобы экспортировать только файлы конфигурации, используйте команду `admin export diagnostic` (см. admin export diagnostics).

Синтаксис

```
admin export logs {tftp | usb} [nodiag]
```

Параметры и ключевые слова

- `tftp` — экспорт на компьютер по протоколу TFTP.
- `usb` — экспорт на USB-носитель.
- `nodiag` — не экспортировать файлы конфигурации. При указании этого параметра экспортируется только системный журнал.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При экспорте на USB-носитель остановите работу служб `iplircfg` (см. iplir stop) и `mftpd` (см. mftp stop).

  При экспорте с пассивного узла кластера остановите также работу службы `failoverd`.

- При экспорте по TFPT остановите работу служб `failoverd`, `iplircfg` (см. iplir stop) и `mftpd` (см. mftp stop).
- При экспорте по TFTP внешний IP-адрес интерфейса `eth1` изменится на 169.254.241.1, остальные сетевые интерфейсы будут отключены.
- Экспортировать файлы журнала и файлы конфигурации по протоколу TFTP в удаленной SSH-сессии запрещено.
- Имя файла экспорта формируется по шаблону `logs-<название ViPNet Coordinator HW>-%Y-%m-%d-%H-%M-%S.tar.gz`. По умолчанию `<название ViPNet Coordinator HW>` включает `<платформа ViPNet Coordinator HW>-<идентификатор узла>`.
- Если ViPNet Coordinator HW работает в составе кластера, экспортировать файлы системного журнала и файлы конфигурации можно только на USB-носитель.
- При просмотре архива журнала в Windows время создания архива может отличаться от реального времени. При этом время событий в журналах будет правильным. Это связано с особенностями работы разных ОС с системным временем.

Пример использования

- Чтобы экспортировать системный журнал и файлы конфигурации на USB-носитель:

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

- Чтобы экспортировать только системный журнал на USB-носитель:

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

admin export packetdb usb

Экспортировать журнал регистрации IP-пакетов на USB-носитель.

Синтаксис

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

Параметры и ключевые слова

`<имя>` — имя файла экспорта.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

```
hostname# admin export packetdb usb ippacket
Put ippacket.tar.gz file onto USB drive.
Insert USB drive and press Enter
1) JetFlash Transcend 4GB partition 3825Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc as is
Partition /dev/sdc was successfully mounted on /usb.
File ippacket.tar.gz to be copied onto the USB drive.
File ippacket.tar.gz was successfully copied onto the USB drive.
You may remove the USB drive.
```

admin export-and-clear logs

Экспортировать файл системного журнала ViPNet Coordinator HW на компьютер по протоколу TFTP или на USB-носитель с их последующим удалением на ViPNet Coordinator HW.

Синтаксис

```
admin export-and-clear logs {tftp | usb}
```

Параметры и ключевые слова

- `tftp` — экспорт на компьютер по протоколу TFTP.
- `usb` — экспорт на USB-носитель.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды рекомендуется остановить службы `iplircfg` (см. iplir stop) и `mftpd` (см. mftp stop).
- При выборе метода экспорта файлов журнала по протоколу TFTP внешний IP-адрес интерфейса `eth1` изменится на 169.254.241.1, а остальные сетевые интерфейсы будут отключены.
- Экспортировать файлы журнала по протоколу TFTP в удаленной SSH-сессии запрещено.
- Имя файла экспорта формируется по шаблону `logs-<название ViPNet Coordinator HW>-%Y-%m-%d-%H-%M-%S.tar.gz`. По умолчанию `<название ViPNet Coordinator HW>` включает `<платформа ViPNet Coordinator HW>-<идентификатор узла>`.
- Если ViPNet Coordinator HW работает в составе кластера горячего резервирования, экспортировать файлы системного журнала можно только на USB-носитель.

Пример использования

```
hostname# admin export-and-clear logs usb
Are you sure to export and remove logs [Yes/No] : Yes
Packing of log files  in progress. Press ^+C to abort.

Stopping system log daemon: syslogd.

Starting system log daemon: syslogd.
Please insert the USB flash drive and press Y to continue [Yes/No] : Yes
Put logs-hw1000-15ea000b-2024-02-09-12-12-12.tar.gz file onto USB drive.
Insert USB drive and press Enter
1) JetFlash Transcend 32GB partition 30639Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc1 as vfat
Partition /dev/sdc1 was successfully mounted on /usb.
Copying files logs-hw1000-15ea000b-2024-02-09-12-12-12.tar.gz to /dev/sdc1. Press ^+C to
abort.
File logs-hw1000-15ea000b-2024-02-09-12-12-12.tar.gz was successfully copied onto the USB
drive.
You may remove the USB drive.
Try to mount /dev/sdc1 as vfat
Logs archive file integrity check successful.
Logs exported and removed from ViPNet Coordinator successfully.
```

admin keys remove

Удалить ключи, справочники и настройки ViPNet Coordinator HW.

Синтаксис

```
admin keys remove
```

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

admin keys update

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

Синтаксис

```
admin keys update
```

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

```
hostname# admin keys update

This command updates all VPN keys and cannot be reverted.

After VPN keys  update all user sessions will be closed

All settings will be updated according to new dst file

All VPN service will be restarted


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

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


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

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

Try to mount /dev/sdc as vfat

Found several application initialization files:

1 - abn_0034.dst Coordinator

2 - abn_0012.dst Coordinator


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

Type password:


Applying keys update.... Please wait.

Keys update completed.
```

admin kick

Завершить сессию командного интерпретатора.

Синтаксис

```
admin kick {tty<N> | ttyS<N> | pts/<N>}
```

Параметры и ключевые слова

- `tty<N>` — номер сессии, запущенной на обычной консоли.

- `ttyS<N>` — номер сессии, запущенной на COM-консоли.
- `pts/<N>` — номер сессии, которая запущена на удаленном узле, подключенном к ViPNet Coordinator HW по протоколу SSH.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Нельзя завершить сессию командного интерпретатора, в которой выполняется команда. Для завершения такой сессии следует использовать команду `exit`.
- Для просмотра информации обо всех запущенных сессиях командного интерпретатора используется команда `who`.

Пример использования

Чтобы завершить работу командного интерпретатора на компьютере tty1:

```
hostname# admin kick tty1
```

admin passwd

Изменить пароль пользователя ViPNet Coordinator HW.

Синтаксис

```
admin passwd
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Внимание! При работе ViPNet Coordinator HW в кластере сначала выполните команду на пассивном узле, затем — на активном.
Пароли на обоих узлах кластера должны совпадать.

- При выполнении команды требуется ввести текущий пароль пользователя или администратора, затем дважды ввести новый пароль для пользователя.
- При вводе пароля на экране не отображаются вводимые символы, а курсор остается неподвижным.
- Минимальная длина пароля — 6 символов.

Пример использования

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

admin show check integrity status

Просмотреть информацию о последней проверке целостности файлов:

- время последней проверки;
- результаты проверки.

Синтаксис

```
admin show check integrity status
```

Режимы командного интерпретатора

Администратор.

Пример использования

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

admin ssh reset-key

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

admin ssh reset-key local

Перевыпустить ключи локального SSH-сервера ViPNet Coordinator HW.

Синтаксис

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

Режимы командного интерпретатора

Администратор.

Особенности

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

Пример использования

```
hostname# admin ssh reset-key local

command: admin ssh remove key local

Resetting DSA-Hostkey...

Generating public/private dsa key pair.

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

```
Your public key has been saved in /mnt/main/etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
SHA256:TvsHXJ9ybY3Rmoy2L8Pfut5JN0TpdLNuOkp3nuXaisw root@hostname
The key's randomart image is:
+---[DSA 1024]----+
|                 |
|                .|
|               *.|
|            . = =|
|        S. . + @.|
|       o .o + @ +|
|        o  = = Bo|
|         ..oBo*=*|
|          .oEBXO=|
+----[SHA256]-----+
Resetting RSA-Hostkey...
Generating public/private rsa key pair.
Your identification has been saved in /mnt/main/etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /mnt/main/etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
SHA256:Q6PlZVt8y5eEh+lnC3yuP5CS6u2P8H4CTkA3xyOFOEY root@hostname
The key's randomart image is:
+---[RSA 2048]----+
|      .E. +.     |
|       = = =  +  |
|      o * * ++.o |
|       * + oooo..|
|      . S . .++=.|
|         + o o*..|
|        o.o . .o |
|         o+..... |
|        ..o*+o...|
+----[SHA256]-----+
```

admin ssh show-key

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы просмотреть информацию о ключах локального SSH-сервера:

```
hostname# admin ssh show-key local
command: admin ssh show key local
Local host ssh public keys:
============================================================
Key type: ssh-dsa(ssh2)
Fingerprint: SHA256:Q5/e7nofhVTre1K72AWf0V0K1FxqUysfVxMQP0PnIuw
```

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

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

Key type: ssh-rsa(ssh2)

Fingerprint: SHA256:Txn8IloRmfAbD+l/F6/UWah4DfwGu2cKXDGiDE5VXQk

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

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

admin upgrade software usb

Обновить ПО ViPNet Coordinator HW вручную с USB-носителя.

Внимание! Не используйте для обновления более раннюю версию ПО, это приведет к неполадкам в работе координатора.

Синтаксис

```
admin upgrade software usb
```

Режимы командного интерпретатора

Администратор.

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
...
Machine will be rebooted. Remove USB disk and press <Enter>
```

Команды группы alg

Управление обработкой прикладных протоколов.

alg module direct-media

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

Чтобы настройки вступили в силу, перезапустите основные службы и драйверы:

```
hostname# vpn stop
```

```
hostname# vpn start
```

Пример использования

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

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

alg module h323 direct-h245

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

Чтобы настройки вступили в силу, перезапустите основные службы и драйверы:

```
hostname# vpn stop
```

```
hostname# vpn start
```

Пример использования

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

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

alg module process off

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

По умолчанию включена обработка всех прикладных протоколов.

Пример использования

Чтобы выключить обработку прикладного протокола `DNS`:

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

alg module process on

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

alg show

Просмотреть текущие параметры обработки прикладных протоколов.

Синтаксис

```
alg show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> alg show
H323 direct media: off
H323 direct h245: off
SIP direct media: off

================================================================================
SERVICE        PROTOCOL PORTS                                           ON/OFF
================================================================================
FTP            TCP      21                                              ON
--------------------------------------------------------------------------------
DNS            UDP      53                                              ON
--------------------------------------------------------------------------------
H323           TCP      1720                                            ON
--------------------------------------------------------------------------------
H323           UDP      1719                                            ON
--------------------------------------------------------------------------------
SCCP           TCP      2000                                            ON
--------------------------------------------------------------------------------
```

```
SIP             TCP      5060,5080                                          ON
-------------------------------------------------------------------------------
SIP             UDP      5060,5080                                          ON
-------------------------------------------------------------------------------
hostname>
```

Таблица с параметрами обработки содержит следующие столбцы:

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

Команды группы failover

Настройка и управление системой защиты от сбоев ViPNet Coordinator HW.

failover config edit

Редактировать конфигурационный файл системы защиты от сбоев failover.ini.

Синтаксис

```
failover config edit
```

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

failover config mode

Задать режим работы системы защиты от сбоев.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы переключить систему защиты от сбоев в режим кластера:

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

failover show active-mac-address

Просмотреть доступность активного узла кластера со стороны пассивного узла.

Синтаксис

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

- Если активный узел кластера доступен:

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

- Если активный узел кластера недоступен:

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

failover show config

Просмотреть конфигурационный файл системы защиты от сбоев failover.ini.

Синтаксис

```
failover show config
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

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

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

failover show info

Просмотреть информацию о текущем состоянии системы защиты от сбоев.

Синтаксис

```
failover show info
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> failover show info
Running failover info
  Versions: ViPNet 4.5.8(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) Wed Feb 21 15:40:48 2024

  failover mode                  * single
  failover uptime                * 0d 0:14
  total cpu                      * 3%
  total memory                   * 2055488 kB
  available memory         * 1170348 kB
  failover state                 * works
  failover cpu                   * 1%
  iplir state              * works
  iplir cpu                      * 4%
  mftp state               * works
  mftp cpu                       * 1%
  webgui state                   * works
  webgui cpu               * 0%
```

По команде отображается следующая информация:

- версия ПО ViPNet Coordinator HW и версия службы `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 служб `mftpd`, `failoverd` и `webgui`.

failover show sync-connections

Просмотреть количество сетевых соединений в кеше узла кластера.

Синтаксис

```
failover show sync-connections
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

```
hostname> failover show sync-connections

Synchronized connections count         150000
```

failover start

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Параметр доступен только в режиме кластера.
- Если в режиме кластера параметр не указан, служба `failoverd` будет запущена в том режиме, в котором она находилась до завершения работы.
- Перед запуском службы `failoverd` в активном режиме убедитесь, что на другом узле кластера служба `failoverd` запущена в пассивном режиме. Запуск службы `failoverd` в активном режиме на обоих узлах кластера приведет к конфликту IP-адресов и другим нежелательным последствиям.

Пример использования

Чтобы запустить службу `failoverd` в пассивном режиме:

```
hostname> failover start passive
```

failover stop

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

Синтаксис

```
failover stop
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

failover view

Просмотреть журнал переключений кластера за заданный период времени.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

```
hostname> failover view 09.03.2024.08.00.00 23.03.2024.19.00.00
  View journal of failover switching
  Versions: ViPNet 4.5.8 (3935), daemon 1.5 (1)
  Workstation configured for ID 1031F
  The workstation works in a cluster mode of protection against failures
  Workstation time (utc: 1174916969) Mon Mar 29 17:49:29 2024

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

Команды группы firewall

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

firewall add

Создать сетевой фильтр или правило трансляции адресов.

Синтаксис

```
firewall <тип> add [<номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя>
[<протокол>] [<расписание>] <действие>
```

Параметры и ключевые слова

- `<тип>` — тип создаваемого сетевого фильтра или указание на создание правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `tunnel` — фильтр туннелируемых узлов;
  - `vpn` — фильтр защищенной сети;
  - `nat` — правило трансляции адресов.
- `<номер>` — порядковый номер фильтра (правила трансляции) в таблице, определяющий его приоритет.
- `<имя>` — имя фильтра (правила трансляции). Не используйте в имени фильтра кириллицу.
- `<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).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если номер не указан, фильтр (правило трансляции) добавляется в конец соответствующей таблицы и будет применяться при анализе IP-трафика в последнюю очередь.
- Если указанный номер меньше последнего номера в таблице, нумерация фильтров (правил трансляции), следующих за новым фильтром (правилом трансляции), будет автоматически изменена (их номера будут увеличены на 1).
- Если в имени фильтра есть пробел, ограничьте имя кавычками (например, `"Rule 2"`).
- В качестве адреса отправителя или получателя можно указать:
  - для локальных фильтров открытой сети — IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску адресов подсети, доменное имя сети, системную группу объектов `any`, `local` или `remote`, одну или несколько пользовательских групп IP-адресов;
  - для транзитных фильтров открытой сети: то же, что для локальных фильтров открытой сети, но в таких фильтрах нельзя использовать системные группы объектов `local` или `remote`;
  - 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. Фильтры защищенной сети используются только для локального защищенного трафика, поэтому:
    - если в качестве адреса получателя задано любое значение, кроме группы `local` или `broadcast`, то в качестве адреса отправителя может быть задана только группа `local`;
    - если в качестве адреса отправителя задано любое значение, кроме группы `local`, то в качестве адреса получателя может быть задана группа `local` или `broadcast`.
  - для фильтров туннелируемых узлов — то же, что для локальных фильтров открытой сети и фильтров защищенной сети, но в таких фильтрах можно использовать только системные группы объектов `any`, `allcoordinators`, `allclients` или `tunneledip`;
  - для правил трансляции адресов — IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску адресов подсети, доменное имя сети, одну или несколько пользовательских групп IP-адресов.
- В качестве адреса отправителя для локальных, 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>}}
  ```

- Для правил трансляции адресов при задании адреса отправителя или получателя можно указывать, соответственно, входящий (`src`) или исходящий (`dst`) интерфейсы собственного узла в виде:
  - входящий интерфейс: `src interface {<системное имя интерфейса> | @<имя группы интерфейсов> | byip {<IP-адрес> | <диапазон IP-адресов> | <маска подсети>}}`
  - исходящий интерфейс: `dst interface {<системное имя интерфейса> | @<имя группы интерфейсов> | byip {<IP-адрес> | <диапазон IP-адресов> | <маска подсети>}}`

при этом:

- в одном правиле трансляции нельзя указывать одновременно и входящий и исходящий интерфейсы;
- для правил с трансляцией адреса назначения можно указать только входящий интерфейс;
- для правил с трансляцией адреса источника можно указать только исходящий интерфейс.

- В качестве адреса получателя также можно указать:
  - для локальных фильтров открытой сети — системную группу `broadcast` или `multicast`;
  - для фильтров защищенной сети — системную группу `broadcast`.
- Протокол можно указать, используя:
  - имена протоколов, написанные строчными буквами и разделенные пробелами. При этом можно также задать дополнительные параметры для протоколов:
    - TCP и UDP: `sport` (порт или диапазон портов источника пакета) и/или `dport` (порт или диапазон портов назначения пакета). При использовании обоих этих параметров сначала укажите параметр `sport`, затем — параметр `dport`. Возможно указать несколько портов или диапазонов портов, в этом случае укажите название протокола (`tcp` или `udp`) перед каждым номером порта (диапазоном портов). Например: `tcp sport 2525 tcp dport 443 tcp dport 4444-4445`.
    - ICMP: только параметр `type` (тип пакета) либо параметр `type` вместе с параметром `code` (код пакета). Если параметр `code` не задан, то под условие будут подпадать все ICMP-пакеты указанного типа;
  - номера протоколов. При этом перед номером каждого протокола укажите ключевое слово `proto`;
  - пользовательские группы протоколов в виде: `service @<имя группы>`.
- Расписание можно задать, используя одну из лексем:
  - `daily <чч:мм>-<чч:мм>` — фильтр действует ежедневно в течение заданного интервала времени. Время указывается в 24-часовом формате: `чч` — часы, `мм` — минуты.
  - `weekly [mo] [tu] [we] [th] [fr] [sa] [su] [at <чч:мм>-<чч:мм>]` — фильтр действует еженедельно в заданные дни недели:
    - `mo` — понедельник;
    - `tu` — вторник;
    - `we` — среда;
    - `th` — четверг;
    - `fr` — пятница;
    - `sa` — суббота;
    - `su` — воскресенье.
  - `calendar <дд.мм.гггг>-<дд.мм.гггг> [at <чч:мм>-<чч:мм>]` — фильтр действует в заданные даты и интервал времени. Дата указывается в следующем формате:

- `дд` — день;
- `мм` — месяц;
- `гггг` — год.

- `schedule @<имя группы объектов>` — фильтр действует по расписанию, описанному группой объектов соответствующего типа.

Также для задания расписания можно использовать соответствующие пользовательские группы объектов.

- Действие задается одной из 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 «Настройка с помощью командного интерпретатора», в главах «Настройка сетевых фильтров» и «Настройка правил трансляции адресов».

Пример использования

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

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

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

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

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

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

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

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

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

firewall add name

Создать группу объектов заданного типа.

Синтаксис

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

Параметры и ключевые слова

- `<тип>` — тип объектов. Можно указать одно из следующих значений:
  - `ip-object` — IP-адреса;
  - `vpn-object` — сетевые узлы ViPNet;
  - `interface-object` — сетевые интерфейсы;
  - `service-object` — протоколы;
  - `schedule-object` — расписания.
- `<имя>` — имя группы объектов. Допустимые символы: a–z, A–Z, 0–9, _ и точка.
- `<состав>` — объекты, входящие в группу.
- `<исключения>` — объекты, не входящие в группу.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Примеры использования

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

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

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

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

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

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

firewall change append

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

Синтаксис

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

Параметры и ключевые слова

- `<тип>` — тип изменяемого сетевого фильтра или указание на изменение правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `tunnel` — фильтр туннелируемых узлов;
  - `vpn` — фильтр защищенной сети;
  - `nat` — правило трансляции адресов.
- `<номер>` — порядковый номер фильтра (правила трансляции) в таблице.
- `<адрес отправителя>` — добавляемый адрес отправителя IP-пакетов.
- `<адрес получателя>` — добавляемый адрес получателя IP-пакетов.
- `<протокол>` — добавляемый протокол, по которому передаются IP-пакеты.
- `<расписание>` — добавляемое расписание применения фильтра (правила трансляции).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Синтаксис адреса отправителя, адреса получателя, протокола и расписания — тот же, что при создании сетевого фильтра (правила трансляции) с помощью команды firewall add.

- Можно указать несколько параметров.

Пример использования

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

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

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

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

firewall delete

Удалить сетевой фильтр или правило трансляции адресов.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

- Поиск фильтров (правил трансляции) для удаления выполняется по строгому совпадению с заданными параметрами.
- Номера фильтров или правил трансляции, следующих за удаленным фильтром или правилом трансляции, автоматически уменьшаются на 1.

Пример использования

Чтобы удалить локальный фильтр открытой сети с номером 7:

```
hostname# firewall local delete 7
+====+=======================+============+==========+
|Num |Name                   |Option      |Schedule  |
+----+-----------+-----------+------------+----------+
|Act |Protocol    |Source    |Destination            |
+====+============+==========+============+==========+
|7   |Allow syslog outgoing   |User        |          |
+----+-----------+-----------+------------+----------+
|pass|udp: to 514 |@local     |@any                   |
+====+============+==========+============+==========+
Do you want to perform the action on the above rule? [Yes/No]:
```

firewall move rule

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

firewall object delete

Удалить группу объектов с заданным именем.

Синтаксис

```
firewall object delete @<имя>
```

Параметры и ключевые слова

`<имя>` — имя группы объектов.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы удалить группу объектов с именем `IP_group`:

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

firewall object show

Просмотреть все группы объектов.

Синтаксис

```
firewall object show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

```
hostname> firewall object show
Ip Objects
================================================================================
Num  Name                                          Creation type
Inclusion                              Exclusion
================================================================================
1    PrivateNetworkIP                              User
10.0.0.0/255.0.0.0, 172.16.0.0/
255.240.0.0, 192.168.0.0/255.255.0.0
--------------------------------------------------------------------------------
2    InternetIP                                    User
@any                                   @PrivateNetworkIP
--------------------------------------------------------------------------------
```

```
Service Objects
================================================================================
Num  Name                                                 Creation type
Inclusion                              Exclusion
================================================================================
1    DHCP                                                 User
udp: from 67-68 to 67-68
--------------------------------------------------------------------------------
2    CITRIX                                               User
tcp: to 1494
--------------------------------------------------------------------------------
...
```

firewall rules show

Просмотреть все сетевые фильтры и правила трансляции адресов.

Синтаксис

```
firewall rules show [<параметр>]
```

Параметры и ключевые слова

`<параметр>` — параметры фильтров (правил трансляции), отбираемых для просмотра. Можно указать следующие параметры: порядковый номер, адрес отправителя, адрес получателя, протокол, действие фильтра или правила.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

- `Num` — порядковый номер фильтра (правила трансляции) в таблице;
- `Name` — имя фильтра (правила трансляции);
- `Option` — категория фильтра (правила трансляции);
- `Schedule` — расписание применения фильтра (правила трансляции);
- `Act` — действие фильтра (правила трансляции);
- `Source` — адрес отправителя IP-пакетов;
- `Destination` — адрес получателя IP-пакетов;

- `Protocol` — протокол, по которому передаются IP-пакеты.

Пример использования

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

firewall show

Просмотреть указанные группы объектов, сетевые фильтры или правила трансляции адресов.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

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`.
- Можно указать несколько параметров.
- Поиск фильтров (правил трансляции) выполняется по строгому совпадению с указанными параметрами.
- В результате выполнения команды отображается таблица, содержащая соответствующие типы групп объектов, сетевых фильтров или правил трансляции адресов.

Пример использования

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

Команды группы inet

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

inet bonding add

Настроить агрегированный интерфейс.

Синтаксис

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

Параметры и ключевые слова

- `<номер>` — номер добавляемого агрегированного интерфейса. Возможные значения: 0–7.
- `<режим>` — режим работы агрегированного интерфейса. Можно указать один из следующих режимов:
  - `balance-rr` — режим, при котором исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные физические интерфейсы поочередно: первый пакет отправляется через один подчиненный интерфейс, второй пакет — через следующий подчиненный интерфейс и так далее.
  - `balance-xor` — режим, при котором подчиненный физический интерфейс, через который отправляется тот или иной пакет, выбирается на основе значения хэш-функции, вычисляемой по алгоритму, задаваемому с помощью команды inet ifconfig bonding xmit-hash-policy. В результате пакеты от одного и того же отправителя к одному и тому же получателю всегда будут отправляться через один и тот же подчиненный интерфейс.
  - `balance-tlb` — режим, при котором ведется подсчет размера исходящих пакетов, переданных через каждый из подчиненных физических интерфейсов, и на основе этого выполняется балансировка исходящего трафика между подчиненными интерфейсами.
  - `802.3ad` — режим динамического агрегирования с использованием протокола LACP. В этом режиме агрегированный интерфейс работает следующим образом:
    - среди подчиненных физических интерфейсов формируются группы — «агрегаторы», скорость передачи данных на интерфейсах которых одинакова;
    - один из агрегаторов выбирается активным в соответствии с алгоритмом, задаваемым с помощью команды inet ifconfig bonding ad-select;
    - внутри агрегатора подчиненный физический интерфейс, через который отправляются исходящие пакеты, выбирается аналогично режиму `balance-xor`;
    - в случае сбоя на физическом интерфейсе, входящем в агрегатор, или при добавлении нового подчиненного физического интерфейса в качестве активного выбирается

другой агрегатор (также в соответствии с алгоритмом, задаваемым с помощью команды inet ifconfig bonding ad-select);

- с другим сетевым оборудованием происходит обмен пакетами LACP с периодичностью, задаваемой с помощью команды inet ifconfig bonding lacp-rate, что позволяет определить сбой подчиненного интерфейса даже в том случае, если этот интерфейс подключен к другому сетевому узлу не напрямую (например, через медиаконвертер).

- `active-backup` — режим, при котором один из подчиненных физических интерфейсов назначается основным (автоматически или явно с помощью команды inet ifconfig bonding primary) и все исходящие пакеты отправляются через него. При этом в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.
- `broadcast` — режим, при котором пакеты, попадающие на агрегированный интерфейс, отправляются через все подчиненные физические интерфейсы одновременно.

- `<интерфейс 1>`, `<интерфейс N>` — физические интерфейсы, подчиненные создаваемому агрегированному интерфейсу. Количество подчиненных интерфейсов ограничено только общим количеством интерфейсов на ViPNet Coordinator HW.

Значения по умолчанию

Агрегированные интерфейсы не заданы.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Можно задать до восьми агрегированных интерфейсов.
- В результате выполнения команды создается агрегированный интерфейс с именем `bond<номер>`.
- Задаваемые подчиненные физические интерфейсы должны относиться к классу `slave` (см. inet ifconfig class).
- При добавлении агрегированного интерфейса задайте хотя бы один подчиненный ему физический интерфейс. Количество подчиненных интерфейсов ограничено только общим количеством интерфейсов на ViPNet Coordinator HW. Вы можете добавить подчиненные физические интерфейсы с помощью команды inet ifconfig bonding add.
- Режим `broadcast` требует специальной настройки сетевого оборудования, предотвращающей дальнейшую передачу по сети нескольких копий пакетов данных.
- Если агрегированный канал работает в режиме `broadcast`, организовать на этом канале защиту соединения по технологии L2OverIP невозможно.
- Для работы агрегированного интерфейса в режиме `balance-tlb` подключите все подчиненные физические интерфейсы к сети через коммутатор.

- Максимальное количество интерфейсов в ViPNet Coordinator HW (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.
- Механизм MC-LAG (MLAG) в режиме 802.3ad не поддерживается. Поэтому физические порты разных ViPNet Coordinator HW нельзя использовать в одном агрегированном интерфейсе.

Пример использования

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

```
hostname# inet ifconfig eth0 class slave

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

and then restart them.

eth0 set to slave class.

hostname# inet ifconfig eth1 class slave

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

and then restart them.

eth1 set to slave class.

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

New bond interface bond1 was created
```

inet bonding delete

Удалить агрегированный интерфейс.

Синтаксис

```
inet bonding delete <номер>
```

Параметры и ключевые слова

`<номер>` — номер удаляемого агрегированного интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

- Если вы хотите удалить агрегированный интерфейс класса `trunk` (см. inet ifconfig class), предварительно удалите все соответствующие ему виртуальные интерфейсы с помощью команды inet ifconfig vlan delete.

Пример использования

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

inet clear mac-address-table

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

Синтаксис

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

Режимы командного интерпретатора

Администратор.

Пример использования

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

inet dgd

В группу команд `inet dgd` входят команды для управления настройками службы DGD (Dead Gateway Detection).

inet dgd configuration default

Сбросить параметры службы DGD на значения по умолчанию:

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

Синтаксис

```
inet dgd configuration default
```

Значения по умолчанию

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

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы сбросить параметры службы DGD на значения по умолчанию:

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

inet dgd configuration interval-time

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию соединение проверяется каждые 3 секунды.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dgd configuration response-time

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию время ожидания ответа составляет 3 секунды.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dgd configuration retries-count

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию проверка работоспособности шлюза выполняется 3 раза.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы считать шлюз нерабочим после 5 проверок:

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

inet dgd configuration syslog-level

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

Синтаксис

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

Параметры и ключевые слова

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

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

Каждый последующий уровень включает в себя предыдущие.

Значение `-1` отключает регистрацию событий службы DGD.

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dgd next-hop add

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

Синтаксис

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

Параметры и ключевые слова

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

- `<адрес шлюза>` — IP-адрес удалённого шлюза.
- `<интерфейс>` — имя сетевого интерфейса ViPNet Coordinator HW. Данный параметр доступен только для сетевых интерфейсов, получающих IP-адрес по протоколу DHCP.
- `<тестовый адрес>` — тестовый IP-адрес шлюза. Несколько шлюзов могут иметь один и тот же тестовый IP-адрес. Он может совпадать с IP-адресом самого шлюза. Если значение параметра не задано, то в качестве тестового IP-адреса используется IP-адрес шлюза.

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

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

Пример использования

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

  ```
  hostname# inet dgd next-hop add gateway1 address 192.168.23.56 test-address 192.168.23.1 check icmp
  ```
- Чтобы отключить проверку по протоколу TCP (порт 443) состояния шлюза с именем `gateway2` по интерфейсу `eth1`:

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

inet dgd next-hop delete

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы удалить проверку состояния шлюза с именем `gateway1`:

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

inet dgd mode

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Автоматический запуск службы DGD выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dgd rule add action-priority

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dgd rule add match-next-hop

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dgd rule clear

Удалить все проверки и действия из ранее заданных правил шлюзов.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dgd rule delete action-priority

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dgd rule delete match-next-hop

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp client route-default-metric

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

`70`

Режимы командного интерпретатора

Администратор.

Пример использования

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

inet dhcp client route-distance

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp relay add backup-interface

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp relay add external-interface

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp relay add listen-interface

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из списка интерфейсов, которые имеются в системе, но отсутствуют в списке принимающих DHCP-запросы.
- Максимальное количество интерфейсов, принимающих DHCP-запросы — 32.
- Добавляемый интерфейс должен иметь статический адрес.
- Добавляемый интерфейс не должен использоваться в других копиях DHCP-relay.
- В качестве сетевого интерфейса нельзя задать:
  - интерфейс модема (ppp0) — нет в исполнении ViPNet Coordinator VA;
  - интерфейс «внутренней петли» (loopback, localhost);
  - виртуальные интерфейсы, созданные после назначения дополнительных IP-адресов физическим интерфейсам (alias).

Пример использования

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

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

inet dhcp relay delete backup-interface

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp relay delete external-interface

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp relay delete listen-interface

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp relay mode

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде изменяется только настройка автоматического запуска службы DHCP-relay, ее текущее состояние не изменяется.

- Невозможно включить автоматический запуск в следующих случаях:
  - Включен автоматический запуск DHCP-сервера.
  - Не заданы какие-либо настройки службы DHCP-relay.

Пример использования

Чтобы включить автоматический запуск службы DHCP-relay:

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

inet dhcp relay reset

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

inet dhcp relay start

Запустить службу DHCP-relay.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

Невозможно запустить службу DHCP-relay в следующих случаях:

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

Пример использования

Чтобы запустить копию 2 процесса DHCP-relay:

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

inet dhcp relay stop

Завершить работу службы DHCP-relay.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы завершить работу копии 2 процесса DHCP-relay:

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

inet dhcp server add default-lease-time

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию время аренды составляет 864000 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add dns

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

- С помощью последовательного выполнения команд можно добавить до 10 IP-адресов DNS-серверов.

Пример использования

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

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

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

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

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

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

inet dhcp server add domain

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

- При добавлении более одного имени домена выдается сообщение, что предыдущее значение будет перезаписано.

Пример использования

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

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

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

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

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

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

inet dhcp server add host

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

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

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

inet dhcp server add interface

Задать рабочий интерфейс DHCP-сервера.

Синтаксис

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

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add max-lease-time

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Время аренды составляет 864000 секунд.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add ntp

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

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

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

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

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

inet dhcp server add option

Добавить опцию DHCP-сервера в соответствии с RFC 2132.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add range

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add relay-interface

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add router

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add subnet-mask

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add tftp

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add voip

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server add wins

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server delete default-lease-time

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server delete dns

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

Синтаксис

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

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес DNS-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес DNS-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес DNS-сервера.
- `<маска>` — маска удаленной подсети.

- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес DNS-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

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

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

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

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

inet dhcp server delete domain

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

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

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

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

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

inet dhcp server delete host

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

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

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

inet dhcp server delete interface

Удалить рабочий интерфейс DHCP-сервера.

Синтаксис

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

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server delete max-lease-time

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server delete ntp

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

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

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

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

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

inet dhcp server delete option

Удалить опцию DHCP-сервера в соответствии с RFC 2132.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы удалить опцию DHCP-сервера 69 (сервер SMTP по умолчанию) для сетевого интерфейса `eth1`:

```
hostname# inet dhcp server delete option 69 interface eth1
```

inet dhcp server delete range

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

Синтаксис

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

Параметры и ключевые слова

- `<начало диапазона>` — начальный IP-адрес диапазона.
- `<конец диапазона>` — конечный IP-адрес диапазона.
- `<интерфейс>` — название сетевого интерфейса в системе, на котором задан диапазон IP-адресов, выделяемых DHCP-сервером.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается информация о диапазоне IP-адресов.

- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы удалить выделяемый DHCP-сервером клиентам сети 192.168.10.0/24 диапазон 192.168.10.2–192.168.10.254:

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

inet dhcp server delete relay-interface

Удалить сетевой интерфейс DHCP-сервера, на котором обрабатываются запросы от агента DHCP-relay, работающего в удаленной подсети.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server delete router

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server delete subnet-mask

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server delete tftp

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server delete voip

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

Синтаксис

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

Параметры и ключевые слова

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

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server delete wins

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

inet dhcp server mode

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Автоматический запуск DHCP-сервера выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде изменяется только настройка автоматического запуска DHCP-сервера, его текущее состояние не изменяется.
- Невозможно включить автоматический запуск в следующих случаях:
  - Включен автоматический запуск службы DHCP-relay.
  - Текущие настройки DHCP-сервера некорректны.

Пример использования

Чтобы включить автоматический запуск DHCP-сервера:

```
hostname# inet dhcp server mode on
```

inet dhcp server reset

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

Синтаксис

```
inet dhcp server reset
```

Режимы командного интерпретатора

Администратор.

Особенности использования

После выполнения команды настройте параметры DHCP-сервера, иначе его запуск будет невозможен.

Пример использования

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

inet dhcp server start

Запустить DHCP-сервер.

Синтаксис

```
inet dhcp server start
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Невозможно запустить DHCP-сервер в следующих случаях:

- Запущена служба DHCP-relay.
- Текущие настройки DHCP-сервера некорректны.

Пример использования

```
hostname# inet dhcp server start

Starting DHCP server ...
```

inet dhcp server stop

Завершить работу DHCP-сервера.

Синтаксис

```
inet dhcp server stop
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet dhcp server stop

Stopping DHCP server ...
```

inet dns clients add

Добавить адрес или подсеть в список клиентов DNS-сервера, развернутого на ViPNet Coordinator HW.

Синтаксис

```
inet dns clients add {<адрес>[/<длина маски>] | any}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес отдельного узла или подсети;
- `<длина маски>` — длина маски подсети;
- `any` — любые узлы.

Значения по умолчанию

По умолчанию список клиентов DNS-сервера содержит ключевое слово `any`.

Режимы командного интерпретатора

Администратор.

Пример использования

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

```
hostname# inet dns clients add 192.168.10.0/16
Client '192.168.10.0/16' appended to the list of allowed clients
```

inet dns clients delete

Удалить адрес или подсеть из списка клиентов DNS-сервера, развернутого на ViPNet Coordinator HW.

Синтаксис

```
inet dns clients delete {<адрес>[/<длина маски>] | any}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес отдельного узла или подсети;
- `<длина маски>` — длина маски подсети;
- `any` — любые узлы.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

```
hostname# inet dns clients delete 192.168.0.7
Client '192.168.0.7' removed from the list of allowed clients
Reloading domain name service...: bind9.
```

inet dns clients list

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

Синтаксис

```
inet dns clients list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> inet dns clients list
Allow DNS requests from the following client(s):
192.168.0.4
192.168.0.3
192.168.0.5
any
```

inet dns forwarders add

Добавить сервер в список DNS-серверов перенаправления (forwarder), которые передают запросы DNS-серверу внешней сети. Дополнительно можно указать имя зоны, для которой выполняется перенаправление запросов.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор

Особенности использования

- Если зона не указана, то DNS-серверу перенаправляются все запросы.

- Если IP-адрес DNS-сервера задается без зоны, то независимо от его предыдущего состояния (с зоной или без зоны), все запросы перенаправляются на DNS-сервер без зоны. При этом выводится сообщение:

  ```
  Forward DNS address <адрес> resolves both named zone and all requests
  ```

- Если IP-адрес DNS-сервера задается с зоной, то независимо от его предыдущего состояния (с зоной или без зоны), все запросы перенаправляются на DNS-сервер с зоной. При этом выводится сообщение:

  ```
  Forward DNS address <адрес> resolves both named zone and all requests
  ```

- Если DNS-сервер перенаправления не может разрешить доменное имя для указанной зоны, то для разрешения этого имени будут использоваться корневые DNS-серверы.

Примеры использования

- Чтобы в список DNS-серверов перенаправления добавить сервер с адресом 10.0.2.3:

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

- Чтобы в список DNS-серверов перенаправления добавить сервер с адресом 10.0.2.4, который перенаправляет запросы от сетевых узлов зоны gov.ru:

  ```
  hostname# inet dns forwarders add 10.0.2.4 for-zone gov.ru
  ```

inet dns forwarders delete

Удалить сервер из списка DNS-серверов перенаправления (forwarder), которые передают запросы DNS-серверу внешней сети.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор

Особенности использования

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

- Если удаляемый DNS-сервер был ранее связан с зоной, то в команде на удаление DNS-сервера эта зона должна быть указана.

Примеры использования

- Чтобы из списка DNS-серверов перенаправления удалить сервер с адресом 10.0.2.3:

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

- Чтобы из списка DNS-серверов перенаправления удалить сервер с адресом 10.0.2.4 и зоной gov.ru:

  ```
  hostname# inet dns forwarders delete 10.0.2.4 for-zone gov.ru
  ```

inet dns forwarders list

Просмотреть список DNS-серверов перенаправления (forwarder).

Синтаксис

```
inet dns forwarders list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Если адреса DNS-серверов перенаправления не заданы (список пустой), выводится информация о том, что используются корневые DNS-серверы.
- DNS-серверы, полученные по DHCP, отмечены как `from DHCP`.
- DNS-серверы, заданные пользователем, отмечены как `from USERS`.

Пример использования

```
hostname> inet dns forwarders list
Forward DNS requests to servers:
10.0.2.3 from USERS
10.0.2.4 from USERS for-zone gov.ru
```

inet dns mode

Включить или выключить автоматический запуск DNS-сервера при загрузке ViPNet Coordinator HW.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Задается при установке справочников и ключей.

Режимы командного интерпретатора

Администратор.

Особенности использования

- По команде изменяется только настройка автоматического запуска DNS-сервера, его текущее состояние не изменяется.
- Изменение настройки автоматического запуска не зависит от текущего состояния DNS-сервера (остановлен или запущен).

Пример использования

```
hostname# inet dns mode on
DNS server will be activated on next reboot
You need to start DNS server manually or reboot to have it running
```

inet dns querylog

Включить или выключить ведение журнала DNS-запросов.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить ведение журнала DNS-запросов;
- `off` — выключить ведение журнала DNS-запросов.

Значения по умолчанию

Ведение журнала включено и начинается после запуска DNS-сервера.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если команда выполняется при запущенном DNS-сервере, он перезапускается.
- В кластере команда выполняется на активном узле.

Пример использования

```
hostname# inet dns querylog on

DNS requests logging was turned on

DNS requests log size: 50 MB
```

inet dns querylog show

Просмотреть журнал DNS-запросов.

Синтаксис

```
inet dns querylog show [filtered <строка>]
```

Параметры и ключевые слова

- `filtered` — выводит записи журнала DNS-запросов, которые содержат текст, заданный в параметре `<строка>`.
- `<строка>` — строка текста, по которой необходимо отфильтровать записи журнала DNS-запросов. Допустимые символы: `A-Z, a-z, 0-9, ! # $ % & () * + , - . / : ; < = > @ [ ] _ { | } ~`, а также пробел. Если в строке используется пробел — заключите её в двойные кавычки (`""`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Без указания `filtered <строка>` выводится содержание текущего файла журнала DNS-запросов. Содержание ротированных файлов не выводится.

- Чтобы завершить просмотр, нажмите **Q**.

Пример использования

```
hostname# inet dns querylog show filtered dns.msftncsi.com

17-Feb-2024 16:42:22.623 client @0x7f847c0a9070 192.168.56.33#50527 (dns.msftncsi.com):
query: dns.msftncsi.com IN A + (192.168.56.1)

17-Feb-2024 16:43:07.629 client @0x7f847c4ed450 192.168.56.33#59237 (dns.msftncsi.com):
query: dns.msftncsi.com IN A + (192.168.56.1)
```

inet dns querylog size

Задать размер журнала DNS-запросов.

Синтаксис

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

Параметры и ключевые слова

`<размер>` — размер журнала DNS-запросов, МБайт:

- 1–50 — для исполнений с одним дисковым накопителем;
- 1–200 — для исполнений с двумя дисковыми накопителями.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если команда выполняется при запущенном DNS-сервере, он перезапускается.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet dns querylog size 100

DNS requests log size: 100 MB
```

inet dns start

Запустить DNS-сервер.

Синтаксис

```
inet dns start
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet dns start
```

```
Starting DNS server...
Starting domain name service...: bind9
```

inet dns stop

Завершить работу DNS-сервера.

Синтаксис

```
inet dns stop
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet dns stop
Stopping domain name service...: bind9.
```

inet ifconfig address

Настроить параметры сетевого интерфейса.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе имени интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен относиться к классу `access` (см. inet ifconfig class).
- Если указанный интерфейс является рабочим для DHCP-сервера, то перед изменением его параметров завершите работу DHCP-сервера (см. inet dhcp server stop).
- При изменении адреса интерфейса в таблице маршрутизации автоматически изменяются все маршруты, связанные с этим интерфейсом. Скорректируйте маршрут по умолчанию и статические маршруты так, чтобы они стали удовлетворять новой адресации.
- Если ранее на указанном интерфейсе был установлен режим DHCP, то после установки параметров будет потеряна информация о DNS- и NTP-серверах, полученная от DHCP-сервера.
- В качестве IP-адреса нельзя использовать 0.0.0.0.
- В качестве маски подсети нельзя использовать маски 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов нельзя задать IP-адреса, относящиеся к одной подсети.
- Не изменяйте параметры сетевых интерфейсов, задействованных в работе кластера. Это приведет к сбою в его работе.

Пример использования

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

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

inet ifconfig address add

Добавить дополнительный IP-адрес на сетевой интерфейс.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Интерфейс должен быть включен и относиться к классу `access` (см. inet ifconfig class).
- На интерфейсе может быть установлен режим DHCP.
- По команде создается виртуальный интерфейс с именем `<интерфейс>:номер`, где `номер` — очередной свободный номер (нумерация дополнительных адресов начинается с 0). На созданном виртуальном интерфейсе задаются указанные IP-адрес и маска.
- В качестве IP-адреса нельзя использовать 0.0.0.0.
- В качестве маски подсети нельзя использовать маски 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов нельзя задать IP-адреса, относящиеся к одной подсети.

Пример использования

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

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

and then restart them.
Alias eth1:0 was created.
```

inet ifconfig address delete

Удалить дополнительный IP-адрес с сетевого интерфейса.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

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` (см. inet ifconfig class).
- На интерфейсе может быть установлен режим DHCP.
- При удалении дополнительного IP-адреса удаляется соответствующий ему виртуальный интерфейс.

Пример использования

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

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

Attention: Upon changing the network interface settings, make similar changes to the
services that use this interface and then restart them.

Alias eth1:0 was deleted
```

inet ifconfig bonding add

Добавить подчиненный физический интерфейс к агрегированному.

Синтаксис

```
inet ifconfig <агрегированный интерфейс> bonding add <подчиненный интерфейс>
```

Параметры и ключевые слова

- `<агрегированный интерфейс>` — имя агрегированного интерфейса.
- `<подчиненный интерфейс>` — имя подчиненного интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Задаваемый подчиненный физический интерфейс должен относиться к классу `slave` (см. inet ifconfig class).
- Задаваемый подчиненный физический интерфейс не должен быть привязан ни к одному агрегированному интерфейсу.
- Количество подчиненных интерфейсов ограничено только общим количеством интерфейсов на ViPNet Coordinator HW.

Максимальное количество интерфейсов в ViPNet Coordinator HW (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

Пример использования

Чтобы для агрегированного интерфейса `bond1` добавить физический интерфейс `eth2`:

```
hostname# inet ifconfig bond1 bonding add eth2
```

inet ifconfig bonding ad-select

Задать режим выбора активного агрегатора на агрегированном интерфейсе, работающем в режиме 802.3ad.

Синтаксис

```
inet ifconfig <интерфейс> bonding ad-select <режим>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `<режим>` — режим выбора активного агрегатора на агрегированном интерфейсе, работающем в режиме 802.3ad. Можно задать следующие значения этого параметра:
  - `stable` — режим, при котором первоначально выбирается агрегатор с наибольшей суммарной пропускной способностью подчиненных физических интерфейсов, а в дальнейшем выбор нового агрегатора выполняется только в случае сбоя всех подчиненных интерфейсов текущего агрегатора.
  - `bandwidth` — режим, при котором первоначально выбирается агрегатор с наибольшей пропускной способностью подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора.
  - `count` — режим, при котором первоначально выбирается агрегатор с наибольшим количеством подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора.

Значения по умолчанию

Используется режим `stable`.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы на агрегированном интерфейсе `bond1`, работающем в режиме 802.3ad, активный агрегатор выбирался в соответствии с режимом `count`:

```
hostname# inet ifconfig bond1 bonding ad-select count
```

inet ifconfig bonding delete

Удалить подчиненный интерфейс из агрегированного.

Синтаксис

```
inet ifconfig <агрегированный интерфейс> bonding delete <подчиненный интерфейс>
```

Параметры и ключевые слова

- `<агрегированный интерфейс>` — имя агрегированного интерфейса.
- `<подчиненный интерфейс>` — имя подчиненного интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

Если агрегированному интерфейсу подчинен только один физический интерфейс, то его удалить нельзя.

Пример использования

Чтобы удалить подчиненный физический интерфейс `eth2` из агрегированного интерфейса `bond1`:

```
hostname# inet ifconfig bond1 bonding delete eth2
```

inet ifconfig bonding lacp-rate

Задать частоту обмена пакетами по протоколу LACP для агрегированных интерфейсов, работающих в режиме 802.3ad.

Синтаксис

```
inet ifconfig <интерфейс> bonding lacp-rate {slow | fast}
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `slow` — обмен пакетами по протоколу LACP выполняется каждые 30 секунд.
- `fast` — обмен пакетами по протоколу LACP выполняется каждую секунду.

Значения по умолчанию

Обмен пакетами по протоколу LACP выполняется каждые 30 секунд (`slow`).

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы на агрегированном интерфейсе `bond1`, работающем в режиме 802.3ad, обмен пакетами по протоколу LACP выполнялся каждую секунду:

```
hostname# inet ifconfig bond1 bonding lacp-rate fast
```

inet ifconfig bonding miimon

Задать частоту проверки соединения на подчиненных физических интерфейсах.

Синтаксис

```
inet ifconfig <интерфейс> bonding miimon <интервал>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `<интервал>` — время в миллисекундах, через которое производится проверка соединения на подчиненных физических интерфейсах (от 1 до 1000 миллисекунд).

Значения по умолчанию

Соединение проверяется каждые 100 миллисекунд (0,1 секунды).

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы на подчиненных интерфейсах агрегированного интерфейса `bond1` соединение проверялось каждые 0,5 секунды:

```
hostname# inet ifconfig bond1 bonding miimon 500
```

inet ifconfig bonding primary

Настроить агрегированный интерфейс, работающий в режиме `balance-tlb` или `active-backup`. Команда используется для принудительного выбора одного из подчиненных физических интерфейсов в качестве основного.

Синтаксис

```
inet ifconfig <агрегированный интерфейс> bonding primary {<подчиненный интерфейс> | none}
```

Параметры и ключевые слова

- `<агрегированный интерфейс>` — имя агрегированного интерфейса.
- `<подчиненный интерфейс>` — имя подчиненного интерфейса.
- `none` — отмена принудительного выбора основного интерфейса.

Значения по умолчанию

Основной интерфейс выбирается в соответствии с выбранным режимом работы агрегированного канала (`none`).

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы на агрегированном интерфейсе `bond1`, работающем в режиме `active-backup`, принудительно выбрать в качестве основного интерфейса подчиненный интерфейс `eth1`:

```
hostname# inet ifconfig bond1 bonding primary eth1
```

inet ifconfig bonding xmit-hash-policy

Настроить агрегированный интерфейс, работающий в режиме `balance-xor` или `802.3ad`. Команда задает алгоритм вычисления хэш-функции, используемой при выборе подчиненного интерфейса, через который будет отправляться исходящий пакет.

Синтаксис

```
inet ifconfig <интерфейс> bonding xmit-hash-policy <layer2 | layer2+3 | layer3+4>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `layer2` — алгоритм, при котором для хэширования используются MAC-адреса отправителя и получателя пакета.
- `layer2+3` — алгоритм, при котором для хэширования используются MAC-адреса отправителя и получателя, а также IP-адреса отправителя и получателя (для протоколов IPv4 или IPv6).
- `layer3+4` — алгоритм, при котором для хэширования используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии).

Значения по умолчанию

По умолчанию используется алгоритм `layer2`.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы на агрегированном интерфейсе `bond1`, работающем в режиме `balance-xor`, при выборе подчиненного интерфейса, через который будет отправляться исходящий пакет, использовался алгоритм `layer2+3`:

```
hostname# inet ifconfig bond1 bonding xmit-hash-policy layer2+3
```

inet ifconfig class

Выбрать класс для сетевого интерфейса.

Синтаксис

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

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `trunk` — класс интерфейсов, предназначенных для передачи трафика из нескольких VLAN.
- `slave` — класс интерфейсов, предназначенных для использования в составе агрегированных интерфейсов.

- `access` — класс интерфейсов, предназначенных для использования во всех остальных случаях.

Значения по умолчанию

Все физические интерфейсы ViPNet Coordinator HW относятся к классу `access`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если для указанного интерфейса смена класса выполняется впервые, то будет запрошено подтверждение операции.
- Класс `trunk` можно установить только для физических и агрегированных интерфейсов. Виртуальные интерфейсы всегда относятся к классу `access`.
- Для агрегированных и виртуальных интерфейсов нельзя установить класс `slave`.
- Нельзя установить класс `trunk`, если на указанном интерфейсе запущен или настроен на автоматический запуск DHCP-сервер или служба DHCP-relay.
- Если на указанном интерфейсе задан один или несколько IP-адресов, то для установки класса `trunk` требуется дополнительное подтверждение. После установки класса `trunk` все адреса будут потеряны.
- Перед установкой класса `access` или `slave` требуется удалить все виртуальные интерфейсы, созданные на базе указанного интерфейса.
- Перед тем как изменить класс интерфейса `slave` на `access` или `trunk`, необходимо, чтобы он не был подчинен ни одному агрегированному интерфейсу.

Пример использования

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

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

inet ifconfig dhcp

Установить режим DHCP на сетевом интерфейсе.

Синтаксис

```
inet ifconfig <интерфейс> dhcp [<настройка> {on | off}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<настройка>` — название настройки, передаваемой с помощью DHCP. Можно указать одно из следующих значений:
  - `dns` — адреса DNS-серверов;
  - `route` — маршруты;
  - `ntp` — адреса NTP-серверов.
- `on` — включить автоматический приём указанной настройки.
- `off` — выключить автоматический приём указанной настройки.

Значения по умолчанию

Для всех настроек, передаваемых с помощью DHCP, автоматический прием включен (`on`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Интерфейс должен относиться к классу `access` (см. inet ifconfig class) или являться агрегированным интерфейсом.
- Если на интерфейсе заданы дополнительные адреса, они будут потеряны после установки режима DHCP.

Пример использования

- Чтобы только установить на интерфейсе `eth1` режим DHCP:

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

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

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

inet ifconfig dhcp route-metric

Задать специфичную метрику маршрутам, поступающим от DHCP-сервера, на сетевом интерфейсе ViPNet Coordinator HW.

Синтаксис

```
inet ifconfig <интерфейс> dhcp route-metric {<метрика> | none}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `<метрика>` — метрика. Возможные значения: 1–255.
- `none` — удаляет метрику на сетевом интерфейсе.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если на сетевом интерфейсе не установлен режим DHCP (см. inet ifconfig dhcp), то заданная метрика будет сохранена. Но метрика начнет учитываться только после того, как режим DHCP будет установлен.
- Интерфейс должен относиться к классу `access` (см. inet ifconfig class) или являться агрегированным интерфейсом.
- При удалении специфичной метрики будет использоваться метрика по умолчанию для маршрутов DHCP-сервера (см. inet dhcp client route-default-metric).

Пример использования

- Чтобы назначить на сетевом интерфейсе `eth0` метрику 50:

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

- Чтобы удалить метрику на сетевом интерфейсе `eth0`:

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

inet ifconfig down

Выключить сетевой интерфейс.

Синтаксис

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

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если существуют виртуальные интерфейсы, созданные на базе указанного интерфейса, то требуется дополнительно подтвердить выключение интерфейса. Вместе с интерфейсом автоматически будут выключены все его виртуальные интерфейсы независимо от их текущего состояния.
- Если указанный интерфейс является рабочим для DHCP-сервера, то его нельзя выключить в следующих случаях:
  - DHCP-сервер запущен.
  - DHCP-сервер не запущен, но включен его автоматический запуск при загрузке ViPNet Coordinator HW.

Пример использования

Чтобы выключить виртуальный интерфейс `eth1.2`:

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

inet ifconfig mtu

Изменить значение MTU для сетевого интерфейса.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию используется значение MTU 1500 байт.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Ограничения ViPNet Coordinator VA на платформах виртуализации:
  - VMware Workstation и VMware vSphere — для изменения MTU предварительно настройте платформу виртуализации, разрешив использование Jumbo-кадров.
  - Oracle VM VirtualBox — изменение MTU не поддерживается при использовании сетевых устройств AMD.
- Команда не используется:
  - для сетевых интерфейсов подключения к беспроводной сети Wi-Fi или мобильной сети (`wlanX` и `pppX`);
  - для сетевых интерфейсов классов `vlan` и `slave`;
  - для интерфейсов синхронизации кластера.
- Значение MTU, заданное для интерфейса класса `trunk`, автоматически применяется ко всем виртуальным интерфейсам класса `vlan`, созданным на этом физическом интерфейсе.
- Значение MTU, заданное для интерфейса класса `bond`, будет использоваться на всех подчиненных физических интерфейсах класса `slave`.
- При создании агрегированного интерфейса с помощью командного интерпретатора для всех подчиненных физических интерфейсов автоматически задается значение MTU 1500 байт.
- Если вы исключаете подчиненный физический интерфейс из агрегированного, для него устанавливается значение MTU 1500 байт.

Пример использования

Задать размер MTU, равный 3000 байт, для интерфейса `eth0`:

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

inet ifconfig pppoe address

Задать способ получения IP-адреса на PPPoE-интерфейсе.

Синтаксис

```
inet ifconfig pppoe <номер> address {auto | <IP-адрес> netmask <маска>}
```

Параметры и ключевые слова

- `<номер>` — номер PPPoE-интерфейса.
- `auto` — автоматическое получение IP-адреса от PPPoE-сервера.
- `<IP-адрес>` — IPv4-адрес.

- `<маска>` — маска подсети. Можно использовать только маски 255.255.255.254 (/31) и 255.255.255.255 (/32).

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию PPPoE-интерфейс получает динамический IP-адрес от PPPoE-сервера. Если провайдер передал вам IP-адрес, назначьте его статически.
- Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

- Чтобы автоматически получать IP-адрес от PPPoE-сервера:

  ```
  hostname# inet ifconfig pppoe 0 address auto
  ```

- Чтобы назначить статический IP-адрес:

  ```
  hostname# inet ifconfig pppoe 0 address 192.168.0.2 netmask 255.255.255.255
  ```

inet ifconfig pppoe auth

Задать тип аутентификации для пользователя на PPPoE-интерфейсе.

Синтаксис

```
inet ifconfig pppoe <номер> auth {chap | pap}
```

Параметры и ключевые слова

- `<номер>` — номер PPPoE-интерфейса.
- `chap` — использовать протокол аутентификации CHAP.
- `pap` — использовать протокол аутентификации PAP.

Режимы командного интерпретатора

Администратор.

Особенности использования

Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

```
hostname# inet ifconfig pppoe 0 auth chap
```

inet ifconfig pppoe comment add

Добавить комментарий к PPPoE-интерфейсу.

Синтаксис

```
inet ifconfig pppoe <номер> comment add <комментарий>
```

Параметры и ключевые слова

- `<номер>` — номер PPPoE-интерфейса.
- `<комментарий>` — комментарий к PPPoE-интерфейсу, например, имя провайдера. Допустимые значения: `a-z`, `A-Z`, `0-9`, `. -` и пробел. Если в названии используется пробел, заключите строку в двойные кавычки (`""`). Максимальная длина — 255 символов.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Можно добавить только один комментарий (новый комментарий заменяет предыдущий).
- Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

```
hostname# inet ifconfig pppoe 0 comment add "rostelecom"
```

inet ifconfig pppoe comment delete

Удалить комментарий PPPoE-интерфейса.

Синтаксис

```
inet ifconfig pppoe <номер> comment delete
```

Параметры и ключевые слова

`<номер>` — номер PPPoE-интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

```
hostname# inet ifconfig pppoe 0 comment delete
```

inet ifconfig pppoe defaultroute

Включить или выключить автоматическое добавление на PPPoE-интерфейс маршрута по умолчанию, в котором в качестве шлюза используется шлюз, полученный от интернет-провайдера.

Синтаксис

```
inet ifconfig pppoe <номер> defaultroute {on | off}
```

Параметры и ключевые слова

- `<номер>` — номер PPPoE-интерфейса.
- `on` — использовать полученный адрес шлюза, как маршрут по умолчанию.
- `off` — не использовать полученный адрес шлюза, как маршрут по умолчанию.

Значения по умолчанию

`off`

Режимы командного интерпретатора

Администратор.

Особенности использования

Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

Чтобы использовать полученный адрес шлюза в качестве маршрута по умолчанию:

```
hostname# inet ifconfig pppoe 0 defaultroute on
```

```
The virtual interface pppoe0 is set as the default route
```

inet ifconfig pppoe disable

Выключить PPPoE-интерфейс.

Синтаксис

```
inet ifconfig pppoe <номер> disable
```

Параметры и ключевые слова

`<номер>` — номер PPPoE-интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

При выполнении команды выдается предупреждение о возможном разрыве установленного соединения. Чтобы выключить интерфейс, введите `Yes` и нажмите **Enter**.

Пример использования

```
hostname# inet ifconfig pppoe 0 disable
If you reset the interface, connection will be terminated.
Do you want to continue? [Yes/No]
```

inet ifconfig pppoe enable

Включить PPPoE-интерфейс.

Синтаксис

```
inet ifconfig pppoe <номер> enable
```

Параметры и ключевые слова

`<номер>` — номер PPPoE-интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для включения на интерфейсе должны быть настроены параметры:

- `interface` (см. inet ifconfig pppoe if-set);
- `username` (см. inet ifconfig pppoe username);
- `password` (см. inet ifconfig pppoe password);
- `auth` (см. inet ifconfig pppoe auth).

Пример использования

```
hostname# inet ifconfig pppoe 0 enable
```

inet ifconfig pppoe if-set

Добавить PPPoE-интерфейс на физический интерфейс.

Синтаксис

```
inet ifconfig pppoe <номер> if-set <физический интерфейс>
```

Параметры и ключевые слова

- `<интерфейс>` — имя PPPoE-интерфейса.
- `<физический интерфейс>` — имя Ethernet-интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Виртуальный PPPoE-интерфейс может быть закреплен только за одним физическим интерфейсом.
- При выполнении команды параметры физического интерфейса сбрасываются до значений по умолчанию.
- Чтобы сменить физический интерфейс, повторно выполните команду с указанием другого интерфейса.
- Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

```
hostname# inet ifconfig pppoe 0 if-set eth0
```

```
The virtual interface pppoe0 is assigned to eth0
```

inet ifconfig pppoe mtu

Установить значение MTU на PPPoE-интерфейсе.

Синтаксис

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

Параметры и ключевые слова

- `<номер>` — номер PPPoE-интерфейса.
- `auto` — задает значение MTU по умолчанию (1492 байта).
- `<значение MTU>` — значение MTU в байтах. Возможные значения: `1280–9000`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если интерфейс используется для текущего подключения, при выполнении команды выдается предупреждение о возможном разрыве установленного соединения. Чтобы подтвердить действие, введите `Yes` и нажмите **Enter**.
- Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

- Чтобы задать MTU по умолчанию:

  ```
  hostname# inet ifconfig pppoe 0 mtu auto
  ```

- Чтобы установить размер MTU `1480`:

  ```
  hostname# inet ifconfig pppoe 0 mtu 1480
  ```

inet ifconfig pppoe password

Задать пароль пользователя для PPPoE-интерфейса.

Синтаксис

```
inet ifconfig pppoe <номер> password <пароль пользователя>
```

Параметры и ключевые слова

- `<номер>` — номер PPPoE-интерфейса.
- `<пароль пользователя>` — пароль пользователя для аутентификации. Допустимые символы: `A-Z, a-z, 0-9, ! # $ % () * + , . / : ; < = > @ [ ] _ { | } ~`. Максимальная длина: 255 символов. Лишние символы обрезаются.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Задать имя пользователя и пароль можно только после выбора типа аутентификации (см. inet ifconfig pppoe auth).
- Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

```
hostname# inet ifconfig pppoe 0 password Pass$[worD)
```

inet ifconfig pppoe reset

Сбросить настройки PPPoE-интерфейса до настроек по умолчанию.

Синтаксис

```
inet ifconfig pppoe <номер> reset
```

Параметры и ключевые слова

`<номер>` — номер PPPoE-интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды выдается предупреждение о возможном разрыве установленного соединения. Чтобы сбросить настройки интерфейса, введите `Yes` и нажмите **Enter**.
- После подтверждения команды настройки сбросятся до настроек по умолчанию:
  - `if-set`, `auth`, `username`, `password`, `ac-name` — сбрасываются;

- address — auto;
- mtu — auto (1492);
- usepeerdns — on;
- defaulroute — off.

- Если выполнить команду на включенном интерфейсе, параметры физического интерфейса восстановятся.

Пример использования

```
hostname# inet ifconfig pppoe 0 reset

If you reset the active pppoe interface, connection will be terminated and interface will be disabled.

The eth interface parameters will be restored.

Do you want to continue? [Yes/No]
```

inet ifconfig pppoe route-metric

Задать метрику маршруту по умолчанию, который формируется на основе IP-адреса шлюза по умолчанию, полученного по протоколу PPPoE.

Синтаксис

```
inet ifconfig pppoe <номер> route-metric {<1-255> | auto}
```

Параметры и ключевые слова

- <номер> — номер PPPoE-интерфейса.
- <1-255> — значение метрики.
- auto — устанавливает значение 70.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Задать метрику можно, только если разрешено получение маршрута по умолчанию от сервера провайдера (см. inet ifconfig pppoe defaultroute).
- Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

- Чтобы назначить маршруту по умолчанию на сетевом интерфейсе `pppoe0` метрику `100`:

  ```
  hostname# inet ifconfig pppoe 0 route-metric 100
  Route metric for pppoe0 is set to 100
  ```

- Чтобы назначить маршруту по умолчанию на сетевом интерфейсе `pppoe0` метрику по умолчанию:

  ```
  hostname# inet ifconfig pppoe 0 route-metric auto
  Route metric for pppoe0 is 70
  ```

inet ifconfig pppoe usepeerdns

Разрешить или запретить получение IP-адреса DNS-сервера провайдера на PPPoE-интерфейсе. Информация о DNS-сервере поступает от интернет-провайдера по протоколу DHCP при установлении соединения.

Синтаксис

```
inet ifconfig pppoe <номер> usepeerdns {on | off}
```

Параметры и ключевые слова

- `<номер>` — номер виртуального PPPoE-интерфейса.
- `on` — разрешить получение информации о DNS-сервере провайдера.
- `off` — запретить получение информации о DNS-сервере провайдера.

Значения по умолчанию

`on`

Режимы командного интерпретатора

Администратор.

Особенности использования

- От интернет-провайдера можно получить IP-адреса максимум двух DNS-серверов.
- Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

```
hostname# inet ifconfig pppoe 0 usepeerdns on
```

inet ifconfig pppoe username

Задать имя пользователя для PPPoE-интерфейса.

Синтаксис

```
inet ifconfig pppoe <номер> username <имя пользователя>
```

Параметры и ключевые слова

- `<номер>` — номер PPPoE-интерфейса.
- `<имя пользователя>` — имя пользователя для аутентификации. Допустимые символы: `A-Z, a-z, 0-9, ! # $ % () * + , . / : ; < = > @ [ ] _ { | } ~`. Максимальная длина: 255 символов. Лишние символы обрезаются.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Задать имя пользователя и пароль можно только после выбора типа аутентификации (см. inet ifconfig pppoe auth).
- Выполнить настройку можно только на выключенном PPPoE-интерфейсе (см. inet ifconfig pppoe disable).

Пример использования

```
hostname# inet ifconfig pppoe 0 username user1
```

inet ifconfig reset

Сбросить настройки одного сетевого интерфейса либо всех интерфейсов.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды с параметром `all` происходит сброс настроек всех физических интерфейсов. Все виртуальные интерфейсы при этом удаляются.
- Если вы хотите выполнить команду для физического интерфейса, для которого созданы `VLAN` или агрегированные (`bond`) интерфейсы, то сначала удалите эти интерфейсы с помощью команды iplir adapter delete. Иначе записи о VLAN и агрегированных интерфейсах останутся в конфигурационном файле `iplir.conf`, и их будет необходимо удалить вручную, чтобы еще раз использовать эти же имена интерфейсов.
- Команда используется для подготовки указанного интерфейса к установке новых параметров.
- По команде будут выполнены изменения в настройках указанного физического интерфейса:
  - Удалены все существующие дополнительные адреса интерфейса и виртуальные интерфейсы, созданные на его базе.
  - Удалена информация об IP-адресе и маске подсети.
  - Установлен режим автоматического определения параметров скорости интерфейса (см. inet ifconfig speed auto).
  - Интерфейс будет выключен.
- Для виртуальных интерфейсов класса `slave` команда не выполняется.
- Для виртуальных интерфейсов VLAN по команде не сбрасываются настройки:
  - Имя соответствующего физического интерфейса.
  - Номер виртуального интерфейса VLAN.
- Для агрегированных интерфейсов по команде не сбрасываются настройки:
  - Имя агрегированного интерфейса.
  - Режим работы агрегированного интерфейса.
  - Частота проверки соединения на подчиненных физических интерфейсах.

Пример использования

Чтобы сбросить настройки интерфейса `eth1`:

```
hostname# inet ifconfig eth1 reset
This command will reset eth1 interface settings to default. Are you sure? [Yes/No]: Yes
done.
```

inet ifconfig speed

Задать параметры скорости сетевого интерфейса.

Примечание. Использование данной команды возможно только для аппаратных исполнений ViPNet Coordinator HW. Для исполнения ViPNet Coordinator VA команда выполняться не будет.

Синтаксис

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

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<скорость>` — скорость в Мбит/с. Возможные значения: `10`, `100`, `1000`, `10000` (для исполнений, оборудованных соответствующими интерфейсами).
- `duplex` — режим передачи данных:
  - `half` — полудуплекс;
  - `full` — полный дуплекс.
- `autoneg` — режим автосогласования скорости интерфейса (autonegotiation):
  - `on` — включен;
  - `off` — выключен.

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

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 (см. inet ifconfig class).
- Установку параметров скорости интерфейса следует использовать с осторожностью и только в тех случаях, когда это действительно необходимо — например, для согласования работы

внешнего интерфейса ViPNet Coordinator HW и коммутационного оборудования, подключенного к данному интерфейсу.

- Нельзя изменить параметры скорости оптических интерфейсов (для исполнений, оборудованных соответствующими разъемами).

Пример использования

На интерфейсе `eth1` установить скорость 100 Мбит/с, режим полудуплекса и отключить режим автосогласования:

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

inet ifconfig speed auto

Установить режим автоматического определения параметров скорости на сетевом интерфейсе.

Примечание. Использование данной команды возможно только для аппаратных исполнений ViPNet Coordinator HW. Для исполнения ViPNet Coordinator VA команда выполняться не будет.

Синтаксис

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

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- После выполнения команды режим автосогласования (autonegotiation) на интерфейсе принимает значение `on` (включен).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Нельзя установить параметры скорости виртуального интерфейса, так как он наследует эти параметры от соответствующего физического интерфейса.
- Команда неприменима к интерфейсам класса slave (см. inet ifconfig class).

Пример использования

Установить режим автоматического определения параметров скорости на интерфейсе `eth1`:

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

inet ifconfig up

Включить сетевой интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> up
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если существуют виртуальные интерфейсы, созданные на базе указанного интерфейса, то требуется дополнительно подтвердить включение интерфейса. Вместе с интерфейсом автоматически будут включены все его виртуальные интерфейсы независимо от их текущего состояния.
- Нельзя включить виртуальный интерфейс, если выключен соответствующий физический интерфейс.

Пример использования

Чтобы включить виртуальный интерфейс `eth1.2`:

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

inet ifconfig vlan add

Создать интерфейс для виртуальной сети с заданным номером.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Физический интерфейс должен относиться к классу `trunk` (см. inet ifconfig class).
- По команде будет создан виртуальный интерфейс с именем `<интерфейс>.<номер>`. Созданный интерфейс будет иметь то же состояние (включен или выключен), что и физический интерфейс.
- Максимальное количество интерфейсов в ViPNet Coordinator HW (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

  Номер виртуальной сети `<номер>` должен находиться в диапазоне от 1 до 4094. Значения 0 и 4095 зарезервированы.

Пример использования

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

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

inet ifconfig vlan delete

Удалить виртуальный интерфейс.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе номера работают автозаполнение и подсказка, данные для подсказки берутся из списка существующих виртуальных интерфейсов.
- Невозможно удалить виртуальный интерфейс, заданный как рабочий в параметрах функции L2OverIP, если эта функция включена (см. iplir set l2overip mode).

Пример использования

Чтобы удалить виртуальный интерфейс `eth1.2`:

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

inet ntp add

Добавить сервер в список NTP-серверов, используемых для синхронизации времени.

Синтаксис

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

Параметры и ключевые слова

- `server` — добавить NTP-сервер, работающий в одностороннем режиме (рассылка данных времени).
- `peer` — добавить NTP-сервер, работающий в двустороннем режиме (рассылка и получение данных времени).
- `<IP-адрес>` — IP-адрес NTP-сервера.
- `<доменное имя>` — доменное имя NTP-сервера.

Режимы командного интерпретатора

Администратор.

Особенности использования

В кластере команда выполняется на активном узле.

Пример использования

Добавить сервер `ntp.psn.ru`, работающий в одностороннем режиме:

```
hostname# inet ntp add server ntp.psn.ru
NTP server ntp.psn.ru has been inserted successfully
```

inet ntp delete

Удалить сервер из списка NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp delete {server | peer} {<IP-адрес> | <доменное имя>}
```

Параметры и ключевые слова

- `server` — удалить NTP-сервер, работающий в одностороннем режиме (рассылка данных времени).
- `peer` — удалить NTP-сервер, работающий в двустороннем режиме (рассылка и получение данных времени).
- `<IP-адрес>` — IP-адрес NTP-сервера.
- `<доменное имя>` — доменное имя NTP-сервера.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе IP-адреса или доменного имени работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка NTP-серверов.
- В кластере команда выполняется на активном узле.

Пример использования

Чтобы из списка NTP-серверов удалить сервер `ntp.psn.ru`, работающий в одностороннем режиме:

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

inet ntp list

Просмотреть список NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp list
```

Режимы командного интерпретатора

- Пользователь.

- Администратор.

Особенности использования

- NTP-серверы, полученные по DHCP, отмечены как `from DHCP`.
- NTP-серверы, заданные пользователем, отмечены как `from USER`.

Пример использования

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

inet ntp mode

Включить или выключить автоматический запуск NTP-сервера при загрузке ViPNet Coordinator HW.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Задается при установке справочников и ключей.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда изменяет только настройку автоматического запуска NTP-сервера, его текущее состояние не изменяется.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Выключить автоматический запуск NTP-сервера:

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

inet ntp orphan

Включить или выключить переход локального NTP-сервера в изолированный (orphan) режим при потере соединения с внешними NTP-серверами.

Синтаксис

```
inet ntp orphan {on <stratum> | off}
```

Параметры и ключевые слова

`<stratum>` — используется для задания уровня внешнего NTP-сервера. Если со всеми внешними NTP-серверами меньше указанного уровня не удается установить соединение в течение 5 минут, то локальный NTP-сервер переходит в изолированный режим. Допустимы значения 1–10, рекомендуемое значение 5.

Значения по умолчанию

По умолчанию для параметра `<stratum>` установлено значение 5.

Режимы командного интерпретатора

Администратор.

Особенности использования

В кластере команда выполняется на активном узле.

Пример использования

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

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

inet ntp start

Запустить NTP-сервер.

Синтаксис

```
inet ntp start
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet ntp start
Starting NTP server...
```

inet ntp stop

Завершить работу NTP-сервера.

Синтаксис

```
inet ntp stop
```

Режимы командного интерпретатора

Администратор.

Пример использования

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

inet ntp use-default

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если необходимо выключить использование NTP-серверов по умолчанию, добавьте не менее четырёх дополнительных NTP-серверов. Иначе, если один из серверов выйдет из строя, у ViPNet Coordinator HW не будет достаточно информации, чтобы определить, какой из оставшихся серверов предоставляет правильное время.
- В режиме кластера команда доступна на активном узле.

Пример использования

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

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

inet ospf area auth

Включить или выключить аутентификацию в протоколе OSPF.

Синтаксис

```
inet ospf area <area-ID> auth {on {pswd | md5} | off}
```

Параметры и ключевые слова

- `area <area-ID>` — область маршрутизации OSPF, целое число в десятичном формате `0-4294967295` или в формате `A.B.C.D`, где `A,B,C,D` — целое число от 0 до 255;
- `on` — включает аутентификацию для выбранной области. Методы аутентификации:
  - `pswd` — аутентификация на основе открытого пароля (Simple Password);
  - `md5` — аутентификация на основе MD5 HMAC.
- `off` — выключает аутентификацию для выбранной области.

Режимы командного интерпретатора

Администратор.

Особенности использования

- В режиме кластера команда доступна на активном узле. При попытке выполнения на пассивном узле выводится предупреждение: `OSPF configuration command is disabled because the cluster appliance is passive.`
- При включении аутентификации для области маршрутизации выводится предупреждение о необходимости настройки идентификационной информации на интерфейсе.
- При выключении аутентификации указание метода аутентификации не применяется.
- При включении аутентификации указание метода аутентификации обязательно.
- Если для области маршрутизации уже назначен метод аутентификации, команда изменяет назначенный способ аутентификации.

Пример использования

Включить аутентификацию для области маршрутизации 1 с использованием MD5 HMAC:

```
hostname# inet ospf area 1 auth on md5
Area 1 authentication using MD5 is ON.
Make sure that authentication method is set up on the appropriate interface.
```

inet ospf interface keys add

Добавить ключ для аутентификации MD5 HMAC.

Синтаксис

```
inet ospf interface <интерфейс> keys add <keyid>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса (физический, `vlan`, `bond`);
- `<keyid>` — идентификатор ключа. Допустимые значения: `1–255`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Ключ вводится интерактивно.
- Требования к ключу:
  - длина : 1–16 символов;

- допустимые символы: A-Z, a-z, 0-9, ! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }.

- В кластере команда выполняется на активном узле.

Пример использования

Добавить ключ с идентификатором 1 на интерфейс eth0:

```
hostname# inet ospf interface eth0 keys add 1

Set key 1:

Confirm key 1:

Key 1 on eth0 added
```

inet ospf interface keys remove

Удалить ключ для аутентификации MD5 HMAC.

Синтаксис

```
inet ospf interface <интерфейс> keys remove {all | <keyid>}
```

Параметры и ключевые слова

- <интерфейс> — имя интерфейса (физический, vlan, bond);
- <keyid> — идентификатор ключа. Допустимые значения: 1-255;
- all — удалить все ключи на интерфейсе.

Режимы командного интерпретатора

Администратор.

Особенности использования

В кластере команда выполняется на активном узле.

Пример использования

Удалить ключ на интерфейсе eth0:

```
hostname# inet ospf interface eth0 keys remove 1

Key 1 on eth0 removed
```

inet ospf interface password

Установить или удалить пароль для аутентификации на выбранном интерфейсе.

Синтаксис

```
inet ospf interface <интерфейс> password [remove]
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса (физический, `vlan`, `bond`);
- `remove` — удалить пароль.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Пароль вводится интерактивно.
- Требования к паролю:
  - длина пароля: 1–8 символов;
  - допустимые символы: `A-Z, a-z, 0-9, ! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.
- В кластере команда выполняется на активном узле.

Пример использования

- Установить пароль на интерфейсе `eth0`:

```
hostname# inet ospf interface eth0 password
Set password for eth0:
Confirm password for eth0:
Password on eth0 set.
```

- Удалить пароль на интерфейсе `eth0`:

```
hostname# inet ospf interface eth0 password remove
Password on eth0 removed
```

inet ospf mode

Включить или выключить использование протокола OSPF.

Синтаксис

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

Параметры и ключевые слова

- `on` — включить использование протокола OSPF;
- `off` — выключить использование протокола OSPF.

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet ospf mode on

Starting ospf...
```

inet ospf network add

Добавить сеть, в которой должна выполняться маршрутизация по протоколу OSPF.

Синтаксис

```
inet ospf network add <IP-адрес назначения> netmask <маска сети> area <area-ID>
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес сети.
- `<маска сети>` — маска сети.
- `area <area-ID>` — область маршрутизации, целое число в десятичном формате `0-4294967295` или в формате `A.B.C.D`, где `A,B,C,D` — целое число от 0 до 255.

Режимы командного интерпретатора

Администратор.

Особенности использования

Если использование протокола OSPF не включено, задать сеть невозможно.

Пример использования

```
hostname# inet ospf network add 10.0.5.0 netmask 255.255.255.0 area 1

The following OSPF network has been added:
```

```
Destination     Netmask           OSPF Area   A.B.C.D       Authentication
-----------     -------           ---------   ---------     ---------
192.168.11.0    255.255.255.0     4444        0.0.17.92     No
10.0.5.0        255.255.255.0     1           127.0.0.0     No
```

inet ospf network delete

Удалить сеть, которая была указана как маршрутизируемая по протоколу OSPF.

Синтаксис

```
inet ospf network delete <IP-адрес назначения> netmask <маска сети> area <area-ID>
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес сети.
- `<маска сети>` — маска сети.
- `area <area-ID>` — область маршрутизации, целое число в десятичном формате `0-4294967295` или в формате `A.B.C.D`, где `A,B,C,D` — целое число от 0 до 255.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если использование протокола OSPF не включено, удалить сеть невозможно.
- Если в конфигурации протокола OSPF указанная сеть не будет найдена, ее удаление будет невозможно.

Пример использования

```
hostname# inet ospf network delete 10.0.5.0 netmask 255.255.255.0 area 1
The following OSPF network has been deleted:
Destination     Netmask           OSPF Area     A.B.C.D
-----------     -------           ---------     ---------
10.0.5.0        255.255.255.0     1             127.0.0.0
```

inet ospf redistribute add

Включить перераспределение статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол OSPF.

Синтаксис

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

Параметры и ключевые слова

- `static` — включить перераспределение статических маршрутов;
- `dhcp` — включить перераспределение маршрутов DHCP-сервера.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда не будет выполнена в следующих случаях:

- Не включено использование протокола OSPF (см. inet ospf mode).
- Перераспределение указанного типа маршрутов было включено ранее.

Пример использования

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

inet ospf redistribute delete

Выключить перераспределение статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол OSPF.

Синтаксис

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

Параметры и ключевые слова

- `static` — выключить перераспределение статических маршрутов;
- `dhcp` — выключить перераспределение маршрутов DHCP-сервера.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда не будет выполнена в следующих случаях:

- Не включено использование протокола OSPF (см. inet ospf mode).
- Перераспределение указанного типа маршрутов не было включено ранее.

Пример использования

```
hostname# inet ospf redistribute delete static

Redistribution of static routes has been disabled.
```

inet ospf priority

Задать приоритет ViPNet Coordinator HW.

Синтаксис

```
inet ospf priority <приоритет> [interface <интерфейс>]
```

Параметры и ключевые слова

- `<приоритет>` — целое число из диапазона 0–255.
- `<интерфейс>` — имя интерфейса.

Значения по умолчанию

Значение приоритета по умолчанию — 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

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

Пример использования

```
hostname# inet ospf priority 10

Stopping ospf ...

Starting ospf ...
```

inet ospf router-id

Задать идентификатор ViPNet Coordinator HW в формате адреса протокола IPv4.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Использование команды разрешено, если на ViPNet Coordinator HW включен протокол маршрутизации OSPF (см. inet ospf mode).
- Если в сети со множественным доступом у двух маршрутизаторов будут одинаковые идентификаторы, то такие маршрутизаторы не смогут установить отношения соседства.

Пример использования

```
hostname# inet ospf router-id 172.16.12.1

Stopping ospf ...

Starting ospf ...
```

```
OSPF router-id 172.16.12.1 has been set for this router.
```

inet ospf show configuration

Просмотреть настройки протокола OSPF.

Синтаксис

```
inet ospf show configuration
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

В режиме кластера команда доступна для выполнения только на активном узле кластера.

Пример использования

```
hostname> inet ospf show configuration


OSPF protocol autostart is on
OSPF protocol has been enabled
OSPF router id is 172.20.20.100
Redistribution of static routes is enabled.
Redistribution of DHCP routes is enabled.
Destination     Netmask            OSPF Area     A.B.C.D       Authentication
---------       ---------          ---------     ---------     ---------
172.20.20.0     255.255.255.0      0             0.0.0.0       No
172.20.21.0     255.255.255.0      1             0.0.0.1       MD5
172.20.22.0     255.255.255.0      2             0.0.0.2       Password


Interface:  OSPF priority   Password    Keyid
------------------------------------------------
eth0:       1               No          1,2,3
eth1:       20              Yes         No
```

По команде выводится следующая информация:

- состояние протокола OSPF: включен/выключен;
- состояние автоматического запуска протокола OSPF при старте ViPNet Coordinator HW: включен/выключен;
- идентификатор ViPNet Coordinator HW;
- состояние перераспределения статических маршрутов: включены/выключены;
- состояние перераспределения DHCP маршрутов: включены/выключены;
- список сетей, в которых ViPNet Coordinator HW выполняет маршрутизацию по протоколу OSPF (IP-адреса, маски и области);
- приоритеты ViPNet Coordinator HW на интерфейсах.

inet ospf show database

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

Синтаксис

```
inet ospf show database
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> inet ospf show database

       OSPF Router with ID (10.0.5.2)

              Router Link States (Area 0.0.0.0)

Link ID       ADV Router   Age      Seq#          CkSum     Link count

10.0.3.2      10.0.3.2     155      0x8000017d    0x590a    2

10.1.30.5     10.1.30.5    220      0x8000029f    0x3fa0    2

              Net Link States (Area 0.0.0.0)

Link ID       ADV Router   Age      Seq#          CkSum

10.0.5.5      10.1.30.5    751      0x80000263    0x3541

              AS External Link States
```

```
Link ID       ADV Router   Age      Seq#          CkSum    Route

10.0.1.0      10.1.30.5    1551     0x80000182    0x9061   E2 10.0.1.0/24 [0x0]

10.0.2.0      10.1.30.5    1001     0x80000183    0x836c   E2 10.0.2.0/24 [0x0]

10.0.3.0      10.1.30.5    210      0x80000182    0x7a75   E2 10.0.3.0/24 [0x0]

10.0.4.0      10.1.30.5    341      0x80000182    0x6f7f   E2 10.0.4.0/24 [0x0]

10.100.1.0    10.1.30.5    911      0x8000029d    0xe1ad   E2 10.100.1.0/24 [0x0]

10.100.2.0    10.1.30.5    180      0x8000029f    0xe0aa   E2 10.100.2.0/24 [0x0]

192.168.0.0   10.1.30.5    821      0x80000182    0x6c27   E2 192.168.0.0/16 [0x0]
```

inet ospf show neighbour

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

Синтаксис

```
inet ospf show neighbour
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> inet ospf show neighbour

Neighbor ID    Pri    State      Dead Time   Address    Interface        RXmtl   Rqstl   DBsml

10.1.30.5      1      Full/DR    33.310s     10.0.5.5   eth0:10.0.5.2    0       0       0
```

По команде выводится следующая информация для каждого маршрутизатора:

- IP-адрес активного сетевого интерфейса, по которому доступен маршрутизатор для обмена информацией по протоколу OSPF;
- порядковый номер маршрутизатора, под которым он известен другим маршрутизаторам при работе по протоколу OSPF;
- тип маршрутизатора (в приведенном примере маршрутизатор-сосед является назначенным, что показывает значение `DR` в поле `State`);

- интервал простоя маршрутизатора, по истечении которого он будет считаться неактивным (выключенным);
- другие параметры.

inet ping

Проверить соединение с сетевым узлом.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

Чтобы проверить соединение с адресом 10.0.2.1:

```
hostname> inet ping 10.0.2.1
Pinging 10.0.2.1, press Ctrl+C to cancel.
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
64 bytes from 10.0.2.1: icmp_req=1 ttl=255 time=2.98 ms
64 bytes from 10.0.2.1: icmp_req=2 ttl=255 time=1.60 ms
64 bytes from 10.0.2.1: icmp_req=3 ttl=255 time=1.14 ms
64 bytes from 10.0.2.1: icmp_req=4 ttl=255 time=1.71 ms
^C
--- 10.0.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packets loss, time 3004ms
rtt min/avg/max/mdev = 1.144/1.862/2.983/0.683 ms
```

inet policy active

Задать действующую политику маршрутизации.

Синтаксис

```
inet policy active {<имя политики> | default}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации.
- `default` — политика маршрутизации по умолчанию.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда может быть использована в качестве параметра команды inet dgd rule add action-priority.

Пример использования

```
hostname# inet policy active policy1
Inet policy active was set to policy1
```

inet policy rule add

Задать действие правила политики маршрутизации.

Синтаксис

```
inet policy rule add <имя политики> <приоритет> {table {<номер таблицы> | name <имя таблицы>
| default} | block}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `<приоритет>` — приоритет таблицы маршрутизации, возможные значения от 1024 до 2048. Чем меньше значение, тем выше приоритет правила.
- `table` — обрабатывать IP-пакеты по указанной таблице маршрутизации.
- `<номер таблицы>` — номер пользовательской таблицы маршрутизации.
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации.

- `default` — таблица маршрутизации по умолчанию.
- `block` — блокировать IP-пакеты без ICMP-сообщений.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если политики с указанным именем не существует, создается новая.
- Если правила с указанным приоритетом не существует в политике маршрутизации, создается новое правило для обработки всех IP-пакетов. Чтобы определить условие применения правила, выполните команду inet policy rule add match.

Пример использования

- Для правила высшего приоритета политики `policy1` задать способ обработки IP-пакетов по пользовательской таблице маршрутизации `table1`:

  ```
  hostname# inet policy rule add policy1 1024 table name table1
  Inet policy policy1 1024 set table table1 was created.
  ```

- Создать правило приоритета 1027 политики `policy2` для обработки IP-пакетов по таблице маршрутизации по умолчанию:

  ```
  hostname# inet policy rule add policy2 1027 table default
  Inet policy policy2 1025 set table default was created.
  ```

inet policy rule add match

Задать условие применения правила политики маршрутизации.

Синтаксис

```
inet policy rule add <имя политики> <приоритет> match {address {from | to} <IP-адрес/маска>
| {inbound-interface | outbound-interface} <интерфейс> | dscp <значение метки DSCP>}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа;
- `<приоритет>` — приоритет правила в списке, возможные значения от 1024 до 2048. Чем меньше значение, тем выше приоритет правила;
- `from` — IP-пакеты получены от указанной подсети;
- `to` — IP-пакеты отправлены в указанную подсеть;

- `<IP-адрес/маска>` — IP-адрес и маска подсети в формате `X.X.X.X/X`;
- `inbound-interface` — IP-пакеты поступили на указанный интерфейс;
- `outbound-interface` — IP-пакеты отправлены с указанного интерфейса;
- `<интерфейс>` — имя сетевого интерфейса;
- `dscp` — IP-пакет с меткой Differentiated Services Code Point (DSCP);
- `<значение метки DSCP>` — значение метки DSCP, шестнадцатеричное или цифро-буквенное значение из следующего списка:
  - 0x28 (AF11);
  - 0x30 (AF12);
  - 0x38 (AF13);
  - 0x48 (AF21);
  - 0x50 (AF22);
  - 0x58 (AF23);
  - 0x68 (AF31);
  - 0x70 (AF32);
  - 0x78 (AF33);
  - 0x88 (AF41);
  - 0x90 (AF42);
  - 0x98 (AF43);
  - 0x20 (CS1);
  - 0x40 (CS2);
  - 0x60 (CS3);
  - 0x80 (CS4);
  - 0xA0 (CS5);
  - 0xC0 (CS6);
  - 0xE0 (CS7);
  - 0xB8 (EF).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если политики с указанным именем не существует, создается новая.

- Если правило с указанным приоритетом существует, условие добавляется в него. Если нет — создается новое правило.
- Правило может содержать несколько условий, которые применяются одновременно.
- Чтобы правило с заданными условиями применялось, задайте действие с помощью команды inet policy rule add.
- Чтобы изменить условие применения правила, удалите его (inet policy rule delete match), а затем задайте новое.

Пример использования

- Создать правило высшего приоритета (1024) политики `policy1` для обработки IP-пакетов от подсети 192.168.1.0/30:

```
hostname# inet policy rule add policy1 1024 match address from 192.168.1.0/30
Inet policy policy1 1024 match from policy1 was created.
```

- Создать правило приоритета 1025 политики `policy2` для обработки IP-пакетов, поступающих на сетевой интерфейс `eth1`:

```
hostname# inet policy rule add policy2 1025 match inbound-interface eth1
Inet policy policy2 1025 match inbound-interface eth1 was created.
```

- Добавить для правила, созданного в предыдущем примере, обработку IP-пакетов, отправленных через интерфейс `eth2`:

```
hostname# inet policy rule add policy2 1025 match outbound-interface eth2
Inet policy policy2 1025 match outbound-interface eth2 was created.
```

- Создать правило приоритета 1026 политики `policy3` для обработки IP-пакетов с меткой DSCP со значением 0x80:

```
hostname# inet policy rule add policy3 1026 match dscp 0x80
Inet policy policy3 1026 match dscp 0x80 was created.
```

inet policy rule clear

Удалить все правила политики маршрутизации или правила заданного приоритета.

Синтаксис

```
inet policy rule clear <имя политики> [priority <приоритет>]
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации;
- `<приоритет>` — приоритет правила в списке, возможные значения от 1024 до 2048.

Режимы командного интерпретатора

Администратор.

Пример использования

- Чтобы удалить все правила, заданные в политике маршрутизации `policy1`:

```
hostname# inet policy rule clear policy1
Delete all policy rules? [Yes/No]: Yes
Inet policy policy1 was deleted.
```

- Чтобы удалить только правила приоритета 1025, заданные в политике маршрутизации `policy2`:

```
hostname# inet policy rule clear policy2 priority 1025
Inet policy policy2 1025 was deleted.
```

inet policy rule delete

Удалить действие правила политики маршрутизации.

Синтаксис

```
inet policy rule delete <имя политики> <приоритет> {table {<номер таблицы> | name <имя таблицы> | default} | block}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации;
- `<приоритет>` — приоритет правила в списке, возможные значения от 1025 до 2048;
- `table` — удалить таблицу маршрутизации, по которой обрабатываются IP-пакеты;
- `<номер таблицы>` — номер пользовательской таблицы маршрутизации;
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации;
- `default` — таблица маршрутизации по умолчанию;
- `block` — удалить блокировку IP-пакетов.

Режимы командного интерпретатора

Администратор.

Пример использования

- Чтобы в правиле приоритета 1025 политики `policy2` удалить обработку по пользовательской таблице маршрутизации `table2`:

```
hostname# inet policy rule delete policy2 1025 table table2
```

```
Inet policy policy2 1025 table table2 was deleted.
```

- Чтобы в правиле приоритета 1026 политики `policy3` удалить обработку по таблице маршрутизации по умолчанию:

```
hostname# inet policy rule delete policy3 1026 table default
Inet policy policy3 1026 table default was deleted.
```

inet policy rule delete match

Удалить условие применения правила политики маршрутизации.

Синтаксис

```
inet policy rule delete <имя политики> <приоритет> match {address {from | to}
<IP-адрес/маска> | {inbound-interface | outbound-interface} <интерфейс> | dscp <значение
метки DSCP>}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации;
- `<приоритет>` — приоритет правила в списке, возможные значения от 1024 до 2048;
- `from` — IP-пакеты получены от указанной подсети;
- `to` — IP-пакеты отправлены в указанную подсеть;
- `<IP-адрес/маска>` — IP-адрес и маска подсети в формате X.X.X.X./X;
- `inbound-interface` — IP-пакеты получены на указанный сетевой интерфейс;
- `outbound-interface` — IP-пакеты отправлены с указанного сетевого интерфейса;
- `<интерфейс>` — имя сетевого интерфейса;
- `dscp` — IP-пакет с меткой Differentiated Services Code Point (DSCP);
- `<значение метки DSCP>` — значение метки DSCP, шестнадцатеричное или цифро-буквенное значение (возможные значения см. в описании команды inet policy rule add match).

Режимы командного интерпретатора

Администратор.

Пример использования

- Чтобы в правиле приоритета 1025 политики `policy2` удалить условие обработки IP-пакетов от подсети 192.168.1.0/30:

```
hostname# inet policy rule delete policy2 1025 match address from 192.168.1.0/30
Inet policy policy2 1025 match from 192.168.1.0/30 was deleted.
```

- Чтобы в правиле приоритета 1026 политики `policy3` удалить условие обработки IP-пакетов при значении метки DSCP 0x80:

  ```
  hostname# inet policy rule delete policy3 1026 match dscp 0x80
  Inet policy policy3 1026 match dscp 0x80 was deleted.
  ```

inet pppoe add

Создать PPPoE-интерфейс с заданным номером.

Синтаксис

```
inet pppoe add <номер> [comment <комментарий>]
```

Параметры и ключевые слова

- `<номер>` — номер PPPoE-интерфейса. Возможные значения: `0-100`.
- `<комментарий>` — комментарий к PPPoE-интерфейсу, например, имя провайдера. Допустимые значения: `a-z`, `A-Z`, `0-9`, `.` `-` и пробел. Если в названии используется пробел, заключите строку в двойные кавычки (`""`). Максимальная длина — 255 символов.

Режимы командного интерпретатора

Администратор.

Особенности использования

По команде будет создан виртуальный интерфейс с именем `pppoe<номер>`.

Пример использования

```
hostname# inet pppoe add 0
New PPPoE interface pppoe0 was created
```

inet pppoe delete

Удалить PPPoE-интерфейс.

Синтаксис

```
inet pppoe delete <номер>
```

Параметры и ключевые слова

`<номер>` — номер PPPoE-интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

При удалении pppoe-интерфейса восстанавливаются параметры ethernet-интерфейса.

Пример использования

```
hostname# inet pppoe delete 0

PPPoE interface pppoe0 was deleted
```

inet route add

Добавить статический маршрут, в том числе в пользовательские таблицы маршрутизации.

Синтаксис

```
inet route add {<IP-адрес назначения> [netmask <маска>] | default} next-hop <IP-адрес
шлюза> [table <номер таблицы> [name <имя таблицы>]] [distance <1-255> [weight <1-255>]]
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес назначения создаваемого маршрута.
- `default` — маршрут по умолчанию, по которому будут пересылаться IP-пакеты с адресом назначения в случае, если для них нет других маршрутов.
- `<IP-адрес шлюза>` — IP-адрес шлюза для доступа к IP-адресу назначения.
- `<маска>` — маска подсети.
- `<номер таблицы>` — номер пользовательской таблицы маршрутизации, в которую требуется добавить данный маршрут, может принимать значения `1024-2048`.
- `<имя таблицы>` — уникальное имя пользовательской таблицы маршрутизации, в которую требуется добавить данный маршрут. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `[distance <1-255>]` — административная дистанция.
- `[weight <1-255>]` — вес.

Значения по умолчанию

- Если маска не указана, то она принимает следующие значения:
  - 0.0.0.0 — если указано ключевое слово `default`;
  - 255.255.255.255 — в остальных случаях.
- Если административная дистанция не указана, то она принимает значение 10.
- Если вес не указан, то он принимает значение 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Можно добавить несколько маршрутов по умолчанию.
- Если при добавлении нескольких маршрутов в одну и ту же сеть (включая и маршруты по умолчанию) не указывается их вес, то он назначается автоматически.
- Для маршрута по умолчанию не указывается маска подсети.
- Вес маршруту требуется задавать, если есть другой маршрут в ту же сеть через другой шлюз, и административная дистанция этих маршрутов совпадает.
- Нельзя задать вес равный `0`.
- Добавленный маршрут можно удалить только с помощью команды `inet route delete`.

Пример использования

- Чтобы добавить маршрут с адресом назначения 10.10.0.0, адресом шлюза 172.16.5.1, маской 255.255.0.0 и дистанцией 15:

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

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

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

- Чтобы добавить маршрут с адресом назначения 172.16.0.0, адресом шлюза 10.0.0.1, маской 255.255.0.0 и пользовательской таблицей маршрутизации `table1`:

  ```
  hostname# inet route add 172.16.0.0 netmask 255.255.0.0 next-hop 10.0.0.1 table 1234 name table1
  ```

- Чтобы добавить несколько маршрутов в одну сеть с разными шлюзами и настроить на них балансировку IP-трафика: в среднем по 50% от всего объема передаваемого IP-трафика на каждый маршрут:

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

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

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

inet route clear

Удалить все маршруты, в том числе маршрут по умолчанию.

Синтаксис

```
inet route clear [table {<номер таблицы> | name <имя таблицы>}]
```

Параметры и ключевые слова

- `<номер таблицы>` — номер пользовательской таблицы маршрутизации (если используется несколько таблиц маршрутизации для одного статического маршрута).
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации (если используется несколько таблиц маршрутизации для одного статического маршрута). Максимальная длина 63 символа.

Значения по умолчанию

Команда без параметров удаляет все маршруты в таблице маршрутизации по умолчанию.

Режимы командного интерпретатора

Администратор.

Пример использования

- Чтобы удалить все маршруты:

  ```
  hostname# inet route clear
  Delete all the static routes? [Yes/No]: y
  The static routes have been removed
  ```

- Чтобы удалить статические маршруты в пользовательской таблице маршрутизации с именем `table1`:

  ```
  hostname# inet route clear table name TABLE1
  Delete all the static routes? [Yes/No]: y
  The static routes have been removed
  ```

inet route delete

Удалить маршрут.

Синтаксис

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

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес назначения.
- `<маска>` — маска подсети.
- `default` — маршрут по умолчанию.
- `<IP-адрес шлюза>` — IP-адрес шлюза.
- `<номер таблицы>` — номер пользовательской таблицы маршрутизации, из которой требуется удалить данный маршрут.
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации, из которой требуется удалить данный маршрут.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если удалить единственный маршрут в таблице, не являющейся таблицей по умолчанию, то таблица тоже будет удалена.
- Если в удаляемом маршруте не указаны маска сети и IP-адрес шлюза, то выполняется поиск всех маршрутов в указанный IP-адрес назначения. Если будет найдено несколько маршрутов в указанный IP-адрес назначения, то в результате выполнения команды будет выдан список этих маршрутов. Вы можете подтвердить удаление всех маршрутов, для этого введите **y** и нажмите **Enter**. Аналогичная ситуация возникнет при удалении маршрута с несколькими шлюзами.

Пример использования

- Чтобы удалить маршрут с адресом назначения 10.0.14.0:

```
hostname# inet route delete 10.0.14.0
You are going to delete the following static routes:
Destination     Netmask           Next hop        Distance        Weight
-----------     -----------       -----------     -----------     -------
10.0.14.0       255.255.255.0     10.0.1.1        10              1
10.0.14.0       255.255.255.0     10.0.2.1        10              1
Continue? (y/n): y
Routes deleted.
```

- Чтобы удалить статический маршрут с адресом назначения 172.16.0.0 в пользовательской таблице маршрутизации `table1`:

```
hostname# inet route delete 172.16.0.0 netmask 255.255.255.0 next-hop 10.0.1.12 table
name table1
```

inet show bonding

Просмотреть статус и параметры агрегированного интерфейса.

Синтаксис

```
inet show bonding [<интерфейс>]
```

Параметры и ключевые слова

`<интерфейс>` — имя агрегированного интерфейса.

Значения по умолчанию

Если интерфейс не указан, выводится информация обо всех агрегированных интерфейсах.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде выводится:

- Общая информация:
  - `Ethernet Channel Bonding Driver` — версия драйвера агрегирования.
  - `Bonding Mode` — режим работы агрегированного интерфейса (см. inet bonding add).
  - `Transmit Hash Policy` — алгоритм вычисления хэш-функции, используемый в режимах balance-xor и 802.3ad (см. inet ifconfig bonding xmit-hash-policy).
  - `MII Status` — статус соединения на агрегированном интерфейсе.
  - `MII Polling Interval (ms)` — период (в миллисекундах) проверки соединения на подчиненных интерфейсах (см. inet ifconfig bonding miimon).
  - `Up Delay (ms)` — время включения подчиненного интерфейса (в миллисекундах) после восстановления соединения. Параметр не настраивается.
  - `Down Delay (ms)` — время выключения подчиненного интерфейса (в миллисекундах) при потере соединения. Параметр не настраивается.
- `802.3ad info` — подробная информация о режиме 802.3ad:

- `LACP rate` — частота обмена пакетами по протоколу LACP (`slow` — 30 секунд, `fast` — 1 секунда). См. inet ifconfig bonding lacp-rate.
- `Min links` — минимальное количество активных соединений для начала передачи данных (по умолчанию — 0). Параметр не настраивается.

  При значении 0 передача данных начинается после включения агрегированного интерфейса.
- `Aggregator selection policy (ad_select)` — режим выбора активного интерфейса в режиме 802.3ad (см. inet ifconfig bonding ad-select).
- `System priority` — приоритет в каскадной балансировке маршрутизаторов (по умолчанию — 65535). Параметр не настраивается.
- `System MAC address` — MAC-адрес для обмена пакетами по протоколу LACP.

- `Active aggregator info` — состояние агрегированного интерфейса:
  - `Aggregator ID` — идентификатор агрегированного интерфейса.
  - `Number of ports` — количество физических портов, участвующих в агрегации.
  - `Actor Key` — идентификатор агрегированного интерфейса для обмена пакетами по протоколу LACP.
  - `Partnet Key` — идентификатор получателя при обмене пакетами по протоколу LACP.
  - `Partner Mac Address` — MAC-адрес получателя при обмене пакетами по протоколу LACP.
- `Slave Interface` — информация о подчиненных интерфейсах:
  - `MII Status` — статус соединения на подчиненном интерфейсе.
  - `Speed` — скорость передачи данных по подчиненному интерфейсу.
  - `Duplex` — дуплекс агрегированного интерфейса (`full` — полный дуплекс).
  - `Link Failure Count` — счетчик ошибок при передаче данных.
  - `Permanent HW addr` — MAC-адрес подчиненного интерфейса.
  - `Slave queue ID` — идентификатор очереди логического интерфейса.
  - `Aggregator ID` — идентификатор агрегированного интерфейса.
  - `Actor Churn State` — статус синхронизации соединения на агрегированном интерфейсе (`none` — соединение синхронизировано, `churned` — соединение в процессе согласования).
  - `Partner Churn State` — статус синхронизации соединения на стороне получателя (`none` — соединение синхронизировано, `churned` — соединение в процессе согласования).
  - `Actor Churned Count, Partner Churned Count` — счетчики синхронизации соединения отправителя и получателя. Если значение параметров совпадает, отправитель и получатель синхронизировали соединение.
- `details actor lacp pdu, details partner lacp pdu` — информация о настройках при обмене пакетами по протоколу LACP на агрегированном интерфейсе и на интерфейсе получателя:
  - `system priority` — приоритет в каскадной балансировке маршрутизаторов.

- `system mac address` — MAC-адрес для обмена пакетами по протоколу LACP.
- `port key`, `oper key` — идентификаторы для обмена пакетами по протоколу LACP.
- `port priority` — приоритет при обмене BPDU-кадрами.
- `port number` — номер порта агрегированного интерфейса.
- `port state` — состояние порта LACP.

Пример использования

```
hostname# inet show bonding
```

inet show dgd configuration

Просмотреть параметры службы DGD.

Синтаксис

```
inet show dgd configuration
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

В выводе команды содержатся значения заданных параметров службы DGD, а также количество заданных шлюзов и правил.

Пример использования

Чтобы просмотреть заданные параметры службы DGD:

```
hostname> inet show dgd configuration
DGD is running
DGD autostart is on
Response-time = 2
Interval-time = 10
Retries-count = 3
Syslog-level= Error (1)
Next-hop configured = 3
Rules configured = 2
```

inet show dgd next-hop

Просмотреть параметры шлюзов.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

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

Пример использования

Чтобы просмотреть заданные параметры всех шлюзов:

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

inet show dgd rule

Просмотреть параметры правил службы DGD.

Синтаксис

```
inet show dgd rule [<имя правила>]
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

В выводе команды содержатся значения заданных параметров правил службы DGD, такие как:

- имя правила;
- имя шлюза;
- режим проверки шлюза;
- действие, выполняемое при совпадении всех признаков проверки шлюза.

Пример использования

Чтобы просмотреть заданные параметры всех правил службы DGD:

```
hostname> inet show dgd rule
```

inet show dhcp client

Просмотреть настройки DHCP на сетевых интерфейсах (настройки DHCP-клиента).

Синтаксис

```
inet show dhcp client
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде выводится следующая информация:

- `Administrative distance for DHCP/PPP routes` — административная дистанция, которая задана для маршрутов, поступающих от DHCP-сервера;
- `Default metric for DHCP/PPP routes` — метрика по умолчанию;
- `Interface` — список сетевых интерфейсов со следующими параметрами:
  - `DHCP` — статус режима DHCP: включен (`yes`) или выключен (`no`);
  - `Routes` — разрешение на автоматическое получение IP-адресов;
  - `Metric` — специфичные метрики на сетевых интерфейсах, если такие заданы;
  - `DNS` — разрешение на автоматическое получение адресов DNS-серверов;
  - `NTP` — разрешение на автоматическое получение адресов NTP-серверов.

Пример использования

```
hostname> inet show dhcp client

Administrative distance for DHCP/PPP routes: 80

Default metric for DHCP/PPP routes: 60

Interface    DHCP       Routes     Metric      DNS         NTP

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

eth0         no         yes        default     yes         yes

eth1         yes        yes        50          yes         yes

...
```

inet show dhcp server

Просмотреть настройки DHCP-сервера и его текущее состояние.

Синтаксис

```
inet show dhcp server
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> inet show dhcp server

DHCP server autostart is on
DHCP server is started
DHCP server interfaces eth0
DHCP server configuration:
default-lease-time = 864000
max-lease-time = 864000
subnet 172.16.1.0 netmask 255.255.255.0
  option subnet-mask = 255.255.255.0
  option broadcast-address = 172.16.1.255
  interface = eth0
  option routers = 172.16.1.1
  range = 172.16.1.2 172.16.1.254
```

inet show dhcp server lease

Просмотреть список клиентов DHCP-сервера.

Синтаксис

```
inet show dhcp server lease [{last | all | full}]
```

Параметры и ключевые слова

- `last` — вывести текущий список клиентов DHCP-сервера (по умолчанию).
- `all` — вывести полный список клиентов DHCP-сервера с историей аренды IP-адресов.
- `full` — вывести полный список клиентов DHCP-сервера без форматирования вывода (см. пример ниже).

Значения по умолчанию

По умолчанию команда без параметров выводит текущий список клиентов DHCP-сервера (`last`).

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Если среди клиентов DHCP-сервера присутствуют клиенты, подключенные к разным интерфейсам VLAN, у который один MAC-адрес, то по умолчанию в выводе команды отображаются IP-адреса клиентов только одного интерфейса VLAN. Для отображения информации о клиентах всех интерфейсов VLAN выполните команду с параметром `all` (`inet show dhcp server lease all`).

Пример использования

- Чтобы просмотреть текущий список клиентов DHCP-сервера:

```
hostname> inet show dhcp server lease
MAC                IP             hostname         valid until
=================  =============  ===============  ========================
90:27:e4:f9:9d:d7  192.168.0.182  iMac-de-mac      2024-12-12 01:37:06
d8:a2:5e:94:40:81  192.168.0.178  foo-2            2024-12-12 01:04:56
e8:9a:8f:6e:0f:60  192.168.0.127  angela           2024-12-11 23:55:32
ec:55:f9:c5:f2:55  192.168.0.179  angela           2024-12-11 23:54:56
f0:4f:7c:3f:9e:dc  192.168.0.183  kindle-1234567   2024-12-11 23:54:31
f4:ec:38:e2:f9:67  192.168.0.185  -NA-             2024-12-11 23:55:40
f8:d1:11:b7:5a:62  192.168.0.184  -NA-             2024-12-11 23:57:34
```

- Чтобы просмотреть полный список клиентов DHCP-сервера без форматирования вывода:

```
hostname> inet show dhcp server lease full
lease 192.168.42.1 {
starts 0 2024/01/30 08:02:54;
ends 5 2024/02/04 08:02:54;
hardware ethernet
00:50:04:53:D5:57;
uid 01:00:50:04:53:D5:57;
client-hostname "PC0097";
}
...
```

inet show dhcp relay

Просмотреть настройки службы DHCP-relay и ее текущее состояние.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

- Пользователь.

- Администратор.

Пример использования

Чтобы просмотреть настройки 2-ой копии службы DHCP-relay:

```
hostname> inet show dhcp relay 2
DHCP relay 2 started
External DHCP server X.X.X.X
External DHCP server interface eth2
Backup DHCP server Y.Y.Y.Y
Backup DHCP server interface eth2
Internal listen interfaces eth3.1 eth3.2
```

inet show dns

Просмотреть информацию о состоянии DNS-сервера.

Синтаксис

```
inet show dns
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> inet show dns
DNS server autostart is on
DNS server is RUNNING
DNS requests logging is on
DNS requests log size: 50 MB
```

inet show interface

Просмотреть параметры и состояние сетевого интерфейса.

Синтаксис

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

Параметры и ключевые слова

- `<имя интерфейса>` — имя физического интерфейса.

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

Значения по умолчанию

Если интерфейс не указан, выводится информация обо всех интерфейсах, включая дополнительные IP-адреса интерфейсов.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Если в качестве параметра вы указали имя виртуального интерфейса, будет выведена краткая информация по основному интерфейсу.
- По команде выводится следующая информация:
  - MAC-адрес физического интерфейса.
  - IP-адрес.
  - Маска подсети.
  - Настройки получения информации от DHCP-сервера и заданная метрика для маршрутов DHCP-сервера, если на интерфейсе включен соответствующий режим.
  - Класс интерфейса (см. inet ifconfig class). В зависимости от класса выводится информация:
    - Для класса `trunk` — список существующих дочерних виртуальных интерфейсов.
    - Для класса `access` — информация о родительском интерфейсе данного виртуального интерфейса.
    - Для класса `slave` — информация о том, какому агрегированному интерфейсу подчинен данный интерфейс либо информация о том, что интерфейс пока не подчинен ни одному из агрегированных интерфейсов.
  - Состояние интерфейса (включен или выключен).
  - Для всех сетевых интерфейсов выводится максимальная возможная скорость 10 Гбит/с. Реальная скорость передачи данных через интерфейс зависит от характеристик аппаратного обеспечения, назначенного для виртуальной машины.
- Если в качестве параметра вы указали имя агрегированного интерфейса, дополнительно будет выведена информация:
  - режим работы агрегированного канала;
  - частота проверки соединения для подчиненных интерфейсов в миллисекундах;

- в режиме `802.3ad` — режим выбора активного агрегатора и частоту обмена пакетами LACP;
- в режиме `802.3ad` и `balance-xor` — алгоритм хэширования пакетов;
- в режимах `active-backup`, `balance-tlb` — основной подчиненный интерфейс;
- список подчиненных физических интерфейсов.

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

Таблица 1. Состояния сетевого интерфейса

Состояние сетевого интерфейса	Выводимые параметры и флаги
Интерфейс включен и функционирует	Флаги: `<UP RUNNING>` — присутствуют Параметры: • `Link detected: yes` • `Speed: определено` • `Duplex: определено`
Интерфейс выключен программно	Флаги: `<UP RUNNING>` — отсутствуют Параметры: • `Link detected: no` • `Speed: определено` • `Duplex: определено`
Отключен сетевой кабель	Флаги: `<UP>` — присутствует `<RUNNING>` — отсутствует Параметры: • `Link detected: no` • `Speed: не определено (Unknown)` • `Duplex: не определено (Unknown)`

Пример использования

Просмотреть информацию об интерфейсе `eth0`:

```
hostname> inet show interface eth0

eth0      Link encap:Ethernet  HWaddr 00:15:17:e4:6c:5a
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:70
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

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

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

inet show mac-address-table

Просмотреть ARP-таблицу (таблицу, содержащую записи о преобразованиях IP-адресов в MAC-адреса).

Примечание. Если узел недоступен, время жизни записей в ARP-таблице от 5 до 10 минут.

Синтаксис

```
inet show mac-address-table [{interface <интерфейс> | address <IP-адрес> | hwaddress
<MAC-адрес> | vlan <интерфейс VLAN>}]
```

Параметры и ключевые слова

- `<интерфейс>` — фильтрация по имени сетевого интерфейса ViPNet Coordinator HW (физического или виртуального):
  - Если вы укажете физический сетевой интерфейс (например, `eth0`), для которого настроены виртуальные сетевые интерфейсы, то в выводе команды будут содержаться записи как для физического сетевого интерфейса, так и для всех виртуальных сетевых интерфейсов, настроенных на нем.
  - Если вы укажете виртуальный сетевой интерфейс (например, `eth0.1`), то в выводе команды будут содержаться записи только для указанного виртуального сетевого интерфейса
- `<IP-адрес>` — фильтрация по IP-адресу в формате X.X.X.X. В случае указания части IP-адреса будут выведены все записи, содержащие в подстроке указанную часть (октеты) IP-адреса.
- `<MAC-адрес>` — фильтрация по MAC-адресу в формате XX:XX:XX:XX:XX:XX. В случае указания только части MAC-адреса будут выведены все записи, содержащие в подстроке указанную часть MAC-адреса.
- `<интерфейс VLAN>` — фильтрация по номеру сетевого интерфейса VLAN ViPNet Coordinator HW (например, `vlan 1`).

Значения по умолчанию

Если параметр не указан, выводится вся ARP-таблица.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

- Просмотреть всю ARP-таблицу:

```
hostname> inet show mac-address-table
Address             HWtype      HWaddress              Flags Mask     Iface
----------------    ---------   --------------------   ------------   -------
172.16.5.1          ether       4c:02:89:0c:53:a2      C              eth3
172.23.221.11       ether       00:0c:29:09:1a:98      C              eth0
172.23.221.99       ether       54:04:a6:d0:f7:1a      C              eth0
172.16.5.3          ether       4c:02:89:08:ef:24      C              eth3
Found: 4
```

- Просмотреть ARP-таблицу с фильтрацией по сетевому интерфейсу `eth0`:

```
hostname> inet show mac-address-table interface eth0
Address             HWtype      HWaddress              Flags          Iface
----------------    ---------   --------------------   ------------   -------
81.30.192.131       ether       1c:74:0d:10:16:3d      C              eth0.1
81.30.192.132       ether       b4:b5:2f:89:bb:0d      C              eth0.1
81.30.192.129       ether       00:1f:ca:b3:6c:c0      C              eth0.2
81.30.192.133       ether       64:d1:54:14:c5:53      C              eth0.2
Found: 4
```

- Просмотреть записи ARP-таблицы, содержащие часть IP-адреса 30.192:

```
hostname> inet show mac-address-table address 30.192
Address             HWtype      HWaddress              Flags          Iface
----------------    ---------   --------------------   ------------   -------
81.30.192.131       ether       1c:74:0d:10:16:3d      C              eth0.1
86.30.192.132       ether       b4:b5:2f:89:bb:0d      C              eth0.1
218.15.30.192       ether       00:1f:ca:b3:6c:c0      C              eth0.2
81.30.192.133       ether       64:d1:54:14:c5:53      C              eth0.2
Found: 4
```

- Просмотреть записи ARP-таблицы, содержащие часть MAC-адреса `b4:b5:2f`:

```
hostname> inet show mac-address-table hwaddress b4:b5:2f
Address             HWtype      HWaddress              Flags          Iface
----------------    ---------   --------------------   ------------   -------
81.30.192.132       ether       b4:b5:2f:89:bb:0d      C              eth0.1
81.30.192.133       ether       14:c5:b4:b5:2f:53      C              eth0.2
10.0.0.1            ether       b4:b5:2f:b4:b5:2f      C              eth1.1
```

```
Found: 3
```

inet show ntp

Просмотреть настройки и состояние NTP-сервера.

Синтаксис

```
inet show ntp
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Режим автозапуска сервера:
  - `NTP server autostart is on` — автозапуск включен;
  - `NTP server autostart is off` — автозапуск выключен.
- Использование NTP-серверов по умолчанию:
  - `used_default on` — использовать NTP-сервера по умолчанию;
  - `used_default off` — не использовать NTP-сервера по умолчанию.
- Возможны следующие состояния NTP-сервера:
  - `NTP server is INITIALIZING` — NTP-сервер в процессе запуска с проверкой доступности публичных или корпоративных NTP-серверов;
  - `NTP server is RUNNING` — NTP-сервер запущен, доступен хотя бы один NTP-сервер;
  - `NTP server is TERMINATING` — работа NTP-сервера в процессе завершения;
  - `NTP server is STOPPED` — NTP-сервер не запущен.
- Если NTP-сервер запущен, выводятся следующие параметры NTP-серверов, используемых для синхронизации:
  - `remote` — IP-адреса NTP-серверов, с которыми синхронизируется время. Перед IP-адресом может отображаться один из символов, определяющий статус сервера:
    - пробел — имеет слишком высокий уровень и/или не может быть проверен;
    - `x` — использует некорректный алгоритм;
    - `.` — исключен из-за большого расстояния;
    - `-` — исключен группирующим алгоритмом;
    - `+` — добавлен в список серверов, отобранных для синхронизации;

    - `#` — отобран для синхронизации, но есть 6 лучших кандидатов;
    - `*` — выбран для синхронизации в настоящий момент;
    - `o` — выбран для синхронизации, но используется PPS сигнал (pulse per second).
  - `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 получением ответа;
  - `offset` — смещение в миллисекундах между ViPNet Coordinator HW и NTP-серверами;
  - `jitter` — абсолютное значение в миллисекундах с указанием среднеквадратичного отклонения смещения относительно ViPNet Coordinator HW;
  - `refid` — код ошибки или идентификатор NTP-сервера.
- Поддержка изолированного режима:
  - `NTP orphan mode support is on with stratum 5` — поддержка изолированного режима включена;
  - `NTP orphan mode support is off` — поддержка изолированного режима выключена.

Пример использования

```
hostname> inet show ntp
NTP server autostart is on
NTP server is RUNNING
Used_default on
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
```

```
NTP orphan mode support is off
NTP use default servers is on
```

inet show policy rule

Просмотреть правила политик маршрутизации.

Синтаксис

```
inet show policy rule {active | all | <имя политики>}
```

Параметры и ключевые слова

- `active` — правила для действующих политик маршрутизации;
- `all` — параметры всех политик маршрутизации;
- `<имя политики>` — уникальное текстовое имя политики маршрутизации. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Чтобы завершить просмотр, нажмите **Q**.
- В кластере команда выполняется на активном узле.

Пример использования

Чтобы просмотреть правила, заданные для активной политики маршрутизации:

```
hostname> inet show policy rule active
Policy default is active.
Policy rule(s) configured: 1
Rule(Policy) Name Priority
  Values
------------------------------------------------------------------------
rule default
      table 254 (default)
```

inet show pppoe config

Просмотреть настройки PPPoE-интерфейса.

Синтаксис

```
inet show pppoe config [<номер>]
```

Параметры и ключевые слова

`<номер>` — номер PPPoE-интерфейса.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Если номер PPPoE-интерфейса не указан, выводится информация о настройке всех PPPoE-интерфейсов.

Пример использования

```
hostname> inet show pppoe config 0

pppoe0: enable

Set to: eth0

Comment: Not set

Username: user1

Password: user1****

Authentication protocol: CHAP

Address: auto

Mask: Not set

MTU: auto

Get provider's DNS servers: Yes

Use interface as default route: No

Route metric: 70
```

inet show pppoe list

Просмотреть список PPPoE-интерфейсов.

Синтаксис

```
inet show pppoe list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname# show pppoe list
Number  Interface   State       Comment
  1       eth1      active
  5       eth3      inactive    ISP-1
  13      eth2      active
```

inet show pppoe session

Просмотреть открытые PPPoE-сессии.

Синтаксис

```
inet show pppoe session [<номер>]
```

Параметры и ключевые слова

<номер> — номер PPPoE-интерфейса.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Если <номер> не указан, выводится информация обо всех открытых сессиях.

Пример использования

- Чтобы просмотреть информацию об открытой сессии на интерфейсе `pppoe5`:

```
hostname> inet show pppoe session 5

Session ID  Port  Local MAC          Remote MAC         Local address  Remote
address
14          eth0  08:00:27:c4:47:08  08:00:27:75:26:65  192.168.0.2    192.168.0.1


Packets
InB     InP     OutB    OutP
613     19      2213    41
```

- Чтобы просмотреть информацию обо всех открытых сессиях:

```
hostname> inet show pppoe session

PPPoE 1 client session
Session ID  Port  Local MAC          Remote MAC         Local address  Remote
address
7           eth1  08:00:27:55:44:34  00:00:5e:00:53:c1  192.168.2.2    192.168.2.1


Packets
InB     InP     OutB    OutP
423     28      150     2


PPPoE 5 client session
Session ID  Port  Local MAC          Remote MAC         Local address  Remote
address
14          eth0  08:00:27:c4:47:08  08:00:27:75:26:65  192.168.0.2    192.168.0.1


Packets
InB     InP     OutB    OutP
613     19      2213    41
```

inet show routing

Просмотреть таблицу маршрутизации по умолчанию, списки маршрутов от конкретного источника (Static, DHCP/PPP, OSPF) или пользовательскую таблицу маршрутизации.

Синтаксис

```
inet show routing [{static [table {<номер таблицы> | name <имя таблицы> | default}] | dhcp
| ospf [<фильтр>]}]
```

Параметры и ключевые слова

- `static` — просмотр статических маршрутов:
  - `table` — из таблицы маршрутизации:
    - `<номер таблицы>` — номер пользовательской таблицы маршрутизации.
    - `<имя таблицы>` — имя пользовательской таблицы маршрутизации;
    - `default` — из таблицы маршрутизации по умолчанию (Main).
- `dhcp` — просмотр маршрутов, получаемых от DHCP/PPP-сервера;
- `ospf` — просмотр маршрутов, передаваемых по протоколу OSPF.
- `<фильтр>` — строка текста, по которой необходимо отфильтровать записи. Допустимые символы: `0-9`, `a-z`, `A-Z`, `/`, `.`, `:`, `[`, `]`. Длина: 1–32 символа.

Значения по умолчанию

Если параметры не указаны, выводится список со всеми маршрутами, кроме маршрутов из пользовательских таблиц маршрутизации.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Фильтрация (параметр `<фильтр>`) работает только для просмотра динамических маршрутов, передаваемых по протоколу OSPF. Без указания параметра отображаются все маршруты, передаваемые по протоколу OSPF.
- 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.
- Пояснения по атрибутам, которые выводятся перед списком маршрутов, приведены в документе «Настройка с помощью командного интерпретатора», в разделе «Просмотр таблиц маршрутизации».

Пример использования

- Чтобы просмотреть пользовательскую таблицу маршрутизации с номером 1234:

```
hostname> inet show routing static table 1234
Table 1234 (TABLE1)
Destination      Netmask          Next hop         Distance Weight
```

```
-----------      -------          --------         -------- ------
172.16.0.0       255.255.0.0      10.0.0.1         10       1
```

- Чтобы просмотреть содержимое таблицы маршрутизации по умолчанию:

```
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
Routing table MAIN (254):
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
```

inet show traffic

Просмотреть статистику передачи данных по интерфейсам: текущее значение скорости и объёма трафика.

Синтаксис

```
inet show traffic [interface <интерфейс>][interval <интервал обновления>]
```

Параметры и ключевые слова

- `<интерфейс>` — интерфейс (физический, агрегированный, виртуальный).
- `<интервал обновления>` — интервал обновления статистики в секундах, целое число от 1 до 10.

Значения по умолчанию

Интервал обновления — 3 секунды.

Режимы командного интерпретатора

- Пользователь.

- Администратор.

Особенности использования

- Без указания интерфейса отображается статистика по всем физическим и агрегированным интерфейсам.
- Статистика включает:
  - имя интерфейса;
  - текущую входящую скорость интерфейс (RX speed);
  - текущую исходящую скорость интерфейс (TX speed);
  - объём входящего трафика с момента начала работы интерфейса (RX Total);
  - объём исходящего трафика с момента начала работы интерфейса (TX Total);
  - время, с которого ведется подсчет объёма трафика (время загрузки ViPNet Coordinator HW).
- Чтобы завершить выполнение команды, нажмите **Ctrl+C**.
- В кластере команда доступна для выполнения на обоих узлах.

Пример использования

```
hostname> inet show traffic

Please wait for 3 sec. Gathering traffic....

Interface          RX speed            TX speed             RX Total         TX Total
---------          --------            --------             --------         --------
eth0               10,24 Kbit/s        12,37 Kbit/s         456,12 KB        517,37 KB
eth1               999,99  bit/s       634,12  bit/s        12,31 KB         6,27 KB
bond0              1,00 Gbit/s         1000,00 Mbit/s       1,10 TB          1022,12 GB
eth2               512,00 Mbit/s       500,00 Mbit/s        563,20 GB        511,06 GB
eth3               512,00 Mbit/s       500,00 Mbit/s        563,20 GB        511,06 GB

Mon Feb 2 09:55:16 2024
```

inet show usb-modem

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Просмотреть информацию о модеме:

- Статус подключения модема.
- Статус модема (найден/не найден).
- Код страны.
- Имя текущего оператора связи.
- Уровень сигнала.
- Состояние SIM-карты.
- ПИН.
- База данных (пользовательская или база провайдеров).
- Код мобильной сети (MCC).
- Мобильный код страны (MNC).
- Идентификатор сети GSM (APN).
- Пользователь и пароль.
- Номер.

Синтаксис

```
inet show usb-modem [provider <код страны> name {<оператор> | all} [type <apn>]]
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны.
- `<оператор>` — имя мобильного оператора.
- `<apn>` — APN , используемый при соединении с оператором. Допустимые символы: `0-9`, a-z, `A-Z`, `- _ @ .`. Длина: 1—32 символа.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

Provider country: us

Cellular provider name: xTelecom

MNC, MCC: 250, 01

APN: internet

Username: gdata

Password: gdata
```

```
Dial number: *99***1#
```

inet show vlan

Просмотреть список виртуальных интерфейсов.

Синтаксис

```
inet show vlan
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Таблица со списком виртуальных интерфейсов содержит следующие столбцы:

- `Id` — номер виртуальной сети.
- `Name` — имя виртуального интерфейса.
- `IP` — IP-адрес виртуального интерфейса.
- `Parent` — имя родительского физического интерфейса.
- `Comment` — комментарий к виртуальной сети.

Пример использования

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

inet show wifi

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

Просмотреть настройки адаптера Wi-Fi.

Синтаксис

```
inet show wifi
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> inet show wifi

WiFi service is enabled

The WiFi service role is client

ssid=TEST

wpa=2

wpa_key_mgt=WPA-PSK

wpa_passphrase=12345

wpa_pairwise=TKIP
```

inet smtp login

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Задать имя пользователя для подключения к SMTP-серверу.

Синтаксис

```
inet smtp login <имя пользователя>
```

Параметры и ключевые слова

`<имя пользователя>` — имя пользователя для аутентификации. Допустимые символы: `A-Z`, `a-z`, `0-9`, `- _ . + @`. Длина: 1—32 символа.

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet smtp login john.smith
```

inet smtp mode

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Включить или выключить отправку SMTP-оповещений.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet smtp mode on
```

inet smtp password

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Задать пароль для подключения к SMTP-серверу.

Синтаксис

```
inet smtp password <пароль>
```

Параметры и ключевые слова

`<пароль>` — пароль пользователя для аутентификации. Допустимые символы: `A-Z`, `a-z`, `0-9`, `~ ! @ # $ % ^ & * () _ + | ` - = : ; " { } [ ] < > , . /`. Длина: 6—64 символа.

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet smtp password pass43
```

inet smtp port

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Указать порт подключения к SMTP-серверу.

Синтаксис

```
inet smtp port <порт>
```

Параметры и ключевые слова

`<порт>` — порт подключения к SMTP-серверу.

Режимы командного интерпретатора

Администратор.

Пример использования

Задать 587 порт подключения к SMTP-серверу:

```
hostname# inet smtp port 587
```

inet smtp recipients add

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Добавить получателя SMTP-оповещений.

Синтаксис

```
inet smtp recipients add <email>
```

Параметры и ключевые слова

`<email>` — адрес электронной почты. Длина 6—254, допустимые символы `A-Z`, `a-z`, `0-9`, `- _ @ .`

Режимы командного интерпретатора

Администратор.

Особенности использования

В команде можно указать только одного получателя. Чтобы добавить нескольких получателей, выполните команду несколько раз.

Пример использования

```
hostname# inet smtp recipients add user1@web.de
```

inet smtp recipients delete

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Удалить получателя SMTP-оповещений.

Синтаксис

```
inet smtp recipients delete <email>
```

Параметры и ключевые слова

`<email>` — электронная почта. Длина 6—254, допустимые символы `A-Z`, `a-z`, `0-9`, `- _ @ .`

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet smtp recipients delete user1@web.de
```

inet smtp secure

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Настроить способ защиты соединения с SMTP-сервером.

Синтаксис

```
inet smtp secure {tls | starttls | off}
```

Параметры и ключевые слова

- `tls` — протокол защиты TLS. Порт по умолчанию 465.
- `starttls` — протокол защиты STARTTLS. Порт по умолчанию 587.
- `off` — не используется. Порт по умолчанию 25.

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet smtp secure tls
```

inet smtp sender

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Добавить отправителя SMTP-оповещений.

Синтаксис

```
inet smtp sender <email>
```

Параметры и ключевые слова

`<email>` — адрес электронной почты. Длина 6—254, допустимые символы `A-Z`, `a-z`, `0-9`, `- _ @ .`

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet smtp sender send1@web.de
```

inet smtp server

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Настроить адрес SMTP-сервер.

Синтаксис

```
inet smtp server <адрес сервера> [login <имя пользователя> password <пароль>]
```

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес или доменное имя SMTP-сервера.
- `<имя пользователя>` — имя пользователя для аутентификации. Допустимые символы: `A-Z`, `a-z`, `0-9`, `- _ . + @`. Длина: 1—32 символа.
- `<пароль>` — пароль пользователя для аутентификации. Допустимые символы: `A-Z`, `a-z`, `0-9`, `~ ! @ # $ % ^ & * () _ + | ` - = : ; " { } [ ] < > , . /`. Длина: 6—64 символа.

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# inet smtp server smtp.web.de login john.smith password pass43
```

inet smtp show

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Посмотреть настройки SMTP-оповещений:

- статус отправки оповещений;
- IP-адрес или доменное имя SMTP-сервера;
- порт SMTP-сервера;

- защита соединения;
- имя пользователя и пароль для аутентификации;
- электронная почта отправителя;
- получатели оповещений.

Синтаксис

```
inet smtp show
```

Режимы командного интерпретатора

Пользователь.

Администратор.

Пример использования

```
hostname# inet smtp show
smtp server smtp.web.de
smtp port   587
secure      starttls
password    *********
login       john.smith
sender      sender@web.de
recipients  user1@web.de user2@web.de
```

inet smtp test

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Отправить тестовое письмо.

Синтаксис

```
inet smtp test
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Отправка тестового письма возможна только если включен режим отправки уведомлений (smtp mode on (см. inet smtp mode)).

Пример использования

```
hostname# inet smtp test
```

inet snmp autostart

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Запуск SNMP-агента при загрузке ViPNet Coordinator HW выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

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

```
hostname# inet snmp autostart on
SNMP agent is enabled and will be activated on next reboot.
You need to start the SNMP agent server manually or reboot to start it.
```

inet snmp cluster node community

Задать community string, который используется для мониторинга узла кластера по протоколам SNMPv1 и SNMPv2c.

Синтаксис

```
inet snmp cluster node <IP-адрес> community
```

Параметры и ключевые слова

`<IP-адрес>` — IP-адрес интерфейса синхронизации узла кластера.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды требуется ввести community string.
- Допустимая длина community string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.
- Команда доступна для выполнения только на активном узле кластера.

Пример использования

```
hostname# inet snmp cluster node 172.168.0.1 community

Type community for 172.168.0.1: public1

Restarting SNMP Agent

New community for 172.168.0.1: public1
```

inet snmp cluster node context

Изменить контекст, назначенный узлу кластера.

Синтаксис

```
inet snmp cluster node <IP-адрес> context <контекст>
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес интерфейса синхронизации узла кластера (без маски).

- `<контекст>` — новое значение контекста для узла кластера. Допустимая длина — от 1 до 32 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита и цифры.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда доступна для выполнения только на активном узле кластера.

Пример использования

```
hostname# inet snmp cluster node 172.168.0.1 context Node1
Restarting SNMP Agent
New context for 172.168.0.1: Node1
```

inet snmp cluster show

Просмотреть конфигурацию мониторинга кластера по протоколу SNMP.

Синтаксис

```
inet snmp cluster show [community]
```

Параметры и ключевые слова

`community` — показывать список community string для мониторинга кластера.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Пользователь — параметр `community` недоступен.
- По команде отображается следующая информация:
  - разрешено или запрещено чтение SNMP-параметров по протоколам SNMPv1 и SNMPv2c;
  - IP-адреса интерфейсов синхронизации узлов кластера;
  - контексты, назначенные узлам кластера;

- community string, заданные на узлах кластера (если не задан, отображается `Not set`), если указан параметр `community`.

- Команда доступна для выполнения только в кластере.

Пример использования

```
hostname# inet snmp cluster show

RO communities for cluster nodes are OFF

IP-address      Context     Community

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

172.168.0.1     Node1       Not set

172.168.0.2     Node2       public2
```

inet snmp cluster v2

Разрешить или запретить чтение SNMP-параметров узлов кластера по протоколам SNMPv1 и SNMPv2c.

Синтаксис

```
inet snmp cluster v2 {on | off}
```

Параметры и ключевые слова

- `on` — разрешить.
- `off` — запретить.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если чтение параметров по протоколам SNMPv1 и SNMPv2c запрещено с помощью команды inet snmp v2, команда не выполняется.
- Если при включении мониторинга кластера хотя бы на одном из узлов кластера не задан community string, выводится соответствующее сообщение.
- Команда доступна для выполнения только на активном узле кластера.

Пример использования

```
hostname# inet snmp cluster v2 on
```

```
Restarting SNMP Agent
RO communities for cluster nodes is ON
```

inet snmp community add

Добавить community string (пароль) для чтения SNMP-параметров ViPNet Coordinator HW.

Синтаксис

```
inet snmp community add
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- На запрос `Type new community string:` введите значение community string.
- Допустимая длина community string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.
- Максимальное количество community string — 16.

Пример использования

Чтобы задать community string со значением `MyCommunity`:

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

inet snmp community change

Изменить community string для чтения SNMP-параметров ViPNet Coordinator HW.

Синтаксис

```
inet snmp community change
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- При выполнении команды требуется ввести текущий и новый community string.
- Допустимая длина community string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.

Пример использования

Чтобы изменить community string со значения `MyCommunity` на значение `MyCommunity1`:

```
hostname# inet snmp community change
Type current community string: MyCommunity
Type new community string: MyCommunity1
Restarting SNMP Agent
RO community MyCommunity changed to MyCommunity1
```

inet snmp community delete

Удалить community string, используемый для чтения SNMP-параметров ViPNet Coordinator HW.

Синтаксис

```
inet snmp community delete
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- На запрос `Type community string to delete:` введите значение community string.
- При вводе команды не поддерживается контекстная подсказка.

Пример использования

Чтобы удалить community string со значением `MyCommunity`:

```
hostname# inet snmp community delete
Type community string to delete: MyCommunity
RO community MyCommunity deleted
```

inet snmp community list

Просмотреть список community string для чтения SNMP-параметров ViPNet Coordinator HW.

Синтаксис

```
inet snmp community list
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1 и SNMPv2c.

Пример использования

```
hostname# inet snmp community list
community ro = private
```

inet snmp logging

Изменить уровень важности событий SNMP-агента, которые будут записываться в системный журнал ViPNet Coordinator HW.

Синтаксис

```
inet snmp logging <уровень важности>
```

Параметры и ключевые слова

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

- `off` — запись событий в журнал выключена.
- `critical` — в журнал записываются критические ошибки, после которых SNMP-агент не может продолжить работу.
- `error` — в журнал записываются ошибки, после которых SNMP-агент может продолжать работу.

- `info` — в журнал записывается полная информация о работе SNMP-агента.
- `debug` — в журнал записывается служебная информация, используемая при отладке.

Каждый последующий уровень включает в себя предыдущие.

Значения по умолчанию

В системный журнал записываются критические ошибки и ошибки, после которых SNMP-агент может продолжать работу (`error`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

- Чтобы выключить регистрацию событий SNMP-агента в системном журнале ViPNet Coordinator HW:

```
hostname# inet snmp logging off
SNMP Agent logging is off
```

- Чтобы протоколировать полную информацию о работе SNMP-агента:

```
hostname# inet snmp logging info
New SNMP Agent syslog level is info
```

inet snmp port

Задать UDP-порт, на котором SNMP-агент будет принимать запросы.

Синтаксис

```
inet snmp port <порт>
```

Параметры и ключевые слова

`<порт>` — номер UDP-порта.

Значения по умолчанию

По умолчанию SNMP-агент использует UDP-порт 161.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- Если UDP-порт используется другой службой ViPNet Coordinator HW — выводится сообщение `UDP port already in use. Please choose another port.`

Пример использования

Чтобы SNMP-агент принимал запросы на UDP-порт 5252:

```
hostname# inet snmp port 5252

SNMP agent port set to 5252 UDP
```

inet snmp reset-engineid

Сгенерировать новый идентификатор `engineID` SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp reset-engineid
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Команду рекомендуется использовать для устранения проблем, связанных с получением сообщений от SNMP-агентов ViPNet Coordinator HW по протоколу SNMPv3, одной из причин которых может быть одинаковый `engineID` у SNMP-агентов. Не следует генерировать новый идентификатор `engineID` при нормальной работе системы мониторинга SNMP-агентов.
- В кластере команда генерирует новый `engineID` только на том узле, на котором она вызвана.

Пример использования

Чтобы сгенерировать новый идентификатор `engineID`:

```
hostname# inet snmp reset-engineid

Reset successful

New EngineID = 0x80002A3C800D992556F6C6745E00000000
```

inet snmp show

Просмотреть информацию о текущем состоянии и настройках SNMP-агента.

Синтаксис

```
inet snmp show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

```
hostname> inet snmp show
Net-SNMP agent is RUNNING.
ViPNet SNMP plugin is RUNNING.
SNMP agent autostart is ON.
Reading OIDs via SNMPv1 and SNMPv2c is OFF and sending traps is OFF
Reading OIDs via SNMPv3 is ON and sending traps is ON
Device info:
      Name = MyCoordinator
      Location = Branch_Office
      Contact = admin@infotecs.ru
      engineID = 0x80002A3C800D992556F6C6745E00000000


Current syslog level is error
SNMP agent use UDP port 161.
```

По команде выводится следующая информация:

- Статус SNMP-агента — запущен (`RUNNING`) или остановлен (`STOPPED`).
- Статус плагина ViPNet SNMP — запущен (`RUNNING`) или остановлен (`STOPPED`).
- Статус запуска SNMP-агента при перезагрузке ViPNet Coordinator HW — запуск включен (`ON`) или выключен (`OFF`).

- Статус работы по протоколам SNMPv1 и SNMPv2c и статус отправки SNMP-оповещений по протоколам SNMPv1 и SNMPv2c — разрешена (`ON`) или запрещена (`OFF`).
- Статус работы по протоколу SNMPv3 и статус отправки SNMP-оповещений по протоколу SNMPv3 — разрешена (`ON`) или запрещена (`OFF`).
- Информация о ViPNet Coordinator HW, доступная по SNMP: имя устройства, месторасположение, контактная информация, идентификатор устройства. Если имя устройства, месторасположение или контактная информация не заданы — выводится сообщение `Not set`.
- UDP-порт, используемый SNMP-агентом.

inet snmp start

Запустить встроенный SNMP-агент ViPNet Coordinator HW.

Синтаксис

```
inet snmp start
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

```
hostname# inet snmp start
Starting SNMP agent... done.
```

inet snmp stop

Завершить работу встроенного SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp stop
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

```
hostname# inet snmp stop
Stopping SNMP agent... done.
```

inet snmp system contact

Задать параметр `mib-2.system.sysContact` («Контактное лицо») SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp system contact
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- На запрос `Type new syscontact:` введите значение параметра mib-2.system.sysContact.
- Допустимая длина строки параметра `mib-2.system.sysContact` — от 1 до 256 символов. Разрешенные символы в строке — прописные и строчные буквы латинского алфавита, цифры, символ пробела и специальные символы: `. * / - : _ ? = @ , & < >`.
- Значение параметра `mib-2.system.sysContact` SNMP-агента ViPNet Coordinator HW сохраняется в объекте MIB с идентификатором 1.3.6.1.2.1.1.4.0 (`iso.identified-organization.dod.internet.mgmt.mib-2.system.sysContact`).
- В кластере команда выполняется на активном узле.

Пример использования

Чтобы задать параметр `mib-2.system.sysContact`:

```
hostname# inet snmp system contact
Type new syscontact: admin@mycompany.ru
Syscontact set successfully. New syscontact = admin@mycompany.ru
```

inet snmp system location

Задать параметр `mib-2.system.sysLocation` («Местоположение») SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp system location
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- На запрос `Type new syslocation:` введите значение параметра `mib-2.system.sysLocation`.
- Допустимая длина строки параметра `mib-2.system.sysLocation` — от 1 до 256 символов. Разрешенные символы в строке — прописные и строчные буквы латинского алфавита, цифры, символ пробела и специальные символы: `. * / - : _ ? = @ , & < >`.
- Значение параметра `mib-2.system.sysLocation` SNMP-агента ViPNet Coordinator HW сохраняется в объекте MIB с идентификатором 1.3.6.1.2.1.1.6.0 (`iso.identified-organization.dod.internet.mgmt.mib-2.system.sysLocation`).
- В кластере команда задает параметр `mib-2.system.sysLocation` только на том узле, на котором она вызвана.

Пример использования

Чтобы задать параметр `mib-2.system.sysLocation` SNMP-агента ViPNet Coordinator HW:

```
hostname# inet snmp system location
Type new syslocation: Branch_Office
Syslocation set successfully. New syslocation = Branch_Office
```

inet snmp system name

Задать параметр `mib-2.system.sysName` («Имя устройства») SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp system name
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- На запрос `Type new sysname:` введите значение параметра `mib-2.system.sysName`.
- Допустимая длина строки параметра `mib-2.system.sysName` — от 1 до 256 символов. Разрешенные символы в строке — прописные и строчные буквы латинского алфавита, цифры, символ пробела и специальные символы: `. * / - : _ ? = @ , & < >`.
- Значение параметра `mib-2.system.sysName` SNMP-агента ViPNet Coordinator HW сохраняется в объекте MIB с идентификатором 1.3.6.1.2.1.1.5.0 (`iso.identified-organization.dod.internet.mgmt.mib-2.system.sysName`).
- В кластере команда задает параметр `mib-2.system.sysName` только на том узле, на котором она вызвана.

Пример использования

Чтобы задать параметр `mib-2.system.sysName` SNMP-агента ViPNet Coordinator HW:

```
hostname# inet snmp system name

Type new sysname: MyCoordinator

Sysname set successfully. New sysname = MyCoordinator
```

inet snmp trapsink add

Добавить адрес сетевого узла, на который SNMP-агент ViPNet Coordinator HW будет отправлять оповещения.

Синтаксис

```
inet snmp trapsink add <адрес> [port <номер>] [{v1 | inform}]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта, на который отправлять оповещения.
- `v1` — отправлять оповещения типа TRAP по протоколу SNMPv1.
- `inform` — отправлять оповещения типа INFORM по протоколу SNMPv2c.

Значения по умолчанию

- Если порт не задан, используется порт UDP 162.
- Если тип оповещений не задан, используется тип TRAP по протоколу SNMPv2c.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- На запрос `Type community string for sending traps:` введите community string, заданный на сетевом узле, получающем SNMP-оповещения (community-trap string).
- Максимальное количество сетевых узлов для SNMP-агента ViPNet Coordinator HW — 16.
- Допустимая длина community-trap string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `. * / - : _ ? = @ , &`.
- При указании параметра `v1` отправка оповещений INFORM невозможна.
- Если вы хотите задать порт, отличный от UDP 162, перед выполнением команды добавьте сетевой фильтр, разрешающий передачу SNMP-оповещений на данный порт (firewall add).

Пример использования

Чтобы SNMP-агент ViPNet Coordinator HW отправлял оповещения INFORM на UDP-порт 162 сетевого узла с IP-адресом 10.0.0.1:

```
hostname# inet snmp trapsink add 10.0.0.1 port 162 inform
Type community string for sending traps: trapcommunity1
Inform -> 10.0.0.1:162 UDP Community = trapcommunity1 added
```

inet snmp trapsink delete

Удалить адрес сетевого узла, на который SNMP-агент ViPNet Coordinator HW отправляет оповещения.

Синтаксис

```
inet snmp trapsink delete <адрес> [port <номер>]
```

Параметры и ключевые слова

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

- `<номер>` — номер UDP-порта.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- Если на SNMP-агенте ViPNet Coordinator HW заданы сетевые узлы с одинаковым IP-адресом и портом, но с разными community-trap string — удаляются все такие сетевые узлы.

Пример использования

Чтобы удалить сетевой узел с IP-адресом 10.0.0.1, принимающий SNMP-оповещения на UDP-порт 162:

```
hostname# inet snmp trapsink delete 10.0.0.1 port 162
Trap -> 10.0.0.1:162 UDP Community = trapcommunity1 deleted
```

inet snmp trapsink list

Просмотреть список сетевых узлов, на которые SNMP-агент отправляет оповещения.

Синтаксис

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

Параметры и ключевые слова

`secure` — отображать community-trap string.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Пользователь — параметр `secure` недоступен.
- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.

Пример использования

- Чтобы просмотреть список сетевых узлов, на которые SNMP-агент отправляет оповещения:

```
hostname> inet snmp trapsink list
Trap {v1|v2c} -> 101.101.101.211:162 UDP

Trap {v1|v2c} -> my-domain.org:162 UDP

Inform -> 10.10.10.3:162 UDP
```

- Чтобы просмотреть список сетевых узлов, на которые SNMP-агент отправляет оповещения, включая community-trap string:

```
hostname# inet snmp trapsink list secure
Trap {v1|v2c} -> 101.101.101.211:162 UDP
Community = trapcommunity2

Trap {v1|v2c} -> my-domain.org:162 UDP
Community = trapcommunity3

Inform -> 10.10.10.3:162 UDP
Community = trapcommunity2
```

inet snmp user add

Добавить пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user add <имя пользователя> [{md5 | sha}]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `md5` или `sha` — алгоритм хэширования пароля пользователя.

Значения по умолчанию

Алгоритм хэширования пароля пользователя — MD5.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.

- Допустимая длина имени пользователя — от 1 до 32 символов. Разрешенные символы имени пользователя — прописные и строчные буквы латинского алфавита и цифры.
- При выполнении команды требуется дважды ввести пароль пользователя. При вводе паролей символы не отображаются, введенные символы отредактировать нельзя.
- Допустимая длина пароля — от 8 до 32 символов. Разрешенные символы пароля — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.
- Максимальное количество пользователей на SNMP-агенте ViPNet Coordinator HW — 32.
- Пользователь создается с правом на чтение SNMP-параметров.

Пример использования

Чтобы добавить нового пользователя `user1` и задать алгоритм хэширования пароля `sha`:

```
hostname# inet snmp user add user1 sha
Type the new user1 password:
Confirm the new user1 password:
User1 created
```

inet snmp user delete

Удалить пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user delete <имя пользователя>
```

Параметры и ключевые слова

`<имя пользователя>` — имя пользователя SNMP.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы удалить пользователя `user1`:

```
hostname# inet snmp user delete user1
```

```
user1 deleted
```

inet snmp user list

Просмотреть список пользователей SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

```
hostname> inet snmp user list
user1:
    hash=MD5 encryption=OFF
    read = ON
    trapsess = OFF
user2:
    hash=SHA encryption=off
    read = OFF
    trapsess = ON
    Trap -> 101.101.101.211:162 UDP
user3:
    hash=SHA encryption=AES
    read = ON view = all
    trapsess = ON
    Trap -> my-domain.org:162 UDP
    Inform -> 10.10.10.3:162 UDP
user4:
    certname=user4
```

```
read = ON view = all
```

По команде выводится список пользователей и настройки каждого из них:

- имя пользователя;
- настройка хэширования пароля;
- настройка шифрования данных;
- право чтения SNMP-параметров;
- право отправки SNMP-оповещений;
- параметры отправки SNMP-оповещений.

Примечание. Если пользователь использует TLS, вместо информации о хэшировании и шифровании выводится имя используемого сертификата.

inet snmp user set key

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

Синтаксис

```
inet snmp user set <имя пользователя> key [off]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `off` — удалить ключ шифрования пользователя.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- При выполнении команды требуется дважды ввести ключ шифрования пользователя. При вводе ключей символы не отображаются, введенные символы отредактировать нельзя.
- Допустимая длина ключа шифрования — от 8 до 32 символов. Разрешенные символы ключа — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

Внимание! Не используйте повторяющиеся последовательности символов в ключе шифрования. Иначе его хэш может совпасть с хэшем другого ключа. Например, ключи AbcdAbcd и AbcdAbcdAbcd будут иметь одинаковые хэши. Подробнее см. RFC 3414.

- Для шифрования данных используется алгоритм AES-128.

Пример использования

- Чтобы создать ключ шифрования пользователя `user1`, для которого ключ не создавался или был удален:

```
hostname# inet snmp user set user1 key
Type the privacy key for user1:
Confirm the privacy key for user1:
Restarting SNMP Agent
Privacy key for User1 created
```

- Чтобы изменить ключ шифрования пользователя:

```
hostname# inet snmp user set user1 key
Type the privacy key for user1:
Confirm the privacy key for user1:
Restarting SNMP Agent
Privacy key for User1 changed
```

- Чтобы удалить ключ шифрования пользователя `user1`:

```
hostname# inet snmp user set user1 key off
Restarting SNMP Agent
Privacy key for User1 deleted
```

inet snmp user set name

Изменить имя пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user set <имя пользователя> name <новое имя пользователя>
```

Параметры и ключевые слова

- `<имя пользователя>` — текущее имя пользователя SNMP.
- `<новое имя пользователя>` — новое имя пользователя SNMP.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Допустимая длина имени пользователя — до 32 символов. Разрешенные символы имени пользователя — прописные и строчные буквы латинского алфавита и цифры.
- При успешном выполнении команды:
  - Пароль пользователя остается без изменений.
  - Если для пользователя настроено шифрование данных (см. inet snmp user set key), ключ шифрования остается без изменений.
  - Если для пользователя выполнены настройки отправки оповещений, имя пользователя в них будет изменено.

Пример использования

Чтобы изменить имя пользователя с `user1` на `user2`:

```
hostname# inet snmp user set user1 name user2
Username for user1 changed to user2
```

inet snmp user set passwd

Изменить пароль пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user set <имя пользователя> passwd [{md5 | sha}]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `md5` или `sha` — алгоритм хэширования пароля.

Значения по умолчанию

Алгоритм хэширования пароля пользователя — MD5.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- При выполнении команды требуется дважды ввести новый пароль пользователя. При вводе паролей символы не отображаются, введенные символы отредактировать нельзя.
- Допустимая длина пароля — от 8 до 32 символов. Разрешенные символы пароля — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

Внимание! Не используйте повторяющиеся последовательности символов в пароле. Иначе его хэш может совпасть с хэшем другого пароля. Например, пароли AbcdAbcd и AbcdAbcdAbcd будут иметь одинаковые хэши. Подробнее см. RFC 3414.

Пример использования

Чтобы изменить пароль пользователя `user1` и задать алгоритм хэширования пароля `sha`:

```
hostname# inet snmp user set user1 passwd sha

Type the new user1 password:

Confirm the new user1 password:

Password for user1 changed
```

inet snmp user set read

Разрешить или запретить чтение SNMP-параметров (OID) для пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user set <имя пользователя> read {on | off}
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `on` — разрешить чтение.
- `off` — запретить чтение.

Значения по умолчанию

При добавлении пользователя (см. inet snmp user add) чтение по умолчанию разрешено.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы запретить пользователю `user1` чтение SNMP-параметров:

```
hostname# inet snmp user set user1 read off
Reading OID for user1 is off
```

inet snmp user set trapsess

Разрешить или запретить отправку SNMP-оповещений для пользователя.

Синтаксис

```
inet snmp user set <имя пользователя> trapsess {on | off}
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `on` — разрешить отправку.
- `off` — запретить отправку.

Значения по умолчанию

Отправка оповещений запрещена (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы разрешить отправку оповещений для пользователя `user1`:

```
hostname# inet snmp user set user1 trapsess on
```

```
Sending traps for user1 is on
```

inet snmp user set trapsess add

Добавить адрес сетевого узла, на который SNMP-агент ViPNet Coordinator HW будет отправлять оповещения для пользователя.

Синтаксис

```
inet snmp user set <имя пользователя> trapsess add <адрес> [port <номер>] [inform]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта, на который отправлять оповещения.
- `inform` — отправлять оповещения типа INFORM.

Значения по умолчанию

- Если порт не задан, используется порт UDP 162.
- Если лексема `inform` не указана, используется тип TRAP.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Максимальное количество сетевых узлов для всех пользователей SNMP-агента ViPNet Coordinator HW — 16.
- Если вы хотите задать порт, отличный от UDP 162, перед выполнением команды добавьте сетевой фильтр, разрешающий передачу SNMP-оповещений на данный порт.

Пример использования

Чтобы SNMP-агент ViPNet Coordinator HW отправлял оповещения TRAP для пользователя `user1` на UDP-порт 162 сетевого узла с IP-адресом 10.0.0.1:

```
hostname# inet snmp user set user1 trapsess add 10.0.0.1
Trap -> 10.0.0.1:162 UDP for user1 added
```

inet snmp user set trapsess delete

Удалить адрес сетевого узла, на который SNMP-агент ViPNet Coordinator HW отправляет оповещения для пользователя.

Синтаксис

```
inet snmp user set <имя пользователя> trapsess delete <адрес> [port <номер>]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта.

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы SNMP-агент ViPNet Coordinator HW перестал отправлять сообщения для пользователя `user1` на TCP-порт 162 сетевого узла с IP-адресом 10.0.0.1:

```
hostname# inet snmp user set user1 trapsess delete 10.0.0.1 port 162
Trap -> 10.0.0.1:162 UDP for user1 deleted
```

inet snmp v2

Разрешить или запретить чтение SNMP-параметров (OID) и отправку SNMP-оповещений по протоколам SNMPv1 и SNMPv2c.

Синтаксис

```
inet snmp v2 {ro | traps} {on | off}
```

Параметры и ключевые слова

- `ro` — чтение SNMP-параметров:
  - `on` — разрешить.

    - `off` — запретить.
- `traps` — отправка SNMP-оповещений:
    - `on` — разрешить.
    - `off` — запретить.

Значения по умолчанию

- Чтение SNMP-параметров запрещено (`off`).
- Отправка SNMP-оповещений запрещена (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

До выполнения команды `inet snmp v2 traps on`, которая разрешает отправку SNMP-оповещений, добавьте хотя бы один сетевой узел (см. inet snmp trapsink add).

Пример использования

- Чтобы разрешить чтение SNMP-параметров:

```
hostname# inet snmp v2 ro on
Reading OIDs via SNMPv1 and SNMPv2c is ON
```

- Чтобы разрешить отправку SNMP-оповещений:

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

inet snmp v3

Разрешить или запретить чтение SNMP-параметров (OID) и отправку SNMP-оповещений по протоколу SNMPv3.

Синтаксис

```
inet snmp v3 {ro | traps} {on | off}
```

Параметры и ключевые слова

- `ro` — чтение SNMP-параметров:
    - `on` — разрешить.
    - `off` — запретить.

- `traps` — отправка SNMP-оповещений:
  - `on` — разрешить.
  - `off` — запретить.

Значения по умолчанию

- Чтение SNMP-параметров запрещено (`off`).
- Отправка SNMP-оповещений запрещена (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

До выполнения команды `inet snmp v3 traps on`, которая разрешает отправку SNMP-оповещений, добавьте хотя бы один сетевой узел (см. inet snmp user set trapsess add).

Пример использования

- Чтобы разрешить чтение SNMP-параметров:

```
hostname# inet snmp v3 ro on
Reading OIDs via SNMPv3 is ON
```

- Чтобы разрешить отправку SNMP-оповещений:

```
hostname# inet snmp v3 traps on
Sending traps via SNMPv3 is ON
```

inet ssh

Подключиться к удаленному узлу по протоколу SSH.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

- `<пользователь>` — `user`.
- `<порт>` — `22`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При вводе идентификатора работают автозаполнение и подсказка, данные для подсказки берутся из списка связей ViPNet Coordinator HW.
- На время установления соединения с удаленным компьютером блокируется доступ к консоли. Максимальное время ожидания — 90 секунд. По истечении этого времени удаленный компьютер считается недоступным и соединение разрывается.
- В ViPNet Coordinator HW поддерживается только кодировка KOI8-R. Поэтому при подключении к компьютеру, на котором используется другая кодировка, возможны проблемы при вводе с клавиатуры и отображении на консоли символов нелатинского алфавита.

Пример использования

Чтобы подключиться к узлу ViPNet с идентификатором `0x270e000a`:

```
hostname# inet ssh id 0x270e000a
user password:
```

inet usb-modem add provider

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Добавить нового оператора в список мобильных операторов.

Синтаксис

```
inet usb-modem add provider <код страны> name <оператор> [type <apn>]
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны.
- `<оператор>` — имя мобильного оператора.
- `<apn>` — APN , используемый при соединении с оператором. Допустимые символы: `0-9`, `a-z`, `A-Z`, `- _ @ .`. Длина: 1—32 символа.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

```
hostname# inet usb-modem add provider us name xTelecom
provider xTelecom was added successfully
```

inet usb-modem clear provider-base

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Очистить список мобильных операторов.

Синтаксис

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

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

```
hostname# inet usb-modem clear provider-base
Are you sure you want to proceed?[Yes,No]
Yes
Provider base was cleared successfully
```

inet usb-modem delete provider

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Удалить оператора из списка мобильных операторов.

Синтаксис

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

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны.
- `<оператор>` — имя мобильного оператора.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

```
hostname# inet usb-modem delete provider us name xTelecom

provider xTelecom was deleted successfully
```

inet usb-modem dns

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

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

Синтаксис

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

Параметры и ключевые слова

- `on` — разрешено обращение к DNS-серверу.
- `off` — запрещено обращение к DNS-серверу.

Значения по умолчанию

По умолчанию разрешено обращение к DNS-серверу (`on`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

Запретить обращение к DNS-серверу оператора связи:

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

inet usb-modem mode

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Включить или выключить модем.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию модем выключен (`off`).
- При выключении модема автоматически выполняется подключение к сети текущего оператора.
- После включения модема проверяется наличие и целостность SIM-карты и правильность ПИНа, что может занять некоторое время. Если сразу выполнить команду inet show usb-modem, статусы SIM-карты и ПИНа могут отображаться неверно.

Пример использования

Включить использование модема:

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

inet usb-modem pin

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Задать ПИН, с помощью которого ViPNet Coordinator HW получает доступ к SIM-карте оператора связи.

Синтаксис

```
inet usb-modem pin <ПИН>
```

Параметры и ключевые слова

`<ПИН>` — ПИН.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

```
hostname# inet usb-modem pin 2398
PIN code was set
```

inet usb-modem provider phone

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Задать номер доступа текущего мобильного оператора, необходимый при подключении через модем.

Синтаксис

```
inet usb-modem provider <код страны> name <оператор> phone <телефон>
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны.
- `<оператор>` — имя мобильного оператора.
- `<телефон>` — телефонный номер.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

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

inet usb-modem provider mc

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Установить код MCC и MNC для указанного оператора мобильной связи.

Синтаксис

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

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны.
- `<оператор>` — имя мобильного оператора.
- `<mcc mnc>` — код MMC и MNC.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

```
hostname# inet usb-modem provider us name xTelecom mc 909 234
provider xTelecom mcc & mnc was set to 909 234
```

inet usb-modem provider password

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Задать пароль пользователя, используемый при аутентификации во время звонка по телефонному номеру текущего оператора связи.

Синтаксис

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

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны.
- `<оператор>` — имя мобильного оператора.
- `<пароль>` — пароль пользователя. Допустимые символы: `0-9`, `a-z`, `A-Z`, `- _ @ .`. Длина: 1—32 символа.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

```
hostname# inet usb-modem provider us name xTelecom password gdata
provider xTelecom password was set to gdata
```

inet usb-modem provider type

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Установить APN для указанного оператора мобильной связи.

Синтаксис

```
inet usb-modem provider <код страны> name <оператор> type <apn>
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны.
- `<оператор>` — имя мобильного оператора.
- `<apn>` — APN, используемый при соединении с оператором. Допустимые символы: `0-9`, `a-z`, `A-Z`, `- _ @ .`. Длина: 1—32 символа.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

```
hostname# inet usb-modem provider us name xTelecom type xtinternet
provider xTelecom connection address was set to xtinternet
```

inet usb-modem provider username

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Задать имя пользователя для аутентификации при звонке по телефонному номеру текущего мобильного оператора.

Синтаксис

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

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны.
- `<оператор>` — имя мобильного оператора.
- `<имя>` — имя пользователя. Допустимые символы: `0-9`, `a-z`, `A-Z`, `- _ @ .`. Длина: 1—32 символа.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

Задать имя пользователя `Smith`:

```
hostname# inet usb-modem provider us name xTelecom username Smith
provider xTelecom user was set to Ivanov
```

inet usb-modem route

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Включить или выключить автоматическое добавление маршрута по умолчанию, в котором в качестве шлюза используется шлюз, полученный от оператора мобильной связи.

Синтаксис

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

Параметры и ключевые слова

- `on` — включение использования полученного адреса шлюза.
- `off` — выключение использования полученного адреса шлюза.

Значения по умолчанию

По умолчанию применение маршрута включено (`on`).

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

Выключить применение маршрута по умолчанию:

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

inet usb-modem route-metric

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

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

Синтаксис

inet usb-modem route-metric {<1-255> | none}

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Задание метрики возможно только при следующих условиях:
  - Выключено использование модема.
  - Разрешено применение маршрута по умолчанию от сервера провайдера при подключении через модем.
- При удалении метрики будет использоваться метрика по умолчанию (см. inet dhcp client route-default-metric).

Пример использования

- Назначить метрику 100 для маршрутов, формируемых в процессе работы через модем:

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

- Удалить метрику:

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

inet usb-modem select provider

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Выбрать текущего мобильного оператора при подключении через модем и отключить автоопределение оператора.

Синтаксис

```
inet usb-modem select provider <код страны> name <оператор> [type <apn>]
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны.
- `<оператор>` — имя мобильного оператора.
- `<apn>` — APN , используемый при соединении с оператором. Допустимые символы: `0-9`, `a-z`, `A-Z`, `- _ @ .`. Длина: 1—32 символа.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для выполнения команды модем должен быть выключен (`inet usb-modem mode`).

Пример использования

Выбрать в качестве текущего оператора связи Verizon (us):

```
hostname# inet usb-modem select provider us name Verizon
Cellular provider was set to Verizon [us]
```

inet usb-modem traffic-limit billing-day

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Установить день начала учета мобильного трафика.

Синтаксис

```
inet usb-modem traffic-limit billing-day <день>
```

Параметры и ключевые слова

`<день>` — день, с которого начинается учет мобильного трафика.

Значения по умолчанию

1

Режимы командного интерпретатора

Администратор.

Особенности использования

- Указанный день не может быть меньше текущего.
- При наступлении указанного дня (в 00:00) счетчик трафика сбрасывается.
- Если изменить указанный ранее день, счетчик трафика не сбрасывается.

- Если в следующем месяце нет указанного дня, счетчик трафика сбрасывается в последний день месяца.

Пример использования

Установить день начала учета 31:

```
hostname# inet usb-modem traffic-limit billing-day 31

The next reset date for the counter was set. If necessary, reset the traffic counter manually.
```

inet usb-modem traffic-limit counter

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Включить, отключить или сбросить счетчик мобильного трафика.

Синтаксис

```
inet usb-modem traffic-limit counter {on | off | reset}
```

Параметры и ключевые слова

- `on` — включить счетчик.
- `off` — выключить счетчик.
- `reset` — сбросить счетчик.

Режимы командного интерпретатора

Администратор.

Пример использования

Включить счетчик мобильного трафика:

```
hostname# inet usb-modem traffic-limit counter on
```

inet usb-modem traffic-limit set

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Установить ограничение на объем используемого мобильного трафика, при котором устройство отправляет уведомление.

Синтаксис

```
inet usb-modem traffic-limit set <объем>
```

Параметры и ключевые слова

<объем> — объем трафика, при котором устройство отправляет уведомление (в Мбайтах, от 0 до 99999).

Значения по умолчанию

0 (неограничен).

Режимы командного интерпретатора

Администратор.

Пример использования

Установить ограничение на объем используемого трафика в размере 1 Гбайт (1024 Мбайта):

```
hostname# inet usb-modem traffic-limit set 1024
```

inet usb-modem traffic-limit show

Примечание. Команда доступна только на аппаратных платформах со встроенным модемом.

Посмотреть настройки учета мобильного трафика:

- объем, отслеживаемый с момента включения счетчика;
- день, когда был включен учет;
- ограничения объема;
- уведомления о превышении установленного ограничения объема трафика.

Синтаксис

```
inet usb-modem traffic-limit show
```

Режимы командного интерпретатора

Пользователь.

Администратор.

Пример использования

```
hostname# inet usb-modem traffic-limit show
counter 987 Mbyte
billing-day 22
traffic-limit 1024 Mbyte
```

inet vlan comment add

Добавить комментарий к виртуальной сети.

Синтаксис

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

Параметры и ключевые слова

- `<номер>` — номер виртуальной сети.
- `<комментарий>` — комментарий. Разрешённые символы: A–Z, a–z, 0–9, _ -. Комментарий, содержащий пробелы, должен быть указан в двойных кавычках.

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

inet vlan comment delete

Удалить комментарий к виртуальной сети.

Синтаксис

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

Параметры и ключевые слова

<номер> — номер виртуальной сети.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы удалить комментарий к виртуальной сети с номером 10:

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

inet wifi access-point channel

Задать номер канала Wi-Fi при работе ViPNet Coordinator HW в режиме точки доступа.

Синтаксис

```
inet wifi access-point channel <номер>
```

Параметры и ключевые слова

<номер> — номер канала Wi-Fi. Допустимый диапазон: 1–11.

Значения по умолчанию

По умолчанию задан канал 1.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы задать номер канала 10:

```
hostname# inet wifi access-point channel 10
```

inet wifi access-point hwmode

Выбрать стандарт сети Wi-Fi при работе ViPNet Coordinator HW в режиме точки доступа.

Синтаксис

```
inet wifi access-point hwmode {b | g}
```

Параметры и ключевые слова

- `b` — стандарт IEEE 802.11b.
- `g` — стандарт IEEE 802.11g.

Значения по умолчанию

Используется стандарт сети IEEE 802.11g.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы выбрать стандарт сети IEEE 802.11b:

```
hostname# inet wifi access-point hwmode b
Configured successfully.
```

inet wifi access-point show

Просмотреть список подключенных клиентов Wi-Fi к ViPNet Coordinator HW, при его работе в режиме точки доступа.

Синтаксис

```
inet wifi access-point show
```

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

По команде выводится список подключенных клиентов Wi-Fi, для каждого клиента — MAC-адрес и уровень сигнала.

```
hostname# inet wifi access-point show
```

```
client: 38:aa:3c:bf:86:5a
  signal: -37 dBm
  signal avg: -36 dBm
```

inet wifi authentication

- Указать тип защиты сети Wi-Fi — при работе ViPNet Coordinator HW в режиме клиента Wi-Fi.
- Задать тип защиты сети Wi-Fi — при работе ViPNet Coordinator HW в режиме точки доступа Wi-Fi.

Синтаксис

```
inet wifi {client | access-point} authentication {open | wpa-psk | wpa2-psk}
```

Параметры и ключевые слова

- `client` — ViPNet Coordinator HW работает в режиме клиента Wi-Fi.
- `access-point` — ViPNet Coordinator HW работает в режиме точки доступа Wi-Fi.
- `wpa-psk` — защита с помощью WPA-PSK.
- `wpa2-psk` — защита с помощью WPA2-PSK.
- `open` — соединение не защищено.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.
- При выполнении команды с типом защиты `wpa-psk` или `wpa2-psk` по запросу введите имя сети (SSID) и пароль доступа к сети.
- При выполнении команды с типом защиты `open` по запросу введите только имя сети (SSID).

Пример использования

- Чтобы подключиться к сети Wi-Fi с именем `WLAN_1` и защитой соединений WPA2-PSK, для которой требуется аутентификация с использованием пароля `Aa12345678`:

  ```
  hostname# inet wifi client authentication wpa2-psk
  WiFi SSID: WLAN_1
  WiFi password: Aa12345678
  WiFi client has been configured successfully
  ```

- Чтобы задать параметры точки доступа Wi-Fi `WLAN_1` с защитой соединений WPA-PSK для подключения к которой клиентов Wi-Fi аутентификация не требуется:

  ```
  hostname# inet wifi access-point authentication open
  WiFi SSID: WLAN_1
  WiFi access point has been configured successfully
  ```

inet wifi mode

Включить или выключить интерфейс Wi-Fi.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Сетевой интерфейс Wi-Fi выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию сетевой интерфейс Wi-Fi выключен (`off`).
- Команда доступна для выполнения только на аппаратных платформах со встроенным модулем Wi-Fi.
- В кластере команда не поддерживается.

Пример использования

Чтобы включить сетевой интерфейс Wi-Fi:

```
hostname# inet wifi mode on
WiFi service has been enabled
WiFi service has been started
```

inet wifi role

Выбрать режим работы ViPNet Coordinator HW в сети Wi-Fi.

Синтаксис

```
inet wifi role {access-point | client}
```

Параметры и ключевые слова

- `access-point` — режим точки доступа Wi-Fi.
- `client` — режим клиента Wi-Fi.

Значения по умолчанию

Установлен режим клиента Wi-Fi (`client`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.
- При изменении режима сбрасываются настройки интерфейса `wlan0`.

Пример использования

Чтобы переключить ViPNet Coordinator HW в режим точки доступа Wi-Fi:

```
hostname# inet wifi role access-point
The WiFi service role has been set to access-point
```

inet wifi scan

Просмотреть доступные сети Wi-Fi.

Синтаксис

```
inet wifi scan
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

```
hostname> inet wifi scan

Scanning...

bssid / frequency / signal level / flags / ssid

10:bf:48:e7:11:f8    2437  -50  [WPA2-PSK-CCMP][WPS][ESS] ASUS

00:3A:99:AA:25:30    2412  -60  [WPA2-EAP-CCMP][ESS] Infotecs

...
```

Команды группы iplir

Настройка параметров работы в защищенной сети ViPNet, а также параметров L2OverIP.

iplir adapter add

Добавить новый сетевой интерфейс.

Синтаксис

```
iplir adapter add <интерфейс> [traffic {on | off}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя добавляемого сетевого интерфейса.
- `traffic` — включение или выключение прохождения IP-трафика через добавляемый сетевой интерфейс (действие параметра аналогично команде iplir adapter traffic). Параметр может принимать следующие значения:
  - `on` — включить прохождение IP-трафика через добавляемый сетевой интерфейс;
  - `off` — выключить прохождение IP-трафика через добавляемый сетевой интерфейс.

Значения по умолчанию

Прохождение IP-трафика через добавляемый сетевой интерфейс выключено (`traffic off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Служба `iplircfg` должна быть запущена (iplir start).
- Добавляемый интерфейс должен быть заранее создан как VLAN (см. inet ifconfig vlan add) или агрегированный (см. inet ifconfig bonding add).

Пример использования

Добавить сетевой интерфейс `eth1.10` и не включать на нём прохождение IP-трафика:

```
hostname# iplir adapter add eth1.10
```

iplir adapter delete

Удалить сетевой интерфейс.

Синтаксис

```
iplir adapter delete <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы удалить сетевой интерфейс `eth1.10`:

```
hostname# iplir adapter delete eth1.10
```

iplir adapter traffic

Включить или выключить прохождение IP-трафика через сетевой интерфейс.

Синтаксис

```
iplir adapter traffic <интерфейс> {on | off}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `on` — включить прохождение IP-трафика через интерфейс.
- `off` — выключить прохождение IP-трафика через интерфейс.

Значения по умолчанию

- Для физических интерфейсов: включено (`on`).
- Для добавленных интерфейсов: выключено (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Служба `iplircfg` должна быть запущена (iplir start).
- После выполнения команды выводится предупреждение о необходимости проверить, соответствуют ли сетевые фильтры политике безопасности вашей организации.

Пример использования

Чтобы включить прохождение IP-трафика для интерфейса `eth2`:

```
hostname# iplir adapter traffic eth2 on

Set eth2 allowTraffic as on

Attention: Upon changing this parameter, make sure that firewall rules match your
organization's security policy.
```

iplir config

Редактировать один из файлов конфигурации: основной файл конфигурации, файл конфигурации заданного интерфейса или группы интерфейсов.

Синтаксис

```
iplir config [{<интерфейс> | <группа интерфейсов>}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя статического интерфейса, для которого требуется редактировать файл конфигурации.
- `<группа интерфейсов>` — имя группы динамических интерфейсов, для которой требуется редактировать файл конфигурации:
  - `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
  - `pppoe` — группа интерфейсов для подключения к сети провайдера по PPPoE;
  - `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если в команде не указан параметр, то будет запущен текстовый редактор с основным файлом конфигурации `iplir.conf`.
- Если в команде указан интерфейс или группа интерфейсов, то будет запущен текстовый редактор с файлом конфигурации этого интерфейса или группы интерфейсов `iplir.conf-<интерфейс или группа интерфейсов>`.
- Перед редактированием файла `iplir.conf` или файла `iplir.conf-<интерфейс или группа интерфейсов>` завершите работу службы `iplircfg` (см. iplir stop).

Пример использования

Чтобы отредактировать файл конфигурации интерфейса `eth0`:

```
hostname# iplir config eth0
```

iplir info

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

Синтаксис

```
iplir info [{<интерфейс> | <группа интерфейсов>}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя статического интерфейса, для которого требуется просмотреть статистику фильтрации IP-пакетов.
- `<группа интерфейсов>` — имя группы динамических интерфейсов, для которой требуется просмотреть статистику фильтрации IP-пакетов:
  - `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
  - `pppoe` — группа интерфейсов для подключения к сети провайдера по PPPoE;
  - `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Если параметр не указан, выводится информация об узле (имя узла, имя сети, версия установленного ПО, активные сетевые интерфейсы и другие параметры), количестве туннельных соединений и статистика фильтрации IP-пакетов по всем интерфейсам.
- Если указан интерфейс, выводится только статистика фильтрации IP-пакетов по этому интерфейсу.
- Если указана группа интерфейсов, выводится статистика фильтрации IP-пакетов по всем активным интерфейсам, входящим в эту группу.
- Для выполнения команды служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Чтобы просмотреть статистику по интерфейсу `eth0`:

```
hostname> iplir info eth0
Interface:              eth0

Category                                                Received            Sent

Non-encrypted packets dropped:                          0                   0
Non-encrypted bytes dropped:                            0                   0

Encrypted packets passed:                               0                   0
Encrypted packets dropped:                              0                   0
Encrypted bytes passed:                                 0                   0
Encrypted bytes dropped:                                0                   0

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

Encrypted broadcast packets passed:                     0                   2
Encrypted broadcast packets dropped:                    0                   0
Encrypted broadcast bytes passed:                       0                   716
Encrypted broadcast bytes dropped:                      0                   0
```

Информация о количестве туннельных соединений выводится в следующем формате:

```
Tunnels statistics: License <лицензионное>, Current <текущее>, Peak <максимальное> -
<дата>
```

где:

- `<лицензионное>` — максимальное количество туннельных соединений, разрешенное для роли, которая назначена узлу ViPNet Coordinator HW.
- `<текущее>` — текущее количество туннельных соединений.
- `<максимальное>` — максимально зарегистрированное количество туннельных соединений с момента последнего старта драйвера сетевой защиты.

- `<дата>` — дата и время последнего старта драйвера сетевой защиты.

iplir option get

Просмотреть состояние или значение одного из параметров межсетевого экрана.

Синтаксис

```
iplir option get <параметр>
```

Параметры и ключевые слова

`<параметр>` — параметр межсетевого экрана:

- `antispoofing` — состояние функции антиспуфинга.
- `block-fragmented-packets` — состояние функции блокирования фрагментированных IP-пакетов, передаваемых по всем сетевым интерфейсам.
- `connection-ttl-ip` — время жизни соединений по протоколу IP (для транспортных протоколов, отличных от TCP или UDP).
- `connection-ttl-tcp` — время жизни соединений по протоколу TCP.
- `connection-ttl-udp` — время жизни соединений по протоколу UDP.
- `max-connections` — максимальное количество параллельно установленных соединений.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть состояние функции блокирования фрагментированных IP-пакетов:

```
hostname> iplir option get block-fragmented-packets
Option: Block-fragmented-packets State: On
```

iplir option set antispoofing

Включить или выключить антиспуфинг.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Антиспуфинг выключен (`off`).

Режимы командного интерпретатора

Администратор.

Пример использования

Включить антиспуфинг:

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

iplir option set block-fragmented-packets

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию блокирование выключено (`off`).

Режимы командного интерпретатора

Администратор.

Пример использования

Включить блокирование:

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

iplir option set connection-ttl-ip

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

300 секунд.

Режимы командного интерпретатора

Администратор.

Пример

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

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

iplir option set connection-ttl-tcp

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

1800 секунд (`1800`).

Режимы командного интерпретатора

Администратор.

Пример

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

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

iplir option set connection-ttl-udp

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

300 секунд (`300`).

Режимы командного интерпретатора

Администратор.

Пример

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

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

iplir option set max-connections

Задать максимальное количество параллельно установленных соединений.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Таблица 2. Значения параметра max-connections для разных аппаратных платформ ViPNet Coordinator HW

Аппаратная платформа ViPNet Coordinator HW	Объем оперативной памяти	Значение по умолчанию	Максимальное значение
HW10 F1	1,8 Гбайт	150 000	150 000
HW50 N1, N2, N3, N4, A1	1,8 Гбайт	150 000	150 000
HW100 N1, N2, N3, Q1, Q2	2 Гбайт	150 000	150 000
HW1000 Q4, Q5, Q6	2 Гбайт	800 000	1 000 000
HW1000 Q7, Q8, Q9	4–16 Гбайт	800 000	1 000 000
HW 1000 Q10	8 Гбайт	800 000	1 000 000
HW2000 Q4	4 Гбайт	2 500 000	3 000 000
HW2000 Q5	32 Гбайт	6 000 000	6 500 000
HW5000 Q1, Q2	8–64 Гбайт	6 000 000	6 500 000
VA100	2 Гбайт	150 000	150 000
VA500	2 Гбайт	400 000	500 000
VA1000	4 Гбайт	800 000	1 000 000
VA2000	8 Гбайт	2 500 000	3 000 000

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы установить максимальное количество одновременных соединений равным 200000:

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

iplir ping

Проверить соединение с сетевым узлом ViPNet.

Синтаксис

```
iplir ping <идентификатор>
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

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

```
hostname> iplir ping 0x15ea000d

Check connection with 0x15ea000d...

Connection successful
```

iplir set l2overip interface

Задать рабочий интерфейс L2OverIP.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы в качестве рабочего задать виртуальный интерфейс `eth0.2`:

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

iplir set l2overip local-port

Добавить параметры локального сегмента сети в настройках L2OverIP.

Синтаксис

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

Параметры и ключевые слова

- `<порт>` — номер порта. Допустимые значения: `1-31`.
- `<IP-адрес>` — IP-адрес внешнего интерфейса ViPNet Coordinator HW.

Режимы командного интерпретатора

Администратор.

Особенности использования

В качестве IP-адреса можно указать только статический адрес.

Пример использования

Чтобы добавить локальный сегмент сети с номером порта 1 и адресом 172.16.1.1:

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

iplir set l2overip mac-ttl

Задать время жизни MAC-адреса в таблице MAC-адресов виртуального коммутатора при отсутствии трафика, поступающего от этого адреса.

Синтаксис

```
iplir set l2overip mac-ttl <время>
```

Параметры и ключевые слова

`<время>` — время в секундах. Допустимые значения: `60-86400`.

Значения по умолчанию

Установлено время 300 секунд.

Режимы командного интерпретатора

Администратор.

Пример использования

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

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

iplir set l2overip mode

Включить или выключить L2OverIP.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию L2OverIP выключен (`none`).
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Чтобы включить L2OverIP:

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

iplir set l2overip remote-port

Добавить параметры удаленного сегмента сети в настройках L2OverIP.

Синтаксис

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

Параметры и ключевые слова

- `<порт>` — номер порта удаленного сегмента.
- `<IP-адрес>` — актуальный IP-адрес видимости ViPNet Coordinator HW, к которому подключен удаленный сегмент сети (реальный или виртуальный адрес удаленного ViPNet Coordinator HW).

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

iplir set l2overip remote-port delete

Удалить порт с заданным номером из настроек L2OverIP.

Синтаксис

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

Параметры и ключевые слова

`<порт>` — номер порта, который требуется удалить.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы удалить порт с номером 2:

```
hostname# iplir set l2overip remote-port 2 delete
Do you want to delete remote port number 2 from L2OverIP configuration? [Yes/No]: y
```

iplir set l2overip unsolicited-frames

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

Синтаксис

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

Параметры и ключевые слова

- `drop` — блокировать.
- `broadcast` — обрабатывать как многоадресные с рассылкой на несколько портов:
  - кадры, принятые от локального порта, пересылать на все удаленные порты и на порт с номером 0;
  - кадры, принятые от удаленного порта, пересылать на локальный порт и на порт с номером 0;
  - кадры, принятые от порта с номером 0, пересылать на все удаленные порты и на локальный порт.

- `smart-broadcast` — аналогично режиму `broadcast`, но без обработки кадров от порта с номером 0. В этом режиме кадры, принятые от порта с номером 0, блокируются. Рекомендуемый режим при использовании технологий агрегирования каналов.

Значения по умолчанию

Установлен режим `drop`.

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы задать режим обработки `smart-broadcast`:

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

iplir set performance-mode

Включить или выключить режим повышенной производительности для одного сетевого соединения.

Синтаксис

```
iplir set performance-mode {single|multi}
```

Параметры и ключевые слова

- `single` — режим повышенной производительности для одного сетевого соединения.
- `multi` — отсутствие режима повышенной производительности для одного сетевого соединения.

Режимы командного интерпретатора

Администратор.

Особенности использования

- В режиме кластера команда выполняется только на активном узле.
- Режим производительности применяется после перезагрузки ViPNet Coordinator HW.
- Режим повышенной производительности можно включить на следующих платформах:
  - ViPNet Coordinator HW100 N1, N2, N3;
  - ViPNet Coordinator HW1000 Q10;

- ViPNet Coordinator HW2000 Q4, Q5;
- ViPNet Coordinator HW5000 Q1, Q2.

Пример использования

Чтобы включить режим повышенной производительности для одного сетевого соединения:

```
hostname# iplir set performance-mode single
Are you sure you want to switch system performance in single connection mode? (Yes/No): Yes
A reboot is required to enable the function. You can reboot system now or later.
Do you want to reboot system now? (Yes/No): Yes
```

iplir show adapter

Просмотреть разрешение на прохождение IP-трафика через сетевой интерфейс.

Синтаксис

```
iplir show adapter <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

Чтобы просмотреть параметры сетевого интерфейса `eth0`:

```
hostname> iplir show adapter eth0
Adapter eth0 single
Allow traffic = on
Type = internal
```

iplir show adapters

Просмотреть все активные статические и динамические сетевые интерфейсы ViPNet Coordinator HW. При просмотре для каждого интерфейса в списке указан параметр `allowtraffic`, который показывает, разрешено или заблокировано прохождения IP-трафика через интерфейс.

Синтаксис

```
iplir show adapters
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

Пример использования

Чтобы просмотреть список активных сетевых интерфейсов:

```
hostname> iplir show adapters
Active interface    Allowtraffic
eth0                on
eth1                on
eth2                off
eth3                on
```

iplir show adapters groups

Просмотреть активные динамические сетевые интерфейсы ViPNet Coordinator HW.

Синтаксис

```
iplir show adapters groups
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> iplir show adapters groups

Interface group: Active interfaces
```

iplir show authentication-type

Просмотреть заданный способ аутентификации пользователя на ViPNet Coordinator HW.

Синтаксис

```
iplir show authentication-type
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# iplir show authentication-type

Current authentication mode: password
```

iplir show ciphertype

Просмотреть информацию о текущем режиме шифрования для сети или отдельного узла ViPNet.

Синтаксис

```
iplir show ciphertype [<nodeid>]
```

Параметры и ключевые слова

`<nodeid>` — идентификатор узла сети ViPNet в HEX-формате.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- При указании параметра `<nodeid>` выводятся параметры шифрования для указанного узла. В случае если алгоритм шифрования для узла не задан, выводятся параметры шифрования для сети.

- При вводе некорректного `<nodeid>` (некорректные символы, отсутствует в справочнике) отображается соответствующее предупреждение, после чего выводится список связанных узлов и выполнение команды прекращается.

Пример использования

```
hostname> iplir show ciphertype

Network ciphertype - GOST-CFB: Cipher Feedback Mode
```

iplir show config

Просмотреть один из файлов конфигурации: основной файл конфигурации или файл конфигурации заданного интерфейса.

Синтаксис

```
iplir show config [{<интерфейс> | <группа интерфейсов>}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя статического интерфейса, файл конфигурации которого требуется просмотреть.
- `<группа интерфейсов>` — имя группы динамических интерфейсов, файл конфигурации которой требуется просмотреть:
  - `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
  - `pppoe` — группа интерфейсов для подключения к сети провайдера по PPPoE;
  - `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- Если параметр не указан, выводится основной файл конфигурации `iplir.conf`.
- Если указан интерфейс или группа интерфейсов, выводится файл конфигурации этого интерфейса или группы интерфейсов `iplir.conf-<интерфейс или группа интерфейсов>`.
- Чтобы завершить просмотр файла конфигурации, нажмите **Q**.

Пример использования

Чтобы просмотреть основной файл конфигурации:

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

iplir show firewall status

Просмотреть статистику работы межсетевого экрана.

Синтаксис

```
iplir show firewall status
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> iplir show firewall status
Max connections   150000
Dynamicport minimum       1024
Dynamicport maximum       65535
TCP SYN timeout   120
Connection ttl TCP   1800
Connection ttl UDP   300
ICMP timeout   30
Connection ttl IP   300
Total connections count   70
Local connections count   25
VPN connections count   10
Forward connections count 30
Tunnel connections count  5
```

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.
- `TCP SYN timeout` — таймаут установления TCP-соединения в секундах.
- `Connection ttl TCP` — таймаут разрыва TCP-соединения в секундах.

- `Connection ttl UDP` — время жизни UDP-соединения.
- `ICMP timeout` — время жизни ICMP-соединения.
- `Connection ttl IP` — время жизни соединения для протоколов, отличных от TCP, UDP, ICMP.
- `Total connections count` — текущее количество открытых, защищенных и туннелируемых соединений по всем протоколам.
- `Local connections count` — текущее количество локальных открытых соединений по всем протоколам.
- `VPN connections count` — текущее количество защищенных (зашифрованных) соединений по всем протоколам.
- `Forward connections count` — текущее количество транзитных открытых соединений по всем протоколам.
- `Tunnel connections count` — текущее количество туннелируемых соединений по всем протоколам.

iplir show key-info

Просмотреть информацию о ключах, установленных на ViPNet Coordinator HW:

- персональный ключ пользователя;
- резервный набор персональных ключей (РНПК);
- ключи узла.

Синтаксис

```
iplir show key-info
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Получение информации о ключах может требоваться в следующих случаях:

- Администратору ViPNet Coordinator HW — чтобы убедиться в наличии или отсутствии файла РНПК на узле.
- Сотрудникам технического сопровождения ИнфоТеКС — для выяснения причин возникновения проблем с ключевой системой ViPNet Coordinator HW (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: 2024-01-23 13:44:57 MSK
  Master personal key number: 1
  Current personal key update date: 2024-01-25 15:40:24 MSK
Spare personals key set info:                       //Информация о РНПК
  User ID: 0x16310029
  Personals key variants: from 0 to 19
  Master personal key date: 2024-06-23 13:44:57 MSK
  Master personal key number: 1
Lck key info:                                       //Информация о ключах узла
  User ID: 0x16310029
  Master defense key date: 2024-06-23 13:44:57 MSK
Current defense key info:
  AP ID: 0x1631002a
  Current defense key variant: 0
  Master defense key date: 2024-06-23 13:44:57 MSK
  Master defense key number: 1
  Current defense key update date: 2024-05-25 15:40:24 MSK
Cck key info:
  Ap ID: 0x1631002a
  Master cck key date: 2024-06-23 13:44:57 MSK
```

iplir show keys-upgrade-log

Просмотреть журнал, в котором содержится информация о принятых обновлениях справочников и ключей.

Синтаксис

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

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# iplir show keys-upgrade-log
19/01/2024 16:37:34.896  Starting upgrade process ...
19/01/2024 16:37:34.896  try find /opt/vipnet/ccc/ap*.dtm
...
```

iplir show l2overip

Просмотреть состояние или настройки L2OverIP.

Синтаксис

```
iplir show l2overip <опция>
```

Параметры и ключевые слова

`<опция>` — параметр, который может принимать одно из значений:

- `clone-fabric-stats` — просмотр статистики «фабрики клонов», которая выполняет обработку широковещательного и многоадресного трафика. Информация предназначена для тестирования и локализации ошибок.
- `config` — просмотр текущих настроек L2OverIP.
- `mac-address-table` — просмотр таблицы MAC-адресов, используемой L2OverIP.
- `mac-hash-stats` — просмотр статистики хэш-таблицы MAC-адресов, используемой L2OverIP. Информация предназначена для тестирования и локализации ошибок.
- `port-table` — просмотр таблицы портов, используемых L2OverIP.
- `status` — просмотр текущего состояния L2OverIP: `switch` — включена, `none` — выключена.
- `virtual-switch-stats` — просмотр статистики по обработке Ethernet-кадров: общее количество обработанных и заблокированных кадров, а также количество обработанных и заблокированных одноадресных кадров с неизвестным MAC-адресом получателя.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть текущие настройки:

```
hostname> iplir show l2overip config
mode = switch
mac_ttl = 300
device = eth0
local_port = 12, 172.16.12.123
remote_port = 13, 172.16.12.124
unsolicited-frames = drop
```

iplir show performance-mode

Просмотреть текущий режим производительности.

Синтаксис

```
iplir show performance-mode
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- В случае, если при включении режима не выполнена перезагрузка ViPNet Coordinator HW, отображается как текущее, так и планируемое состояние после перезагрузки.
- Команду можно выполнить на следующих платформах:
  - ViPNet Coordinator HW100 N1, N2, N3;
  - ViPNet Coordinator HW1000 Q10;
  - ViPNet Coordinator HW2000 Q4, Q5;
  - ViPNet Coordinator HW5000 Q1, Q2.

Пример использования

```
hostname# iplir show performance-mode
Current performance mode: single connection
After system reboot performance mode will be switched to: multi connection
```

iplir show tcptunnel-info

Просмотреть настройки TCP-туннеля на ViPNet Coordinator HW.

Синтаксис

```
iplir show tcptunnel-info
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> iplir show tcptunnel-info

TCP-tunnel server is running

TCP server port: 80

Max TCP-tunnels: 100

Current TCP-tunnels: 0
```

В результате выполнения команды будет выведена следующая информация:

- включен или выключен TCP-туннель;
- номер порта для входящих TCP-соединений;
- возможное количество TCP-соединений;

Примечание. ViPNet Coordinator HW текущей версии может поддерживать не более 100 соединений через TCP-туннель.

- количество текущих TCP-соединений.

iplir start

Запустить управляющую службу `iplircfg`.

Синтаксис

```
iplir start
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> iplir start
Loading IpLir
```

iplir stop

Завершить работу управляющей службы `iplircfg`.

Синтаксис

```
iplir stop
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

iplir tcptunnel client mode

Изменить режим работы клиента TCP-туннеля.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

iplir tcptunnel client on/off

Включить или выключить работу клиента TCP-туннеля.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Включить работу клиента TCP-туннеля:

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

iplir tcptunnel client port

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Задать порт 5252 для доступа к серверу TCP-туннелей:

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

iplir tcptunnel role

Назначить ViPNet Coordinator HW роль сервера TCP-туннелей или TCP-клиента.

Синтаксис

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

Параметры и ключевые слова

- `server` — ViPNet Coordinator HW назначается роль сервера TCP-туннелей.
- `client` — ViPNet Coordinator HW назначается роль TCP-клиента.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Роль можно назначить только для координаторов которые работают в режиме «С динамической трансляцией адресов».
- Служба `iplircfg` должна быть запущена (iplir start).
- Исполнения HW10 и HW50 не поддерживают роль «Сервер TCP-туннелей».

Пример использования

Назначить ViPNet Coordinator HW роль TCP-клиента:

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

iplir tcptunnel server on/off

Запустить или остановить сервер TCP-туннелей.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Запустить сервер TCP-туннелей:

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

iplir tcptunnel server port

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

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

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

iplir view

Просмотреть журнал регистрации IP-пакетов.

Синтаксис

```
iplir view
```

Режимы командного интерпретатора

Администратор.

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.
- Служба `iplircfg` должна быть запущена (iplir start).
- При работе ViPNet Coordinator HW в режиме кластера горячего резервирования на пассивном узле кластера нельзя просмотреть журнал IP-пакетов.

Пример использования

```
hostname# iplir view
```

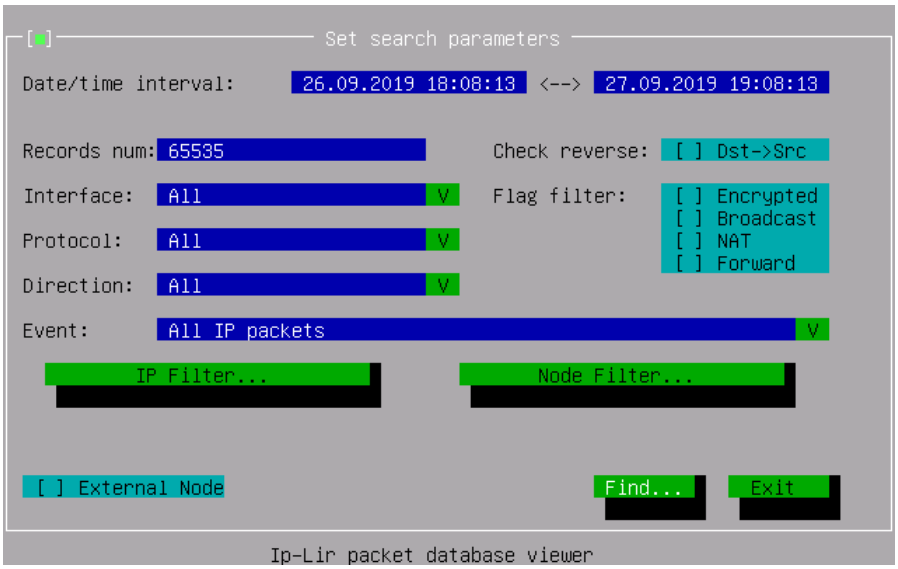

Рисунок 1. Задание параметров поиска записей в журнале регистрации IP-пакетов

Команды группы machine

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

machine halt

Выключить компьютер.

Синтаксис

```
machine halt
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> machine halt
```

machine logs clear dns

Очистить журнал DNS-запросов.

Синтаксис

```
machine logs clear dns
```

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

```
hostname# machine logs clear dns
```

```
This will clear log files.

Are you sure?

Continue? [Yes/No]: Yes

Removing DNS request log... Done
```

machine reboot

Перезагрузить ViPNet Coordinator HW.

Синтаксис

```
machine reboot
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Для аппаратных платформ HW100 N1,N2,N3 с аппаратной ревизией PDB4963-012 выполнение команды не приводит к перезагрузке устройства (номер аппаратной ревизии находится на этикетке на нижней стороне устройства). Чтобы перезагрузить указанные аппаратные платформы отключите разъем питания и подключите его снова. Данное ограничение действует для аппаратных платформ, изготовленных до апреля 2021 года.

Пример использования

```
hostname> machine reboot
```

machine reboot-schedule

Включить или выключить перезагрузку ViPNet Coordinator HW по расписанию.

Синтаксис

```
machine reboot-schedule {on | off}
```

Параметры и ключевые слова

- `on` — включить перезагрузку по расписанию.
- `off` — выключить перезагрузку по расписанию.

Значения по умолчанию

Перезагрузка по расписанию выключена (`off`).

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# machine reboot-schedule on
Automatic reboot is scheduled at 23:00 on saturdays
```

machine reboot-schedule show

Просмотреть настройку перезагрузки ViPNet Coordinator HW по расписанию.

Синтаксис

```
machine reboot-schedule show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> machine reboot-schedule show
Automatic reboot is scheduled at 23:00 on saturdays
```

machine reboot-schedule time

Задать расписание перезагрузки ViPNet Coordinator HW.

Синтаксис

```
machine reboot-schedule time <время> [day <день>]
```

Параметры и ключевые слова

- `<время>` — время перезагрузки. Указывается в формате `hh:mm`, где `hh` — часы (24-часовой формат), `mm` — минуты;
- `<день>` — день недели перезагрузки. Указываются английские полные названия без учета регистра — `Sunday`, `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`.

Значения по умолчанию

Расписание перезагрузки по умолчанию — `02:00 on mondays`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если день недели не указан, выполняется ежедневная перезагрузка ViPNet Coordinator HW в указанное время.
- В кластере выполните команду на обоих узлах. Рекомендуется устанавливать время перезагрузки узлов, различающееся не менее чем на 30 минут.

Пример использования

Чтобы настроить перезагрузку в субботу в 06.00 часов утра:

```
hostname# machine reboot-schedule time 06:00 day Saturday
Automatic reboot is scheduled at 06:00 on saturdays
```

machine self-test

Запустить регламентное тестирование ViPNet Coordinator HW.

Синтаксис

```
machine self-test
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команду нельзя использовать при удаленном администрировании с помощью SSH.
- До начала тестирования работа всех служб будет автоматически завершена, а после успешного окончания тестирования — автоматически восстановлена.
- 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 успешной проверке на экран выводятся имена проверенных файлов и шестнадцатеричные значения их контрольных сумм.

- При обнаружении ошибок компьютер попытается восстановить искаженные файлы из резервных копий.
- Если резервная копия искаженного файла не найдена, ViPNet Coordinator HW загрузится, однако службы, отвечающие за работу в сети ViPNet, не будут запущены. Если у вас есть файл экспорта справочников, ключей и настроек с расширением `*.vbe`, попробуйте восстановить систему, импортировав этот файл. Если восстановить работу ViPNet Coordinator HW не удалось, обратитесь в службу поддержки ИнфоТеКС.
- После успешной проверки в исполнениях ViPNet Coordinator HW с двумя накопителями (все исполнения, кроме HW10 и HW50) автоматически создается резервная копия конфигурационных и исполняемых файлов ПО, а также справочников и ключей.

Пример использования

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

machine set date

Изменить дату и время.

Синтаксис

```
machine set date <дата> <время>
```

Параметры и ключевые слова

- `<дата>` — дата. Указывается в формате `YYYY-MM-DD`, где `YYYY` — год, `MM` — месяц, `DD` — день.
- `<время>` — время. Указывается в формате `hh:mm:ss`, где `hh` — часы, `mm` — минуты, `ss` — секунды.

Режимы командного интерпретатора

Администратор.

Особенности использования

- После ввода даты и времени необходимо подтвердить действие — ввести `Yes` и нажать **Enter**.
- Дата и время на ViPNet Coordinator HW не должны отличаться от даты и времени узлов сети ViPNet более чем на величину `timediff`. Иначе текущие управляющие соединения с ViPNet

Coordinator HW будут разорваны, а новые управляющие соединения невозможно будет установить.

- При работе в режиме кластера горячего резервирования выполнение команды на пассивном узле кластера невозможно. Дата и время на пассивном узле синхронизируются с датой и временем на активном узле кластера. Подробнее см. описание параметра `syncdatetime` секции `[misc]` конфигурационного файла `failover.ini`.

Пример использования

Чтобы установить дату 22 февраля 2024 года и время, равное 12 часам:

```
hostname# machine set date 2024-02-22 12:00:00
warning: changing date-time process requires VPN services to be restarted
warning: incorrect date and time settings may lead to appliance malfunction
Change current time?
Continue? [Yes/No]: Yes
```

machine set hostname

Изменить имя компьютера.

Синтаксис

```
machine set hostname <имя>
```

Параметры и ключевые слова

`<имя>` — имя компьютера.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При инициализации ViPNet Coordinator HW имя компьютера формируется по шаблону `<название>-<идентификатор>`:
  - `название` — наименование аппаратной платформы ViPNet Coordinator HW без последних двух символов;
  - `идентификатор` — идентификатор сетевого узла.

  Например: `HW1000-270E033A`, `HW100-2A15000D`.
- При выполнении команды служба `syslogd` перезапускается.

- Имя компьютера используется, в том числе, в SNMP-параметрах:
  - `sysDescr` (OID .1.3.6.1.2.1.1.1.0);
  - `sysName` (OID .1.3.6.1.2.1.1.5.0) — если параметр `sysName` не задан при настройке SNMP-агента.

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

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

Пример использования

Чтобы установить имя компьютера HW1000:

```
hostname# machine set hostname HW1000
Restarting system log daemon: syslog
```

machine set loghost

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

Синтаксис

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

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сетевого узла, на котором будет храниться системный журнал (удалённое ведение журнала).
- `local` — хранить системный журнал на ViPNet Coordinator HW (локальное ведение журнала).
- `null` — выключить ведение журнала.

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию системный журнал хранится на ViPNet Coordinator HW (`local`).
- Если системный журнал будет храниться на удалённом узле, этот узел должен быть доступен для ViPNet Coordinator HW. Если узел является открытым, то на ViPNet Coordinator HW создайте фильтр открытой сети, разрешающий исходящий трафик по протоколу UDP на 514-й порт этого узла.

- Для настройки удалённого ведения журнала в кластере задайте место хранения журнала как на активном, так и на пассивном узле кластера, так как эти настройки не синхронизируются.
- Не рекомендуется настраивать удалённое ведение журнала в кластере, так как на удалённый узел не будут передаваться события с пассивного узла.

Пример использования

Чтобы отправить системный журнал на узел с адресом 192.168.10.10:

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

machine set session-timeout

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Время неактивности удаленной сессии 30 минут.

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

Чтобы установить допустимое время неактивности удаленной сессии 1 час:

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

machine set timezone

Задать временную зону (часовой пояс).

Синтаксис

```
machine set timezone <временная зона>
```

Параметры и ключевые слова

`<временная зона>` — временная зона, заданная в формате `Континент/Зона`, или значение `UTC` для установки времени UTC.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Название континента и зоны должны начинаться с прописной буквы.
- При вводе континента или зоны работает подсказка.
- Если временная зона не указана, выводится список всех существующих временных зон.
- В кластере команда выполняется только на активном узле. Временная зона на пассивном узле синхронизируются с временной зоной на активном узле кластера. Подробнее см. описание параметра `syncdatetime` секции `[misc]` конфигурационного файла `failover.ini`.

Примеры использования

- Чтобы просмотреть список временных зон в Антарктике:

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

- Чтобы установить часовой пояс Москвы:

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

machine serial

Установить серийный номер ViPNet Coordinator HW.

Синтаксис

```
machine serial <серийный номер>
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Команда доступна на исполнениях ViPNet Coordinator HW на аппаратных платформах, серийный номер которых не был установлен при производстве.
- Длина серийного номера: 8–9 символов.
- Допустимые символы:
  - Арабские цифры: `0–9`.
  - Специальный символ `-`.
- Серийный номер имеет формат XXX-XXXXX(X).

Пример использования

```
hostname# machine serial 431-24758

Appliance serial number successfully set.
```

machine show date

Просмотреть дату и время, установленные на ViPNet Coordinator HW.

Синтаксис

```
machine show date
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> machine show date
Thu Jan 27 19:11:56 MSK +7 2024
```

machine show hostname

Просмотреть имя ViPNet Coordinator HW.

Синтаксис

```
machine show hostname
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

machine show loghost

Просмотреть настройки хранения системного журнала.

Синтаксис

```
machine show loghost
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде выводится одно из следующих значений:

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

Пример использования

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

machine show logs

Просмотреть системный журнал.

Синтаксис

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

Параметры и ключевые слова

- `reversed` — вывод списка записей в обратном хронологическом порядке.
- `<время>` — вывод записей, начиная с указанного момента времени.
- `<служба>` — вывод записей только для указанной службы в составе ПО ViPNet Coordinator HW. Список служб представлен в документе «Настройка с помощью командного интерпретатора».
- `<строка>` — поиск записей журнала по части строки.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Чтобы завершить просмотр, нажмите **Q**.
- Параметр `<время>` задается в формате `YYYY-MM-DD hh:mm:ss`
- В параметре `<служба>` можно указать одну из служб в составе ПО ViPNet Coordinator HW. Полный список служб см. в документе «Настройка с помощью командного интерпретатора», разделе «Список служб в составе ПО ViPNet Coordinator HW».
- Для параметра `<строка>` можно использовать символы `A-Z`, `a-z`, `0-9`, а также следующие символы:

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

  Также можно использовать пробел, в этом случае возьмите часть строки в двойные кавычки ("").
- В одной команде `machine show logs` можно одновременно указать только один из параметров `since` или `filtered`. При указании параметра `filtered` можно указать только один из его вариантов `<служба>` или `string <строка>`.

Пример использования

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

  ```
  hostname# machine show logs
  ```
- Чтобы найти все записи системного журнала, начиная с 14:50 22 февраля 2024 года, и отобразить их в обратном порядке:

  ```
  hostname# machine show logs reversed since 2024-02-22 14:50:00
  ```
- Чтобы найти все записи системного журнала для службы `vmunix`:

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

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

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

machine show memory

Просмотреть информацию об использовании оперативной памяти, файла подкачки и дискового пространства.

Синтаксис

```
machine show memory
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

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

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

  Таблица включает следующие столбцы:

  `Filesystem` — имя раздела файловой системы;

  `Size` — размер раздела файловой системы;

`Used` — объем использованного пространства;

`Avail` — объем доступного пространства;

`Use%` — процент использования раздела файловой системы;

`Mounted on` — точка монтирования раздела файловой системы.

По умолчанию значения доступного и используемого дискового пространства выводятся в Кбайт. Для сокращенного вывода некоторых величин используются модификаторы размера:

- M — Мбайт;
- G — Гбайт.

Например, значение `2.0G` означает 2 Гбайт.

Пример использования

```
hostname> machine show memory
        total     used     free      shared     buff/cached     available
Mem:    2007      420      1485      0          102             362
Swap:   0         0        0

Filesystem      Size    Used   Avail   Use%   Mounted on
tmpfs           1004M   60M    944M    6%     /mnt/root
overlay         2.0G    93M    1.9G    5%     /

...
```

machine show session-timeout

Просмотреть допустимое время неактивности сессии.

Синтаксис

```
machine show session-timeout
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

machine show timezone

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

Синтаксис

```
machine show timezone
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

machine show uptime

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

Синтаксис

```
machine show uptime
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде отображается следующая информация:

- текущее время;
- время работы ViPNet Coordinator HW после загрузки;
- текущее количество пользователей;
- среднее количество процессов в очереди ожидания процессора за последние 1, 5 и 15 минут. Выводимые значения следует интерпретировать в зависимости от количества процессорных ядер исполнения ViPNet Coordinator HW. Для исполнений с многоядерными процессорами (в том числе с двумя процессорами) критическими являются значения, превышающие общее

количество ядер. Например, для исполнений с 4-мя процессорными ядрами значения не должны превышать 4.00 — такие значения говорят о том, что ViPNet Coordinator HW перегружен.

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

Пример использования

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

machine swap mode

Включить или выключить использование файла подкачки.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

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

Пример использования

```
hostname# machine swap mode on
SWAP is enabled and will be enabled after reboot.
```

machine swap set

Задать размер файла подкачки, если такой будет использоваться в процессе работы ViPNet Coordinator HW.

Синтаксис

```
machine swap set <размер>
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- Использование файла подкачки в исполнениях с одним дисковым накопителем (HW10 и HW50) невозможно. В результате выполнения команды в указанных исполнениях появится соответствующее сообщение.
- При задании размера файла подкачки на диске должно остаться не менее 256 Мбайт свободного пространства. Если будет задан размер файла подкачки, превышающий размер доступного пространства на диске, появится соответствующее сообщение.
- Просмотреть сведения об использовании оперативной памяти и файле подкачки можно с помощью команды machine show memory.

Пример использования

```
hostname# machine swap set 2048
Creating swap. Please, wait...Setting up swapspace version 1, size 2097148 KiB
no label, UUID=of389079-f9f5-4abb-ac2e-a26848eca54c
 done.
Activating swap...
 done.
```

Команды группы mftp

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

mftp config

Редактировать конфигурационный файл службы `mftpd`.

Синтаксис

```
mftp config
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед редактированием конфигурационного файла завершите работу службы `mftpd` (mftp stop).
- При выполнении команды запускается текстовый редактор, в который загружается файл `mftp.conf`.
- При сохранении файла происходит проверка его корректности. В случае ошибки предлагается отказаться от изменений или продолжить редактирование. Если проверка прошла успешно, файл применяется для работы службы `mftpd`, а информация об изменении конфигурации сохраняется в системный журнал.

Пример использования

Чтобы включить режим немедленной передачи конвертов по каналу обмена с узлом `0x270e000a`:

```
hostname# mftp config
```

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

```
[channel]
id = 0x270e000a
name = Client-1

type = mftp
off_flag = no
call_flag = yes
...
```

mftp info

Просмотреть очередь исходящих транспортных конвертов MFTP.

Синтаксис

```
mftp info
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- При выполнении команды в одном из исполнений ViPNet Coordinator HW10, HW50 или HW100 на консоль выводится не более 10000 записей о конвертах. При выполнении команды в остальных исполнениях число выводимых записей о конвертах ограничено временем ожидания ответа (30 секунд), но не превышает 400000 записей.
- Для просмотра очереди исходящих конвертов используйте навигационные клавиши.
- Чтобы завершить просмотр, нажмите **Q**.

Пример использования

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

Очередь исходящих конвертов отображается в следующем формате:

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

Receiver ID  Receiver Name
```

где:

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

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

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

mftp show config

Просмотреть конфигурационный файл транспортного сервера MFTP.

Синтаксис

```
mftp show config
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Чтобы завершить просмотр конфигурационного файла, нажмите **Q**.

Пример использования

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

mftp start

Запустить службу `mftpd` (транспортный сервер MFTP).

Синтаксис

```
mftp start
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

mftp stop

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

Синтаксис

```
mftp stop
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

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

mftp view

Вывести журнал конвертов транспортного сервера MFTP.

Синтаксис

```
mftp view
```

Режимы командного интерпретатора

Пользователь.

Администратор.

Особенности использования

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

Пример использования

```
hostname# mftp view
=== MFTP envelopes journal dump at Tue Feb 11 16:45:48 2024
-------------------------------------------------------------------------------
-------------------------------------------------------------
| Envelope filename | Personal envelope name | Sender | Receiver            |Date-Time
 |     Event         |      Size   |      Description   |      Task          |
-------------------------------------------------------------
| ~OJ)(#(A.RJ9      | ~OJ)(#(A.RJ9               | Admin    | xfva | 11.02.2024 16:45:48
 |     Received      |      19090  |                    | File exchange      |
-------------------------------------------------------------------------------
-------------------------------------------------------------
```

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 service

Настройка и управление прокси-сервером.

service cert delete

Удалить сертификат, список аннулированных сертификатов (CRL) или закрытый ключ.

Синтаксис

```
service cert delete {cert | crl | private} <pem>
```

Параметры и ключевые слова

- Тип удаляемого объекта:
  - `cert` — сертификат.
  - `crl` — список аннулированных сертификатов.
  - `private` — закрытый ключ.
- `<pem>` — имя файла сертификата, CRL или закрытого ключа соответственно.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При удалении из хранилища сертификата протокола HTTPS, который используется для доступа к ViPNet Coordinator HW с помощью веб-интерфейса, выводится предупреждение `After the command is executed, the HTTPS certificate will be deleted. WebUI will be switched to HTTP mode. Continue? Yes/No`. После подтверждения сертификат будет удален, протокол доступа к ViPNet Coordinator HW изменен на HTTP и выведено сообщение `Certificate for HTTPS deleted. The WebUI protocol is switched to HTTP.`
- Признак типов в PEM-файле:
  - Сертификат: `-----BEGIN CERTIFICATE-----`
  - CRL: `-----BEGIN X509 CRL-----`
  - Закрытый ключ: `-----BEGIN PRIVATE KEY-----`

Пример использования

- Чтобы удалить сертификат с именем `Cert1.pem`:

```
hostname# service cert delete cert Cert1.pem
```

```
Certificate Cert1.pem is deleted
```

- Чтобы удалить CRL с именем `CRL1.pem`:

```
hostname# service cert delete crl CRL1.pem
CRL CRL1.pem is deleted
```

- Чтобы удалить закрытый ключ с именем файла `Cert1_key.pem`:

```
hostname# service cert delete private Cert1_key.pem
Private key Cert1_key.pem is deleted
```

service cert import

Импортировать в локальное хранилище ViPNet Coordinator HW закрытый ключ сертификата, сертификат или список аннулированных сертификатов (CRL) с USB-носителя.

Синтаксис

```
service cert import
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Поддерживает импорт только сертификатов, подписанных с использованием алгоритма RSA.
- Поддерживает импорт сертификатов в кодировке DER и Base64.
- В контейнере PEM (`.pem`) используется стандарт PKCS#12 (`.p12`).
- По команде выполняется поиск на USB-носителе файлов с расширениями `*.pem`, `*.cer` и `*.crl` и предлагается выбрать нужный сертификат, закрытый ключ сертификата или CRL.
- При импорте файлов с расширением `*.cer` и `*.crl` выполняется их конвертация в формат PEM.
- При импорте проверяется уникальность сертификата по содержимому и по имени:
  - Если имя и содержимое уникальны — сертификат импортируется, имя остается без изменения.
  - Если содержимое уникально, а имя нет — сертификат импортируется, к имени добавляется уникальный индекс (`<filename>_yyyy-mm-dd-hhmmss.<ext>`), об изменении имени файла выводится сообщение.
  - Если содержимое сертификата дублируется — сертификат не импортируется, выводится предупреждение о дублировании.

Пример использования

```
hostname# service cert import

Insert USB flash drive into empty USB slot and press <Enter>

Try to mount /dev/sdc1 as vfat

/dev/sdc1 mounted

1 - /usb/Cert1.cer

2 - /usb/CRL1.crl

Enter file number [1-2] or [q] to cancel: 1

Certificate /usb/Cert1.cer will be converted to PEM

Certificate:

...

/usb/Cert1.cer was imported as certnew.pem
```

service cert list

Просмотреть установленные закрытые ключи, сертификаты и списки аннулированных сертификатов (CRL).

Синтаксис

```
service cert list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service cert list

Certificates:

...

Certificate revocation list:

...

Private keys:

...
```

service cert request create

Создать закрытый ключ и запрос на сертификат в формате PKCS#12.

Синтаксис

```
service cert request create name <имя> bits <длина ключа> digest {sha256 | sha384 | sha512}
[subj <subj>]
```

Параметры и ключевые слова

- `<имя>` — имя сертификата;
- `<длина ключа>` — размер создаваемого RSA-ключа в битах, можно задавать следующие значения: 2048, 3072, 4096;
- `sha256` — алгоритм хэширования SHA-256;
- `sha384` — алгоритм хэширования SHA-384;
- `sha512` — алгоритм хэширования SHA-512;
- `subj` — дополнительные параметры запроса:
  - `/C` — страна;
  - `/ST` — область;
  - `/L` — город;
  - `/O` — организация;
  - `/OU` — отдел организации;
  - `/CN` — доменное имя сайта;
  - `/emailAddress` — электронный адрес;
  - `/subjectAltName` — альтернативные адреса ресурса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды в стандартном режиме необходимо следовать правилам заполнения параметров запроса:
  - Параметры запроса `subj` записываются единой строкой в двойных кавычках.
  - Названия полей параметров запроса отделяются от значений знаком `=`.
  - Пробелы между параметрами запроса не ставятся.
- Дополнительные параметры `subj` можно задавать в интерактивном режиме.

В процессе выполнения команды у вас будут запрошены личные данные, необходимые для создания сертификата. Не все поля обязательны к заполнению. Чтобы отказаться от заполнения тех или иных сведений, нажмите клавишу **Enter**.

- В контейнере PEM (`.pem`) используется стандарт PKCS#12 (`.p12`).
- По команде создается файл запроса на сертификат с именем `<имя сертификата>_req.pem` и файл с закрытым ключом с именем `<имя сертификата>_key.pem`.

Пример использования

Чтобы создать запрос на сертификат с длиной ключа 2048 бита, используя алгоритм шифрования SHA-256:

```
hostname# service cert request create name Cert1 bits 2048 digest sha256

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value

If you enter '.', the field will be left blank.

If you want to create a certificate for the VPN network, fill in the CommonName and
AlternativeNames parameters.

Country Name (2 letter code) [AU]:RU

State or Province Name (full name) [Some-State]:

Locality Name (eg, city) []:Moscow

Organization Name (eg, company) [Internet Widgets Pty Ltd]:Infotecs

Organizational Unit Name (eg, section) []:IT

Common Name (e.g. server FQDN or IP-address or domain name, one value) []:infotecs.biz

Email Address []:post@infotecs.ru

Please enter the following 'extra' attributes

to be sent with your certificate request

An optional company name (e.g. server FQDN or IP-address or domain name, several value)
[]:infotecs.biz

Generating a RSA private key

.....................................................................................
.................. ....+++++

.................................................+++++

writing new private key to '/etc/cert/Cert1_key.pem'

-----
```

```
Creating request Cert1_req.pem is completed
```

Чтобы создать запрос на сертификат с длиной ключа 2048 бита, используя алгоритм шифрования SHA-256 и дополнительные параметры запроса:

```
hostname# service cert request create name Cert1 bits 2048 digest sha256 subj
"/C=RU/ST=Moscow/L=Moscow/O=Infotecs/OU=IT/CN=infotecs.ru/emailAddress=post@infotecs.r
u/subjectAltName=DNS:infotecs.biz,IP:127.50.50.50"

Generating a RSA private key

..............................+++++

........+++++

writing new private key to '/etc/cert/Cert1_key.pem'

-----

Creating request Cert1_req.pem is completed
```

service cert request delete

Удалить запрос на сертификат.

Синтаксис

```
service cert request delete <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат.

Режимы командного интерпретатора

Администратор.

Особенности использования

Признак запроса на сертификат в PEM файле: `-----BEGIN CERTIFICATE REQUEST-----`.

Пример использования

Чтобы удалить запрос на сертификат с именем `Cert1_req.pem`:

```
hostname# service cert request delete Cert1_req.pem

Certificate request Cert1_req.pem is deleted
```

service cert request export

Экспортировать запрос на сертификат на USB-носитель.

Синтаксис

```
service cert request export <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат.

Режимы командного интерпретатора

Администратор.

Особенности использования

Признак запроса на сертификат в PEM файле: `-----BEGIN CERTIFICATE REQUEST-----`.

Пример использования

Чтобы экспортировать запрос на сертификат с именем `Cert1_req.pem`:

```
hostname# service cert request export Cert1_req.pem
Insert USB flash drive into empty USB slot and press <Enter>
Try to mount /dev/sdc1 as vfat
/dev/sdc1 mounted
Cert1_req.pem was exported
```

service cert request list

Просмотреть список созданных запросов на сертификат.

Синтаксис

```
service cert request list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service cert request list

Cert1_req.pem
```

service cert request show

Просмотреть содержимое запроса на сертификат с заданным именем или всех запросов на сертификаты, созданных в ViPNet Coordinator HW.

Синтаксис

```
service cert request show <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат. Если вместо имени указать `all`, будет отображено содержимое всех запросов на сертификаты, созданных в ViPNet Coordinator HW.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть содержимое файла запроса на сертификат с именем `Cert1_req.pem`:

```
hostname> service cert request show Cert1_req.pem

Certificate request:

    Data:

        ..

    Signature algorithm: md5WithRSAEncryption

        ..

...

(END)
```

service cert show cert

Просмотреть содержимое сертификата с заданным именем или всех сертификатов, установленных в локальное хранилище ViPNet Coordinator HW.

Синтаксис

```
service cert show cert <сертификат>
```

Параметры и ключевые слова

`<сертификат>` — имя файла сертификата. Если вместо имени сертификата указать `all`, то будет отображено содержимое всех сертификатов, установленных в локальное хранилище ViPNet Coordinator HW.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть содержимое сертификата с именем `Cert1.pem`:

```
hostname> service cert show cert Cert1.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            8c:93:38:27:1b:36:9c:be
    Signature Algorithm: sha256WithRSAEncryption
...
```

service cert show crl

Просмотреть содержимое списка аннулированных сертификатов (CRL) с заданным именем или всех списков аннулированных сертификатов, установленных в локальное хранилище ViPNet Coordinator HW.

Синтаксис

```
service cert show crl <CRL>
```

Параметры и ключевые слова

`<CRL>` — имя файла списка аннулированных сертификатов CRL. Если вместо имени CRL указать `all`, то будет отображено содержимое всех списков аннулированных сертификатов, установленных в локальное хранилище ViPNet Coordinator HW.

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

Чтобы просмотреть содержимое списка аннулированных сертификатов с именем `CRL.pem`:

```
hostname> service cert show cert CRL.pem
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
...
```

service http-proxy antivirus bypass

Включить или выключить блокировку трафика, проходящего через прокси-сервер при недоступности ICAP-сервера внешнего антивируса.

Синтаксис

```
service http-proxy antivirus bypass {on | off}
```

Параметры и ключевые слова

- `on` — при недоступности ICAP-сервера внешнего антивируса прокси-сервер разрешает проходящий через него трафик.
- `off` — при недоступности ICAP-сервера внешнего антивируса прокси-сервер блокирует проходящий через него трафик.

Значения по умолчанию

`on`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды:
  - выключите антивирусную проверку (см. service http-proxy antivirus mode);
  - остановите прокси-сервер (см. service http-proxy stop).

- Команду нельзя выполнить, пока не задан адрес и метод подключения к ICAP-серверу.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# service http-proxy antivirus bypass on

HTTP proxy antivirus set bypass option: on
```

service http-proxy antivirus mode

Включить или выключить антивирусную проверку трафика, проходящего через прокси-сервер.

Синтаксис

```
service http-proxy antivirus mode {on | off}
```

Параметры и ключевые слова

- `on` — антивирусная проверка трафика включена.
- `off` — антивирусная проверка трафика выключена.

Значения по умолчанию

`off`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- Команду можно выполнить, если заданы параметры ICAP-сервера. После выполнения команды проверяются настроенные URL для ICAP-сервера (URL, порт, метод).

Пример использования

```
hostname# service http-proxy antivirus mode off

HTTP proxy antivirus mode is disabled
```

service http-proxy antivirus server-url add

Задать адрес и метод подключения к ICAP-серверу внешнего антивируса.

Синтаксис

```
service http-proxy antivirus server-url add {reqmod | respmod} <URL>
```

Параметры и ключевые слова

- `reqmod` — проверяется исходящий трафик (запросы от пользователей сети к прокси-серверу);
- `respmod` — проверяется входящий трафик (ответы прокси-сервера на запросы пользователей);
- `<URL>` — адрес ICAP-сервера антивируса в формате `icap://адрес[:порт]/<путь>`.

Значения по умолчанию

Если в адресе ICAP-сервера не указан порт, будет использоваться порт по умолчанию 1344.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# service http-proxy antivirus server-url add respmod icap://192.168.1.45/respmod
HTTP proxy antivirus add respmod service success
```

service http-proxy antivirus server-url delete

Удалить параметры подключения к ICAP-серверу внешнего антивируса.

Синтаксис

```
service http-proxy antivirus server-url delete {reqmod | respmod}
```

Параметры и ключевые слова

- `reqmod` — будет удален адрес доступа к ICAP-серверу для проверки исходящего трафика (запросы от пользователей сети к прокси-серверу);

- `respmod` — будет удален адрес доступа к ICAP-серверу для проверки входящего трафика (ответы прокси-сервера на запросы пользователей).

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды:
  - выключите антивирусную проверку (см. service http-proxy antivirus mode);
  - остановите прокси-сервер (см. service http-proxy stop).
- Команду нельзя выполнить, пока не задан адрес и метод подключения к ICAP-серверу.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# service http-proxy antivirus server-url delete respmod
HTTP proxy antivirus delete respmod service success
```

service http-proxy antivirus server-url list

Просмотреть текущие настройки доступа к ICAP-серверу антивируса.

Синтаксис

```
service http-proxy antivirus server-url list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service http-proxy antivirus server-url list
HTTP proxy antivirus server-url address: icap://192.168.1.45:1344/reqmod, method reqmod
HTTP proxy antivirus server-url address: icap://192.168.1.45:1344/respmod, method respmod
```

service http-proxy antivirus show-status

Просмотреть текущие настройки и состояние антивирусной защиты.

Синтаксис

```
service http-proxy antivirus show-status
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

В кластере команда доступна для выполнения на обоих узлах.

Пример использования

```
hostname> service http-proxy antivirus show-status
Probing connection with I-CAP server, please be patient...
HTTP proxy antivirus mode is disabled
HTTP proxy antivirus bypass is on
HTTP proxy antivirus reqmod server-url: icap://192.168.1.45:1344/reqmod is offline
HTTP proxy antivirus respmod server-url: icap://192.168.1.45:1344/respmod is offline
```

service http-proxy cache

Задать размер кеша прокси-сервера.

Синтаксис

```
service http-proxy cache <размер>
```

Параметры и ключевые слова

`<размер>` — размер кеша в мегабайтах.

Значения по умолчанию

- для однодисковых платформ — 100 Мбайт;
- для остальных платформ — 256 Мбайт.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Кеш используется для хранения копии данных, к которым часто обращаются пользователи.
- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- Для однодисковых платформ размер кеша не может превышать 100 Мбайт.
- Невозможно задать размер кеша, превышающий 80% от объема свободного места на диске.

Пример использования

Чтобы задать размер кеша 512 мегабайт:

```
hostname# service http-proxy cache 512
```

service http-proxy content-filter add

Добавить правило фильтрации содержимого трафика, передаваемого через прокси-сервер.

Синтаксис

```
service http-proxy content-filter add [num <номер>] [rule <имя>] src <адрес отправителя>
dst <адрес получателя> {command <HTTP-метод> | mime-type <тип содержимого>} <действие>
```

Параметры и ключевые слова

- `<номер>` — порядковый номер правила в таблице, определяющий его приоритет.
- `<имя>` — имя правила.
- `<адрес отправителя>` — адрес отправителя IP-пакетов.
- `<адрес получателя>` — адрес получателя IP-пакетов.
- `<HTTP-метод>` — метод протокола HTTP. Параметр чувствителен к регистру (необходимо вводить значение в верхнем регистре, например, `GET`).
- `<тип содержимого>` — MIME-тип содержимого трафика. Поддерживаемые MIME-типы представлены в документе «Настройка с помощью командного интерпретатора».
- `<действие>` — действие с HTTP-трафиком, соответствующим условиям правила фильтрации содержимого трафика. Действие задается одной из следующих лексем:
  - `pass` — пропускать HTTP-трафик;
  - `drop` — блокировать HTTP-трафик.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).
- В качестве адреса отправителя задавайте адрес клиента прокси-сервера, в качестве получателя — адрес удаленного HTTP-сервера.
- Если номер не указан, правило добавляется в конец соответствующей таблицы и будет применяться при анализе IP-трафика в последнюю очередь.
- Если указанный номер правила меньше последнего номера в таблице, нумерация правил, следующих после нового правила, будет автоматически изменена (их номера будут увеличены на 1). Например: последний номер правила в таблице — 5, вы добавили правило с номером 3. Правило добавится с указанным номером, при этом правило с номером 3, которое было создано ранее добавленного вами, получит номер 4. Правила с номерами 4 и 5, соответственно, получат номер 5 и 6.
- Если указанный номер правила больше последнего номера в таблице, то правило будет добавлено с номером на 1 больше последнего номера в таблице. Например: последний номер правила в таблице — 5, вы добавили правило с номером 8. В этом случае правило добавится с номером 6.
- Если имя правила не задано, будет создано правило без имени.
- В качестве адреса отправителя можно задать IP-адрес узла, маску адресов подсети, системную группу объектов `any`.
- В качестве адреса получателя можно IP-адрес или доменное имя узла, системную группу объектов `any`.

  Контентный фильтр прокси-сервера работает на прикладном уровне модели OSI. Поэтому при использовании в качестве адреса назначения доменного имени узла фильтрация будет осуществляться только по доменному имени, а при использовании IP-адреса узла — только по IP-адресу (без взаимного разрешения доменное имя — IP-адрес).
- Можно задать только один из параметров: `<HTTP-метод>` или `<тип содержимого>`. При указании HTTP-метода нельзя указать тип содержимого, и наоборот.
- При неверном указании значения параметра `<тип содержимого>` выводится полный список поддерживаемых значений.
- Для блокировки сайта задайте HTTP-метод GET.

Пример использования

- Чтобы заблокировать просмотр видео на сайте youtube.com для сети 192.168.1.1/24:

```
hostname# service http-proxy content-filter add rule deny_youtube src 192.168.1.1/24
dst youtube.com mime-type video/mp4 drop
```

- Чтобы заблокировать использование поисковой формы на сайте yandex.ru для всех пользователей:

  ```
  hostname# service http-proxy content-filter add rule deny_post_yandex src @any dst yandex.ru command POST drop
  ```

- Чтобы полностью заблокировать доступ к сайту yandex.ru:

  ```
  hostname# service http-proxy content-filter add rule deny_yandex src @any dst yandex.ru command GET drop
  ```

service http-proxy content-filter change num

Редактировать правило фильтрации трафика, передаваемого через прокси-сервер.

Синтаксис

```
service http-proxy content-filter change num <номер правила> [rule <имя правила>] src <адрес отправителя> dst <адрес получателя> {command <HTTP-метод> | mime-type <тип содержимого>} <действие>
```

Параметры и ключевые слова

- `<номер правила>` — номер редактируемого правила фильтрации трафика в таблице;
- `<имя правила>` — имя редактируемого правила фильтрации трафика;
- `<адрес отправителя>` — адрес отправителя IP-пакетов;
- `<адрес отправителя>` — адрес получателя IP-пакетов;
- `<HTTP-метод>` — метод протокола HTTP;
- `<тип содержимого>` — MIME-тип содержимого трафика. Поддерживаемые MIME-типы представлены в документе «Настройка с помощью командного интерпретатора»;
- `<действие>` — действие с HTTP-трафиком, соответствующим условиям правила фильтрации содержимого трафика. Действие задается одной из следующих лексем:
  - `pass` — пропускать HTTP-трафик;
  - `drop` — блокировать HTTP-трафик.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).
- В качестве адреса отправителя задайте адрес клиента прокси-сервера, в качестве получателя — адрес удаленного HTTP-сервера.

- Если номер не указан, правило добавляется в конец соответствующей таблицы и будет применяться при анализе IP-трафика в последнюю очередь.
- Если указанный номер правила меньше последнего номера в таблице, нумерация правил, следующих после нового правила, будет автоматически изменена (их номера будут увеличены на 1). Например: последний номер правила в таблице — 5, вы добавили правило с номером 3. Правило добавится с указанным номером, при этом правило с номером 3, которое было создано ранее добавленного вами, получит номер 4. Правила с номерами 4 и 5, соответственно, получат номер 5 и 6.
- Если указанный номер правила больше последнего номера в таблице, то правило будет добавлено с номером на 1 больше последнего номера в таблице. Например: последний номер правила в таблице — 5, вы добавили правило с номером 8. В этом случае правило добавится с номером 6.
- Если имя правила не задано, будет создано правило без имени.
- В качестве адреса отправителя можно задать IP-адрес узла, маску адресов подсети, системную группу объектов `any`.
- В качестве адреса получателя можно задать IP-адрес или доменное имя узла, системную группу объектов `any`.

  Контентный фильтр прокси-сервера работает на прикладном уровне модели OSI. Поэтому при использовании в качестве адреса назначения доменного имени узла фильтрация будет осуществляться только по доменному имени, а при использовании IP-адреса узла, только по IP-адресу, без взаимного разрешения доменное имя — IP-адрес.
- Можно задать только один из параметров: `<HTTP-метод>` или `<тип содержимого>`. При указании HTTP-метода нельзя указать тип содержимого, и наоборот.
- При неверном указании значения параметра `<тип содержимого>` выводится полный список поддерживаемых значений.
- Для блокировки сайта задайте HTTP-метод GET.

Пример использования

Предположим, в таблице существует правило без имени с номером 15, которое полностью блокирует доступ к сайту yandex.ru для всех пользователей сети. Вы можете изменить имя блокируемого ресурса, например на google.com, выполнив команду:

```
hostname# service http-proxy content-filter change num 15 src @any dst google.com command GET drop
```

service http-proxy content-filter default-reply-action

Задать действие по умолчанию для ответов от HTTP-ресурсов, которые не подошли под условия других правил контент-фильтрации.

Синтаксис

```
service http-proxy content-filter default-reply-action <действие>
```

Параметры и ключевые слова

`<действие>` — действие с ответами от HTTP-ресурсов:

- `pass` — пропускать;
- `drop` — блокировать.

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию ответы от HTTP-ресурсов пропускаются.
- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).

Пример использования

```
hostname# service http-proxy content-filter default-reply-action drop
Set default-reply-action to drop
```

service http-proxy content-filter default-request-action

Задать действие по умолчанию для запросов к HTTP-ресурсам, которые не подошли под условия других правил контент-фильтрации.

Синтаксис

```
service http-proxy content-filter default-request-action <действие>
```

Параметры и ключевые слова

`<действие>` — действие с запросами к HTTP-ресурсам:

- `pass` — пропускать;
- `drop` — блокировать.

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию запросы к HTTP-ресурсам пропускаются.
- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).

Пример использования

```
hostname# service http-proxy content-filter default-request-action drop
Set default-request-action to drop
```

service http-proxy content-filter delete

Удалить правило контент-фильтрации.

Синтаксис

```
service http-proxy content-filter delete {num <номер> | rule <имя>}
```

Параметры и ключевые слова

- `<номер>` — порядковый номер правила в таблице.
- `<имя>` — имя правила.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).

Пример использования

- Чтобы удалить правило с именем `deny_youtube`:

  ```
  hostname# service http-proxy content-filter delete rule deny_youtube
  ```

- Чтобы удалить правило с порядковым номером 5:

  ```
  hostname# service http-proxy content-filter delete num 5
  ```

service http-proxy content-filter list

Просмотреть список правил контент-фильтрации.

Синтаксис

```
service http-proxy content-filter list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service http-proxy content-filter list

Content filter rules

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

       num           1

       act           drop

       name          rule1

       src           @any

       dst           @any

       mime-type     image/jpeg


       num           2

       act           drop

       name          rule2

       src           @any

       dst           @any

       mime-type     image/png
```

service http-proxy content-filter mode

Включить или выключить контент-фильтрацию HTTP-трафика.

Синтаксис

```
service http-proxy content-filter mode {on | off}
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию контент-фильтрация включена.
- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).
- Контент-фильтрация трафика работает при запущенном прокси-сервере (см. service http-proxy start).

Пример использования

Чтобы включить контент-фильтрацию трафика:

```
hostname# service http-proxy content-filter mode on
```

service http-proxy content-filter move

Изменить порядковый номер правила контент-фильтрации.

Синтаксис

```
service http-proxy content-filter move {num <номер> | rule <имя>} to <новый номер>
```

Параметры и ключевые слова

- `<номер>` — порядковый номер правила в таблице.
- `<имя>` — имя правила.
- `<новый номер>` — новый порядковый номер правила.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).

Пример использования

- Чтобы назначить новый порядковый номер правилу с именем `deny_youtube`:

  ```
  hostname# service http-proxy content-filter move rule deny_youtube to 7
  ```

- Чтобы назначить новый порядковый номер правилу с порядковым номером 5:

```
hostname# service http-proxy content-filter move num 5 to 7
```

service http-proxy content-filter show-status

Просмотреть информацию о статусе контент-фильтрации трафика.

Синтаксис

```
service http-proxy content-filter show-status
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service http-proxy content-filter show-status
HTTP-proxy content-filter is enabled with 4 rules
HTTP-proxy content-filter default-request-action is pass
HTTP-proxy content-filter default-reply-action is pass
HTTP-proxy service is stopped
```

service http-proxy external-address set

Задать внешний IP-адрес прокси-сервера.

Синтаксис

```
service http-proxy external-address set <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса, подключенного к интернету.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).

- При вводе интерфейса работает подсказка. Данные для нее берутся из списка интерфейсов в системе (включая виртуальные интерфейсы, созданные при назначении дополнительных IP-адресов основным интерфейсам).
- На указанном интерфейсе должен быть задан IP-адрес.

Пример использования

Чтобы задать IP-адрес интерфейса `eth1` в качестве внешнего адреса прокси-сервера:

```
hostname# service http-proxy external-address set eth1
```

service http-proxy external-address show

Просмотреть внешний IP-адрес прокси-сервера.

Синтаксис

```
service http-proxy external-address show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service http-proxy external-address show
External address: 10.0.14.110 (eth0)
```

service http-proxy fw-rules apply

Сгенерировать сетевые фильтры и правила трансляции адресов, соответствующие текущим настройкам прокси-сервера.

Синтаксис

```
service http-proxy fw-rules apply
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- Невозможно создать сетевые фильтры и правила трансляции, если заданы не все параметры прокси-сервера.
- Автоматически созданные фильтры и правила трансляции добавляются в конец соответствующих таблиц и имеют зарезервированное название HTTP-Proxy auto.
- Редактировать созданные сетевые фильтры и правила трансляции не рекомендуется.
- Предыдущие сетевые фильтры и правила трансляции, соответствующие измененным настройкам прокси-сервера, будут удалены.

Пример использования

Чтобы после настройки прокси-сервера создать необходимые сетевые фильтры и правила трансляции:

```
hostname# service http-proxy fw-rules apply
```

service http-proxy fw-rules delete

Удалить сетевые фильтры и правила трансляции адресов, необходимые для работы прокси-сервера.

Синтаксис

```
service http-proxy fw-rules delete
```

Режимы командного интерпретатора

Администратор.

Особенности использования

По команде из соответствующих таблиц будут удалены сетевые фильтры и правила трансляции с названием HTTP-Proxy auto, автоматически созданные с помощью команды service http-proxy fw-rules apply.

Пример использования

Чтобы удалить имеющиеся сетевые фильтры и правила трансляции, автоматически созданные для работы прокси-сервера:

```
hostname# service http-proxy fw-rules delete
```

service http-proxy fw-rules show

Просмотреть существующие сетевые фильтры и правила трансляции адресов, необходимые для работы прокси-сервера.

Синтаксис

```
service http-proxy fw-rules show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service http-proxy fw-rules show
Local:
=============================================================================
Num   Name                                          Option        Schedule
Act   Protocol                  Source               > Destination
=============================================================================
11    HTTP-Proxy auto                                 User
pass  tcp:                      @HttpProxyUsers      > 169.254.241.1
       to 1024
-----------------------------------------------------------------------------
12    HTTP-Proxy auto                                 User
pass  tcp:                      192.168.1.1         > @InternetIP
       to 80,
      tcp:
       to 21,
      tcp:
       to 443
-----------------------------------------------------------------------------
...
```

service http-proxy listen-address add

Добавить интерфейс и порт, через которые будут приниматься запросы от клиентов прокси-сервера.

Синтаксис

```
service http-proxy listen-address add <интерфейс> <порт>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<порт>` — номер порта.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- При вводе интерфейса работает подсказка, данные для подсказки берутся из списка интерфейсов в системе (включая виртуальные интерфейсы, созданные при назначении дополнительных IP-адресов основным интерфейсам).
- На указанном интерфейсе должен быть задан IP-адрес.
- Разрешено задавать номер порта, который не используется другими службами.

Пример использования

Чтобы указать интерфейс `eth1` и номер порта 6789 для приема запросов от клиентов прокси-сервера:

```
hostname# service http-proxy listen-address add eth1 6789
```

service http-proxy listen-address delete

Удалить интерфейс из списка слушающих интерфейсов прокси-сервера.

Синтаксис

```
service http-proxy listen-address delete <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).

- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из текущего списка прослушивания.

Пример использования

Чтобы удалить интерфейс `eth1` из списка интерфейсов, по которым принимаются запросы от клиентов прокси-сервера:

```
hostname# service http-proxy listen-address delete eth1
```

service http-proxy listen-address list

Просмотреть текущий список адресов интерфейсов и портов, через которые принимаются запросы от клиентов прокси-сервера.

Синтаксис

```
service http-proxy listen-address list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service http-proxy listen-address list
Listen:
10.0.14.110:6789 (eth0)
```

service http-proxy mode

Включить или выключить автоматический запуск прокси-сервера при загрузке ViPNet Coordinator HW.

Синтаксис

```
service http-proxy mode {on | off}
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию автоматический запуск прокси-сервера выключен.
- По команде изменяется только настройка автоматического запуска прокси-сервера, его текущее состояние не изменяется.
- Невозможно включить автоматический запуск, если заданы не все параметры, необходимые для работы прокси-сервера.

Пример использования

Чтобы выключить автоматический запуск прокси-сервера:

```
hostname# service http-proxy mode off
```

service http-proxy reset

Сбросить текущие настройки прокси-сервера.

Синтаксис

```
service http-proxy reset
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды запрашивается подтверждение очистки всех настроек прокси-сервера.
- При выполнении команды не удаляются сетевые фильтры и правила трансляции адресов, если такие создавались в соответствии с текущими настройками прокси-сервера с помощью команды service http-proxy fw-rules apply. После очистки настроек прокси-сервера данные фильтры и правила трансляции можно удалить вручную с помощью команды service http-proxy fw-rules delete.

Пример использования

Чтобы очистить настройки прокси-сервера:

```
hostname# service http-proxy reset
```

service http-proxy show

Просмотреть состояние и настройки прокси-сервера.

Синтаксис

```
service http-proxy show
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> service http-proxy show
HTTP Proxy autostart is on
Service is running
Transparent: on
Cache size: 256
Listen:
169.254.241.1:6789 (eth1)
External address: 10.0.14.110 (eth0)
```

service http-proxy start

Запустить прокси-сервер.

Синтаксис

```
service http-proxy start
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Невозможно запустить прокси-сервер, если заданы не все параметры, необходимые для его работы.

Пример использования

```
hostname# service http-proxy start
HTTP Proxy started
```

service http-proxy stop

Завершить работу прокси-сервера.

Синтаксис

```
service http-proxy stop
```

Режимы командного интерпретатора

Администратор.

Пример использования

```
hostname# service http-proxy stop
...
HTTP Proxy stopped
```

service http-proxy transparent-mode

Включить или выключить «прозрачный» режим работы прокси-сервера.

Синтаксис

```
service http-proxy transparent-mode {on | off}
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Особенности использования

- По умолчанию «прозрачный» режим выключен.
- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- Невозможно включить «прозрачный» режим, если заданы не все параметры, необходимые для работы прокси-сервера.
- При работе прокси-сервера в «прозрачном» режиме настройка на рабочих местах пользователей не требуется.

Пример использования

Чтобы включить «прозрачный» режим работы прокси-сервера:

```
hostname# service http-proxy transparent-mode on
```

Команды группы ups

Настройка взаимодействия ViPNet Coordinator HW с источником бесперебойного питания (ИБП).

Примечание. Для исполнений ViPNet Coordinator VA и HW10 команды выполняться не будут, так как эти исполнения не поддерживают работу с ИБП.

ups set driver

Выбрать драйвер `UPS`.

Синтаксис

```
ups set driver <драйвер>
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы выбрать драйвер `UPS`:

```
hostname# ups set driver usbhid-ups
```

ups set mode

Настроить режим взаимодействия ViPNet Coordinator HW с ИБП.

Синтаксис

```
ups set mode {master | slave <IP-адрес мастера>}
```

Параметры и ключевые слова

- `master` — взаимодействие в режиме главного компьютера. Главным является компьютер, к которому подключен интерфейсный кабель ИБП и который непосредственно взаимодействует с ИБП.
- `slave` — взаимодействие в режиме подчиненного компьютера. Подчиненный компьютер взаимодействует с ИБП через главный компьютер.
- `<IP-адрес мастера>` — IP-адрес главного компьютера, находящегося в режиме `master`.

Режимы командного интерпретатора

Администратор.

Особенности использования

Перед выполнением команды требуется вручную завершить работу служб пакета NUT (Network UPS Tools) с помощью команды ups stop.

Пример использования

```
hostname# ups set mode master
```

ups set monitoring

Включить или выключить мониторинг состояния ИБП.

Синтаксис

```
ups set monitoring {on | off}
```

Параметры и ключевые слова

- `on` — включить мониторинг;
- `off` — выключить мониторинг.

Значения по умолчанию

Мониторинг состояния ИБП выключен (`off`).

Режимы командного интерпретатора

Администратор.

Особенности использования

- После включения мониторинга запустите службы пакета NUT с помощью команды ups start.
- При выключении мониторинга будет автоматически завершена работа служб пакета NUT.

Пример использования

```
hostname# ups set monitoring on
```

ups show config

Просмотреть текущие настройки взаимодействия ViPNet Coordinator HW с ИБП.

Синтаксис

```
ups show config
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Команда выводит следующую информацию:

- Включен или выключен мониторинг состояния ИБП. Остальная информация выводится только в случае, если мониторинг включен.
- Режим взаимодействия ViPNet Coordinator HW с ИБП (`master` или `slave`).
- Используемый драйвер `UPS` (только в режиме `master`).
- IP-адрес мастера (только в режиме `slave`).
- Состояние служб пакета `NUT` (запущены или работа служб завершена).

Пример использования

```
hostname> ups show config
UPS service mode is Master. Driver: usbhid-ups
UPS service is RUNNING
```

ups show status

Просмотреть информацию о состоянии ИБП.

Синтаксис

```
ups show status [extended]
```

Параметры и ключевые слова

`extended` — просмотр всех параметров состояния ИБП в формате утилиты `upsc`, входящей в состав пакета `NUT`. Эта возможность предназначена для квалифицированных системных администраторов, которые могут самостоятельно интерпретировать результат вывода утилиты `upsc`.

Особенности использования

Команда выводит следующую информацию:

- производитель ИБП;
- модель ИБП;
- текущая нагрузка по мощности (в процентах от максимальной нагрузки);
- текущий режим питания (`OL` — питание от сети, `OB` — питание от батареи);
- текущий уровень заряда батареи (в процентах от максимального уровня);
- расчетное время работы от батареи при текущих нагрузке и уровне заряда (в секундах);
- максимальное время работы от батареи, по истечении которого ИБП посылает сигнал о необходимости выключения компьютера (задается производителем ИБП).

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> ups show status
Manufacturer:   American Power Conversion
Model:          Smart-UPS 750 RM
Load:           24.0%
Power status:   OL
Battery charge: 100%
Runtime:        2520
Runtime to low: 1380
```

ups start

Запустить службы пакета `NUT`, обеспечивающие взаимодействие ViPNet Coordinator HW с ИБП.

Синтаксис

```
ups start
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> ups start
```

ups stop

Завершить работу служб пакета `NUT`, обеспечивающих взаимодействие ViPNet Coordinator HW с ИБП.

Синтаксис

```
ups stop
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> ups stop
```

Команды группы vpn

Загрузка и выгрузка драйверов и служб ViPNet.

vpn start

Загрузить все драйверы и запустить все службы ViPNet Coordinator HW.

Синтаксис

```
vpn start
```

Режимы командного интерпретатора

Администратор.

Особенности использования

Команда выполняется только в том случае, если перед этим была выполнена команда `vpn stop` или если службы и драйверы не были запущены при загрузке ViPNet Coordinator HW (например, если вы не выбрали запуск служб VPN после разворачивания дистрибутива ключей). Если некоторые службы 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 служб. Например, после выполнения команд `iplir stop` и `mftp stop` для запуска служб `iplircfg` и `mftpd` выполните команды `iplir start` и `mftp start`.

Пример использования

```
hostname# vpn start
```

vpn stop

Выгрузить драйверы и завершить работу служб ViPNet Coordinator HW.

Синтаксис

```
vpn stop
```

Режимы командного интерпретатора

Администратор.

Пример использования

Чтобы выгрузить драйверы и завершить работу служб ViPNet Coordinator HW:

```
hostname# vpn stop
Shutting down failover daemon
Shutting down ViPNet Web GUI service
Shutting down MFTP daemon
Shutting down IpLir
Flushing firewall tables.
Unloading VPN modules
```

Команды группы webui

Управление службой `WebUI` ViPNet Coordinator HW, на основе которой функционирует веб-интерфейс.

webui https-cert

Установить сертификат для доступа к ViPNet Coordinator HW по протоколу HTTPS.

Синтаксис

```
webui https-cert <сертификат>
```

Параметры и ключевые слова

`<сертификат>` — имя файла сертификата в формате `*.cer`.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если в хранилище отсутствует устанавливаемый сертификат — отображается список доступных для выбора сертификатов.
- Если в момент установки сертификата для доступа к ViPNet Coordinator HW с помощью веб-интерфейса используется протокол HTTPS, то после установки нового сертификата перезапустите службу `WebUI` (webui restart).

Пример использования

```
hostname# webui https-cert webuihttps.cer
Certificate has been set successfully
```

webui info

Просмотреть состояние службы `WebUI`.

Синтаксис

```
webui info
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

По команде выводятся:

- Статус службы — запущена или остановлена.
- Протокол для доступа к ViPNet Coordinator HW с помощью веб-интерфейса.
- Имя файла сертификата протокола HTTPS, если установлен.
- Номер TCP-порта.

Пример использования

```
hostname> webui info
WebUI server is running
Protocol HTTPS
HTTPS cert webuihttps.cer
Port 8080
```

webui port

Задать TCP-порт для доступа к ViPNet Coordinator HW с помощью веб-интерфейса.

Синтаксис

```
webui port <порт>
```

Параметры и ключевые слова

`<порт>` — номер TCP-порта.

Значения по умолчанию

Используется TCP-порт 8080.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Если TCP-порт используется другой службой ViPNet Coordinator HW — выводится сообщение `Port in use. Release port or select another.`

- После установки номера TCP-порта:
  - Измените в правиле межсетевого экрана Allow ViPNet WebGui номер TCP-порта: `@any @local tcp: to <порт> pass`.
  - Перезапустите службу WebUI (webui restart).

Пример использования

```
hostname# webui port 443

Web Access port has been set successfully.

For Web Access to function correctly, change port in the Allow WebGUI rule and restart the
Web Access service
```

webui protocol

Выбрать протокол, используемый для доступа к ViPNet Coordinator HW с помощью веб-интерфейса.

Синтаксис

```
webui protocol {http | https}
```

Параметры и ключевые слова

- `http` — протокол HTTP.
- `https` — протокол HTTPS.

Значения по умолчанию

Используется протокол HTTPS.

Режимы командного интерпретатора

Администратор.

Особенности использования

- До переключения протокола с HTTP на HTTPS установите сертификат (см. webui https-cert).
- При переключении протокола перезапускается служба `WebUI`.

Пример использования

```
hostname# webui protocol https

Protocol HTTPS has been set successfully
HTTPS cert webuihttps.cer
```

webui recreate-cert

Перевыпустить самоподписанный сертификат, используемый для подключения к веб-интерфейсу по протоколу HTTPS.

Синтаксис

```
webui recreate-cert [bits <длина ключа> digest {sha256 | sha384 | sha512} span <срок действия> [subj <subj>]]
```

Параметры и ключевые слова

- `<длина ключа>` — размер создаваемого RSA-ключа в битах, можно задавать следующие значения: 2048, 3072, 4096;
- `sha256` — алгоритм хэширования SHA-256;
- `sha384` — алгоритм хэширования SHA-384;
- `sha512` — алгоритм хэширования SHA-512;
- `<срок действия>` — срок действия самоподписанного сертификата в днях. Возможные значения: `30–1825;`
- `subj` — дополнительные параметры:
  - `/C` — код страны;
  - `/ST` — область (до 64-х символов);
  - `/L` — город (до 64-х символов;
  - `/O` — организация (до 64-х символов);
  - `/OU` — отдел организации (до 64-х символов);
  - `/CN` — доменное имя;
  - `/emailAddress` — электронный адрес;
  - `/subjectAltName` — альтернативные адреса ресурса.

Значения по умолчанию

- Без указания параметров и ключевых слов используются значения, как при инициализации ViPNet Coordinator HW:
  - длина ключа — 2048;
  - алгоритм хэширования — sha256;
  - срок действия — 1825 дней;
  - имя субъекта — имя узла.

- Без указания дополнительных параметров (`subj`) в качестве доменного имени и альтернативного адреса ресурса указывается имя узла (`hostname`), а остальные дополнительные параметры сертификата отсутствуют.

Режимы командного интерпретатора

Администратор.

Особенности использования

- Перевыпущенный сертификат назначается действующим для подключения к веб-интерфейсу ViPNet Coordinator HW по протоколу HTTPS.
- Если служба `WebUI` работала по протоколу HTTPS, то она автоматически перезапустится для применения изменений.
- Если служба `WebUI` работала по протоколу HTTP, установите для нее протокол HTTPS (`webui protocol https` (см. webui protocol)).

Пример использования

```
hostname# webui recreate-cert bits 2048 digest sha512 span 365 subj
"/subjectAltName=DNS:infotecs.biz,IP:127.50.50.50"
Web access certificate would be recreated and set.
Continue? [Yes/No]: y
Certificate recreated and set.
```

webui restart

Перезапустить службу `WebUI`.

Синтаксис

```
webui restart
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> webui restart
Shutting down ViPNet Web GUI service
Loading ViPNet Web GUI service
spawn-fcgi: child spawned successfully: PID: 22996
```

Прочие команды

К прочим относятся команды, которые не входят ни в одну из групп команд, описанных выше.

debug off

Выключить вывод сообщений о событиях.

Синтаксис

```
debug off [<источник> <уровень важности>]
```

Параметры и ключевые слова

- `<источник>` — процесс, для которого требуется выключить вывод сообщений. Например:
  - `kern` — ядро;
  - `user` — пользовательские программы;
  - `mail` — почтовая система;
  - `daemon` — службы.
- `<уровень важности>` — уровень важности сообщений. Например:
  - `err` — сообщения об ошибках;
  - `info` — информационные сообщения;
  - `debug` — отладочные сообщения.

Режимы командного интерпретатора

Администратор.

Особенности использования

Если в команде не указаны параметры, то будет выключен вывод всех сообщений.

Пример использования

Чтобы выключить вывод сообщений об ошибках служб:

```
hostname# debug off daemon err
```

debug on

Включить вывод сообщений о событиях.

Синтаксис

```
debug on [<источник> <уровень важности>]
```

Параметры и ключевые слова

- `<источник>` — процесс, для которого должны выводиться сообщения. Например:
  - `kern` — ядро;
  - `user` — пользовательские программы;
  - `mail` — почтовая система;
  - `daemon` — службы.
- `<уровень важности>` — уровень важности выводимых сообщений. Например:
  - `err` — события содержащие ошибки;
  - `info` — информационные сообщения;
  - `debug` — отладочные сообщения.

Значения по умолчанию

- `<источник>` — `daemon`.
- `<уровень важности>` — `debug`.

Режимы командного интерпретатора

Администратор.

Особенности использования

Для служб сообщения будут выводиться только в случае, если в их файлах конфигураций в секции `[debug]` задано протоколирование для указанных источника и важности сообщений.

Пример использования

Чтобы включить вывод сообщений об ошибках служб:

```
hostname# debug on daemon err
```

enable

Перейти в режим администратора.

Синтаксис

```
enable
```

Режимы командного интерпретатора

Пользователь.

Особенности использования

- После выполнения команды требуется указать пароль администратора сетевого узла ViPNet или пароль администратора группы сетевых узлов ViPNet.
- При вводе пароля на экране ничего не отображается, введенные символы отредактировать нельзя.
- Если пароль администратора введен верно, то выполняется переход в режим администратора, в системном журнале создается запись об успешном переходе в режим администратора.

Пример использования

```
hostname> enable
Type the administrator password:
```

exit

Выйти из текущего режима командного интерпретатора.

Синтаксис

```
exit
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

- В результате выполнения команды в режиме администратора происходит переход в режим пользователя.

- В результате выполнения команды в режиме пользователя происходит завершение работы командного интерпретатора. При этом отображается приглашение ввести имя пользователя и пароль для запуска командного интерпретатора.

Пример использования

```
hostname# exit
```

version

Просмотреть текущую версию ViPNet Coordinator HW и его компонентов.

Синтаксис

```
version [full]
```

Параметры и ключевые слова

`full` — просмотр текущей версии всех компонентов, а также других параметров (набор функций, архитектура процессора).

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

По команде выводится название и версия продукта. При указании ключевого слова `full` выводятся дополнительные параметры:

```
hostname> version full

Product: ViPNet Coordinator HW

Platform: HW1000

Serial number: <Serial>

License: HW1000

Software version: 4.5.8


WebGUI software version: 2.1.0.2270

VPN software version: 4.7.1-1

Iplir driver software version: 4.1.3

Watchdog driver software version: 1.0.5
```

```
Crypto driver version: 2.1.0.2528

Crypto core version: 2.4.1.81

Feature set: base

Architecture: x86_64
```

version features list

Просмотреть список функциональных модулей, входящих в состав текущей версии ViPNet Coordinator HW.

Синтаксис

```
version features list
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Пример использования

```
hostname> version features list
bonding
dhcp-client
dhcp-relay
dhcp-server
...
```

who

Просмотреть информацию о запущенных сессиях командного интерпретатора (локальной и удаленных).

Синтаксис

```
who
```

Режимы командного интерпретатора

- Пользователь.
- Администратор.

Особенности использования

Информация о запущенных сессиях командного интерпретатора обновляется каждые 7 секунд.

Пример использования

```
hostname> who
LINE  HOST           IDLE      MODE  COMMENTS
tty1  local console  00:00:06  user  current
```

Информация отображается в следующем формате:

```
LINE HOST IDLE MODE COMMENTS
```

где:

- `LINE` — имя консоли.
- `HOST` — адрес подключения (для своего узла — `local console`).
- `IDLE` — время неактивности (отсутствие нажатия каких-либо клавиш).
- `MODE` — командный режим: `user` (Пользователь) или `admin` (Администратор).
- `COMMENTS` — комментарий, содержащий информацию о консоли (обычно информация о местонахождении).

2

Справочник конфигурационных файлов

Файл iplir.conf

Параметры защищенной сети ViPNet содержатся в файле `iplir.conf`. Чтобы их настроить:

1. Остановите управляющую службу:

   ```
   hostname# iplir stop
   ```

2. Откройте файл:

   ```
   hostname# iplir config
   ```

3. Настройте параметры, используя описание секций.

4. Запустите управляющую службу:

   ```
   hostname# iplir start
   ```

Секция [adapter]

Секции `[adapter]` описывают статические сетевые интерфейсы. Каждому интерфейсу соответствует своя секция. Если статический интерфейс не описан секцией `[adapter]`, то все проходящие через него IP-пакеты блокируются.

Примечание. В процессе работы ViPNet Coordinator HW могут создаваться динамические интерфейсы, например, при подключении ViPNet Coordinator HW к сети 3G или Wi-Fi. В ViPNet Coordinator HW по умолчанию разрешена работа динамических интерфейсов, которые входят в одну из групп:

- `ppp` — интерфейсы для встроенных модемов;
- `pppoe` — интерфейсы для подключения к сети провайдера по PPPoE;
- `wifi` — интерфейсы для внешних адаптеров Wi-Fi. В эту группу не входит встроенный интерфейс `wlan0`.

Добавление интерфейсов данных групп в файл `iplir.conf` не требуется.

Если в файле `iplir.conf` нет ни одной секции `[adapter]`, то управляющая служба при запуске получает от системы список сетевых интерфейсов и автоматически создает соответствующие секции.

В процессе работы управляющая служба и драйвер ViPNet периодически получают информацию о параметрах известных им интерфейсов с интервалом времени, заданным параметром `ifcheck_timeout` секции `[misc]` (см. Секция [misc]). Если обнаруживается, что интерфейс выключен в системе, он выключается и в драйвере ViPNet. После включения или изменения IP-адреса интерфейса эти изменения автоматически загружаются в драйвер ViPNet.

В секции `[adapter]` указываются параметры:

- `allowtraffic` — разрешение или блокирование прохождения IP-трафика через интерфейс:

- `on` (по умолчанию) — IP-пакеты пропускаются или блокируются в соответствии с сетевыми фильтрами, заданными на узле.
- `off` – IP-пакеты блокируются независимо от остальных настроек.

- `type` — тип интерфейса для драйвера ViPNet. Возможные значения: `internal` (внутренний) или `external` (внешний).

  Тип интерфейса выбирается, исходя из следующего:

  - Если ViPNet Coordinator HW работает в режиме «Без использования межсетевого экрана» или «С динамической трансляцией адресов», то все интерфейсы должны иметь тип `internal`.
  - Если ViPNet Coordinator HW работает в режиме «Координатор» или «Со статической трансляцией адресов» (с фиксированным внешним адресом), то интерфейсу, посредством которого ViPNet Coordinator HW будет связываться с узлом, выполняющим функции межсетевого экрана, следует назначить тип `external`, остальным интерфейсам ViPNet Coordinator HW — тип `internal`.

Нередактируемые параметры

`name` — системное имя интерфейса (например, `eth0`). Если в системе задано несколько IP-адресов на одном интерфейсе и присутствуют один или несколько виртуальных интерфейсов (`eth0:0`, `eth0:1` и так далее), то для управляющей службы и драйвера ViPNet все они будут представлять одно физическое устройство с базовым именем (`eth0`).

Секция [debug]

Секция `[debug]` определяет параметры ведения системного журнала управляющей службы `iplircfg`:

Внимание! В исполнениях с одним дисковым накопителем:

- По умолчанию уровень важности равен 1.
- При локальном протоколировании доступны уровни важности от –1 до 3.
- При удаленном протоколировании доступны уровни важности от –1 до 4. При этом если вы используете 4 уровень и выполняете переключение на локальное протоколирование, уровень не изменяется автоматически. Чтобы уровень важности принял значение по умолчанию, перезапустите службу `iplircfg`.

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (системные службы).
  - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

  Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

Секция [dynamic]

Секция `[dynamic]` содержит параметры для настройки режима подключения к внешней сети через межсетевой экран с динамической трансляцией адресов:

- `always_use_server` — включение или выключение режима, при котором весь трафик с внешними узлами направляется через сервер соединений, указанный в `forward_id` данной секции. Возможные значения: `off` (по умолчанию) или `on`.
- `dynamic_proxy` — включение или выключение режима «С динамической трансляцией адресов». Возможные значения: `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 HW. С помощью сервера соединений ViPNet Coordinator HW будет устанавливать соединения с другими узлами — всегда, если включен режим в `always_use_server`, либо до тех пор, пока соединение с другими узлами не будет установлено напрямую. Указывается в шестнадцатеричном формате с префиксом `0x`, например: `0x15c8000a`.

  Внимание! Указанный сервер соединений должен быть доступен из внешней сети по публичному IP-адресу.

- `timeout` — интервал отправки IP-пакетов серверу соединений для поддержания активного соединения с ним и пропуска входящего трафика через межсетевой экран. Указывается в секундах, значение по умолчанию — `25`. Как правило, интервала, заданного по умолчанию, достаточно для поддержки связи с сервером соединений при работе через большинство межсетевых экранов.
- `port_auto_change` — включение или выключение автоматической смены порта при недоступности сервера соединений. Возможные значения: `off` (по умолчанию) или `on`.

Секция [id]

Секция `[id]` используется для описания адресных настроек защищенных узлов, связанных с ViPNet Coordinator HW. Каждому узлу, с которым у ViPNet Coordinator HW есть связь, соответствует своя секция `[id]`. Первая секция соответствует собственным настройкам ViPNet Coordinator HW (собственная секция).

Секция `[id]` содержит параметры:

- `accessiplist` — IP-адреса доступа к узлу и их приоритет, если узел имеет множественные адреса доступа. В каждой секции `[id]` может быть указано любое количество параметров `accessiplist` — по количеству адресов доступа к узлу. Причем в первом параметре `accessiplist` каждой секции в качестве адреса доступа должен быть указан тот же адрес, что и в параметре `firewallip` данной секции. Если в секции не будет параметров `accessiplist`,

то параметр `firewallip` тоже будет отсутствовать. Остальные параметры `accessiplist` в секции используются для формирования списка адресов доступа к узлу с узла ViPNet Coordinator HW.

Параметр `accessiplist` может быть указан во всех секциях `[id]`, кроме собственной, в виде:

`accessiplist = <IP-адрес доступа>, <метрика>, <реальный IP-адрес узла>, <номер интерфейса>, <тип регистрации>`, где:

Примечание. Вручную в параметре `accessiplist` можно указать только IP-адрес узла или IP-адрес узла и метрику, остальные значения определяются системой автоматически в процессе работы управляющей службы.

- `<IP-адрес доступа>` — IP-адрес доступа к узлу.
- `<метрика>` — метрика указанного адреса доступа. Она определяет задержку (в миллисекундах) отправки тестовых сообщений при определении адреса доступа узла. Опросы осуществляются периодически (см. параметры `server_pollinterval` и `client_pollinterval` секции `[misc]`). Возможные значения: от `0` до `9999`. По умолчанию метрика имеет значение `auto`, то есть определяется автоматически.
- `<реальный IP-адрес узла>` — реальный IP-адрес узла, соответствующий сетевому интерфейсу, через который будут передаваться IP-пакеты для выбранного IP-адреса доступа. Присваивается автоматически.
- `<номер интерфейса>` — условный номер сетевого интерфейса. Возможные значения: от `0` до `255`.
- `<тип регистрации>` — тип регистрации данного IP-адреса доступа узла:
  - `auto` — задан ViPNet Coordinator HW.
  - `manual` — задан администратором вручную (редактированием файла конфигурации VPN).
  - `addrdoc` — взят из справочников, полученных из ViPNet ЦУС или Prime.

- `blockforward` — включение или выключение блокирования транзитных пакетов, передаваемых через ViPNet Coordinator HW узлу ViPNet, связанному с ним. Используется только в секциях `[id]`, описывающих настройки узлов ViPNet, связанных с ViPNet Coordinator HW. Возможные значения:
  - `off` — все транзитные пакеты в направлении узла пропускаются;
  - `on` — все транзитные пакеты в направлении узла блокируются с кодом 70.

  По умолчанию данный параметр отсутствует, что эквивалентно значению `off`.
- `fqdn` — доменное имя координатора, которое используется для восстановления соединения в случае смены его IP-адреса доступа (параметр `firewallip`). В собственной секции `[id]` параметр используется для задания доменного имени ViPNet Coordinator HW, а в любой секции `[id]`, кроме собственной — для задания доменного имени координатора, связанного с ViPNet Coordinator HW. Значение параметра присваивается автоматически ViPNet ЦУС или Prime и может быть изменено вручную администратором ViPNet Coordinator HW. При этом, если впоследствии администратор сети ViPNet изменит значение параметра в ViPNet ЦУС или

Prime, оно будет присвоено несмотря на изменения, сделанные администратором ViPNet Coordinator HW.

Доменное имя, заданное в параметре, должно быть зарегистрировано на DNS-сервере (корпоративном или любом другом, публично доступном).

Примечание. Для параметра `fqdn` действуют следующие ограничения:

- В веб-интерфейсе недоступен просмотр доменного имени координатора.
- При обновлении ViPNet Coordinator HW до версии 4.2.4 с более ранних версий координатору не назначается доменное имя, ранее заданное в ViPNet ЦУС или Prime, даже если администратор сети ViPNet повторно отправил справочники и ключи на ViPNet Coordinator HW. Чтобы ViPNet Coordinator HW был доступен по доменному имени, назначьте ему дополнительное доменное имя в ViPNet ЦУС или Prime и затем отправьте на ViPNet Coordinator HW обновление справочников и ключей.

- `fixfirewall` — режим фиксации настроек работы собственного узла через внешний межсетевой экран:
  - `off` (по умолчанию) — внешний IP-адрес и порт доступа к ViPNet Coordinator HW определяются автоматически по информации от узлов внешней сети;
  - `on` — внешний IP-адрес и порт доступа к ViPNet Coordinator HW:
    - порт доступа задается администратором в параметре `port` данной секции;
    - внешний IP-адрес передается из управляющего ПО и отображается в параметре `firewallip` данной секции.
- `ip` — реальный IP-адрес и соответствующий ему виртуальный IP-адрес узла. Первым указывается реальный адрес, затем после запятой — виртуальный (например: `ip = 192.168.201.10, 10.1.0.5`). Если указан только реальный адрес, то считается, что ему еще не сопоставлен виртуальный.

  Если узел имеет несколько сетевых интерфейсов или несколько IP-адресов на интерфейсе, в каждой секции `[id]` может быть несколько параметров `ip`. При этом первым должен быть указан параметр, содержащий наиболее приоритетный IP-адрес доступа к данному узлу. При автоматическом обновлении адресов наиболее приоритетный IP-адрес доступа становится первым автоматически. При изменении порядка следования реальных IP-адресов, порядок следования виртуальных адресов не меняется.
- `port` — порт источника или порт назначения. В каждой секции `[id]` может быть только один такой параметр.
- `proxyid` — режим работы узла, находящегося за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр. Возможные значения:
  - в собственной секции:
    - `0xfffffffe` — при работе в режиме «С динамической трансляцией адресов» (если в секции `[dynamic]` параметр `dynamic_proxy` установлен в `on` (см. Секция [dynamic]));
    - `0` — при работе в режиме «Со статической трансляцией адресов» (если в собственной секции `[id]` параметр `usefirewall` установлен в `on`);

- идентификатор координатора, через который происходит обмен информацией с другими узлами — при работе в режиме «Координатор» (если в соответствующей секции `[id]` параметр `usefirewall` установлен в `on`). Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`;
- идентификатор собственного координатора — при работе в режиме «Без использования межсетевого экрана» (если в собственной секции `[id]` параметр `usefirewall` установлен в `off`). Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`.

o в любой секции `[id]`, кроме собственной:

- `0xfffffffe` — при работе в режимах «Со статической трансляцией адресов» или «С динамической трансляцией адресов», если ViPNet Coordinator HW является сервером соединений для узла;
- `0` — при работе в режиме «Без использования межсетевого экрана»;
- идентификатор координатора — при работе в режимах «Координатор» или «С динамической трансляцией адресов». Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`.

- `tcptunnelport` — порт координатора для входящих соединений по протоколу TCP. Возможные значения: от 1 до 65535, значение по умолчанию 443. Заданный порт используется для работы TCP-туннеля (см. параметр `tcptunnel_establish` секции `[misc]` (см. Секция [misc])).

  Если параметр задан, то он автоматически рассылается на клиенты, для которых данный координатор служит сервером соединений.

- `tunnel` — адреса узлов, туннелируемых ViPNet Coordinator HW (указаны в собственной секции) или другими координаторами, в виде: `<ip1>-<ip2> to <ip3>-<ip4>`, где:

  o `<ip1>-<ip2>` — начальный и конечный реальные адреса диапазона туннелируемых узлов;

  o `<ip3>-<ip4>` — диапазон виртуальных адресов, которые соответствуют реальным адресам из диапазона `<ip1>-<ip2>`. Они используются вместо реальных адресов туннелируемых узлов, если на узле, который к ним обращается, настроена видимость по виртуальным адресам. Например, в случае, когда адреса из диапазона `<ip1>-<ip2>` относятся к внутренней сети и уже используются в локальной сети данного координатора. В частных случаях этот диапазон может совпадать с диапазоном `<ip1>-<ip2>`. Значение `ip4` формируется путем прибавления к `ip3` разницы между `ip2` и `ip1`.

  При этом учитывается параметр `tunnel_virt_assignment` секции `[misc]` (см. Секция [misc]), который может принимать одно из двух значений:

  o `auto` — параметры `<ip1>` и `<ip2>` задаются администратором сети ViPNet в ViPNet ЦУС или Prime или вручную на ViPNet Coordinator HW.

  Например, чтобы в автоматическом режиме указать, что координатор туннелирует адреса с 192.168.0.1 по 192.168.0.100, сделайте следующую запись:

  ```
  tunnel = 192.168.0.1-192.168.0.100
  ```

- `manual` — параметры `<ip1>-<ip2>` и `<ip3>` задаются вручную. Начальный адрес диапазона виртуальной видимости туннелируемых узлов `ip3` также необходимо указать вручную на каждом узле ViPNet, который будет работать с этими узлами.

  Например, чтобы вручную указать, что координатор туннелирует адреса с 192.168.0.1 по 192.168.0.100, а соответствующий им виртуальный диапазон адресов — 192.120.0.1-192.120.0.100, сделайте следующую запись:

  ```
  tunnel = 192.168.0.1-192.168.0.100 to 192.120.0.1
  ```

В одной секции `[id]` можно задать несколько параметров `tunnel`. Общее число заданных диапазонов туннелируемых узлов не должно превышать 1000.

Внимание! В зависимости от значения параметра `tunnel_virt_assignment` секции `[misc]` (см. Секция [misc]), настройки параметра `tunnel` действуют следующим образом:

- для автоматического режима назначения виртуальных адресов — можно задавать только первый и второй IP-адрес.
- для ручного режима назначения виртуальных адресов — можно задать значения всех четырех IP-адресов.

- `exclude_from_tunnels` — исключает адреса из списка туннелируемых координатором адресов, указанных в параметре `tunnel`. Задается в виде: `ip1-ip2`, где `ip1` и `ip2` — начальный и конечный реальные адреса диапазона, который не надо туннелировать.

  Например, чтобы исключить адрес 192.168.201.7 из туннелируемого диапазона 192.168.201.5-192.168.201.10 (то есть не шифровать трафик при соединении с узлом, имеющим адрес 192.168.201.7), сделайте следующую запись:

  ```
  exclude_from_tunnels = 192.168.201.7-192.168.201.7
  ```

  Используется в любой секции `[id]`, кроме собственной. В одной секции можно задать несколько таких параметров.

Внимание! Параметр `exclude_from_tunnels` имеет приоритет над настройками туннелирования, получаемыми из ViPNet ЦУС или Prime, и не изменяется при получении новых настроек туннелирования.

- `tunnel_local_networks` — параметр, который позволяет ViPNet Coordinator HW не туннелировать IP-адреса, входящие в локальную подсеть ViPNet Coordinator HW. Он задается в секциях [id] координаторов, связанных с ViPNet Coordinator HW. Возможные значения:
  - `on` (по умолчанию) — обращаться к туннелируемым узлам только через координатор, который их туннелирует.
  - `off` — обращаться к узлам, находящимся в локальной подсети, минуя координатор, который их туннелирует. Рекомендуется использовать в случае, если затруднен доступ к туннелируемым узлам в локальной подсети.
- `tunnelvisibility` — тип видимости для всех узлов, туннелируемых координатором:

- `real` — всегда обращаться к туннелируемым узлам по их реальным адресам;
- `virtual` — всегда обращаться к туннелируемым узлам по их виртуальным адресам.

При обновлении ViPNet Coordinator HW до версии 4.2.x и выше проверяется файл `iplir.conf` и в случае, если в какой-либо секции `[id]` есть назначенные виртуальные адреса, то параметру присваивается значение `virtual`. Значение данного параметра по умолчанию определяется параметром `tunneldefault` секции `[visibility]` (см. Секция [visibility]).

- `usetunnel` — 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 HW с узлами, которые туннелирует данный координатор, трафик шифроваться не будет. Используется в любой секции `[id]`, кроме собственной.
- `usefirewall` — может принимать значение `on` или `off` и используется в секциях `[id]` в следующих целях:
  - Во всех секциях `[id]`, кроме собственной, — указывает на использование настроек работы через межсетевой экран с данным узлом. Если этот параметр имеет значение `off`, то параметры `firewallip`, `port` и `proxyid` в этой секции игнорируются, и работа с данным узлом будет возможна только по одному из его реальных IP-адресов.
  - В собственной секции `[id]` — указывает на использование внешнего межсетевого экрана. В случае если межсетевой экран использоваться не будет, он установлен в значение `off`, в остальных случаях — в значение `on` (см. описание параметра `proxyid` данной секции).
- `visibility` — тип видимости узла:
  - `auto` — автоматически определять тип видимости узла, в зависимости от текущего адреса видимости узла.
  - `real` — всегда обращаться к данному узлу по его реальному адресу.
  - `virtual` — всегда обращаться к данному узлу по его виртуальному адресу.

Этот параметр не является обязательным и используется, только если для данного узла необходимо индивидуально задать тип видимости. В случае отсутствия параметра `visibility` видимость узла определяется параметрами секции `[visibility]` (см. Секция [visibility]), то есть параметрами видимости всей сети, к которой этот узел принадлежит, либо параметрами видимости узлов по умолчанию.

Примечание. Использовать параметр `visibility` нужно осторожно, так как у сетевых узлов, которые видны по виртуальным адресам, могут совпадать реальные адреса (если эти узлы находятся в частных сетях).

Нередактируемые параметры

- `accessip` — текущий IP-адрес доступа к узлу со стороны ViPNet Coordinator HW. Может принимать значение одного из реальных или виртуальных IP-адресов, в зависимости от физической топологии сети, режимов подключения к внешней сети ViPNet Coordinator HW и данного узла.
- `always_use_server` — признак работы узла в режиме использования межсетевого экрана с динамической трансляцией адресов с направлением трафика через выбранный координатор. Параметр присутствует только в случае работы данного узла в указанном режиме и принимает значение `on`.
- `dynamic_timeout` — период опроса (в секундах) ViPNet-координатора, выбранного в качестве межсетевого экрана для данного узла, с целью обеспечения пропуска входящего трафика через межсетевой экран. Данный параметр присутствует во всех секциях `[id]`, кроме собственной.
- `id` — уникальный идентификатор узла. По этому параметру управляющая служба отличает одну секцию `[id]` от другой. Идентификатор присваивается сетевому узлу ViPNet при его создании в ViPNet ЦУС или Prime. В каждой секции `[id]` может быть только один такой параметр.
- `firewallip` — внешний IP-адрес доступа к узлу в случае, если этот узел находится за межсетевым экраном. При работе с узлом, установленным за межсетевым экраном, все направленные к нему зашифрованные пакеты инкапсулируются в единый UDP-пакет с адресом назначения, указанным в данном параметре, и портом назначения, указанным в параметре `port` данной секции. Если узел не находится за межсетевым экраном, то параметр `firewallip` отсутствует или установлено его значение `0.0.0.0`. В каждой секции `[id]` может быть только один такой параметр.
- `name` — имя узла. Задается администратором сети ViPNet в ViPNet ЦУС или Prime и предназначен для удобства настройки. Данный параметр записывается в конфигурационный файл автоматически при его сохранении. В каждой секции `[id]` может быть только один такой параметр.
- `virtualip` — базовый виртуальный адрес узла. В каждой секции `[id]` может быть только один такой параметр.
- `version` — версия протокола обмена служебной информацией между узлами сети ViPNet.

Секция [misc]

Секция `[misc]` содержит дополнительные параметры:

- `cef_enabled: yes` — запустить, `no` — остановить экспорт CEF.
- `cef_ip` — IP-адрес сетевого узла, на который будут посылаться сообщения CEF.

  Нельзя указывать локальный узел `localhost`, собственные IP-адреса и дополнительные IP-адреса (alias) интерфейсов.

- `cef_port` — порт UDP для передачи сообщений CEF. Значение по умолчанию — `514`.
- `client_pollinterval` — период опроса координатора ViPNet Coordinator HW клиентами, для которых он выполняет функцию сервера IP-адресов. Значение этого параметра координатор сообщает своим клиентам в каждом сеансе работы. Если от какого-либо клиента, который должен обмениваться пакетами с координатором, не было получено никаких служебных пакетов в течение времени, указанного в данном параметре, то такому клиенту посылается специальный пакет, на который должен прийти ответ. Если ответ не приходит, то узел клиента считается недоступным (выключенным). Указывается в секундах, значение по умолчанию — `300` (5 минут). Уменьшение значения данного параметра позволяет более оперативно определять неработоспособность узла, но повышает объем служебного трафика.
- `config_version` — версия модуля шифрования.
- `ifcheck_timeout` — период опроса параметров сетевых интерфейсов, известных управляющей службе. Указывается в секундах, значение по умолчанию — `30`.
- `iscaggregate` — включение или выключение накопления служебного трафика, обрабатываемого на координаторе. С помощью этого параметра вы можете снизить постоянную нагрузку на сеть за счет того, что служебный трафик будет накапливаться и передаваться периодически, а не постоянно. Возможные значения:
  - `on` (по умолчанию) — накопление служебного трафика происходит в течение минуты с последующей рассылкой на узлы не чаще, чем раз в минуту;
  - `off` — накопление служебного трафика выключено. В этом случае служебный трафик передается постоянно.
- `ipforwarding` — управление IP-форвардингом (маршрутизацией транзитных IP-пакетов через координатор ViPNet Coordinator HW). Возможные значения:
  - `on` — включать IP-форвардинг при запуске управляющей службы;
  - `off` — выключать IP-форвардинг при запуске управляющей службы;
  - `system` — не изменять текущие настройки IP-форвардинга при запуске управляющей службы.

Примечание. При выключенном IP-форвардинге не работают пересылка транзитных IP-пакетов и туннелирование, поэтому рекомендуется устанавливать параметр `ipforwarding` в значение `on`. Значения `off` и `system` рекомендуется использовать только при отладке.

- `msg_compress_level` — степень сжатия служебных межсерверных сообщений. Возможные значения: от 1 (минимальное сжатие, максимальная скорость) до 9 (максимальное сжатие, минимальный объем служебного трафика). По умолчанию — `3`.

Примечание. На высоконагруженных узлах не рекомендуется устанавливать значение параметра `msg_compress_level` больше 5.

- `mssdecrease` — число байт, на которое будет уменьшен параметр MSS (максимальный размер сегмента) протокола TCP. По умолчанию — `0`.

  Уменьшать параметр MSS рекомендуется, если между вашим и другими защищенными или туннелируемыми узлами успешно проходит проверка соединения (ping), но не устанавливается TCP-соединение. Причиной блокирования шифрованных IP-пакетов, передаваемых в рамках TCP-соединения, может быть фрагментация этих IP-пакетов на устройствах, стоящих на пути от отправителя к получателю.

  Во избежание фрагментации рекомендуется уменьшить размер IP-пакетов, принимаемых на узле, присвоив параметру `mssdecrease` значение от 20 до 40 байт. Чтобы уменьшить размер исходящих IP-пакетов узла, значение параметра `mssdecrease` следует изменить на узле получателя этих IP-пакетов. Для установления TCP-соединения достаточно изменить параметр `mssdecrease` на одном из взаимодействующих узлов.

Внимание! Не изменяйте параметр `mssdecrease` без крайней необходимости.

- `ompnumthreads` — количество ядер процессора, используемое для обработки служебных сообщений (по умолчанию — `1`).
- `packettype` — формат шифрованных пакетов. Возможные значения: `4.1` (по умолчанию) или `4.0`. Определяет только формат пакетов, отправляемых данным сетевым узлом. Формат входящих пакетов определяется автоматически, и их расшифрование производится независимо от установленного значения параметра `packettype`. Формат пакетов 4.0 рекомендуется использовать только, если необходимо связываться с узлами, на которых установлены старые версии ПО ViPNet.
- `server_pollinterval` — период опроса данным координатором других координаторов. Если от какого-либо координатора, который должен обмениваться пакетами с данным координатором, не было получено никаких служебных пакетов в течение времени, указанного в данном параметре, то такому координатору направляется специальный пакет, на который должен прийти ответ. Если ответ не приходит, то узел координатора считается недоступным (выключенным). Указывается в секундах, значение по умолчанию — `900` (15 минут).
- `tcptunnel_client` — включение или выключение функции TCP-клиента. Возможные значения: `on` или `off` (по умолчанию). Используется только если координатору назначена роль TCP-клиента.
- `tcptunnel_client_mode` — режим работы TCP-клиента. Возможные значения:
  - `auto` (по умолчанию) — автоматическое включение TCP-туннеля при пропадании UDP связи и выключение при ее появлении.
  - `forced` — TCP-туннель устанавливается всегда, когда возможно, даже при доступе к серверу соединения по UDP.

  Используется только если координатору назначена роль TCP-клиента.

- `tcptunnel_client_port` — TCP-порт сервера, на который будут отправляться пакеты. Используется только если координатору назначена роль TCP-клиента. Значение по умолчанию: `443`.
- `tcptunnel_establish` — включение или выключение функции сервера TCP-туннелей. Возможные значения: `on` или `off` (по умолчанию). Для входящих соединений по протоколу TCP по умолчанию используется порт `443` — параметр `tcptunnelport` секции `[id]`.
- `tcptunnel_role` — роль координатора для функции TCP-туннеля. Возможные значения: `server` (сервер TCP-туннелей) или `client` (TCP-клиент). Значения по умолчанию:
  - для HW10, HW50, HW100 — `client`;
  - для остальных исполнений — `server`.
- `timediff` — максимально допустимая разница между временем отправки и приема IP-пакетов. Из соображений безопасности драйвер ViPNet блокирует входящие IP-пакеты, если время их отправки отличается от времени их приема более чем на число секунд, указанное в этом параметре. Значение параметра должно быть не меньше 1 секунды и не больше 7200 секунд. Значение по умолчанию — `7200` (2 часа).
- `timesync` — параметр используется только для клиентского ПО, на координаторе значение установлено в `off`, изменять его нельзя.
- `tunnel_virt_assignment` — режим назначения виртуальных адресов для узлов, туннелируемых координатором:
  - `auto` (по умолчанию) — задаются автоматически;
  - `manual` — задаются вручную в параметрах `tunnel` и `exclude_from_tunnels` секции `[id]`.

Внимание! После обновления ПО ViPNet Coordinator HW до версии 4.5.2 и выше ручная настройка виртуальных адресов туннелируемых узлов сохраняется. В случае автоматической настройки все виртуальные адреса для туннелируемых узлов будут переназначены.

- `warnoldautosave` — включение или выключение предупреждения о наличии конфигураций, содержащих настройки ПО ViPNet, которые были автоматически сохранены более месяца назад. Возможные значения: `on` (по умолчанию) или `off`. Если параметр установлен в значение `on`, то предупреждения выводятся каждый раз при запуске управляющей службы.

Секция [servers]

Секция `[servers]` содержит список координаторов, известных данному сетевому узлу. Каждому координатору соответствует один нередактируемый параметр `server`, в котором через запятую указаны идентификатор координатора и его имя.

Секция [virtualip]

Секция `[virtualip]` описывает настройки виртуальных IP-адресов и содержит параметры:

- `maxvirtualip` — максимальный адрес для формирования базовых виртуальных адресов защищенных узлов (по умолчанию параметр не используется). Используется для задания верхнего ограничения диапазона назначаемых базовых виртуальных адресов вручную. Значение параметра `maxvirtualip` должно быть больше значения параметра `startvirtualip`.
- `startvirtualip` — стартовый адрес для формирования базовых виртуальных адресов защищенных узлов (значение по умолчанию — `11.0.0.1`). При изменении данного параметра назначение всех базовых виртуальных адресов узлов производится заново, как при начальном формировании файлов конфигурации. Кроме того, для узлов производится назначение виртуальных адресов в параметрах `ip`.
- `starttunnelvirtualip` — стартовый адрес для формирования диапазонов виртуальных адресов туннелируемых узлов в автоматическом режиме (по умолчанию для диапазонов адресов туннелируемых узлов — `12.0.0.1`, для адресов одиночных туннелируемых узлов — `11.0.0.1`).

Секция [visibility]

Секция `[visibility]` содержит настройки видимости защищенных сетевых узлов, с которыми связан ViPNet Coordinator HW. В отличие от параметра `visibility`, с помощью которого в секциях [id] задается видимость отдельных узлов, в этой секции можно задать видимость сразу для всех узлов сетей или подсетей ViPNet. Настройки, заданные в секции `[visibility]`, учитываются при определении видимости узлов со стороны собственного узла.

Секция может содержать параметры:

- `default` — видимость узлов по умолчанию. Возможные значения:
  - `auto` (по умолчанию) — автоматическое определение видимости узлов;
  - `real` — доступ к узлам по их реальным IP-адресам;
  - `virtual` — доступ к узлам по их виртуальным IP-адресам.
- `subnet_real` — идентификаторы сетей ViPNet, для которых настраивается видимость узлов по реальным IP-адресам.

  Идентификатор сети вы можете посмотреть в ViPNet ЦУС или Prime или с помощью команды `iplir info`. Идентификаторы сетей указываются в шестнадцатеричном формате с префиксом `0x`. В одной секции `[visibility]` можно задать несколько параметров `subnet_real`. При этом в каждом параметре можно указать либо один идентификатор, либо несколько идентификаторов через запятую. Например:

  ```
  subnet_real = 0x5155
  subnet_real = 0x5156,0x5157,0x5158
  ```

- `subnet_virtual` — идентификаторы сетей ViPNet, для которых настраивается видимость узлов по виртуальным IP-адресам. Задается так же, как параметр `subnet_real`.

Внимание! Один и тот же идентификатор сети ViPNet можно указать только в одном из параметров `subnet_auto`, `subnet_real` или `subnet_virtual`.

- `subnet_auto` — идентификаторы сетей ViPNet, для которых автоматически определяется видимость узлов. Задается так же, как параметр `subnet_real`. В секции `[visibility]` можно задать несколько параметров `subnet_auto`.

  Параметры `subnet_real`, `subnet_virtual` и `subnet_auto` являются необязательными и по умолчанию отсутствуют в секции `[visibility]`.

  При старте управляющей службы идентификаторы, заданные в параметрах `subnet_real`, `subnet_virtual` и `subnet_auto`, автоматически сортируются в порядке возрастания и группируются в строки, каждая из которых содержит максимум 8 идентификаторов.

- `tunneldefault` — тип видимости для всех узлов, туннелируемых координатором, который будет указываться по умолчанию вне зависимости от режима назначения адресов туннелируемых узлов (см. параметр `tunnel_virt_assignment` секции `[misc]`) при отсутствии в секции `[id]` параметра `tunnelvisibility`. Возможные значения:
  - `real` (по умолчанию) — всегда обращаться к туннелируемым узлам по их реальным адресам;
  - `virtual` — всегда обращаться к туннелируемым узлам по их виртуальным адресам.

Файл iplir.conf-<интерфейс или группа интерфейсов>

Параметры журнала прохождения трафика через любой активный сетевой интерфейс настраиваются в конфигурационных файлах `iplir.conf-<интерфейс или группа интерфейсов>`. Для каждого статического интерфейса, описанного секцией `[adapter]` в файле `iplir.conf`, а также для каждой группы динамических интерфейсов управляющая служба при запуске автоматически создает такой файл с параметрами по умолчанию.

Примечание. В ViPNet Coordinator HW по умолчанию разрешена работа динамических интерфейсов, которые входят в одну из групп:

- `ppp` — интерфейсы для встроенных модемов;
- `pppoe` — интерфейсы для подключения к сети провайдера по PPPoE;
- `wifi` — интерфейсы для внешних адаптеров Wi-Fi. В эту группу не входит встроенный интерфейс `wlan0`.

Чтобы отредактировать файл `iplir.conf-<интерфейс или группа интерфейсов>`:

1. Остановите управляющую службу:

   ```
   hostname# iplir stop
   ```

2. Откройте файл для редактирования:

   ```
   hostname# iplir config <интерфейс или группа интерфейсов>
   ```

3. Выполните изменения.

4. Запустите управляющую службу:

   ```
   hostname# iplir start
   ```

Внимание! Конфигурационный файл `iplir.conf-<интерфейс>` может отсутствовать для статического интерфейса, если соответствующая секция `[adapter]` была добавлена в файл `iplir.conf` вручную и после этого управляющая служба не перезапускалась. Поэтому после добавления секций `[adapter]` в файл `iplir.conf`:

1. Запустите управляющую службу: `iplir start`.
2. Завершите работу управляющей службы: `iplir stop`.
3. Отредактируйте нужный файл `iplir.conf-<интерфейс>`.
4. Запустите управляющую службу: `iplir start`.

Секция [db]

Для каждого статического интерфейса и группы динамических интерфейсов ведется свой журнал регистрации IP-пакетов, который хранится в файле `iplir.db-<интерфейс или группа интерфейсов>`, расположенном в подкаталоге `iplirdb` каталога, содержащего файлы `iplir.conf-<имя интерфейса или группа интерфейсов>`.

Записи о пакетах регистрируются в журнале до тех пор, пока не будет достигнут его максимальный размер, после чего самые ранние записи стираются и на их место записываются новые. Для уменьшения размера журнала, а также для удобства его просмотра одинаковые записи о пакетах, зарегистрированные в течение заданного времени, объединяются в одну запись. Поэтому при просмотре журнала можно узнать, сколько раз было зафиксировано событие, описываемое этой записью.

Секция `[db]` содержит параметры:

- `maxsize` — максимальный размер журнала в Мбайтах:

  Таблица 3. Значение параметра по умолчанию и рекомендованное максимальное значение

Исполнение	Значение по умолчанию (Мбайт)	Рекомендованное максимальное значение* (Мбайт)
HW10	10	10
HW50	10	10
HW100	50	50
HW1000	50	для физических интерфейсов — 1800 для виртуальных интерфейсов — 200
HW2000	50	для физических интерфейсов — 1800 для виртуальных интерфейсов — 200
HW5000	50	для физических интерфейсов — 1800 для виртуальных интерфейсов — 200
ViPNet Coordinator VA	50	для физических интерфейсов — 1800 для виртуальных интерфейсов — 200

* рекомендованное максимальное значение рассчитано при использовании максимального количества интерфейсов (ограничения на количество интерфейсов указаны в документе «Подготовка к работе»)

Внимание! При работе ViPNet Coordinator HW в кластере горячего резервирования общий объем всех журналов IP-пакетов не должен превышать 90% оперативной памяти аппаратной платформы. При превышении объема могут возникнуть проблемы с передачей данных через интерфейс синхронизации. Размеры оперативной памяти указаны в описании аппаратных платформ в документе «Подготовка к работе».

Каждый раз при запуске управляющей службы в значение параметра `maxsize` после размера журнала автоматически дописывается слово `MBytes`, если оно отсутствует. Поэтому при изменении значения этого параметра его можно не писать. Значение параметра `0` выключает ведение журнала. При этом если до выключения журнала в нем были записи, то просмотреть их будет невозможно.

- `timediff` — интервал времени, в течение которого одинаковые события объединяются в журнале в одну запись. Задается в секундах, значение по умолчанию — `60`. Если этот параметр установлен в `0`, то объединение событий не используется. В этом случае при интенсивном трафике в журнале могут регистрироваться не все пакеты.
- `registerall` — включение или выключение регистрации записей обо всех пакетах, проходящих через интерфейс. Возможные значения: `off` (по умолчанию) или `on`. То есть по умолчанию регистрируются только записи о блокированных пакетах и изменении адресов сетевых узлов.
- `registerbroadcast` — включение или выключение регистрации записей о широковещательных пакетах. Возможные значения: `off` (по умолчанию) или `on`.
- `omittcpclientport` — включение или выключение скрытия информации о порте VPN-клиента при соединении по протоколу TCP. Возможные значения: `off` (по умолчанию) или `on`.

  Обычно порт клиента при TCP-соединении выделяется динамически и никакой полезной информации не несет. Если с какого-либо сетевого ресурса производятся попытки подключиться к какому-либо порту на компьютере, а соединение по каким-то причинам не будет установлено, то при следующей попытке установить соединение с того же ресурса будет использоваться другой порт. При использовании сканеров портов или каких-либо сетевых атаках число таких попыток может достигать нескольких сотен в секунду. Поскольку клиент использует каждый раз разные порты, то такие пакеты не считаются одинаковыми и для каждого из них создается своя запись в журнале, что засоряет его и затрудняет последующий анализ. Если параметр `omittcpclientport` установлен в значение `on`, порт клиента при TCP-соединении не регистрируется и не учитывается, а в журнале числовое значение номера порта указывается равным нулю, что позволяет объединить события о попытках подключения к какому-либо порту на компьютере с определенного адреса в одну запись. Это часто бывает удобно.
- registerevents — включение или выключение регистрации служебных событий. Список служебных событий см. в документе «Настройка с помощью командного интерпретатора», в приложении «Типы событий в журнале регистрации IP-пакетов». Возможные значения: `off` или `on` (по умолчанию).

Секция [cef]

Секция `[cef]` содержит параметры:

- `event` — формирование сообщений CEF при регистрации IP-пакетов, проходящих через интерфейс:
  - `all` — для всех IP-пакетов;

- `blocked` — для блокированных IP-пакетов (значение по умолчанию);

- `exclude` — формирование сообщений CEF, заданных в `event`, за исключением указанных номеров типов событий. Допускается перечисление номеров типов событий в любом порядке через запятую.

Файл failover.ini

Настройка параметров работы системы защиты от сбоев выполняется путем редактирования конфигурационного файла `failover.ini`.

Чтобы отредактировать файл `failover.ini`:

1. Завершите работу службы `failoverd`:

   ```
   hostname# failover stop
   ```

2. Откройте файл для редактирования:

   ```
   hostname# failover config edit
   ```

3. Внесите изменения.

4. Запустите службу `failoverd`:

   ```
   hostname# failover start
   ```

Секция [channel]

Каждый сетевой интерфейс активного узла, работоспособность которого должна контролироваться системой защиты от сбоев при работе в режиме кластера, должен быть описан секцией `[channel]`. Это необходимо для своевременного обнаружения неработоспособности интерфейса и переключения кластера.

Примечание. Параметры секций `[channel]` интерпретируются только при работе системы защиты от сбоев в режиме кластера.

Чтобы отключить контроль работоспособности какого-либо интерфейса, удалите из файла `failover.ini` соответствующую секцию `[channel]`.

Секция `[channel]` содержит параметры:

- `activeip` — IP-адрес и маска, которые будет иметь интерфейс активного узла кластера. Маска может быть указана после IP-адреса через символ «/» в нотации CIDR или в прямой нотации. Например:
  - в нотации CIDR: `activeip = 192.168.201.1/24`
  - в прямой нотации: `activeip = 68.21.12.34/255.255.252.0`

Примечание. Независимо от того, в какой нотации была указана маска, после сохранения файла `failover.ini` и запуска службы `failoverd` маска будет перезаписана в нотации CIDR.

- `checkonlyidle` — способ проверки доступности сетевых узлов через интерфейс. Возможные значения:
  - `yes` (по умолчанию) — проверять доступность сетевых узлов, только если интерфейс неактивный.

    Если за период опроса через интерфейс не проходят входящие или исходящие пакеты, на IP-адреса из `testip` отправляются эхо-запросы.
  - `no` — всегда проверять доступность сетевых узлов.

    Эхо-запросы на IP-адреса из `testip` отправляются раз в период опроса.

  Особенности использования:
  - Узлы кластера переключаются, если нет ответа на эхо-запросы. Время ожидания ответа определяется параметром `timeout` секции `[network]`.
  - Период опроса определяется параметром `checktime` секции `[network]`.
- `device` — имя интерфейса (`eth0`, `eth1` и так далее).
- `ident` — текстовая строка, идентифицирующая интерфейс. Для интерфейсов, подключенных к одинаковым сетям, параметры `ident` должны совпадать.

Примечание. Не рекомендуется использовать разные имена (несимметричные конфигурации) интерфейсов кластера.

- `testdevice` — имя сетевого интерфейса, для которого необходимо контролировать состояние физического соединения. При потере соединения на указанном интерфейсе будет выполнено переключение узлов кластера.

  В качестве сетевого интерфейса в параметре `testdevice` вы можете указать только физический интерфейс. Не допускается задавать виртуальные, агрегированные или VLAN интерфейсы, а также `localhost`. При этом вы можете указать физический интерфейс, который задан как trunk-интерфейс для VLAN.

  В каждой секции `[channel]` можно задать только один параметр `testdevice`.

Внимание!

- Не изменяйте параметры сетевого интерфейса, указанного в `testdevice`, если служба `failoverd` запущена в режиме кластера горячего резервирования. Иначе это будет воспринято системой как потеря физического соединения и приведет к смене ролей узлов кластера.
- В качестве `device` и `testdevice` указывайте только те сетевые интерфейсы, состояние которых действительно должно контролироваться для работоспособности кластера.

- `testip` — IP-адрес маршрутизатора или другого стабильного объекта сети, которому будут посылаться эхо-запросы для проверки работоспособности интерфейса.

При необходимости можно для каждого из интерфейсов указать несколько параметров `testip`. В этом случае сбоем интерфейса будет считаться ситуация, когда ни от одного из заданных IP-адресов не будет получено ответа.

Например, чтобы эхо-запросы отправлялись на IP-адреса 192.168.100.34 и 192.168.100.25, добавьте следующие строки:

```
testip = 192.168.100.34
testip = 192.168.100.25
```

Внимание! Для каждого интерфейса, описанного секцией `[channel]`, в параметре `testip` должен быть задан свой адрес, принадлежащий подсети данного интерфейса.

Если в параметре `testip` один и тот же адрес указан для нескольких интерфейсов, будет проверяться работоспособность только сетевого интерфейса, указанного в конфигурационном файле первым.

Если в параметре `testip` задан адрес, не принадлежащий подсети данного интерфейса, то для этого адреса должен быть задан статический маршрут или шлюз по умолчанию.

В качестве параметра `testip` не рекомендуется задавать адрес интерфейса «внутренней петли» (loopback), например, `127.0.0.1`, так как в этом случае реальной проверки работоспособности сетевого интерфейса не производится.

- `usevirtualmac` — включает или выключает использование виртуальных MAC-адресов для сетевых интерфейсов кластера, заданных в данной секции `[channel]`. Возможные значения:
  - `yes` — использовать виртуальные MAC-адреса для сетевых интерфейсов;
  - `no` (по умолчанию) — не использовать виртуальные MAC-адреса для сетевых интерфейсов.

  Использование параметра `usevirtualmac` имеет особенности:
  - Исполнение ViPNet Coordinator VA не поддерживает использование виртуальных MAC-адресов для сетевых интерфейсов кластера.
  - Виртуальные MAC-адреса для сетевых интерфейсов кластера генерируются на основе значения параметра `virtualmacprefix` в секции `[network]`.
  - Если параметр `usevirtualmac` включен, то на активном узле кластера для сетевых интерфейсов, описанных в данной секции `[channel]`, используются виртуальные MAC-адреса, а после переключения в пассивном режим для интерфейсов восстанавливаются аппаратно заданные MAC-адреса.
  - Если параметр `usevirtualmac` выключен, то система не проверяет MAC-адреса на сетевых интерфейсах кластера.
  - Если параметр `usevirtualmac` использовался и затем был выключен, то для сетевых интерфейсов кластера могут использоваться виртуальные MAC-адреса до перезагрузки ViPNet Coordinator HW. Чтобы сбросить MAC-адреса, перезагрузите ViPNet Coordinator HW с помощью команды `machine reboot`.
  - Для работы этой функции настройте коммутационное оборудование таким образом, чтобы разрешить использование двух MAC-адресов для одного Ethernet-порта.

Секция [debug]

Секция `[debug]` определяет параметры ведения журнала событий службы `failoverd` и содержит параметры:

- `debuglevel` — уровень важности событий, записываемых в журнал. Возможные значения: от `-1` до `4` (по умолчанию `3`). Чем выше уровень важности, тем более подробная информация записывается в журнал. Значение параметра `-1` выключает ведение журнала (при этом некоторые важные системные события по-прежнему будут выводиться в журнал).

  Уровень важности `4` используется только для диагностики возможных проблем и должен быть включен по рекомендации специалистов ИнфоТеКС. Не задавайте его для постоянного использования.

Внимание! В исполнениях с одним дисковым накопителем:

- По умолчанию уровень важности равен `1`.
- При локальном протоколировании доступны уровни важности от `-1` до `3`.

При удаленном протоколировании доступны уровни важности от `-1` до `4`. При этом если вы используете `4` уровень и выполняете переключение на локальное протоколирование, уровень не изменяется автоматически. Чтобы уровень важности принял значение по умолчанию, перезагрузите службу `failoverd`: failover stop и failover start.

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (системные службы).
  - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

  Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

Секция [misc]

Секция `[misc]` содержит дополнительные параметры работы системы защиты от сбоев в режиме кластера и в одиночном режиме:

- `maxjournal` — максимальное количество дней, за которое необходимо хранить записи в журнале переключений кластера горячего резервирования. По умолчанию это ограничение отсутствует.
- `reboot` — задает действия системы в случае обнаружения полной неработоспособности какой-либо службы или драйвера ViPNet Coordinator HW. Возможные значения:

- `yes` (по умолчанию) — включить механизм регистрации в watchdog-драйвере и перезагружать систему, если какая-либо служба или драйвер не может восстановить свою работу;
- `no` — выключить механизм регистрации в watchdog-драйвере и не перезагружать систему, если какая-либо служба или драйвер не может восстановить свою работу.

- `syncconnections` — включает или выключает синхронизацию сетевых соединений при работе в режиме кластера горячего резервирования. Возможные значения:
  - `yes` — синхронизация соединений при работе в кластере включена. В этом случае при переключении узлов кластера соединения, открытые на активном узле до момента переключения узлов, продолжат работу на пассивном узле после его переключения в активный режим. При этом не будут синхронизированы:
    - открытые сессии разрешения доменных имен;
    - защищенные соединения по TCP-туннелям;
    - локальные соединения (открытые и защищенные соединения, в которых сетевой узел ViPNet Coordinator HW является источником или назначением);
    - соединения, использующие прикладные протоколы.

    После переключения узлов кластера связь по указанным типам соединений может быть прервана.
  - `no` (по умолчанию) — синхронизация соединений при работе в кластере выключена.

  Для работы функции синхронизации соединений параметр должен иметь значение `yes` на обоих узлах кластера.
- `syncdatetime` — включает или выключает синхронизацию времени и часового пояса между узлами кластера.
  - `yes` (по умолчанию) — активный узел кластера передает пассивному узлу данные времени и часового пояса;
  - `no` — синхронизация времени между узлами кластера выключена.

  Значение параметра должно быть одинаковым для обоих узлов кластера (для корректного переключения их режимов работы).

Нередактируемые параметры

- `activeconfig` — абсолютный путь к файлу конфигурации управляющей службы, который будет использоваться на активном узле кластера. Значение по умолчанию — `/etc/iplirpsw`.
- `passiveconfig` — абсолютный путь к файлу конфигурации управляющей службы, который будет использоваться на пассивном узле кластера. Значение по умолчанию — `/etc/iplirpsw`.

Примечание. Параметры `activeconfig`, `passiveconfig` и `maxjournal` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования.

Секция [network]

Секция `[network]` описывает параметры работы системы защиты от сбоев, относящиеся к посылке пакетов в сеть в режиме кластера.

Примечание. Все параметры секции `[network]` интерпретируются только при работе системы защиты от сбоев в режиме кластера.

Все параметры этой секции рекомендуется настроить одинаково на обоих узлах кластера.

Секция `[network]` содержит параметры:

- `activeretries` — количество неуспешных попыток опроса пассивным узлом активного узла, после которых делается вывод об отсутствии активного узла с опрашиваемым IP-адресом. По умолчанию — `3`.
- `channelretries` — количество неуспешных попыток опроса интерфейса тестового узла, после которых этот интерфейс считается неработоспособным. По умолчанию — `3`.
- `checktime` — период опроса:
  - на активном узле — для проверки работоспособности интерфейса;
  - на пассивном узле — для поиска IP-адресов активного узла.

  Указывается в секундах, по умолчанию — `10`.

  

  Внимание! Значение параметра `checktime` должно быть больше, чем значение параметра `timeout`.
- `fastdown` — указывает на принудительное выключение сетевых интерфейсов перед перезагрузкой узла. Возможные значения: `yes` (по умолчанию) или `no`. Значение, выбранное по умолчанию, позволяет быстрее установить отсутствие активного узла в сети и дать возможность второму узлу перейти в активный режим, однако при этом завершение работы сетевых служб происходит уже при выключенных интерфейсах и может быть некорректным.
- `synctime` — период отправки пакетов синхронизации между узлами кластера. Указывается в секундах, значение по умолчанию — `5`.
- `timeout` — время ожидания ответа на запрос (эхо-запрос или запрос IP-адресов активного узла), по истечении которого делается вывод о неуспешности этого запроса. Указывается в секундах, по умолчанию — `2`.
- `virtualmacprefix` — исходное значение для расчета первого октета виртуального MAC-адреса, генерируемого для сетевых интерфейсов кластера (см. описание параметра `usevirtualmac` в секции `[channel]`). Указывается в десятичном виде, значение по умолчанию — `39`.

  Виртуальный MAC-адрес для IP-адреса интерфейса генерируется следующим образом:
  - 1-й октет: вычисляется на основе значения параметра `virtualmacprefix`;
  - 2-й—5-й октеты: активный IP-адрес сетевого интерфейса в шестнадцатеричном виде;

- 6-й октет: 0.

Например, для IP-адреса 10.20.2.1 при значении параметра `virtualmacprefix` по умолчанию будет сгенерирован виртуальный MAC-адрес 9e:0a:14:02:01:00.

Значения параметра `virtualmacprefix` должны совпадать на активном и пассивном узлах кластера.

Секция [sendconfig]

В секции `[sendconfig]` задаются параметры, контролирующие отправку конфигурационных файлов с активного узла на пассивный для их резервирования и синхронизации настроек узлов кластера.

Примечание. Все параметры секции `[sendconfig]` интерпретируются только при работе системы защиты от сбоев в режиме кластера.

Секция `[sendconfig]` содержит параметры:

- `activeip` — IP-адрес интерфейса синхронизации другого узла кластера.
- `config` — включение или выключение резервирования группы конфигурационных файлов. Возможные значения: `yes` (по умолчанию) или `no`. В группу входят следующие конфигурационные файлы:
  - `iplir.conf`;
  - `iplir.conf-<интерфейс или группа интерфейсов>`, кроме файла для интерфейса синхронизации;
  - `mftp.conf` (см. Файл mftp.conf);
  - файлы, содержащие сетевые фильтры и правила трансляции (заданные пользователем и полученные из ViPNet Policy Manager или Policy Management (модуль ViPNet Prime));
  - файлы с настройками функции L2OverIP;
  - файлы `*.crg` с контрольными суммами конфигурационных файлов;
  - файлы с настройками маршрутизации и статическими маршрутами (если такие создавались);
  - другие служебные конфигурационные файлы.
- `connectport` — номер порта, используя который данный узел кластера при работе в пассивном режиме соединяется с активным узлом и принимает от него файлы для резервирования. По умолчанию этот параметр отсутствует и равен значению параметра `port` данной секции.

Внимание! Номер порта, заданный в параметре `connectport`, по умолчанию используется пассивным узлом кластера для проверки доступности сетевых интерфейсов активного узла, поэтому изменять значение этого параметра без явной необходимости не рекомендуется.

- `device` — имя интерфейса синхронизации текущего узла кластера.

Внимание! Запрещено использовать имена дополнительных (alias) или агрегированных (bond) интерфейсов.

- `file` — абсолютный путь к файлу для резервирования. По умолчанию отсутствует. В секции может быть несколько таких параметров, в каждом из которых может быть указан любой файл, который требуется резервировать и который не входит в группы конфигурационных файлов (`config`), файлов справочников и ключей (`keys`) и файлов журналов (`journals`). Размер указанного файла не должен превышать 1 Мбайт, и для его пересылки должно быть достаточно времени, указанного в параметре `sendtime` данной секции.

Примечание. Чтобы выбрать для резервирования не все, а один или несколько файлов, входящих в группы конфигурационных файлов или журналов, установите параметр `config` или `journal` в значение `no` и укажите нужные файлы в параметрах `file`.

- `journals` — включение или выключение резервирования группы файлов журналов ПО ViPNet. Возможные значения: `yes` (по умолчанию) или `no`. В группу входят:
  - файлы журналов IP-пакетов сетевых интерфейсов, кроме интерфейса синхронизации;
  - файлы журнала конвертов транспортного сервера MFTP;
  - другие служебные файлы журналов.
- `keys` — включение или выключение резервирования группы файлов справочников и ключей. Возможные значения: `yes` (по умолчанию) или `no`.

Внимание! Набор файлов, входящих в группы конфигурационных файлов (`config`), файлов справочников и ключей (`keys`) и файлов журналов (`journals`), определяется службой `failoverd` автоматически на активном узле. Пассивный узел в каждом цикле синхронизации запрашивает сначала список файлов, входящих в каждую группу, для которой включено резервирование, и другие файлы для резервирования (`file`), а затем инициирует передачу этих файлов.

Резервирование групп файлов производится только при запущенных на активном узле службах `iplircfg` и `mftpd`, а также если параметры `config`, `keys` и `journal` установлены в значение `yes`. Не рекомендуем отключать резервирование групп файлов, так как это может привести к некорректной работе ПО ViPNet.

- `port` — номер порта, на котором данный узел кластера при работе в активном режиме ожидает соединения от пассивного узла, чтобы передать ему файлы для резервирования. По умолчанию — `10090`.

- `sendtime` — период резервирования файлов, то есть период между попытками пересылки файлов для синхронизации настроек узлов кластера. Указывается в секундах, по умолчанию — `60`.

Файл mftp.conf

Параметры работы транспортного сервера MFTP содержатся в файле `mftp.conf`.

Чтобы отредактировать файл `mftp.conf`:

1. Завершите работу службы `mftpd`:

   ```
   hostname# mftp stop
   ```

2. Откройте файл для редактирования:

   ```
   hostname# mftp config
   ```

3. Внесите изменения.

4. Запустите службу `mftpd`:

   ```
   hostname# mftp start
   ```

Секция [channel]

Секции `[channel]` содержат настройки каналов, по которым ViPNet Coordinator HW может обмениваться данными с другими узлами. Каждому узлу, зарегистрированному за ViPNet Coordinator HW в ViPNet ЦУС или Prime (координатор является сервером IP-адресов), а также каждому координатору, с которым есть межсерверный канал связи, соответствует своя секция `[channel]`.

Внимание! Секции `[channel]` добавляются и удаляются автоматически, делать это вручную не следует.

Секции `[channel]` содержат следующие параметры:

- `type` — тип канала: `mftp`.
- `off_flag` — признак выключения канала. Возможные значения:
  - `no` (по умолчанию) — канал включен. В этом случае попытка передачи конверта по каналу производится немедленно.
  - `yes` — канал выключен. В этом случае исходящие конверты, передаваемые по каналу, остаются в очереди до тех пор, пока канал не будет включен или инициатором соединения по данному каналу не станет удаленный транспортный сервер (координатор). Если инициатором соединения станет удаленный клиент, то предназначенные ему конверты не отправляются, а этому клиенту передается специальная команда, которая выключает соответствующий канал в настройках его транспортного сервера.
- `call_flag` — признак немедленной передачи конвертов по каналу MFTP:
  - `yes` — попытка передачи конверта по каналу производится немедленно (по умолчанию для каналов обмена с координаторами);

- `no` — конверт остается в очереди до тех пор, пока инициатором соединения не станет удаленный узел (по умолчанию для каналов обмена с клиентами).

Примечание. Если параметры `type`, `off_flag`, `call_flag` отсутствуют в секции, то используются их значения по умолчанию.

- `ip` — IP-адрес удаленного сетевого узла. Определяется управляющей службой. Если значение этого параметра по каким-либо причинам не было получено от управляющей службы, то оно будет установлено в `0.0.0.0`. В этом случае его можно задать вручную, а затем перезапустить транспортный сервер. Данный параметр может изменяться в процессе работы.
- `call_timeout` — период опроса удаленного сетевого узла в секундах (время следующего опроса узла отсчитывается с момента разрыва последнего соединения с этим узлом). По умолчанию имеет значение `-1`, то есть опрос не производится. Если параметр `call_timeout` отсутствует, то используется его значение по умолчанию.
- `transit` — идентификатор узла, на который необходимо перенаправлять конверты, отправляемые по данному каналу. Используется для настройки каналов обмена с координаторами при межсетевом взаимодействии и позволяет снизить нагрузку на шлюзовой координатор за счет передачи через него конвертов без обработки транспортным сервером. Задается в шестнадцатеричном формате с префиксом `0x`.

  По умолчанию параметр `transit` отсутствует, и при межсетевом взаимодействии используется значение, заданное в ViPNet ЦУС или Prime. Если параметр указан, изменение значения в ViPNet ЦУС или Prime не учитывается.

Нередактируемые параметры

- `id` — уникальный идентификатор сетевого узла ViPNet, с которым происходит обмен данными по каналу. Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`, например: `id = 0x270e000a`.
- `name` — имя сетевого узла ViPNet, с которым происходит обмен данными по каналу.
- `last_port` — порт, по которому осуществлялось последнее удачное MFTP-соединение. Этот порт будет использоваться при следующей попытке соединения с этим узлом.
- `last_call` — время последней попытки опроса канала.
- `last_err` — время, когда произошла последняя ошибка при попытке соединения или в процессе передачи данных.

Секция [debug]

Секция `[debug]` определяет параметры ведения журнала событий транспортного сервера MFTP и содержит следующие параметры:

- `debuglevel` — уровень важности событий, записываемых в журнал. Возможные значения: от `-1` до `4` (по умолчанию `3`). Чем выше уровень важности, тем более подробная информация записывается в журнал. Значение параметра `-1` выключает ведение журнала (при этом некоторые важные системные события по-прежнему будут выводиться в журнал).

  Уровень важности `4` используется только для диагностики возможных проблем и должен быть включен по рекомендации специалистов ИнфоТеКС. Не задавайте его для постоянного использования.

Внимание! В исполнениях с одним дисковым накопителем:

- По умолчанию уровень важности равен `1`.
- При локальном протоколировании доступны уровни важности от `-1` до `3`.

При удаленном протоколировании доступны уровни важности от `-1` до `4`. При этом если вы используете `4` уровень и выполняете переключение на локальное протоколирование, уровень не изменяется автоматически. Чтобы уровень важности принял значение по умолчанию, перезагрузите транспортный сервер MFTP с помощью команд mftp stop и mftp start.

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (системные службы).
  - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

  Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

Секция [journal]

Секция `[journal]` содержит параметры настройки журнала MFTP-конвертов, обрабатываемых транспортным сервером. В процессе работы транспортный сервер записывает в этот журнал информацию о полностью принятых, отправленных, удаленных и поврежденных конвертах.

Секция `[journal]` содержит следующие параметры:

- `dump_interval` — период выгрузки информации из журнала конвертов в днях. В процессе работы транспортный сервер записывает информацию об обработанных конвертах в текстовый файл. По истечении периода времени, заданного данным параметром, создается новый файл, в имени которого содержится текущая дата. По умолчанию каждый день создается новый файл (`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. Допустимые значения:

- 1—100 Мбайт для однодисковых исполнений;
- 1—500 Мбайт для остальных.

Внимание! Не рекомендуется задавать размер журнала более чем 100 мегабайт, так как при превышении этого значения могут возникнуть проблемы с просмотром журнала конвертов в веб-интерфейсе.

- `use_journal` — включение или выключение ведения журнала работы транспортного сервера. Возможные значения: `yes` (по умолчанию) или `no`.
- `max_log_space` — максимальный объем дискового пространства доступного для хранения текстовых файлов, в которые выгружается информация из журнала конвертов в мегабайтах (по умолчанию — `100`). Если суммарный размер всех файлов превышает значение этого параметра, то удаляются файлы, записанные раньше других. Допустимые значения:
  - 1—500 Мбайт для однодисковых исполнений;
  - 1—2500 Мбайт для остальных.

  Рекомендуем устанавливать значение параметра в 5 раз больше, чем значение параметра `max_size`. Тогда количество записей журнала конвертов в веб-интерфейсе и командном интерпретаторе не будут отличаться.

Примечание. Если параметры `dump_interval`, `max_size`, `use_journal`, `max_log_space` отсутствуют в секции, то используются их значения по умолчанию.

Нередактируемые параметры

- `dump_filename` — префикс имени текстового файла, в который регулярно выгружается информация из журнала конвертов. 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: `/var/log/mftpenv.log.2024.09.23`.
- `last_dump` — время последней выгрузки информации из журнала конвертов.

Секция [misc]

Секция `[misc]` содержит различные параметры, определяющие работу транспортного сервера MFTP в целом:

- `connect_timeout` — интервал времени в секундах, в течение которого клиент будет пытаться установить соединение с удаленным узлом по каналу MFTP (от `2` до `300`, по умолчанию — `5`). Если по истечении этого времени соединение не установлено, то повторные попытки

соединения будут производиться по истечении времени, указанного в параметре `outenv_timeout` данной секции.

- `max_connections` — максимальное количество входящих и исходящих соединений по каналам MFTP (от `1` до `1000`, по умолчанию — `900`).
- `max_listen_ports` — диапазон значений перебора портов для соединений по каналу MFTP с удаленным узлом в случае неудачи (от `1` до `10`, по умолчанию — `3`). Транспортный сервер циклично перебирает порты в диапазоне от `port` до `port+max_listen_ports-1`. Ожидая входящие соединения, транспортный сервер прослушивает все порты указанного диапазона.
- `num_attempts` — количество последовательных попыток соединения, после которых устанавливается тайм-аут, если соединиться так и не удалось (от `1` до `10`, по умолчанию — `3`).
- `outenv_timeout` — интервал времени в секундах, в течение которого исходящие конверты для канала, на котором произошла ошибка передачи, не могут быть повторно отправлены (от `5` до `600`, по умолчанию — `300`). Если на каком-либо канале произошла ошибка передачи (например, из-за разрыва соединения) и для этого канала существуют исходящие конверты, то следующая попытка передачи произойдет по истечении времени, указанного в параметре `outenv_timeout`.
- `pingpong` — включение или выключение режима поочередного обмена конвертами по каналу MFTP:
  - `yes` (по умолчанию) — сторона, передавшая конверт, позволяет передать конверт другой стороне, то есть узлы обмениваются конвертами поочередно;
  - `no` — сторона, начавшая передавать конверты, будет их передавать, пока они не закончатся, и только после этого позволит передавать конверты другой стороне.
- `port` — порт, на котором служба `mftpd` ожидает соединения по каналу MFTP от удаленных сетевых узлов (от `1` до `65535`, по умолчанию — `5000`).
- `recv_buff_size` — размер буфера приема в байтах. Параметр имеет нередактируемое значение `65500`.
- `send_buff_size` — размер буфера передачи в байтах. Параметр имеет нередактируемое значение `65500`.

Примечание. Обычно значение `65500` параметров `send_buff_size` и `recv_buff_size` оптимально для обеспечения максимальной скорости приема и передачи конвертов транспортным сервером.

- `save_sent` — включение или выключение хранения имен отправленных прикладных конвертов:
  - `no` (по умолчанию) — имена отправленных конвертов не сохраняются;
  - `yes` — при успешной отправке конверта в подкаталоге `sent` каталога, указанного в параметре `out_path` секции `[transport]`, создается файл нулевой длины с именем отправленного конверта.

- `ttl_ctl` — время жизни конвертов, содержащих управляющие запросы, в исходящей очереди. Указывается в днях, возможные значения от `10` до `90`, значение по умолчанию — `10`. Если по истечении времени, указанного в параметре `ttl_ctl`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.
- `ttl_invalid` — время хранения заблокированных конвертов. В список заблокированных конвертов попадают все незашифрованные конверты, а также конверты, не прошедшие проверку подлинности. Указывается в днях. Возможные значения от `0` до `90`, значение по умолчанию — `30`. По истечении указанного времени конверт удаляется. При значении `0` заблокированные конверты удаляются сразу.
- `ttl_out` — время хранения конвертов в исходящей очереди в днях, возможные значения от `10` до `90`, значение по умолчанию — `30`. Если по истечении времени, указанного в параметре `ttl_out`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.
- `ttl_trash` — время хранения конвертов в корзине в днях, возможные значения от `10` до `90`, значение по умолчанию — `90`. Если время хранения конверта в корзине превышает указанное в параметре `ttl_trash`, то он удаляется.
- `wait_timeout` — время ожидания активности в установленном MFTP-соединении. Указывается в секундах, возможные значения от `3` до `300`, значение по умолчанию — `30`. Если в течение этого времени узлы, установившие соединение, не обменялись никакой информацией, то данное соединение закрывается. Если в процессе обмена исходящие конверты для удаленного узла были переданы не полностью, то повторные попытки соединения будут происходить по истечении времени, указанного в параметре `outenv_timeout`.
- `task_envelope_limit` — минимальный размер свободного места на диске для приема прикладных конвертов (деловая почта, файловый обмен). Значение параметра указывается в процентах от общего размера диска (от `0` до `20`), значение по умолчанию — `20`. Если процент свободного места на диске станет ниже заданного значения, конверты от сетевых узлов приниматься не будут.
- `control_envelope_limit` — минимальный размер свободного места на диске для приема управляющих конвертов (квитанции, обновление ПО, криптографическая информация, политики). Значение параметра указывается в процентах от общего размера диска (от `0` до `10`), значение по умолчанию — `10`. Если процент свободного места на диске станет ниже заданного значения, конверты от сетевых узлов приниматься не будут.
- `remote_net_route` — включение или выключение использования прямой маршрутизации между сетями ViPNet:
  - `yes` (по умолчанию) — при настройке перенаправления конвертов с помощью параметра `transit` в секции `[channel]` шлюзовые координаторы не будут обрабатывать конверты, передаваемые между сетями ViPNet;
  - `no` — все настройки прямой маршрутизации будут сброшены, и обрабатывать конверты будут шлюзовые координаторы. При последующем включении использования прямой маршрутизации потребуется повторная настройка обхода шлюзовых координаторов.

Секция [reserv]

Секция `[reserv]` содержит параметры настройки транспортного сервера MFTP на координаторе, работающем в составе кластера:

- `cmd_port` — порт, на котором служба `mftpd` пассивного узла ожидает соединений с активным узлом через интерфейс синхронизации для приема управляющих команд (по умолчанию — `6084`). Данный параметр должен иметь одинаковое значение в файлах конфигурации транспортного сервера на «активном» и «пассивном» координаторах.
- `unpack_timeout` — период времени в секундах, в течение которого активный узел будет ожидать ответы на команды от пассивного узла, и в случае отсутствия ответов повторять команды (по умолчанию — `60`). Этот параметр используется системой удаленного обновления ПО. Он также определяет период сканирования каталога, заданного параметром `upgrade_path` секции `[upgrade]`, для анализа состояния процесса обновления ПО.
- `transfer_timeout` — период времени в секундах, в течение которого активный узел будет пытаться передавать копии MFTP-конверта пассивному узлу в случае неполного дублирования данного конверта (по умолчанию — `60`). В течение этого времени обработка конверта на активном узле блокируется. Если по истечении этого времени конверт не будет передан на пассивный узел, то его обработка продолжится.
- `use_reserv` — включение или выключение режима резервирования конвертов в кластере:
  - `yes` (по умолчанию) — конверты резервируются;
  - `no` — резервирование конвертов не производится. В этом случае синхронизировать данные и обновление ПО на узлах кластера необходимо вручную. Кроме того, для корректной работы кластера настройки узлов кластера должны быть одинаковы.

  При частом переключении режимов на пассивном узле могут сохраняться файлы устаревших обновлений. Файлы будут удалены при переключении узла кластера в активный режим или через промежуток времени, указанный в параметре `ttl_ctl` секции `[misc]`.

Секция [transport]

Секция `[transport]` содержит ряд параметров, определяющих пути к транспортным каталогам, то есть к каталогам, участвующим в обмене конвертами и их обработке. Эти параметры задают лишь основные каталоги. Вспомогательные каталоги создаются транспортным сервером MFTP в процессе работы как подкаталоги основных. При создании конфигурационного файла значения параметров этой секции определены по умолчанию относительно каталога, содержащего справочники и ключи.

Примечание. Транспортный сервер MFTP при каждом запуске проверяет наличие каталогов, заданных параметрами секции `[transport]`, и при необходимости создает их.

Секция `[transport]` содержит следующие параметры:

- `in_path` — абсолютный путь к каталогу, в который помещаются полностью принятые конверты (по умолчанию — `/opt/vipnet/in`).
- `out_path` — абсолютный путь к каталогу, в который внешние приложения помещают сформированные конверты для отправки (по умолчанию — `/opt/vipnet/out`).
- `trash_path` — абсолютный путь к каталогу, в который помещаются устаревшие конверты из очереди исходящих конвертов — так называемая «корзина» (по умолчанию — `/opt/vipnet/trash`).
- `local_path` — абсолютный путь к каталогу, в который помещаются прикладные конверты, предназначенные для передачи по локальному каналу другим узлам сети ViPNet (по умолчанию — `/opt/vipnet/local`). Данный параметр не используется в ViPNet Coordinator HW.
- `app_in_path` — абсолютный путь к каталогу, в который помещаются файлы, полученные от других узлов сети ViPNet (по умолчанию — `/opt/vipnet/in/app`). Данный параметр не используется в ViPNet Coordinator HW.

Секция [upgrade]

Данная секция содержит параметры, которые определяют поведение транспортного сервера MFTP при приеме обновлений ПО ViPNet из ViPNet ЦУС или Prime:

- `confsave` — тип конфигурации, автоматически создаваемой перед обновлением:
  - `partial` (по умолчанию) — частичная конфигурация, включающая только конфигурационные файлы (без справочников и ключей).
  - `full` — полная конфигурация, включающая конфигурационные файлы, справочники и ключи.
  - `off` — конфигурация не создается автоматически.
- `maxautosaves` — максимальное число автоматически сохраненных конфигураций. Возможные значения: от 1 до 10. Значение по умолчанию — `10`. Перед автоматическим созданием очередной конфигурации проверяется число ранее сохраненных конфигураций. Если это число равно значению `maxautosaves`, то конфигурация, созданная раньше остальных, удаляется, после чего сохраняется текущая конфигурация.
- `upgrade_checktimeout` — период проверки транспортного каталога, заданного параметром `upgrade_path`, на наличие файлов обновления программного обеспечения. Указывается в секундах, значение по умолчанию — `300`. В случае соответствия обнаруженных файлов обновления (время обновления и так далее) вызывается модуль обновления.
- `upgrade_for_kc_path` — абсолютный путь к каталогу, в который внешние приложения помещают файлы `*.sok` с запросами на сертификаты (по умолчанию — `/opt/vipnet/ccc/for_kc`).
- `upgrade_ini` — имя конфигурационного файла для процесса обновления (по умолчанию — `/opt/vipnet/user/upgrade.conf`).

- `upgrade_path` — абсолютный путь к каталогу, в который помещаются файлы обновления программного обеспечения после распаковки соответствующих конвертов (по умолчанию — `/opt/vipnet/ccc`).

A

Термины и сокращения

CEF (Common Event Format)

Открытый текстовый формат описания событий. Позволяет агрегировать события различных типов сетевых устройств и приложений в едином формате.

DGD (Dead Gateway Detection)

Технология проверки доступности шлюза путем отправки эхо-запросов через определенный промежуток времени. Если в течение определенного времени ответ не поступил, считается, что данный шлюз недоступен. Данная технология может определять политику маршрутизации в зависимости от доступности шлюзов.

ICAP

Протокол для расширения функциональности прокси-серверов. Чаще всего используется для внедрения функций антивирусной проверки и контентной фильтрации трафика, проходящего через прокси-сервер.

ICAP-сервер

Сервер, выполняющий обработку трафика по протоколу ICAP.

IP-форвардинг

IP-форвардинг или маршрутизация транзитных IP-пакетов (не предназначенных для этого компьютера), является опциональной возможностью стека протоколов TCP/IP в операционной системе GNU/Linux. Данная функция обеспечивает пересылку транзитных IP-пакетов через сетевые интерфейсы компьютера.

L2OverIP

Технология, которая позволяет организовать защиту удаленных сегментов сети, использующих одно и то же адресное пространство, на канальном уровне модели OSI. В результате узлы из разных сегментов сети смогут взаимодействовать друг с другом в одном широковещательном домене. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой.

MIME-тип

Тип данных, которые могут быть переданы с помощью интернета с применением стандарта MIME.

MTU (Maximum Transmission Unit)

Максимальный размер полезного блока данных одного пакета, который может быть передан протоколом через сетевой интерфейс без фрагментации.

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.

PPP (Point-to-Point Protocol)

Протокол канального уровня, использующийся для установления прямой связи между двумя узлами сети.

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, со своим сервером соединений, а затем и с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг интернета.

TCP-туннель настраивается на координаторе, который является для клиента сервером соединений.

ViPNet Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задает связи между ними.

- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в нее устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

VLAN

Виртуальная локальная компьютерная сеть, представляет собой группу сетевых узлов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к 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.

Автономная система

Один или несколько сегментов сети, в которых выполняется маршрутизация по одному протоколу (OSPF, IGRP, EIGRP, IS-IS, RIP, BGP, Static). Также может трактоваться как домен маршрутизации — группа маршрутизаторов сети, работающих по одинаковым протоколам маршрутизации.

Административная дистанция

Характеристика маршрута. Позволяет определить меру доверия к маршруту. Задается для любого маршрута в виде целого числа в диапазоне от 1 до 255.

Адреса видимости

IP-адреса, виртуальные или реальные, по которым данный узел видит остальные узлы сети ViPNet и по которым приложения отправляют свой трафик.

Адреса доступа

IP-адреса, по которым узел доступен в сети (например, адреса межсетевого экрана, за которым он находится).

Антиспуфинг

Защита от спуфинг-атак, при которых злоумышленник подделывает адрес источника для обхода межсетевых экранов и организации DoS-атак (от англ. Denial of Service, отказ в обслуживании).

Базовый виртуальный адрес

Является точкой отсчета при назначении виртуальных адресов для каждого из реальных адресов узла. Если в данный момент узел виден по виртуальному адресу, его адресом доступа считается либо базовый виртуальный адрес, либо вторичный виртуальный адрес, соответствующий первому в списке реальному адресу.

Вес

Параметр, который задается для шлюза в статическом маршруте в виде целого числа в диапазоне от 1 до 255. Позволяет настроить балансировку IP-трафика между шлюзами в одинаковый адрес назначения. Определяет долю IP-трафика, который должен передаваться по маршруту на указанный шлюз.

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если сетевые узлы ViPNet работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

Внешние IP-адреса

Адреса внешней сети.

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

Динамический сетевой интерфейс

Разновидность сетевого интерфейса, который добавляется в процессе работы при наступлении некоторого события (например, при подключении встроенного или USB-модема, предоставляющего данный интерфейс).

Динамические интерфейсы объединяются в группы по типу интерфейса. Поэтому иногда может встречаться термин «групповой динамический интерфейс».

Существуют следующие группы динамических интерфейсов:

- `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
- `pppoe` — группа интерфейсов для подключения к сети провайдера по PPPoE;
- `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi с помощью внешних адаптеров Wi-Fi. В эту группу не входит встроенный интерфейс `wlan0` (для исполнений ПАК со встроенным модулем Wi-Fi).

Дуплекс

Способ связи, при котором сетевой интерфейс может одновременно и передавать, и принимать информацию.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Инкапсуляция пакетов

Принцип передачи данных, при котором данные в формате одного протокола упаковываются в формат другого протокола.

Источник бесперебойного питания (ИБП)

Автоматическое электронное устройство с аккумуляторной батареей, предназначенное для бесперебойного кратковременного снабжения электрической энергией с целью корректного завершения работы и сохранения данных в случае резкого падения или отсутствия входного питающего напряжения системы.

Класс сетевого интерфейса

Признак, определяющий назначение сетевого интерфейса. В ViPNet Coordinator HW интерфейсам можно назначить следующие классы: `access`, `trunk`, `slave`.

По умолчанию сетевому интерфейсу назначен класс `access`. Если требуется, чтобы интерфейс Ethernet или агрегированный интерфейс обрабатывал трафик из нескольких VLAN, ему необходимо назначить класс `trunk`. Чтобы объединить несколько интерфейсов Ethernet в агрегированный интерфейс, каждому из таких интерфейсов необходимо предварительно назначить класс `slave`.

Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных ViPNet Coordinator HW, один из которых (активный) выполняет функции координатора сети ViPNet, а другой (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet Coordinator HW на активном ViPNet Coordinator HW, пассивный ViPNet Coordinator HW переключается в активный режим для выполнения функций. При этом сбойный ViPNet Coordinator HW перезагружается и становится пассивным.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключи 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 HW с помощью ряда специальных команд.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

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 преобразует внутренние IP-адреса в адреса, доступные из внешней сети (выполняет NAT).

Метрика адреса доступа

Определяет задержку (в миллисекундах) отправки тестовых пакетов при выполнении опроса узла для определения доступности адреса. Предназначена для задания приоритета использования каналов связи.

Метрика маршрута

Параметр, определяющий приоритет маршрута передачи IP-трафика.

Область маршрутизации

Одна или несколько IP-сетей, в которых происходит обмен информацией по определенному протоколу, в частности, по протоколу OSPF.

Протокол OSPF рассматривает межсетевую среду как множество областей, соединенных друг с другом через некоторую базовую область (backbone area). Для идентификации областей каждой из них выделяется специальный идентификатор (area ID), представляющий собой целое число в десятичном формате.

Перераспределение маршрутов

Обмен маршрутной информацией между двумя различными маршрутизирующими протоколами.

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте.

Полудуплекс

Способ связи, при котором сетевой интерфейс в один момент времени может только передавать или только принимать информацию.

Прикладная квитанция

Файл, оповещающий отправителя о доставке и (или) прочтении прикладного конверта.

Прикладной конверт

Файл, формируемый приложениями ViPNet (например, «Деловая почта», «Файловый обмен») для передачи другим сетевым узлам.

Прозрачный режим работы прокси-сервера

Режим работы, при котором не требуется выполнять настройку программного обеспечения на рабочих местах пользователей, подключающихся к интернету через прокси-сервер.

Прокси-сервер

Программа, транслирующая соединения по некоторым протоколам из внутренней сети во внешнюю и выступающая при этом как посредник между клиентами и сервером.

Реальный IP-адрес

IP-адрес, назначенный сетевому интерфейсу компьютера в локальной сети или интернете.

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ создает для пользователя. Имя этого файла имеет маску `AAAA.pk`, где `AAAA` — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервер соединений для клиента также является сервером IP-адресов.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер принимает и передаёт IP-пакеты. Физическим интерфейсом может служить сетевая плата, модем и другие подобные устройства, виртуальным — агрегированный интерфейс, интерфейс для VLAN.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Сетевой фильтр

Совокупность параметров, на основании которых сетевой экран программного обеспечения ViPNet пропускает или блокирует IP-пакет.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Статический сетевой интерфейс

Сетевой интерфейс, для работы которого требуется задать секцию `[adapter]` в файле `iplir.conf` с описанием параметров этого интерфейса. К таким интерфейсам относятся физические (Ethernet) и виртуальные (VLAN) интерфейсы.

Стоимость маршрута

Количество издержек, которые возникнут при отправке IP-пакета в сеть назначения через тот или иной шлюз. Стоимость маршрута обратно пропорциональна его пропускной способности канала связи.

Таблица маршрутизации

Таблица, согласно которой происходит процесс выбора пути для передачи данных в сети.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки транспортного конверта MFTP.

Транспортный сервер MFTP

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.

Файл подкачки

Файл подкачки представляет собой дополнительную виртуальную память, которая позволяет увеличить объем памяти, доступной для использования на компьютере.

Фильтрация содержимого трафика

Функция прокси-сервера ViPNet Coordinator HW, позволяющая фильтровать трафик по MIME-типу содержимого и методам протокола HTTP.

Шлюзовой координатор

Координатор, через который происходит обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие. Шлюзовые координаторы назначаются в ViPNet ЦУС или Prime каждой сети при организации взаимодействия между двумя различными сетями ViPNet.