ViPNet Coordinator HW 4

Справочное руководство по конфигурационным файлам

infotecs

ФРКЕ.00130-03 90 07

ОАО «ИнфоТеКС»

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

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

Сайт компании «ИнфоТеКС»: http://www.infotecs.ru

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В данном документе приведено подробное описание параметров следующих конфигурационных файлов ViPNet Coordinator HW:

- `iplir.conf` — конфигурационный файл управляющего демона (см. «Файл iplir.conf» на стр. 8).
- `iplir.conf-<интерфейс или группа интерфейсов>` — конфигурационные файлы сетевых интерфейсов ViPNet Coordinator HW (см. «Файл iplir.conf-<интерфейс или группа интерфейсов>» на стр. 22).
- `failover.ini` — конфигурационный файл системы защиты от сбоев (см. «Файл failover.ini» на стр. 25).
- `mftp.conf` — конфигурационный файл транспортного модуля MFTP (см. «Файл mftp.conf» на стр. 32).

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

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

Таблица 1. Обозначения, используемые в примечаниях

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

Таблица 2. Обозначения, используемые для выделения информации в тексте

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

Обратная связь

Дополнительная информация

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

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet http://www.infotecs.ru/products/line/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Регистрация продуктов и консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6196,

  8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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

Файл iplir.conf

Параметры защищенной сети ViPNet (см. глоссарий, стр. 44) содержатся в файле `iplir.conf`. Для редактирования этого файла используется команда `iplir config`. Перед редактированием файла `iplir.conf` необходимо завершить работу управляющего демона командой `iplir stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его командой `iplir start`.

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

Секция [adapter]

Секции `[adapter]` описывают статические сетевые интерфейсы компьютера (см. глоссарий, стр. 44). Каждому интерфейсу соответствует своя секция `[adapter]`. Если статический интерфейс не описан секцией `[adapter]`, то все проходящие через него IP-пакеты (см. глоссарий, стр. 41) блокируются.

Примечание. В процессе работы ViPNet Coordinator HW могут создаваться динамические интерфейсы (см. глоссарий, стр. 42), например, при подключении ViPNet Coordinator HW к сети 3G, 4G или WiFi. В ViPNet Coordinator HW по умолчанию разрешена работа динамических интерфейсов, которые входят в одну из следующих групп интерфейсов:

- `ppp` — группа интерфейсов для встроенных модемов;
- `wifi` — группа интерфейсов для WiFi.

Добавление интерфейсов данных групп в файл `iplir.conf` не требуется.

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

В процессе работы управляющий демон и драйвер ViPNet периодически получают информацию о параметрах известных им интерфейсов с интервалом времени, заданным параметром `ifcheck_timeout` секции `[misc]` (см. «Секция [misc]» на стр. 16). Если обнаруживается, что интерфейс выключен в системе, то он выключается и в драйвере ViPNet. После включения или изменения IP-адреса интерфейса эти изменения автоматически загружаются в драйвер ViPNet.

В секции `[adapter]` указываются следующие параметры:

- `allowtraffic` — разрешение или блокирование прохождения IP-трафика через интерфейс. Возможные значения:

- `on` (по умолчанию) — IP-пакеты пропускаются или блокируются в соответствии с сетевыми фильтрами, заданными на узле.
- `off` – IP-пакеты блокируются независимо от остальных настроек.

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

  Тип интерфейса выбирается, исходя из следующего:

  - Если ViPNet Coordinator 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 (см. глоссарий, стр. 42)), то интерфейсу, посредством которого ViPNet Coordinator HW будет связываться с узлом, выполняющим функции межсетевого экрана (см. глоссарий, стр. 43), следует назначить тип `external`, остальным интерфейсам ViPNet Coordinator HW — тип `internal`.

Нередактируемые параметры секции [adapter]

- `name` — системное имя интерфейса (например, eth0). Если в системе задано несколько IP-адресов на одном интерфейсе и присутствуют один или несколько виртуальных интерфейсов (eth0:0, eth0:1 и так далее), то для управляющего демона и драйвера ViPNet все они будут представлять одно физическое устройство с базовым именем (eth0).

Секция [debug]

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

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

  

  Внимание! В исполнениях с одним дисковым накопителем (HW50 N1, N2, N3 и HW100 X1, X8) по умолчанию уровень детализации равен 1.

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:

  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы), `mail` (почтовая система) или `daemon` (демоны).
  - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

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

Секция [dynamic]

Секция `[dynamic]` содержит параметры для настройки режима подключения к внешней сети через межсетевой экран с динамической трансляцией адресов:

- `always_use_server` — включение или выключение режима, при котором весь трафик с внешними узлами направляется через сервер соединений (см. глоссарий, стр. 44), 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.

Нередактируемые параметры секции [dynamic]

- `firewallip` — внешний IP-адрес доступа (см. глоссарий, стр. 42) к ViPNet Coordinator HW, работающему в режиме «С динамической трансляцией адресов», со стороны других сетевых узлов.
- `port` — порт назначения, на который следует посылать пакеты для ViPNet Coordinator HW, работающего в режиме «С динамической трансляцией адресов».

Секция [id]

Секция `[id]` используется для описания адресных настроек защищенных сетевых узлов (см. глоссарий, стр. 45), связанных с ViPNet Coordinator HW. Каждому узлу, с которым у ViPNet Coordinator HW есть связь, соответствует своя секция `[id]`. Первая секция `[id]` соответствует собственным настройкам ViPNet Coordinator HW (собственная секция).

Секция [id] содержит следующие параметры:

- accessiplist — определяет IP-адреса доступа (см. глоссарий, стр. 42) 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 при запуске управляющего демона.

  - <IP-адрес доступа> — IP-адрес доступа к узлу. Принимает значение 0.0.0.0, когда данный узел не находится за межсетевым экраном.
  - <метрика> — метрика (см. глоссарий, стр. 43) указанного адреса доступа. Метрика определяет задержку (в миллисекундах) отправки служебных сообщений при выполнении процедуры определения адреса доступа узла. Опросы осуществляются периодически (см. параметры server_pollinterval и client_pollinterval секции [misc] (см. «Секция [misc]» на стр. 16)). Возможные значения: от 0 до 9999. По умолчанию метрика имеет значение auto, то есть определяется автоматически.
  - <реальный IP-адрес узла> — реальный IP-адрес узла, соответствующий сетевому интерфейсу (см. глоссарий, стр. 44), через который будут передаваться IP-пакеты для выбранного IP-адреса доступа.
  - <номер интерфейса> — условный номер сетевого интерфейса. Возможные значения: от 0 до 255.
  - <тип регистрации> — тип регистрации данного IP-адреса доступа узла. Возможные значения:
    - auto — адрес задан ViPNet Coordinator HW.
    - manual — адрес задан администратором вручную (редактированием файла iplir.conf).
    - addrdoc — адрес взят из справочников, полученных из программы ViPNet Центр управления сетью (см. глоссарий, стр. 41).
    - other — адрес добавлен другим способом (например, в качестве адреса доступа добавлен координатор, выбранный внешним межсетевым экраном).
- blockforward — включение или выключение блокирования транзитных пакетов, идущих через узел. Используется в секциях, описывающих настройки координаторов, связанных с

ViPNet Coordinator HW. Возможные значения: `off` — все транзитные пакеты на координаторе пропускаются, `on` — все транзитные пакеты на координаторе блокируются с кодом 70. По умолчанию данный параметр отсутствует, что эквивалентно значению `off`.

- `checkconnection_interval` — период автоматической отправки координатором сообщения другому связанному с ним координатору для оперативного определения недоступности этого координатора по текущему адресу доступа и попытки подключения к нему по альтернативному каналу доступа. Указывается в секундах, возможные значения: от `20` до `3600`. Если данный параметр не указан в секции `[id]` координатора, то автоматическая проверка связи с ним не производится.
- `fixfirewall` — определяет режим фиксации настроек работы собственного узла через внешний межсетевой экран. Возможные значения:
  - `off` (по умолчанию) — внешний IP-адрес и порт доступа к ViPNet Coordinator HW определяются автоматически по информации от узлов внешней сети;
  - `on` — внешний IP-адрес и порт доступа к ViPNet Coordinator HW жестко заданы администратором в параметрах `firewallip` и `port` данной секции.
- `ip` — содержит реальный IP-адрес (см. глоссарий, стр. 43) и соответствующий ему виртуальный IP-адрес (см. глоссарий, стр. 42) узла. Причем первым указывается реальный адрес, затем после запятой — виртуальный (например: `ip = 192.168.201.10,10.1.0.5)`. Если указан только реальный адрес, то считается, что ему еще не сопоставлен виртуальный.

  Если узел имеет несколько сетевых интерфейсов или несколько IP-адресов на интерфейсе, в каждой секции `[id]` может быть несколько параметров `ip`. При этом первым должен быть указан параметр, содержащий наиболее приоритетный IP-адрес доступа к данному узлу. При автоматическом обновлении адресов наиболее приоритетный IP-адрес доступа становится первым автоматически. Причем в случае изменения порядка следования IP-адресов виртуальный адрес всегда перемещается вместе с соответствующим реальным.
- `port` — определяет порт назначения, на который следует посылать пакеты для узла, если этот узел находится за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр.
- `proxyid` — определяет режим работы узла, находящегося за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр. Возможные значения:
  - в собственной секции `[id]`:
    - `0xfffffffe` — при работе в режиме «С динамической трансляцией адресов» (если в секции `[dynamic]` параметр `dynamic_proxy` установлен в `on` (см. «Секция [dynamic]» на стр. 10));
    - `0` — при работе в режиме «Со статической трансляцией адресов» (если в собственной секции `[id]` параметр `usefirewall` установлен в `on`);
    - идентификатор координатора, через который осуществляется 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`.

  - 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 (см. глоссарий, стр. 44) 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` — номер порта координатора для входящих соединений по протоколу TCP (см. глоссарий, стр. 41). Возможные значения: от 0 до 65535. По умолчанию данный параметр отсутствует в секции и для входящих соединений по протоколу TCP используется порт 80 (см. параметр `tcptunnel_establish` секции `[misc]` (см. «Секция [misc]» на стр. 16)).

  Если параметр задан, то он автоматически рассылается на клиенты, для которых данный координатор служит сервером соединений.

  Примечание. Если порт 80 используется какой-либо службой, в параметре `tcptunnelport` рекомендуется указать другой порт. В противном случае TCP-туннель будет выключен.

- `tunnel` — содержит адреса незащищенных компьютеров, туннелируемых ViPNet Coordinator HW (указаны в собственной секции) или другими координаторами (см. глоссарий, стр. 45), в виде: `<ip1>-<ip2> to <ip3>-<ip4>`, где:

  - `<ip1>-<ip2>` — начальный и конечный реальные адреса диапазона туннелируемых узлов;
  - `<ip3>-<ip4>` — диапазон виртуальных адресов, которые соответствуют реальным адресам из диапазона `<ip1>-<ip2>`, и которые будут использоваться вместо реальных адресов туннелируемых узлов, если на узле, который к ним обращается, настроена видимость по виртуальным адресам. Например, в случае, когда адреса из диапазона `<ip1>-<ip2>` относятся к частной 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]» на стр. 16), который может принимать одно из двух значений:

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

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

    ```
    tunnel = 192.168.0.1-192.168.0.100
    ```

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

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

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

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

Внимание! В зависимости от значения параметра `tunnel_virt_assignment` секции [misc] (см. «Секция [misc]» на стр. 16), настройки параметра `tunnel` действуют следующим образом:

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

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

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

  ```
  exclude_from_tunnels = 192.168.201.7-192.168.201.7
  ```

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

- `tunnelvisibility` — позволяет настроить тип видимости для всех узлов, туннелируемых координатором. Возможные значения:

  - `real` — всегда обращаться к туннелируемым узлам по их реальным адресам;
  - `virtual` — всегда обращаться к туннелируемым узлам по их виртуальным адресам.

  При обновлении ViPNet Coordinator HW до версии 4.2.x и выше проверяется файл `iplir.conf` и в случае, если в нем есть назначенные виртуальные адреса, отличные от реальных, то присваивается значение `virtual`. Значение данного параметра по умолчанию определяется параметром `tunneldefault` секции `[visibility]` (см. «Секция [visibility]» на стр. 20).

- `usetunnel` — используется в любой секции `[id]`, кроме собственной. Включает или выключает туннелирование незащищенных узлов координатором. Возможные значения: `on` (по умолчанию) или `off`. Если этот параметр на координаторе имеет значение `off`, то при соединении ViPNet Coordinator HW с узлами, которые туннелирует данный координатор, трафик шифроваться не будет.

- `usefirewall` — может принимать значение `on` или `off` и используется в секциях `[id]` в следующих целях:
  - Во всех секциях `[id]`, кроме собственной, — указывает на использование настроек работы через межсетевой экран с данным узлом. Если этот параметр имеет значение `off`, то параметры `firewallip`, `port` и `proxyid` в этой секции игнорируются, и работа с данным узлом будет возможна только по одному из его реальных IP-адресов.
  - В собственной секции `[id]` — указывает на использование внешнего межсетевого экрана. В случае если межсетевой экран использоваться не будет, он установлен в значение `off`, в остальных случаях — в значение `on` (см. описание параметра `proxyid` данной секции).
- `visibility` — позволяет настроить тип видимости узла. Возможные значения:
  - `auto` — автоматически определять тип видимости узла, в зависимости от текущего адреса видимости узла (см. глоссарий, стр. 41).
  - `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]» на стр. 20), 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 секции [id]

- `accessip` — текущий IP-адрес доступа к узлу (см. глоссарий, стр. 42) 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 управляющий демон отличает одну секцию `[id]` от другой. Идентификатор присваивается сетевому узлу ViPNet при его

создании в программе ViPNet Центр управления сетью (см. глоссарий, стр. 41). В каждой секции `[id]` может быть только один такой параметр.

- `firewallip` — определяет внешний IP-адрес доступа к узлу в случае, если этот узел находится за межсетевым экраном. При работе с узлом, установленным за межсетевым экраном, все направленные к нему зашифрованные пакеты инкапсулируются (см. глоссарий, стр. 43) 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 имеет значение `0.0.0.0`. В каждой секции `[id]` может быть только один такой параметр.
- `name` — имя узла. Задается администратором сети ViPNet в программе ViPNet Центр управления сетью и предназначен для удобства настройки. Данный параметр записывается в файл конфигурации автоматически при его сохранении. В каждой секции `[id]` может быть только один такой параметр.
- `virtualip` — базовый виртуальный адрес узла. В каждой секции `[id]` может быть только один такой параметр.

Секция [misc]

Секция `[misc]` содержит различные дополнительные параметры:

- `ciphertype` — алгоритм шифрования исходящих пакетов, адресованных сетевым узлам ViPNet. Может принимать только значение `gost` (шифрование с помощью алгоритма ГОСТ).
- `client_pollinterval` — период опроса координатора ViPNet Coordinator HW клиентами (см. глоссарий, стр. 43), для которых этот координатор выполняет функцию сервера IP-адресов. Значение этого параметра координатор сообщается своим клиентам в каждом сеансе работы. Если от какого-либо клиента, который должен обмениваться пакетами с координатором, не было получено никаких служебных пакетов в течение времени, указанного в данном параметре, то такому клиенту посылается специальный пакет, на который должен прийти ответ. Если ответ не приходит, то узел клиента считается недоступным (выключенным). Указывается в секундах, значение по умолчанию — `300` (5 минут). Уменьшение значения данного параметра позволяет более оперативно определять неработоспособность узла, но повышает объем служебного трафика.
- `config_version` — версия конфигурационного файла (совпадает с версией ViPNet Coordinator HW, с помощью которой файл последний раз был сохранен).
- `ifcheck_timeout` — период опроса параметров сетевых интерфейсов, известных управляющему демону. Указывается в секундах, значение по умолчанию — `5`.
- `iscaggregate` — включение или выключение накопления служебного трафика, обрабатываемого на координаторе. 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 объем служебного трафика увеличивается.

- `ipforwarding` — управление IP-форвардингом (маршрутизацией транзитных IP-пакетов через координатор ViPNet Coordinator HW). Возможные значения:
  - `on` — включать IP-форвардинг (см. глоссарий, стр. 41) при запуске управляющего демона;
  - `off` — выключать IP-форвардинг при запуске управляющего демона;
  - `system` — не изменять текущие настройки IP-форвардинга при запуске управляющего демона.

Примечание. При выключенном IP-форвардинге не работают пересылка транзитных IP-пакетов и туннелирование, поэтому рекомендуется устанавливать параметр `ipforwarding` в значение `on`. Значения `off` и `system` рекомендуется использовать только при отладке.

- `msg_compress_level` — степень сжатия служебных межсерверных сообщений. Возможные значения: от 1 (минимальное сжатие, максимальная скорость) до 9 (максимальное сжатие, минимальный объем служебного трафика). Значение по умолчанию — 3.

Примечание. На высоконагруженных узлах не рекомендуется устанавливать значение параметра `msg_compress_level` больше 5.

- `mssdecrease` — число байт, на которое будет уменьшен параметр MSS (максимальный размер сегмента) протокола TCP. Значение по умолчанию — `0`.

  Уменьшать параметр MSS рекомендуется только, если между вашим и другими защищенными или туннелируемыми узлами успешно проходит проверка соединения (ping), но не устанавливается TCP-соединение. Причиной блокирования шифрованных IP-пакетов, передаваемых в рамках TCP-соединения, может быть фрагментация этих IP-пакетов на устройствах, стоящих на пути от отправителя к получателю.

  Во избежание фрагментации рекомендуется уменьшить размер IP-пакетов, принимаемых на узле, присвоив параметру `mssdecrease` значение от 20 до 40 байт. Чтобы уменьшить размер исходящих IP-пакетов узла, значение параметра `mssdecrease` следует изменить на узле получателя этих IP-пакетов. Для установления TCP-соединения достаточно изменить параметр `mssdecrease` на одном из взаимодействующих узлов.

Внимание! Параметр `mssdecrease` не следует изменять без крайней необходимости.

- `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 (см. глоссарий, стр. 43). Если от какого-либо координатора, который должен обмениваться пакетами с данным координатором, не было получено никаких служебных пакетов в течение времени, указанного в данном параметре, то такому координатору направляется специальный пакет, на который должен прийти ответ. Если ответ не приходит, то узел координатора считается недоступным (выключенным). Указывается в секундах, значение по умолчанию — `900` (15 минут).
- `tcptunnel_establish` — включение или выключение TCP-туннеля. Возможные значения: `on` или `off` (по умолчанию). Для входящих соединений по протоколу TCP по умолчанию используется порт 80 (см. параметр `tcptunnelport` секции [id] (см. «Секция [id]» на стр. 10, на стр. 11)).
- `timediff` — максимально допустимая разница между временем отправки и временем приема IP-пакетов. Из соображений безопасности драйвер ViPNet блокирует входящие IP-пакеты, если время их отправки отличается от времени их приема более чем на число секунд, указанное в этом параметре. Значение параметра должно быть больше либо равно 1 секунде и меньше либо равно 7200 секунд. Значение по умолчанию — `7200` (2 часа).
- `timesync` — включение или выключение автоматической установки времени на клиенте в соответствии со временем на координаторе, который служит сервером IP-адресов для этого клиента. На координаторе этот параметр по умолчанию установлен в значение `off`, изменять его не следует.
- `tunnel_local_network` — параметр, который позволяет не туннелировать IP-адреса, входящие в локальную подсеть ViPNet Coordinator HW. Возможные значения:
  - `off` (по умолчанию) — обращаться к туннелируемым узлам, находящимся в локальной подсети, минуя туннелирующий координатор;
  - `on` — обращаться к туннелируемым узлам, находящимся в локальной подсети, через координатор, который туннелирует данные узлы. В этом случае доступ к туннелируемым узлам в локальной подсети может быть затруднен.
- `tunnel_virt_assignment` — параметр, определяющий режим назначения виртуальных адресов для узлов, туннелируемых координатором. Возможные значения:
  - `auto` (по умолчанию) — виртуальные адреса туннелируемых узлов задаются автоматически.
  - `manual` — виртуальные адреса туннелируемых узлов задаются вручную в параметрах `tunnel` и `exclude_from_tunnels` секции [id] (см. «Секция [id]» на стр. 10, на стр. 11).

Внимание! В случае обновления ViPNet Coordinator HW до версии 4.2 на узле, на котором вручную были заданы виртуальные адреса для туннелируемых узлов, эти настройки сохраняются. В случае перехода в автоматический режим все виртуальные адреса для туннелируемых узлов будут переназначены.

- `warnoldautosave` — параметр, включающий или выключающий 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 управляющего демона.

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 (см. глоссарий, стр. 42) и содержит следующие параметры:

- `endvirtualip` — служебный параметр, в котором хранится следующий за последним назначенным базовый виртуальный адрес (см. глоссарий, стр. 42). Используется в качестве точки отсчета при поиске и назначении базовых виртуальных адресов для новых защищенных узлов. При назначении базовых виртуальных адресов сначала производится поиск первого свободного адреса в диапазоне от `endvirtualip` до `maxvirtualip`. Если в этом диапазоне свободных адресов нет, то производится поиск в диапазоне от `startvirtualip` до `endvirtualip`.

Внимание! Параметр `endvirtualip` не следует изменять (особенно увеличивать) без крайней необходимости.

- `maxvirtualip` — максимальный адрес для формирования базовых виртуальных адресов защищенных узлов (по умолчанию — `11.0.254.254`). Используется для ограничения диапазона назначаемых базовых виртуальных адресов. По умолчанию параметр `maxvirtualip` соответствует максимально возможному адресу, то есть адресу, у которого два старших октета совпадают с этими же октетами стартового адреса `startvirtualip`, а два младших октета равны 254. Данное значение можно уменьшить, при этом необходимо следить за тем, чтобы оно было больше значения параметра `endvirtualip`.
- `startvirtualip` — стартовый адрес для формирования базовых виртуальных адресов защищенных узлов (по умолчанию — `11.0.0.1`). При изменении данного параметра назначение всех базовых виртуальных адресов узлов производится заново, как при начальном формировании файлов конфигурации. Кроме того, для узлов производится назначение виртуальных адресов в параметрах `ip` (см. «Секция [id]» на стр. 10, на стр. 11).

- `starttunnelvirtualip` — стартовый адрес для формирования 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] (см. «Секция [id]» на стр. 10, на стр. 11) задается видимость отдельных узлов, в этой секции можно задать видимость сразу для всех узлов сетей или подсетей ViPNet. Настройки, заданные в секции `[visibility]`, учитываются при определении видимости узлов со стороны собственного узла.

Секция может содержать следующие параметры:

- `default` — видимость узлов по умолчанию. Возможные значения:
  - `auto` (по умолчанию) — автоматическое определение видимости узлов;
  - `real` — доступ к узлам по их реальным IP-адресам (см. глоссарий, стр. 43);
  - `virtual` — доступ к узлам по их виртуальным IP-адресам (см. глоссарий, стр. 42).
- `subnet_real` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по реальным IP-адресам.

  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 необходимо настроить видимость узлов по виртуальным IP-адресам. Задается так же, как параметр `subnet_real`.

  

  Внимание! Один и тот же идентификатор сети ViPNet можно указать только в одном из параметров `subnet_real` или `subnet_virtual`.

  При старте управляющего демона идентификаторы, заданные в параметрах `subnet_real` и `subnet_virtual`, автоматически сортируются в порядке возрастания и группируются в строки, каждая из которых содержит максимум 8 идентификаторов.

  Параметры `subnet_real` и `subnet_virtual` являются необязательными и по умолчанию отсутствуют в секции `[visibility]`.

- `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]` (см. «Секция

[misc]» на стр. 16)) при отсутствии в секции `[id]` параметра `tunnelvisibility` (см. «Секция [id]» на стр. 10, на стр. 11). Возможные значения:

- `real` (по умолчанию) — всегда обращаться к туннелируемым узлам по их реальным адресам;
- `virtual` — всегда обращаться к туннелируемым узлам по их виртуальным адресам.

Файл iplir.conf-<интерфейс или группа интерфейсов>

Параметры журнала прохождения трафика через любой активный сетевой интерфейс настраиваются в конфигурационных файлах `iplir.conf-<интерфейс или группа интерфейсов>`. Для каждого статического интерфейса, описанного секцией [adapter] в файле `iplir.conf` (см. «Секция [adapter]» на стр. 8), а также для каждой группы динамических интерфейсов (см. глоссарий, стр. 42) управляющий демон 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 следующих групп интерфейсов:

- `ppp` — группа интерфейсов для встроенных модемов;
- `wifi` — группа интерфейсов для WiFi.

Для редактирования этих файлов используется команда:

```
iplir config <интерфейс или группа интерфейсов>
```

Перед редактированием файла `iplir.conf-<имя интерфейса или группа интерфейсов>` необходимо завершить работу управляющего демона командой `iplir stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его командой `iplir start`.

Внимание! Конфигурационный файл `iplir.conf-<интерфейс или группа интерфейсов>` может отсутствовать для статического интерфейса, если соответствующая секция `[adapter]` была добавлена в файл `iplir.conf` вручную и после этого управляющий демон не перезапускался. Поэтому после добавления секций `[adapter]` в файл `iplir.conf` вручную рекомендуется сначала запустить управляющий демон командой `iplir start`, затем завершить его работу командой `iplir stop`, после чего отредактировать нужный файл `iplir.conf-<интерфейс или группа интерфейсов>` и снова запустить управляющий демон.

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

Для каждого статического интерфейса и группы динамических интерфейсов ведется свой журнал, который хранится в файле `iplir.db-<интерфейс или группа интерфейсов>`, расположенном в подкаталоге `iplirdb` каталога, содержащего файлы `iplir.conf-<имя интерфейса или группа интерфейсов>`.

Примечание. В более ранних версиях ViPNet Coordinator HW файлы `iplir.db-<интерфейс>` располагались в каталоге, содержащем файлы `iplir.conf-<интерфейс>`. При обновлении ViPNet Coordinator HW до версии 4.2 файлы `iplir.db-<интерфейс>` автоматически переносятся в подкаталог `iplirdb`.

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

Секция `[db]` содержит следующие параметры:

- `maxsize` — максимальный размер журнала в мегабайтах.

  В исполнениях с одним дисковым накопителем (HW50 N1, N2, N3 и HW100 X1, X8) максимальный размер журнала не должен превышать 10 Мбайт. Значение по умолчанию — 10 Мбайт. При указании большего размера журнала он автоматически устанавливается равным 10 Мбайт.

  В исполнениях HW100 с двумя дисковыми накопителями (HW100 X2, X3, N1, N2, N3) максимальный размер журнала не должен превышать 50 Мбайт. Значение по умолчанию — 50 Мбайт. При указании большего размера журнала он автоматически устанавливается равным 50 Мбайт.

  В исполнениях HW1000, HW2000, HW5000 и HW-VA ограничений на размер журнала не установлено. Значение по умолчанию — 50 Мбайт.

  Реальный размер журнала из-за наличия в нем служебного заголовка получается примерно на 1 Кбайт больше. Каждый раз при запуске управляющего демона после размера журнала автоматически дописывается слово `MBytes`, если оно отсутствует. Поэтому при изменении значения этого параметра его можно не писать. Значение параметра `0` выключает ведение журнала. При этом если до выключения журнала в нем были записи, то просмотреть их будет невозможно.

- `timedif` — интервал времени, в течение которого одинаковые события объединяются в журнале в одну запись. Задается в секундах, значение по умолчанию — `60`. Если это 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`.

- `registertcpserverport` — включение или выключение регистрации информации о порте клиента ViPNet при соединении TCP. Возможные значения: `off` (по умолчанию) или `on`.

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

  

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

- `registerevents` — включение или выключение регистрации служебных событий. Список служебных событий см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», в приложении «Типы событий в журнале регистрации IP-пакетов». Возможные значения: `off` или `on` (по умолчанию).

Файл failover.ini

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

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

Секция [channel]

Каждый сетевой интерфейс активного сервера, работоспособность которого должна контролироваться системой защиты от сбоев при работе в режиме кластера горячего резервирования (см. глоссарий, стр. 43), должен быть описан секцией `[channel]`.

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

Чтобы выключить контроль работоспособности какого-либо интерфейса, необходимо удалить из файла `failover.ini` соответствующую секцию `[channel]`.

Секция `[channel]` содержит следующие параметры:

- `activeip` — IP-адрес и маска, которые будет иметь интерфейс активного сервера кластера. Если маска не указана, то будет использовано значение маски, установленное в системе. Маска может быть указана после IP-адреса через символ «/» в нотации CIDR или в прямой нотации. Например:
  - в нотации CIDR: `activeip = 192.168.201.1/24`
  - в прямой нотации: `activeip = 68.21.12.34/255.255.252.0`

Примечание. Указывать маску необходимо при организации схемы кластера горячего резервирования в условиях ограничений по выделению IP-адресов (подробнее см. в документе «ViPNet Coordinator HW. Сценарии работы»).

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

- `checkonlyidle` — указание на необходимость проверки только неактивных интерфейсов. Возможные значения:
  - `yes` (по умолчанию) — активный сервер посылает эхо-запросы на интерфейсы, адреса которых указаны в соответствующих параметрах `testip`, только если за период опроса IP-адресов, указанный в параметре `checktime` в секции `[network]`, на данных интерфейсах не было входящих или исходящих пакетов.
  - `no` — эхо-запросы на интерфейсы, адреса которых указаны в соответствующих параметрах `testip`, посылаются постоянно.
- `device` — имя интерфейса (`eth0`, `eth1` и так далее).
- `ident` — текстовая строка, идентифицирующая интерфейс. Для интерфейсов, подключенных к одинаковым сетям, параметры `ident` должны совпадать.

Примечание. Не рекомендуется использовать разные имена (несимметричные конфигурации) интерфейсов кластера горячего резервирования.

- `passiveip` — IP-адрес и маска, которые будет иметь интерфейс пассивного сервера кластера. Если маска не указана, то будет использовано значение маски, установленное в системе. Маска может быть указана в таком же формате как в параметре `activeip`.
- `testip` — IP-адрес маршрутизатора или другого стабильного объекта сети, которому будут посылаться эхо-запросы для проверки работоспособности интерфейса.

  При необходимости можно для каждого из интерфейсов указать несколько параметров `testip`. В этом случае сбоем интерфейса будет считаться ситуация, когда ни от одного из заданных IP-адресов не будет получено ответа.

  Например, чтобы эхо-запросы отправлялись на IP-адреса 192.168.100.34 и 192.168.100.25, добавьте следующие строки:

```
testip = 192.168.100.34
testip = 192.168.100.25
```

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` или `localhost`, так как в этом случае реальной проверки работоспособности сетевого интерфейса не производится.

Секция [debug]

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

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

  

  Внимание! В исполнениях с одним дисковым накопителем (HW50 N1, N2, N3 и HW100 X1, X8) по умолчанию уровень детализации равен 1.

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:

  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы), `mail` (почтовая система) или `daemon` (демоны).
  - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

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

Секция [misc]

Секция `[misc]` содержит дополнительные параметры работы системы защиты от сбоев в режиме кластера горячего резервирования и в одиночном режиме:

- `maxjournal` — максимальное количество дней, за которое необходимо хранить записи в журнале переключений кластера горячего резервирования. По умолчанию это ограничение отсутствует.
- `reboot` — задает действия системы в случае обнаружения полной неработоспособности какого-либо демона или драйвера ViPNet Coordinator HW. Возможные значения:
  - `yes` (по умолчанию) — включить механизм регистрации в watchdog-драйвере и перезагружать систему, если какой-либо демон или драйвер не может восстановить свою работу;
  - `no` — выключить механизм регистрации в watchdog-драйвере и не перезагружать систему, если какой-либо демон или драйвер не может восстановить свою работу.

Нередактируемые параметры секции [misc]

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

- `passiveconfig` — абсолютный путь к файлу конфигурации управляющего демона, который будет использоваться на пассивном сервере кластера. Значение по умолчанию — `/etc/iplirpsw`.

Примечание. Параметры `activeconfig`, `passiveconfig` и `maxjournal` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования.

Секция [network]

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

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

Все параметры этой секции рекомендуется настроить одинаково на обоих серверах кластера.

Секция `[network]` содержит следующие параметры:

- `activeretries` — количество неуспешных попыток опроса пассивным сервером активного сервера, после которых делается вывод об отсутствии активного сервера с опрашиваемым IP-адресом. По умолчанию — `3`.
- `afterifconf` — имя скрипта, содержащего команды, которые выполняются непосредственно после конфигурирования всех интерфейсов при смене активного сервера.
- `beforeifconf` — имя скрипта, содержащего команды, которые выполняются перед конфигурированием всех интерфейсов при смене активного сервера.

Примечание. Параметры `afterifconfig` и `beforeifconfig` используются для организации схемы кластера горячего резервирования в условиях ограничений по выделению IP-адресов (подробнее см. в документе «ViPNet Coordinator HW. Сценарии работы»). Они не являются обязательными и могут отсутствовать в секции.

- `channelretries` — количество неуспешных попыток опроса интерфейса активного сервера, после которых этот интерфейс считается неработоспособным. По умолчанию — `3`.
- `checktime` — период опроса:
  - на активном сервере — для проверки работоспособности интерфейса;
  - на пассивном сервере — для поиска IP-адресов активного сервера.

  Указывается в секундах, по умолчанию — `10`.

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

Секция [sendconfig]

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

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

Секция `[sendconfig]` содержит следующие параметры:

- `activeip` — адрес резервного канала другого сервера кластера (который работает в режиме, противоположном режиму данного сервера).
- `config` — включение или выключение резервирования группы конфигурационных файлов. Возможные значения: `yes` (по умолчанию) или `no`. В группу входят следующие конфигурационные файлы:
  - файл `iplir.conf`;
  - файлы `iplir.conf-<интерфейс или группа интерфейсов>`, кроме файла для интерфейса резервного канала;
  - файл `mftp.conf` (см. «Файл mftp.conf» на стр. 32);
  - файлы, содержащие сетевые фильтры и правила трансляции (заданные пользователем и полученные из программы ViPNet Policy Manager);
  - файлы с настройками функции L2OverIP;
  - файлы `*.crg` с контрольными суммами конфигурационных файлов;
  - файлы с настройками маршрутизации (см. глоссарий, стр. 43) и статическими маршрутами (если такие создавались);
  - другие служебные конфигурационные файлы.

- `connectport` — номер порта, используя который данный пассивный сервер кластера соединяется с активным сервером и принимает от него файлы для резервирования. По умолчанию этот параметр отсутствует и равен значению параметра `port` данной секции.
- `device` — системное имя интерфейса, который используется для организации резервного канала.
- `file` — абсолютный путь к файлу для резервирования. По умолчанию отсутствует. В секции может быть несколько таких параметров, в каждом из которых может быть указан любой файл, который требуется резервировать и который не входит в группы конфигурационных файлов (`config`), файлов справочников и ключей (`keys`) и файлов журналов (`journals`). Размер указанного файла не должен превышать 1 Мбайт, и для пересылки этого файла должно быть достаточно времени, указанного в параметре `sendtime` данной секции.

Примечание. Чтобы выбрать для резервирования не все, а один или несколько файлов, входящих в группы конфигурационных файлов или файлов журналов, необходимо установить параметр `config` или `journal` в значение `no` и указать нужные файлы в параметрах `file`.

- `journals` — включение или выключение резервирования группы файлов журналов ПО ViPNet. Возможные значения: `yes` (по умолчанию) или `no`. В группу входят следующие файлы:
  - файлы журналов IP-пакетов сетевых интерфейсов, кроме интерфейса резервного канала;
  - файлы журнала конвертов транспортного модуля MFTP;
  - другие служебные файлы журналов.
- `keys` — включение или выключение резервирования группы файлов справочников и ключей (см. глоссарий, стр. 44). Возможные значения: `yes` (по умолчанию) или `no`.

Внимание! Набор файлов, входящих в группы конфигурационных файлов (`config`), файлов справочников и ключей (`keys`) и файлов журналов (`journals`), определяется демоном failoverd автоматически на активном сервере. Пассивный сервер в каждом цикле резервирования запрашивает сначала список файлов, входящих в каждую группу, для которой включено резервирование, и другие файлы для резервирования (`file`), а затем инициирует передачу этих файлов.

Резервирование групп файлов производится только при запущенных на активном сервере демонах `iplircfg` и `mftpd`, а также если параметры `config`, `keys` и `journal` установлены в значение `yes`. Установка параметра `config`, `keys` или `journal` в значение `no` означает выключение резервирования соответствующей группы. Не рекомендуется устанавливать параметры `config` и `keys` в значение `no`, так как это может привести к некорректной работе ПО ViPNet.

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

Файл mftp.conf

Параметры работы транспортного модуля MFTP содержатся в файле `mftp.conf`. Для редактирования этого файла используется команда `mftp config`. Перед редактированием файла необходимо завершить работу демона `mftpd` командой `mftp stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его с помощью команды `mftp start`.

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

Секция [channel]

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

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

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

- `type` — тип канала. Возможные значения: `mftp` (по умолчанию), `smtp`, `viaroute` (подробнее см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», в главе «Настройка транспортного модуля»).
- `off_flag` — признак выключения канала. Возможные значения:
  - `no` (по умолчанию) — канал включен. В этом случае попытка передачи конверта по каналу производится немедленно.
  - `yes` — канал выключен. В этом случае исходящие конверты, передаваемые по каналу, остаются в очереди до тех пор, пока канал не будет включен или инициатором соединения по данному каналу не станет удаленный транспортный сервер (координатор). Если инициатором соединения станет удаленный клиент, то предназначенные ему конверты не отправляются, а этому клиенту передается специальная команда, которая выключает соответствующий канал в настройках его транспортного модуля (см. глоссарий, стр. 44).
- `call_flag` — признак немедленной передачи конвертов по каналам MFTP и SMTP. Возможные значения:

- `yes` — попытка передачи конверта по каналу производится немедленно (по умолчанию для каналов обмена с координаторами).
- `no` — конверт остается в очереди до тех пор, пока в случае использования канала MFTP инициатором соединения не станет удаленный узел или в случае использования канала SMTP не будет вызван модуль MailTrans (по умолчанию для каналов обмена с клиентами).

Примечание. Если параметры `type`, `off_flag`, `call_flag` отсутствуют в секции, то используются их значения по умолчанию.

Нередактируемые параметры секции [channel] для каналов любого типа

- `id` — уникальный идентификатор сетевого узла ViPNet, с которым происходит обмен данными по каналу. Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`, например: `id = 0x270e000a`.
- `name` — имя сетевого узла ViPNet, с которым происходит обмен данными по каналу.

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

Специфические параметры для канала MFTP

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

- `ip` — IP-адрес удаленного сетевого узла. Определяется управляющим демоном. Если значение этого параметра по каким-либо причинам не было получено от управляющего демона, то оно будет установлено в `0.0.0.0`. В этом случае его можно задать вручную, а затем перезапустить транспортный модуль. Данный параметр может изменяться в процессе работы.
- `call_timeout` — период опроса удаленного сетевого узла в секундах (время следующего опроса узла отсчитывается с момента разрыва последнего соединения с этим узлом). По умолчанию имеет значение `-1`, то есть опрос не производится. Если параметр `call_timeout` отсутствует, то используется его значение по умолчанию.
- `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 (см. глоссарий, стр. 45) за счет передачи через него конвертов без обработки транспортным модулем. Задается в шестнадцатеричном формате с префиксом `0x`.

  По умолчанию параметр `transit` отсутствует, и при межсетевом взаимодействии используется значение, заданное в программе ViPNet Центр управления сетью. Если параметр указан, изменение значения в программе ViPNet Центр управления сетью не учитывается.

Нередактируемые параметры для канала MFTP

- `last_port` — порт, по которому осуществлялось последнее удачное MFTP-соединение. Этот порт будет использоваться при следующей попытке соединения с этим узлом.
- `last_call` — время последней попытки опроса канала.
- `last_err` — время, когда произошла последняя ошибка при попытке соединения или в процессе передачи данных.

Специфические параметры для канала SMTP

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

- `maxsmtpsize` — максимальный размер почтового SMTP-конверта при отправке (в килобайтах). Используется в случае, если в параметре `version` данной секции установлена версия протокола `2.0`. При отправке MFTP-конверт разбивается на несколько SMTP-конвертов, размер каждого из которых не превышает заданный параметром `maxsmtpsize`. Возможные значения: от 100 до 2048000 (2 Гбайт). Значение `0` означает, что ограничение на размер SMTP-конвертов отсутствует.
- `reportaddress` — адрес электронной почты, на который будут отправляться исходящие конверты, в формате: `reportaddress = <имя пользователя>@<сервер>.<домен>`. Например: `reportaddress = user@example.com`
- `version` — версия протокола инкапсуляции конверта MFTP в почтовый конверт RFC-822, передаваемый по данному каналу. Возможные значения: `1.0` и `2.0`.

Примечание. В случае отсутствия параметров `maxsmtpsize` и `version` в данной секции используется их значения, заданные для всех каналов SMTP в секции `[mailtrans]` (см. «Секция [mailtrans]» на стр. 36).

Секция [debug]

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

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

Внимание! В исполнениях с одним дисковым накопителем (HW50 N1, N2, N3 и HW100 X1, X8) по умолчанию уровень детализации равен 1.

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:

- `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы), `mail` (почтовая система) или `daemon` (демоны).
- `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

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

Секция [journal]

Секция `[journal]` содержит параметры настройки журнала MFTP-конвертов, обрабатываемых транспортным модулем. В процессе работы транспортный модуль записывает в этот журнал информацию о полностью принятых, отправленных, удаленных и поврежденных конвертах.

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

Секция `[journal]` содержит следующие параметры:

- `dump_interval` — период выгрузки информации из журнала конвертов в днях. В процессе работы транспортный модуль записывает информацию об обработанных конвертах в текущий файл дампа. По истечении периода времени, заданного данным параметром, создается новый файл дампа, в имени которого содержится текущая дата. По умолчанию каждый день создается новый файл дампа (`dump_interval = 1`).
- `max_size` — максимальный размер файла журнала конвертов в мегабайтах (по умолчанию — `1`). Если размер текущего файла журнала превышает значение этого параметра, то новая информация будет записываться в этот файл на место информации, которая была записана раньше остальной. В случае изменения значения этого параметра, если размер этого файла превышает новое значение, то из него удаляется информация, которая была записана раньше остальной.
- `use_journal` — включение или выключение ведения журнала работы транспортного модуля. Возможные значения: `yes` (по умолчанию) или `no`.

Примечание. Если параметры `dump_interval`, `max_size`, `use_journal` отсутствуют в секции, то используются их значения по умолчанию.

Нередактируемые параметры секции [journal]

- `dump_filename` — префикс имени текстового файла, в который регулярно выгружается информация из журнала конвертов (файла дампа). Значение по умолчанию — `/var/log/mftpenv.log`.

  Постфикс имени этого файла определяется текущей датой и зависит от периода выгрузки информации (см. параметр `dump_interval` данной секции). Пример имени файла дампа: `/var/log/mftpenv.log.2015.09.23`.
- `last_dump` — время последней выгрузки информации из журнала конвертов.

Секция [mailtrans]

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

Секция `[mailtrans]` содержит следующие параметры:

- `frommailbox` — адрес электронной почты отправителя SMTP-конвертов в формате:

  `frommailbox = <имя пользователя>@<сервер>.<домен>`

- `inputmailbox` — адрес электронной почты, по которому модуль почтового обмена будет забирать конверты по протоколу POP3, в формате:

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

- `mailtrans_bin` — абсолютный путь к исполняемому файлу модуля почтового обмена (по умолчанию — `/sbin/mailtrans`).

- `mail_call_timeout` — период вызова модуля почтового обмена, то есть период опроса адреса электронной почты для входящих и исходящих конвертов по каналу SMTP. По умолчанию вызов не производится (`mail_call_timeout = -1`). Однако при наличии в очереди исходящих конвертов, предназначенных для отправки по каналу SMTP, вызов будет производиться, если это не запрещено параметром `call_flag` соответствующего канала.

- `mail_in_chunks_path` — абсолютный путь к каталогу, в который модуль почтового обмена помещает принятые фрагменты SMTP-конвертов в случае использования протокола версии 2.0 (см. «Специфические параметры для канала SMTP» на стр. 34). По умолчанию — `/opt/vipnet/smtpin/chunks`.

- `mail_in_path` — абсолютный путь к каталогу, в который модуль почтового обмена помещает принятые конверты. По умолчанию — `/opt/vipnet/smtpin`.

- `mail_out_path` — абсолютный путь к каталогу, в котором транспортный модуль формирует заголовочные файлы на отправляемые конверты. По умолчанию — `/opt/vipnet/smtpout`.

- `outputmailbox` — IP-адрес SMTP-сервера, на который модуль почтового обмена будет отправлять конверты по протоколу SMTP.

Секция [misc]

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

- `connect_timeout` — интервал времени в секундах, в течение которого клиент будет пытаться установить соединение с удаленным узлом по каналу MFTP (по умолчанию — `5`). Если по истечении этого времени соединение не установлено, то повторные попытки соединения будут производиться по истечении времени, указанного в параметре `outenv_timeout` данной секции.

- `max_connections` — максимальное количество входящих и исходящих соединений по каналам MFTP (по умолчанию — `900`).
- `max_listen_ports` — диапазон значений перебора портов для соединений по каналу MFTP с удаленным узлом в случае неудачи (по умолчанию — `3`). Транспортный модуль циклично перебирает порты в диапазоне от `port` до `port+max_listen_ports-1`. Ожидая входящие соединения, транспортный модуль прослушивает все порты указанного диапазона.
- `num_attempts` — количество последовательных попыток соединения, после которых устанавливается тайм-аут, если соединиться так и не удалось (по умолчанию — `3`).
- `outenv_timeout` — интервал времени в секундах, в течение которого исходящие конверты для канала, на котором произошла ошибка передачи, не могут быть повторно отправлены (по умолчанию — `300`). Если на каком-либо канале произошла ошибка передачи (например, из-за разрыва соединения) и для этого канала существуют исходящие конверты, то следующая попытка передачи произойдет по истечении времени, указанного в параметре `outenv_timeout`.
- `pingpong` — включение или выключение режима поочередного обмена конвертами по каналу MFTP. Возможные значения:
  - `yes` (по умолчанию) — сторона, передавшая конверт, позволяет передать конверт другой стороне, то есть узлы обмениваются конвертами поочередно.
  - `no` — сторона, начавшая передавать конверты, будет их передавать, пока они не закончатся, и только после этого позволит передавать конверты другой стороне.
- `port` — порт, на котором демон mftpd ожидает соединения по каналу MFTP от удаленных сетевых узлов (по умолчанию — `5000`).
- `recv_buff_size` — размер буфера приема в байтах. Значение по умолчанию — `65500`, минимально допустимое значение — `1024`.
- `send_buff_size` — размер буфера передачи в байтах. Значение по умолчанию — `65500`, минимально допустимое значение — `1024`.

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

- `save_sent` — включение или выключение хранения имен отправленных прикладных конвертов. Возможные значения:
  - `no` (по умолчанию) — имена отправленных конвертов не сохраняются;
  - `yes` — при успешной отправке конверта в подкаталоге `sent` каталога, указанного в параметре `out_path` секции `[transport]`, создается файл нулевой длины с именем отправленного конверта.
- `ttl_ctl` — время жизни конвертов, содержащих управляющие запросы, в исходящей очереди. Указывается в днях, значение по умолчанию — `10`. Если по истечении времени, указанного в параметре `ttl_ctl`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.

- `ttl_out` — время хранения конвертов в исходящей очереди в днях. 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. 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, значение по умолчанию — `30`. Если в течение этого времени узлы, установившие соединение, не обменялись никакой информацией, то данное соединение закрывается. Если в процессе обмена исходящие конверты для удаленного узла были переданы не полностью, то повторные попытки соединения будут происходить по истечении времени, указанного в параметре `outenv_timeout`.
- `remote_net_route` — включение или выключение использования прямой маршрутизации между сетями ViPNet. Возможные значения:
  - `yes` (по умолчанию) — в этом случае при настройке перенаправления конвертов с помощью параметра `transit` в секции `[channel]` (см. «Специфические параметры для канала MFTP» на стр. 33) шлюзовые координаторы не будут обрабатывать конверты, передаваемые между сетями ViPNet.
  - `no` — в этом случае все настройки прямой маршрутизации будут сброшены, и обрабатывать конверты будут шлюзовые координаторы. При последующем включении использования прямой маршрутизации потребуется повторная настройка обхода шлюзовых координаторов.

Секция [reserv]

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

- `cmd_port` — порт, на котором демон mftpd пассивного сервера ожидает соединений с активным сервером по резервному каналу для приема управляющих команд (по умолчанию — `6084`). Данный параметр должен иметь одинаковое значение в файлах конфигурации транспортного модуля на «активном» и «пассивном» координаторах.
- `unpack_timeout` — период времени в секундах, в течение которого активный сервер будет ожидать ответы на команды от пассивного сервера, 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 сервер будет пытаться передавать копии MFTP-конверта пассивному серверу в случае неполного дублирования данного конверта (по умолчанию — `60`). В течение этого времени обработка конверта на активном сервере координаторе блокируется. Если по истечении этого времени конверт не будет передан на пассивный сервер, то его обработка продолжится.

- `use_reserv` — включение или выключение режима резервирования конвертов в кластере горячего резервирования. Возможные значения:
  - `yes` (по умолчанию) — конверты резервируются.
  - `no` — резервирование конвертов не производится. В этом случае синхронизировать данные и обновление ПО на серверах кластера необходимо вручную. Кроме того, для корректной работы кластера настройки серверов кластера должны быть одинаковы.

Секция [transport]

Секция `[transport]` содержит ряд параметров, определяющих пути к транспортным каталогам, то есть к каталогам, участвующим в обмене конвертами и их обработке. Эти параметры задают лишь основные каталоги. Вспомогательные каталоги создаются транспортным модулем в процессе работы как подкаталоги основных. При создании конфигурационного файла значения параметров этой секции определены по умолчанию относительно каталога, содержащего справочники и ключи.

Примечание. Транспортный модуль при каждом запуске проверяет наличие каталогов, заданных параметрами секции `[transport]`, и при необходимости создает их.

Секция `[transport]` содержит следующие параметры:

- `in_path` — абсолютный путь к каталогу, в который помещаются полностью принятые конверты (по умолчанию — `/opt/vipnet/in`).
- `out_path` — абсолютный путь к каталогу, в который внешние приложения помещают сформированные конверты для отправки (по умолчанию — `/opt/vipnet/out`).
- `trash_path` — абсолютный путь к каталогу, в который помещаются устаревшие конверты из очереди исходящих конвертов — так называемая «корзина» (по умолчанию — `/opt/vipnet/trash`).

Секция [upgrade]

Данная секция содержит параметры, которые определяют поведение транспортного модуля при приеме обновлений ПО ViPNet из программы ViPNet Центр управления сетью:

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

  - `off` — конфигурация не создается автоматически.

- `maxautosaves` — максимальное число автоматически сохраненных конфигураций. Возможные значения: от 1 до 10. Значение по умолчанию — `10`. Перед автоматическим созданием очередной конфигурации проверяется число ранее сохраненных конфигураций. Если это число равно значению `maxautosaves`, то конфигурация, созданная раньше остальных, удаляется, после чего сохраняется текущая конфигурация.
- `upgrade_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 модуля 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`).

Глоссарий

IP-пакет

Форматированный блок информации, передаваемый в сети по протоколу IP.

IP-форвардинг

IP-форвардинг или маршрутизация транзитных IP-пакетов (не предназначенных для этого компьютера), является опциональной возможностью стека протоколов TCP/IP в операционной системе GNU/Linux. Данная функция обеспечивает пересылку транзитных IP-пакетов через сетевые интерфейсы компьютера.

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг Интернета.

TCP-туннель разворачивается на координаторе, который является для клиента сервером соединений.

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

Адреса видимости

IP-адреса, виртуальные или реальные, по которым данный узел видит остальные узлы сети ViPNet и по которым приложения отправляют свой трафик.

Адреса доступа

IP-адреса, по которым узел доступен в сети (например, адреса межсетевого экрана, за которым он находится).

Базовый виртуальный адрес

Базовый виртуальный адрес является точкой отсчета при назначении виртуальных адресов для каждого из реальных адресов узла. Если в данный момент узел виден по виртуальному адресу, то его адресом доступа считается либо базовый виртуальный адрес, либо вторичный виртуальный адрес, соответствующий первому в списке реальному адресу.

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet Б назначаются непосредственно на узле А. На других узлах узлу ViPNet Б могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если узлы работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

Внешние IP-адреса

Адреса внешней сети.

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

Динамический сетевой интерфейс

Разновидность сетевого интерфейса (см. глоссарий, стр. 44), 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;
- `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi.

Инкапсуляция пакетов

Принцип передачи данных, при котором данные в формате одного протокола упаковываются в формат другого протокола.

Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных серверов ViPNet Coordinator HW, один из которых (активный) выполняет функции координатора сети ViPNet, а другой сервер (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet на активном сервере, пассивный сервер переключается в активный режим для выполнения функций сбойного сервера. При этом сбойный сервер 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.

Координатор (ViPNet-координатор)

Сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или специальный программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Маршрутизация

Процесс выбора пути для передачи информации в сети.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

Метрика адреса доступа

Определяет задержку (в миллисекундах) отправки тестовых пакетов при выполнении опроса узла для определения доступности адреса. Предназначена для задания приоритета использования каналов связи.

Реальный IP-адрес

IP-адрес, назначенный сетевому интерфейсу компьютера в локальной сети или Интернете.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервером соединений для клиента назначен сервер IP-адресов.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN.

Сетевой узел ViPNet

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

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

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

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Статический сетевой интерфейс

Сетевой интерфейс (см. глоссарий, стр. 44), для работы которого требуется задать секцию `[adapter]` в файле `iplir.conf`.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Транспортный модуль (MFTP)

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

Туннелирование

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

Узел сети ViPNet

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Шлюзовой координатор

Координатор, через который осуществляется обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие.

Шлюзовые координаторы назначаются в ЦУСе каждой сети при организации взаимодействия между двумя различными сетями ViPNet.

Указатель

Ш