

ViPNet Coordinator IG 5

Настройка с помощью командного интерпретатора

Версия продукта: 5.2.0

ViPNet Coordinator IG10
ViPNet Coordinator IG100
ViPNet Coordinator IG1000

infotecs

© АО «ИнфоТеКС», 2025

ФРКЕ.467759.003ИС2

Версия продукта 5.2.0

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

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

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

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

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

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение **12**

О документе 13

Соглашения документа 14

Обратная связь 16

Глава 1. Работа с командным интерпретатором **17**

Основные сведения по работе с командным интерпретатором 18

Интерфейс командного интерпретатора 20

Сокращённый ввод команд 20

Автодополнение команд 20

Контекстная справка 21

Сочетания клавиш 22

Локальное подключение с помощью консоли 23

Удалённое подключение по SSH 25

Глава 2. Настройка подключения к сети **26**

Настройка сетевых интерфейсов Ethernet 27

Назначение дополнительных IP-адресов 29

Настройка обработки трафика из нескольких VLAN 30

Подключение к мобильной сети 3G/4G 32

Предварительная настройка 32

Настройка подключения к мобильной сети 33

Подключение к сети Wi-Fi 38

Использование динамических интерфейсов 40

Использование агрегированных сетевых интерфейсов 41

Создание агрегированного интерфейса 41

Режимы работы агрегированного сетевого интерфейса 43

Настройка получения параметров от DHCP-сервера 46

Изменение значения MTU для сетевых интерфейсов 47

Просмотр параметров сетевых интерфейсов 48

Настройка Power over Ethernet 49

Настройка питания внешних устройств 49

Настройка проверки внешних устройств 50

Просмотр настроек PoE 51

Глава 3. Настройка VPN **52**
Общие принципы настройки VPN 53
Настройка подключения к внешней сети 54
Режим «Со статической трансляцией адресов» 54
Режим «С динамической трансляцией адресов» 57
Настройка виртуальных IP-адресов 61
Общие сведения о виртуальных IP-адресах 61
Настройка параметров виртуальных IP-адресов 62
Настройка видимости узлов 63
Настройка туннелирования на сетевом уровне 67
Общие сведения о туннелировании 67
Ручная настройка туннелирования 68
Настройка IP-адресов доступа к узлу и их приоритета 71
Настройка TCP-туннеля 73
Настройка сервера TCP-туннелей 73
Настройка клиента TCP-туннеля 74
Настройка туннелирования на канальном уровне по технологии L2OverIP 76
Общие сведения об L2OverIP 76
Особенности реализации L2OverIP в ViPNet Coordinator IG 77
Настройка L2OverIP 77

Глава 4. Настройка фильтрации трафика **80**
Настройка сетевых фильтров 81
Типы трафика 81
Принципы фильтрации трафика 82
Общие сведения о сетевых фильтрах 85
Группы объектов 87
Системные группы объектов 88
Пользовательские группы объектов по умолчанию 89
Создание пользовательской группы объектов 90
Просмотр групп объектов 91
Удаление пользовательских групп объектов 92
Создание сетевого фильтра 92
Адрес отправителя 94
Адрес получателя 96
Протокол 96
Расписание 97
Регистрация IP-пакетов 98
Действие 98

Изменение сетевого фильтра 99
Просмотр сетевых фильтров 99
Настройка регистрации IP-пакетов при срабатывании фильтров 101
Удаление сетевого фильтра 101
Настройка фильтрации промышленных протоколов 103
Общие сведения о фильтрации промышленных протоколов 103
Основные принципы фильтрации промышленных протоколов 104
Принципы фильтрации протокола Modbus на прикладном уровне 105
Принципы фильтрации протокола МЭК 60870-5-104 на прикладном уровне 106
Порядок настройки фильтрации промышленных протоколов 107
Работа с наборами правил фильтрации промышленных протоколов 107
Настройка правил фильтрации транспортного уровня 108
Настройка правил фильтрации прикладного уровня 110
Примеры создания правил фильтрации прикладного уровня 113
Настройка формата протокола МЭК 60870-5-104 114
Просмотр правил фильтрации промышленных протоколов 115
Настройка прокси-сервера 116
Общие сведения о работе прокси-сервера 116
Настройка основных параметров прокси-сервера 117
Настройка правил контент-фильтрации трафика 119
Адрес отправителя 121
Адрес получателя 121
HTTP-метод 122
MIME-тип 122
Действие 123
Настройка антивирусной проверки трафика 123
Настройка межсетевого экрана 125
Обработка фрагментированных пакетов 125
Настройка антиспуфинга 126
Настройка дополнительных параметров межсетевого экрана 128

Глава 5. Настройка правил трансляции адресов 129
Трансляция сетевых адресов (NAT) 130
Трансляция адреса назначения 131
Трансляция адреса источника 132
Создание правила трансляции адресов 133
Просмотр, изменение, удаление правил трансляции сетевых адресов 135

Глава 6. Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP 137

О прикладных протоколах ... 138
Настройка параметров обработки прикладных протоколов ... 140
Особенности обработки прикладных протоколов DNS, FTP, SIP и H.323 ... 141
Синхронизация сессий прикладных протоколов в кластере ... 145

Глава 7. Настройка сетевых служб ... 147
Настройка DHCP-сервера ... 148
Настройка DHCP-relay ... 150
Настройка DNS-сервера ... 152
Настройка NTP-сервера ... 154
Настройка точки доступа к сети Wi-Fi ... 157
Настройка шлюза Modbus ... 159
Настройка интерфейса GPIO ... 163

Глава 8. Настройка маршрутизации ... 165
Общие сведения о маршрутизации ... 166
Принципы маршрутизации ... 167
Просмотр таблиц маршрутизации ... 171
Настройка статической маршрутизации ... 173
Создание статических маршрутов ... 173
Удаление статических маршрутов ... 174
Просмотр статических маршрутов ... 175
Настройка балансировки IP-трафика ... 175
Настройка маршрутов протоколов DHCP и PPP ... 177
Настройка административной дистанции для маршрутов DHCP-протокола ... 177
Настройка метрики для маршрутов DHCP-протокола ... 178
Настройка метрики для маршрутов PPP-протокола ... 179
Изменение метрики по умолчанию для маршрутов протоколов DHCP и PPP ... 180
Просмотр настроек DHCP в режиме клиента ... 180
Просмотр маршрутов DHCP/PPP-протокола ... 181
Настройка OSPF ... 182
Общие сведения о протоколе OSPF ... 182
Настройка протокола OSPF ... 184
Настройка перераспределения маршрутов ... 186
Просмотр настроек протокола OSPF ... 187
Настройка протокола OSPF в сетях со множественным доступом ... 188
Просмотр состояния каналов связи между маршрутизаторами ... 189
Просмотр информации о соседних маршрутизаторах ... 190
Просмотр маршрутов, сформированных по протоколу OSPF ... 191

Настройка BGP ... 192
Общие сведения о протоколе BGP ... 192
Настройка соседей ... 193
Анонсирование подсетей и перераспределение маршрутов ... 194
Настройка фильтров и префикс-листов маршрутов ... 195
Настройка карт маршрутов ... 198
Настройка распространения маршрутов внутри AS ... 203
Поддержка ECMP и UCMP ... 205
Настройка функции MultiWAN ... 207
Настройка политик маршрутизации ... 208
Настройка проверки состояния шлюзов (DGD) ... 210

Глава 9. Настройка системных параметров ... 213
Настройка даты и времени ... 214
Переключение режимов работы межсетевого экрана ... 215
Просмотр активных сессий пользователей ... 216
Установка допустимого времени неактивности сессии пользователя ... 217
Настройка расписания перезагрузки ... 218
Просмотр лицензии ... 219
Просмотр серийного номера ... 220
Использование резервного раздела ... 221
Сброс к заводским настройкам ... 222

Глава 10. Настройка параметров безопасности ... 224
Управление локальными учётными записями ... 225
Блокирование и разблокирование учётных записей ... 225
Изменение паролей ... 226
Издание сертификатов ... 227
Особенности управления учетными записями в кластере ... 228
Предотвращение подбора пароля ... 228
Обновление справочников и ключей ... 230
Просмотр сведений о ключе защиты обновлений и ключах обмена ... 231
Обновление ключей по истечении срока их действия ... 234
Настройка оповещения об истечении срока действия ключей ... 235
Перевыпуск ключей локального SSH-сервера ... 236
Настройка подключения с помощью веб-интерфейса ... 237
Смена типа межсетевого экрана с сохранением сетевых фильтров ... 240
Контроль целостности файлов ПО ... 241

Глава 11. Обеспечение отказоустойчивости ... 243
Настройка системы защиты от сбоев ... 244
Назначение системы защиты от сбоев ... 244
Работа системы защиты от сбоев в одиночном режиме ... 244
Работа системы защиты от сбоев в режиме кластера ... 245
Развёртывание кластера ... 247
Подключение к пассивному узлу кластера ... 254
Запуск и завершение работы системы защиты от сбоев ... 254
Переключение системы защиты от сбоев в одиночный режим ... 255
Замена неисправного узла кластера ... 255
Работа кластера с коммутационным оборудованием ... 257
Просмотр информации о работе системы защиты от сбоев ... 258
Текущее состояние системы защиты от сбоев ... 258
Журнал переключений ... 260
Подключение к источнику бесперебойного питания ... 262

Глава 12. Настройка транспортного сервера MFTP ... 265
Назначение транспортного сервера MFTP ... 266
Настройка протоколирования событий транспортного сервера MFTP ... 267

Глава 13. Резервное копирование и восстановление настроек ... 268
Способы резервирования и восстановления настроек ... 269
Управление копиями конфигурации VPN ... 270
Создание копии конфигурации VPN ... 270
Просмотр списка копий конфигурации VPN ... 271
Восстановление настроек из копии конфигурации VPN ... 271
Удаление копии конфигурации VPN ... 272
Управление индивидуальной конфигурацией ... 273
Резервное копирование индивидуальной конфигурации ... 274
Восстановление из резервной копии индивидуальной конфигурации ... 275
Управление универсальной конфигурацией ... 279
Экспорт универсальной конфигурации ... 280
Импорт настроек универсальной конфигурации ... 281

Глава 14. Обновление и восстановление программного обеспечения ... 285
Обновление ПО с версий 4.5.x до версии 5.2.0 ... 286
Подготовка к обновлению 4.5.x > 5.2.0 ... 288
Локальное обновление 4.5.x > 5.2.0 ... 289
Удалённое обновление 4.5.x > 5.2.0 ... 292

Обновление на кластере 4.5.x > 5.2.0 ... 293
Обновление ПО с версий 5.1.x до версии 5.2.0 ... 296
Подготовка к обновлению 5.1.x > 5.2.0 ... 297
Локальное обновление 5.1.x > 5.2.0 ... 297
Удалённое обновление 5.1.x > 5.2.0 ... 298
Обновление на кластере 5.1.x > 5.2.0 ... 299
Восстановление ПО ViPNet Coordinator IG ... 301
Запись образа ПО ViPNet Coordinator IG на USB-носитель ... 302
Удаление ПО ... 302
Удаление ПО с помощью командного интерпретатора ... 303
Удаление ПО с помощью кнопки Reset ... 304
Установка ПО с USB-носителя ... 304

Глава 15. Работа с журналами ... 306
Журнал IP-пакетов ... 307
Просмотр журнала ... 308
Экспорт журнала IP-пакетов на USB-носитель ... 315
Экспорт журнала IP-пакетов по сети в формате CEF ... 316
Журнал пакетов промышленных протоколов ... 319
Просмотр журнала пакетов промышленных протоколов ... 319
Экспорт журнала пакетов промышленных протоколов ... 328
Журналы аудита и СКЗИ ... 330
Журнал DNS-запросов ... 332
Журнал MFTP ... 333
Системный журнал ... 335
Экспорт журналов на USB-носитель ... 338

Глава 16. Мониторинг состояния и просмотр статистики ... 339
Мониторинг по SNMP ... 340
Настройка SNMP-агента ... 341
Мониторинг кластера ... 345
Просмотр статистики передачи данных ... 348
Просмотр состояния оборудования ... 350

Приложение A. Сетевые фильтры по умолчанию ... 351

Приложение B. Пользовательские группы протоколов по умолчанию ... 356

Приложение C. События журнала IP-пакетов ... 360

Приложение D. Структура записи журнала IP-пакетов в формате CEF **366**

Приложение E. События системного журнала и журнала аудита **369**

Приложение F. Базы управляющей информации (MIB) для протокола SNMP **382**

MIB-II System 382
IF-MIB 386
IP-MIB 388
IP-FORWARD-MIB 394
Ethernet-Like MIB 398
TCP-MIB 399
UDP-MIB 402
HOST-RESOURCES-MIB 403
UCD-SNMP-MIB 407
UCD-DISKIO-MIB 410
NET-SNMP-MIB 411
SNMP-MPD-MIB 414
SNMP-TARGET-MIB 414
SNMP-USER-BASED-SM-MIB 415
SNMP-VIEW-BASED-ACM-MIB 416
SNMP-FRAMEWORK-MIB 418
VIPNET-MIB 418
VIPNETMULTIWAN-MIB 421
MonitoringAgent-MIB 422
System-MonitoringAgent-MIB 423

Приложение G. Список служб ПО ViPNet Coordinator IG **424**

Приложение H. Поддерживаемые MIME-типы **426**

Приложение I. Использование ViPNet Coordinator IG в качестве межсетевого экрана типа А/Б четвертого класса защиты **430**

Приложение J. Использование ViPNet Coordinator IG в качестве межсетевого экрана типа Д четвертого класса защиты **431**

Приложение K. Возможные неполадки **432**

Утерян пароль администратора 432
Ошибка обновления справочников, ключей и лицензий 432
Ошибка обновления ПО, справочников, ключей и лицензий 433

Ошибка создания резервной копии индивидуальной конфигурации на ViPNet Prime ... 433
Сбои в работе агрегированного канала ... 434
После настройки системного времени недоступна аутентификация пользователей ... 434
Не импортировались правила фильтрации промышленных протоколов из файла универсальной конфигурации ... 435
Блокирование медиа-сессии SIP-соединения при завершении сигнальной сессии по таймауту ... 435
Неполадки в работе сервисов IP-телефонии, видео- и аудиоконференций после переключения кластера ... 435
Циклическая перезагрузка ... 435

Приложение L. Термины и сокращения ... 437



Введение

О документе 13

Соглашения документа 14

Обратная связь 16

О документе

В документе описаны основные сценарии настройки программно-аппаратного комплекса ViPNet Coordinator IG 5 (далее — ViPNet Coordinator IG) с помощью командного интерпретатора, а также работа с журналами ViPNet Coordinator IG. Документ предназначен для администраторов ViPNet Coordinator IG.

Соглашения документа

Внимание! Все сценарии работы с ViPNet Coordinator IG приведены для локального администратора `admin` в режимах просмотра или настройки.

Обозначение	Описание
	**Внимание!** Содержит критически важную информацию
	**Примечание.** Содержит рекомендательную информацию
	**Совет.** Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
`Код`	Имя файла, службы, интерфейса, путь или команда

Описание команд:

- Приглашение команд, которые могут быть выполнены аудитором или администратором в режиме просмотра, заканчивается символом >:

  ```
  hostname> firewall local show
  ```

- Приглашение команд, которые могут быть выполнены администратором в режиме настройки, заканчивается символом #:

  ```
  hostname# admin upgrade software
  ```

- Параметры, которые должны быть заданы аудитором или администратором, заключены в угловые скобки <>:

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

  При вводе в командный интерпретатор параметры вводятся без угловых скобок:

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

- Необязательные параметры или ключевые слова заключены в квадратные скобки []:

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

  При вводе в командный интерпретатор необязательные параметры или ключевые слова вводятся без квадратных скобок:

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

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки `{}` и разделены вертикальной чертой `|`:

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

  При вводе в командный интерпретатор выбранные варианты параметров вводятся без фигурных скобок:

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

- Идентификатор сетевого узла ViPNet указывается в шестнадцатеричном формате с префиксом `0x`:

  ```
  hostname# iplir ping 0x270e000a
  ```

Обратная связь

Контактная информация

- Единый многоканальный телефон:

  +7 (495) 737-6192,

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

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телеграм-канал поддержки: t.me/vhd21.

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

- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

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

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

1

Работа с командным интерпретатором

Основные сведения по работе с командным интерпретатором 18

Интерфейс командного интерпретатора 20

Локальное подключение с помощью консоли 23

Удалённое подключение по SSH 25

Основные сведения по работе с командным интерпретатором

Работа в командном интерпретаторе возможна при локальном или удалённом подключении к ViPNet Coordinator IG:

- Локальное подключение с помощью консоли.
- Удалённое подключение по SSH.

Независимо от способа подключения командный интерпретатор запускается автоматически. Для аутентификации вы можете использовать учётные записи пользователей двух типов: локальные (`user` и `admin`) и централизованные (заданные в ViPNet Prime). После успешной аутентификации командный интерпретатор находится в режиме просмотра, в котором:

- Администратору доступны команды просмотра настроек и некоторые команды управления, например активация локальной учётной записи `user`.
- Аудитору доступны только команды просмотра настроек и команда изменения пароля своей учётной записи.

Строка приглашения интерпретатора в режиме просмотра заканчивается символом `>`.

Администратору доступен режим настройки, в котором разрешено выполнение всех команд ViPNet Coordinator IG. Чтобы перейти в этот режим, выполните команду `enable`. Строка приглашения интерпретатора в режиме настройки заканчивается символом `#`.

Одновременно может быть запущено до пяти копий командного интерпретатора, в которых открыты сессии пользователей различных типов и ролей. При этом интерпретаторы могут находиться в разных режимах.

- Чтобы просмотреть информацию обо всех запущенных сессиях пользователей, выполните команду `who`.
- Чтобы из режима настройки перейти в режим просмотра, выполните команду `exit`.
- Чтобы выйти из командного интерпретатора:
  - В режиме просмотра или настройки нажмите **Ctrl+D**.
  - В режиме просмотра выполните команду `exit`.

  При этом в консоли снова появится приглашение для аутентификации пользователя.
- Чтобы прервать длительное выполнение команды, используйте сочетание клавиш **Ctrl+C**.

Примечание. При высокой нагрузке на ViPNet Coordinator IG увеличивается время выполнения команд. Например, время выполнения команд может превышать 10 секунд при полезной нагрузке:

- от 5 Мбит/с — для исполнения ViPNet Coordinator IG10;
- от 50 Мбит/с — для исполнения ViPNet Coordinator IG100.

Интерфейс командного интерпретатора

Командный интерпретатор принимает текстовые команды, состоящие из слов, разделённых пробелами, латинских и специальных символов. Для облегчения ввода команд в интерпретаторе предусмотрены:

- сокращённый ввод команд;
- автодополнение команд;
- контекстная справка;
- сочетания клавиш.

Сокращённый ввод команд

Слова команды распознаются по минимальному числу символов, отличающих вводимую команду от других. Например, если есть только две команды, первое слово которых начинается с символа «i» (`inet` и `iplir`), то для указания первой команды достаточно набрать `in`, для указания второй — `ip`. Если после слова `iplir` в качестве второго слова возможны только `stop` и `start`, то для их указания достаточно набрать `sto` и `sta` соответственно. Таким образом, вместо полной команды `iplir start` достаточно ввести `ip sta`.

Если среди введённых символов есть ошибочные, то вся команда считается ошибочной, даже если её можно однозначно определить по первым правильно введённым символам (то есть в приведённом выше примере команда `iplor sta` будет ошибочной).

Автодополнение команд

Если введённые символы однозначно определяют команду или параметр команды, то вы можете автоматически дополнить недостающие символы, нажав **Tab**:

```
hostname> en<Tab>

hostname> enable _
```

Автодополнение работает только для слова, на котором находится курсор. Автодополнение не работает для параметров, значение которых вы задаёте (например, имена создаваемых объектов).

Контекстная справка

Контекстная справка позволяет вам просмотреть информацию о командах и параметрах, ввод которых возможен в текущей ситуации. Контекстная справка вызывается с помощью символа «?».

Чтобы просмотреть список всех доступных вам групп команд, в приглашении командного интерпретатора введите символ «?»:

```
hostname# ?
```

license	shows information about license status and expiration date
inet	a group of commands intended for working with routing, interfaces and network tools
failover	manage command for Failover daemon
iplir	manage command for IpLir daemon
machine	a group of system commands
webui	manage WebUI service
admin	perform management tasks
enable	switch to the administrator mode
exit	exit the command line interface
version	view the versions of the appliance
user	perform administrative tasks for user
who	view currently running sessions of the command line interface
vpn	manage VPN services
debug	manage displaying syslog messages on the current console
service	manage additional services
firewall	firewall's objects commands
mftp	manage MFTP daemon
ipf	manage filtering of industrial protocols
alg	manage application-level gateway

```
hostname# _
```

Левая колонка списка содержит первое слово группы команд, правая — краткое описание ее назначения.

В случае ввода символа «?» в процессе набора команд, интерпретатор предложит вам варианты завершения текущего или следующего слова команды, в зависимости от положения курсора:

```
hostname> machi?
machine a group of system commands
hostname> machi_
hostname> machine ?
```

logs	set or show system logging configuration
show	a group of commands for viewing system settings

```
update-queue      show update queue
set               a group of commands for changing system settings
```

После информации о вариантах завершения команды отображается приглашение интерпретатора с ранее введенной командой для редактирования. Редактировать команды можно как обычно: стирать символы клавишей **Backspace** или **Delete**, перемещаться по тексту с помощью клавиш со стрелками влево и вправо.

Сочетания клавиш

Сочетание клавиш	Действие
Ctrl+U	стереть всю команду
Ctrl+K	стереть всё от курсора до конца строки
Ctrl+A	перейти в начало строки
Ctrl+E	перейти в конец строки
Ctrl+B	перейти на один символ назад
Ctrl+F	перейти на один символ вперед
Ctrl+H	стереть символ перед курсором
Ctrl+W	стереть слово перед курсором

Локальное подключение с помощью консоли

Для управления ViPNet Coordinator IG вы можете использовать один из вариантов консоли:

- компьютер с Windows или Linux, подключённый к консольному порту ViPNet Coordinator IG;
- монитор и клавиатура, подключённые к портам VGA и USB на ViPNet Coordinator IG. Этот вариант доступен только для ViPNet Coordinator IG1000 Q1.

Чтобы подключиться к ViPNet Coordinator IG:

1. Подключите компьютер к порту **Console** на аппаратной платформе ViPNet Coordinator IG с помощью консольного кабеля. При отсутствии порта RS-232 на компьютере используйте переходник USB-DB9.

   Если у вас исполнение ViPNet Coordinator IG1000 Q1, то вместо компьютера вы можете подключить монитор и клавиатуру к портам VGA и USB.

2. Если вы подключились к консольному порту, запустите программу для терминального подключения (например: PuTTY, minicom, picocom) и задайте параметры подключения (приведены настройки для PuTTY):
   - Тип терминала — VT100 (**Terminal** > **Keyboard** > **VT100+**).
   - Кодировка символов — KOI8-R (**Window** > **Translation**, в списке **Remote character set** выберите **KOI8-R**).
   - Параметры подключения через последовательный порт (**Connection** > **Serial**):
     - Скорость обмена данными:

       Для аппаратной платформы IG100 I4 — 115200 (в поле **Speed** введите **115200**).

       Для других платформ — 38400 (в поле **Speed** введите **38400**).
     - Размер данных — 8 (в поле **Data bits** введите **8**).
     - Стоповые биты — 1 (в поле **Stop bits** введите **1**).
     - Чётность — None (в поле **Parity** выберите **None**).
     - Контроль потока — None (в поле **Flow control** выберите **None**).
3. Выполните аутентификацию:

   В зависимости от способа аутентификации, используемого в защищённой сети, порядок аутентификации будет отличаться:
   - При аутентификации по паролю — введите имя учётной записи и пароль:

     ```
     login as: admin
     Password:
     Last login: Tue Feb  8 13:27:12 MSK 2022 from 10.0.112.104 on tty1
     ```

```
Loading command shell, please wait...
```

Если вы используете централизованную учётную запись и её имя совпадает с именем локальной учётной записи (`user` или `admin`), введите префикс `center\`. Например:

```
login as: center\admin
```



Примечание. Для предотвращения подбора пароля учетных записей реализована прогрессивная задержка ввода пароля и оповещение о попытках подбора пароля. Количество таких попыток отображается при каждой успешной аутентификации в строке `Password guessing attempts registered`.

- При аутентификации по сертификату — введите имя учётной записи, подключите USB-токен, введите PIN-код:

```
login as: admin
Plug authentication token to USB port and press any key to continue.
Enter the PIN:
Access is allowed
Loading command shell, please wait...
```



Внимание! Не отключайте USB-токен во время работы с ViPNet Coordinator IG. Иначе сессия будет завершена.

Если вы используете централизованную учётную запись и её имя совпадает с именем локальной учётной записи (`user` или `admin`), введите префикс `center\`. Например:

```
login as: center\admin
```



Примечание.

- Если вы введёте некорректный PIN-код несколько раз подряд, он будет заблокирован (максимальное количество попыток ввода см. в документации на USB-токен).
- При ошибке аутентификации, например, когда ключ на USB-токене не соответствует сертификату или нарушена целостность сертификата, учётная запись блокируется на 10 минут.

В обоих случаях издайте новый сертификат пользователя ViPNet Coordinator IG.

Если на ViPNet Coordinator IG истекает или уже истёк срок действия ключа защиты обновлений, ключей обмена или сертификата пользователя, на экран будет выведено оповещение, например:

```
WARNING: Node security keys expire. Validity period < 30 day(s).
```

Удалённое подключение по SSH

Внимание! Удалённое подключение к ViPNet Coordinator IG разрешено только с узлов защищённой сети, для которых в ViPNet Prime настроена связь с ViPNet Coordinator IG.

По умолчанию встроенный межсетевой экран блокирует доступ к ViPNet Coordinator IG по SSH. Чтобы разрешить доступ, создайте фильтр защищённой сети:

```
hostname# firewall vpn add rule "Allow SSH server" src <идентификатор узла> dst @local service @ssh pass
```

В параметре `<идентификатор узла>` укажите один идентификатор или группу идентификаторов узлов ViPNet, с которых вы хотите подключаться к ViPNet Coordinator IG по SSH.

Примечание. Если для узлов сети ViPNet настроена аутентификация по сертификату, то при подключении по SSH она не используется:

- вход под локальной учётной записью выполняется по паролю;
- вход под централизованной учётной записью запрещается.

Для удалённого подключения вы можете использовать любой SSH-клиент, поддерживающий аутентификацию по паролю и кодировку KOI8-R, например PuTTY:

1. Запустите PuTTY и в параметрах сессии укажите IP-адрес интерфейса ViPNet Coordinator IG, по которому выполняется подключение, TCP-порт 22, кодировку KOI8-R.
2. Введите имя учётной записи и пароль:

```
login as: admin
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
Last login: Thu Feb 10 11:48:21 MSK 2022 on tty1
...
Loading command shell, please wait...
```

Примечание. Для предотвращения подбора пароля учётных записей используется прогрессивная задержка ввода пароля и оповещение о попытках подбора пароля. Количество таких попыток отображается при каждой успешной аутентификации в строке `Password guessing attempts registered`.



2

Настройка подключения к сети

Настройка сетевых интерфейсов Ethernet 27

Назначение дополнительных IP-адресов 29

Настройка обработки трафика из нескольких VLAN 30

Подключение к мобильной сети 3G/4G 32

Подключение к сети Wi-Fi 38

Использование динамических интерфейсов 40

Использование агрегированных сетевых интерфейсов 41

Настройка получения параметров от DHCP-сервера 46

Изменение значения MTU для сетевых интерфейсов 47

Просмотр параметров сетевых интерфейсов 48

Настройка Power over Ethernet 49

Настройка сетевых интерфейсов Ethernet



Внимание! Не изменяйте параметры сетевых интерфейсов, задействованных в работе кластера (см. Развёртывание кластера). Это может вызвать сбои в его работе.

Сетевым интерфейсам Ethernet ViPNet Coordinator IG присваиваются имена `eth0`, `eth1` и так далее по количеству интерфейсов. Чтобы настроить подключение к сети, задайте параметры сетевых интерфейсов Ethernet:

1. Задайте класс интерфейса:

   ```
   hostname# inet ifconfig <имя интерфейса> class {access | trunk | slave}
   ```

   - По умолчанию назначен класс `access`.
   - Если требуется, чтобы данный интерфейс обрабатывал трафик из нескольких VLAN, назначьте ему класс `trunk`.
   - Если вы хотите объединить данный интерфейс с другими в составе агрегированного интерфейса, назначьте ему класс `slave`.

2. Присвойте интерфейсу IP-адрес одним из способов:

   - Чтобы включить на интерфейсе режим автоматического получения параметров от DHCP-сервера:

     ```
     hostname# inet ifconfig <имя интерфейса> dhcp
     ```

     Дополнительно см. Настройка получения параметров от DHCP-сервера.

     Внимание! IP-адрес, получаемый от DHCP-сервера, не должен принадлежать подсетям, в которые входят IP-адреса других интерфейсов ViPNet Coordinator IG.

   - Чтобы присвоить интерфейсу статический IP-адрес:

     ```
     hostname# inet ifconfig <имя интерфейса> address <IP-адрес> netmask <маска сети>
     ```

     Например, чтобы присвоить интерфейсу `eth1` IP-адрес 192.168.10.1 и маску подсети 255.255.255.0, выполните:

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

     Если до выполнения этой команды интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

Примечание. При задании IP-адреса действуют ограничения:

- Нельзя задавать IP-адрес 0.*.*.*.
- Нельзя задавать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов нельзя задавать IP-адреса, относящиеся к одной подсети или широковещательному каналу (broadcast). Если интерфейс получил от DHCP-сервера маршрут по умолчанию, который уже задан на другом интерфейсе, то такой интерфейс не будет использоваться при маршрутизации.

3 Включите сетевой интерфейс:

```
hostname# inet ifconfig <имя интерфейса> up
```

4 Если хотя бы на одном используемом интерфейсе Ethernet задано автоматическое получение маршрутов от DHCP-сервера, проверьте, что хотя бы один маршрут по умолчанию получен:

```
hostname# inet show routing
```

Если маршрут по умолчанию не был получен, задайте статический маршрут по умолчанию. Маршрут по умолчанию также необходимо задать при ручной настройке параметров интерфейса Ethernet.

Внимание! Убедитесь, что заданный в маршруте шлюз по умолчанию доступен для сетевого узла ViPNet Coordinator IG. Если шлюз по умолчанию окажется недоступен, многие функции ViPNet Coordinator IG не будут работать (например, виртуальные IP-адреса, обработка прикладных протоколов, сетевые службы и другие).

5 Выполните дополнительные настройки:

- Задайте дополнительные IP-адреса для сетевого интерфейса.
- Настройте маршрутизацию.
- Измените значение MTU для сетевого интерфейса (только для исполнений ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1).

6 При необходимости вы можете сбросить параметры сетевого интерфейса:

```
hostname# inet ifconfig <имя интерфейса> reset
```

Назначение дополнительных IP-адресов

С помощью дополнительных IP-адресов вы можете разделить сеть на логические подсети. Например, чтобы разрешить доступ в интернет только некоторым узлам, когда в остальной сети доступ закрыт.



Примечание. Максимальное количество сетевых интерфейсов в ViPNet Coordinator IG — 128 (как физических, так и виртуальных, включая loopback).

Чтобы добавить дополнительный IP-адрес:

1. Проверьте, что на интерфейсе задан статический основной IP-адрес и класс `access`:

   ```
   hostname# inet show interface <имя интерфейса>
   ```

   В выводе команды:

   - Назначен IP-адрес, например:

     ```
     inet 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255
     ```

   - В строке `Configured by DHCP` значение `no`.
   - В строке `Class` значение `access`.

   Если на интерфейсе не настроен статический IP-адрес, выберите другой интерфейс или измените настройки (см. Настройка сетевых интерфейсов Ethernet).

2. Добавьте дополнительный IP-адрес:

   ```
   hostname# inet ifconfig <имя интерфейса> address add <IP-адрес> netmask <маска подсети>
   ```

   После выполнения команды создается виртуальный сетевой интерфейс с именем `<интерфейс>:номер`, где `номер` — очередной свободный номер (нумерация дополнительных IP-адресов начинается с 0). На созданном виртуальном интерфейсе задаются указанные IP-адрес и маска подсети.

   Например, чтобы добавить на интерфейс `eth1` дополнительный IP-адрес 192.168.10.2 с маской подсети 255.255.255.0:

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

   Будет создан виртуальный интерфейс `eth1:0` с IP-адресом 192.168.10.2 и маской подсети 255.255.255.0.

Настройка обработки трафика из нескольких VLAN

Вы можете использовать ViPNet Coordinator IG для обработки трафика в физической локальной сети, разделённой на несколько независимых виртуальных локальных сетей — VLAN. Это возможно благодаря поддержке виртуальных сетевых интерфейсов и тегированию (маркировке) трафика в соответствии со стандартом IEEE 802.1Q. Каждой VLAN присваивается идентификатор из диапазона от 1 до 4094 (значения 0 и 4095 зарезервированы).

Чтобы настроить обработку трафика из нескольких VLAN:

1 Подключите один из сетевых интерфейсов ViPNet Coordinator IG к коммутатору, объединяющему виртуальные сети.

2 Назначьте физическому интерфейсу класс `trunk`:

```
hostname# inet ifconfig <имя физического интерфейса> class trunk
```

3 Задайте номера виртуальных интерфейсов, которые будут соответствовать виртуальным сетям за коммутатором:

```
hostname# inet ifconfig <имя физического интерфейса> vlan add <номер виртуального интерфейса>
```



Примечание.

- В исполнении ViPNet Coordinator IG10 I2 номера виртуальных интерфейсов 4093–4094 зарезервированы для служебного использования на физических интерфейсах `eth0` и `eth1`.
- В исполнении ViPNet Coordinator IG100 I4 номера виртуальных интерфейсов 4086–4094 зарезервированы для служебного использования на всех физических интерфейсах.
- Максимальное количество сетевых интерфейсов в ViPNet Coordinator IG — 128 (как физических, так и виртуальных, включая loopback).

В результате будет создан виртуальный интерфейс с именем `<имя физического интерфейса>.<номер виртуального интерфейса>`. Например, `eth1.10`.

4 Присвойте IP-адреса виртуальным интерфейсам одним из способов:

- Чтобы включить на виртуальном интерфейсе режим автоматического получения параметров от DHCP-сервера:

  ```
  hostname# inet ifconfig <имя виртуального интерфейса> dhcp
  ```

  Дополнительно см. Настройка получения параметров от DHCP-сервера.

- Чтобы присвоить виртуальному интерфейсу статический IP-адрес:

  ```
  hostname# inet ifconfig <имя виртуального интерфейса> address <IP-адрес> netmask <маска сети>
  ```

Если до выполнения этой команды интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

5 Добавьте виртуальные интерфейсы в конфигурационный файл `iplir.conf`:

```
hostname# iplir adapter add <имя виртуального интерфейса> traffic on
```

Если пока не нужно разрешать трафик через виртуальный интерфейс, выполните команду без параметра `traffic on`. Позже вы сможете разрешить прохождение трафика командой:

```
hostname# iplir adapter traffic <имя виртуального интерфейса> on
```

6 Чтобы трафик проходил только через виртуальные интерфейсы, запретите прохождение трафика через физический интерфейс, к которому подключен коммутатор:

```
hostname# iplir adapter traffic <имя физического интерфейса> off
```

7 В исполнении ViPNet Coordinator IG100 I4 вы можете изменить значение MTU, чтобы оптимизировать передачу данных через интерфейс.

8 Включите физический интерфейс, к которому подключен коммутатор:

```
hostname# inet ifconfig <имя физического интерфейса> up
```

Виртуальные интерфейсы будут включены автоматически.

Теперь ViPNet Coordinator IG сможет обрабатывать трафик из виртуальных сетей на соответствующих виртуальных интерфейсах.

Пример организации обработки трафика из нескольких VLAN см. в документе «Сценарии работы».

Подключение к мобильной сети 3G/4G

Примечание. Подключение к сети 3G/4G возможно только в исполнениях ViPNet Coordinator IG со встроенным модемом.

Беспроводные сети, такие как Wi-Fi и 3G/4G, менее надёжны, чем проводные. Воздействие различного рода помех на беспроводные сети может приводить к потерям среди IP-пакетов и снижению скорости передачи данных.

Подключение к мобильной сети выполняется по протоколу PPP. Модем представлен сетевым интерфейсом с именем `pppX`.

IMEI модема указан на корпусе аппаратной платформы ViPNet Coordinator IG.

Для подключения к интернету вы можете пользоваться услугами любого оператора мобильной связи. Для этого приобретите SIM-карту и установите её в соответствующий разъём ViPNet Coordinator IG (см. документ «Описание аппаратных платформ», раздел «Установка SIM-карты»).

Примечание. Тариф мобильного оператора должен предусматривать использование SIM-карты в модемах.

Предварительная настройка

Перед организацией подключения к сети 3G/4G вы можете:

- Отказаться от получения маршрута по умолчанию.

  При первом подключении модема к сети 3G/4G на ViPNet Coordinator IG добавляется новый маршрут по умолчанию, в котором в качестве шлюза задан адрес узла сети вашего мобильного оператора. Чтобы отказаться от получения маршрута:

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

- Изменить метрику маршрута по умолчанию.

  Первоначально для нового маршрута задана метрика по умолчанию (см. Изменение метрики по умолчанию для маршрутов протоколов DHCP и PPP). Чтобы изменить метрику:

  ```
  hostname# inet usb-modem route-metric <метрика>,
  ```

  где `<метрика>` — число из интервала 1–255.

- Отказаться от добавления адреса DNS-сервера, получаемого от вашего мобильного оператора при первом подключении модема:

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

Настройка подключения к мобильной сети

Настройки для подключения к сети 3G/4G зависят от оператора мобильной связи. ViPNet Coordinator IG автоматически определяет мобильного оператора по SIM-карте. Для этого в памяти ViPNet Coordinator IG предустановлен список мобильных операторов с необходимыми настройками для подключения к мобильной сети.

Подключение к мобильной сети с помощью автоматического определения мобильного оператора

Чтобы настроить подключение ViPNet Coordinator IG к мобильной сети:

1. Отключите модем:

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

2. В исполнениях ViPNet Coordinator IG с поддержкой двух SIM-карт, вы можете выбрать SIM-карту, которая будет использоваться при включении модема. Для этого выполните команду:

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

   где, `<номер SIM-карты>` — номер разъёма, в который установлена SIM-карта (`1` или `2`). По умолчанию используется SIM-карта, установленная в разъём 1.

3. Если на вашей SIM-карте установлен PIN-код, задайте его с помощью команды:

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

   Лексема `sim` с параметром `<номер SIM-карты>` используются в исполнениях ViPNet Coordinator IG с поддержкой двух SIM-карт.

   Примечание. Если потребуется удалить PIN-код из настроек, выполните команду без параметра `<PIN-код>`:

   ```
   hostname# inet usb-modem pin
   ```

   или

   ```
   hostname# inet usb-modem pin sim <номер SIM-карты>
   ```

   PIN-код на самой SIM-карте при этом не изменится.

   ---

4. Включите модем:

   ```
   hostname# inet usb-modem mode on
   ```

   При включении модема ViPNet Coordinator IG запрашивает у модема коды MCC и MNC, комбинация которых используется для идентификации оператора в списке мобильных операторов. Если нужная комбинация найдена, устанавливаются настройки подключения к мобильной сети соответствующего оператора.

В результате подключение к сети 3G/4G будет установлено.

Просмотр настроек и решение проблем подключения

Чтобы просмотреть информацию о модеме, выбранном операторе связи, а также параметры мобильного подключения (включая уровень сигнала):

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



Примечание. Уровень сигнала может отображаться не сразу — требуется время для инициализации модема.

После включения модема проверьте доступность интернета через мобильное соединение любым удобным для вас способом. Перед проверкой убедитесь, что настройки межсетевого экрана и маршрутизации позволяют обращаться к другим узлам в интернете.

Если после автоматического определения оператора доступ в интернет отсутствует:

1. Запросите у вашего оператора настройки для подключения к мобильной сети;
2. Проверьте текущие настройки модема:

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

3. На основании полученных сведений выберите один из вариантов настройки:
   - Если оператор не определился или определился не верно, выберите оператора вручную из списка мобильных операторов или добавьте нового оператора (порядок выбора и добавления оператора см. ниже).

     Примечание. Просмотреть предустановленный список мобильных операторов с настройками подключения вы можете с помощью команды `hostname# inet show usb-modem provider {<код страны> | all}`
     Чтобы завершить просмотр списка, нажмите клавишу **Q**.

   - Если заданы неверные настройки подключения к сети оператора, измените их вручную (порядок изменения настроек см. ниже).

Принципы работы со списком мобильных операторов

- Предустановленный список мобильных операторов нельзя изменить. Он используется как хранилище настроек по умолчанию.
- Для добавления новых операторов или редактирования настроек подключения текущего оператора используется пользовательский список мобильных операторов:
  - При автоматическом или ручном выборе оператора (`inet usb-modem select provider`), запись с настройками для выбранного оператора автоматически копируется из предустановленного списка в пользовательский список мобильных операторов, где можно осуществлять ее редактирование.
  - При создании нового оператора, он добавляется в пользовательский список мобильных операторов.

- При автоматическом или ручном выборе оператора сначала производится поиск по пользовательскому, а затем по предустановленному списку мобильных операторов. Выбранный оператор помечается как активный и будет автоматически выбираться при следующем запуске ViPNet Coordinator IG.

Выбор мобильного оператора вручную

Чтобы выбрать оператора из списка или выбрать другую точку доступа оператора (APN):

1 Отключите модем:

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

2 Выберите оператора, который будет использоваться для мобильного подключения:

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

Укажите параметр `<точка доступа>`, если необходимо выбрать конкретную точку доступа мобильного оператора (иначе будет выбрано первое значение в списке).

Лексема `sim` с параметром `<номер SIM-карты>` используются в исполнениях ViPNet Coordinator IG с поддержкой двух SIM-карт, и определяет, для какой SIM-карты будет выбран оператор или точка доступа.

Примечание. Если на момент выполнения команды коды MCC и MNC, полученные от модема, отличаются от заданных для выбранного оператора (и не равны 0), в пользовательский список запишутся коды, полученные от модема.

---

3 Для подключения к мобильной сети выбранного оператора включите модем:

```
hostname# inet usb-modem mode on
```

Изменение настроек мобильного оператора

Чтобы изменить настройки подключения для мобильного оператора, выбранного в качестве активного:

1 Отключите модем:

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

2 Задайте параметры, которые вы хотите изменить:

- Чтобы задать точку доступа к сети мобильного оператора (APN):

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

  где `<точка доступа>` — доменное имя или IP-адрес (например, `internet.mts.ru`).

- Чтобы задать имя пользователя и пароль к точке доступа, последовательно выполните команды:

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

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

Для имени и пароля допустимо использовать латинские буквы, цифры и символы: `. - _ @`.

- Чтобы задать номер телефона, используемого для соединения с мобильным оператором:

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

При вводе номера телефона вы можете использовать цифры и символы * и #. Длина номера: 3–10 символов. По умолчанию установлен номер: `*99***1#`.

- Чтобы задать коды MCC и MNC мобильного оператора:

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

Примечание. Коды MCC и MNC не могут быть заданы вручную если они уже установлены и не равны 0.

3 Для подключения к мобильной сети с использованием заданных настроек включите модем:

```
hostname# inet usb-modem mode on
```

Добавление нового мобильного оператора

Чтобы добавить нового оператора в пользовательский список мобильных операторов:

1 Отключите модем:

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

2 Задайте нового оператора:

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

При выполнении команды у модема запрашиваются коды MCC и MNC, которые затем записываются в пользовательский список мобильных операторов в качестве уникального идентификатора оператора. При дублировании кодов старая запись стирается.

Внимание! Если вы добавите оператора без установленной SIM-карты, коды MCC и MNC не будут получены. В этом случае добавьте коды MCC и MNC с помощью команды:

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

3 Выберите оператора в качестве активного:

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

Лексема `sim` с параметром `<номер SIM-карты>` используются в исполнениях ViPNet Coordinator IG с поддержкой двух SIM-карт, и определяют, для какой SIM-карты будет выбран оператор.

4 Задайте недостающие настройки для оператора (см. «Изменение настроек мобильного оператора»).

5 Для подключения к мобильной сети добавленного оператора включите модем:

```
hostname# inet usb-modem mode on
```

Сброс настроек

Чтобы вернуть настройки по умолчанию для оператора, удалите его из пользовательского списка мобильных операторов и включите модем. Для этого последовательно выполните команды:

```
hostname# inet usb-modem mode off
hostname# inet usb-modem delete provider <код страны> name <имя оператора>
hostname# inet usb-modem mode on
```

Чтобы удалить все записи в пользовательском списке мобильных операторов и запустить автоматическое определение оператора, последовательно выполните команды:

```
hostname# inet usb-modem mode off
hostname# inet usb-modem clear provider-base
hostname# inet usb-modem mode on
```

Подключение к сети Wi-Fi

Примечание.

- Подключение к сети Wi-Fi возможно только в исполнениях ViPNet Coordinator IG со встроенным модулем Wi-Fi.
- Беспроводные сети, такие как Wi-Fi и 3G/4G, менее надежны, чем проводные. Воздействие различного рода помех на беспроводные сети может приводить к потерям среди IP-пакетов и снижению скорости передачи данных.
- ViPNet Coordinator IG может также работать в качестве точки доступа Wi-Fi (см. Настройка точки доступа к сети Wi-Fi). Использование ViPNet Coordinator IG одновременно в качестве клиента и точки доступа Wi-Fi не поддерживается.

Чтобы подключить ViPNet Coordinator IG к сети Wi-Fi:

1. Отключите сетевой интерфейс `wlan0`:

   ```
   hostname# inet wifi mode off
   ```

2. По умолчанию `wlan0` работает в режиме клиента. Если `wlan0` работает в режиме точки доступа, переключите его в режим клиента:

   ```
   hostname# inet wifi role client
   ```

3. Присвойте IP-адрес интерфейсу `wlan0` одним из способов:

   - Чтобы включить режим автоматического получения параметров от DHCP-сервера:

     ```
     hostname# inet ifconfig wlan0 dhcp
     ```

     Дополнительно см. Настройка получения параметров от DHCP-сервера.

   - Чтобы присвоить интерфейсу статический IP-адрес:

     ```
     hostname# inet ifconfig wlan0 address <IP-адрес> netmask <маска сети>
     ```

     Если до выполнения этой команды интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

4. Просмотрите список доступных сетей Wi-Fi:

   ```
   hostname# inet wifi scan
   ```

   При большом количестве точек доступа Wi-Fi в радиусе действия, команда может выполняться до 2 минут.

5. Укажите параметры доступа к сети Wi-Fi, к которой хотите подключиться:

   - Если аутентификация в сети не требуется:

     ```
     hostname# inet wifi client authentication open
     ```

     В ответ на запрос `WiFi SSID` введите имя сети.

   - Если для аутентификации используется режим WPA-PSK или WPA2-PSK:

     ```
     hostname# inet wifi client authentication {wpa-psk | wpa2-psk}
     ```

В ответ на запросы `WiFi SSID` и `WiFi password` введите имя сети и пароль соответственно. Пароль можно узнать у администратора сети Wi-Fi.

Вы можете подключиться к скрытой сети Wi-Fi, если знаете её имя.

6 Включите `wlan0`:

```
hostname# inet wifi mode on
```

Чтобы проверить параметры подключения к сети Wi-Fi и настройки сетевого интерфейса, используйте команды:

- `hostname# inet show wifi`
- `hostname# inet show interface wlan0`



Внимание! Модуль Wi-Fi в ViPNet Coordinator IG работает в режимах 802.11b и 802.11g. Если связь с точкой доступа Wi-Fi обрывается, настройте её на использование только указанных выше режимов. Перед новой попыткой подключения перезагрузите ViPNet Coordinator IG.

Вы можете настроить запись уровня сигнала Wi-Fi в системный журнал с помощью команды:

```
hostname# inet wifi log signal <периодичность>
```

где `<периодичность>` — интервал времени, через который уровень сигнала будет записываться в журнал (в минутах). Чтобы выключить запись уровня сигнала, введите `off` вместо интервала времени.

Использование динамических интерфейсов

При подключении к мобильной сети или беспроводной сети Wi-Fi на ViPNet Coordinator IG автоматически добавляются и удаляются динамические интерфейсы. По умолчанию разрешена работа динамических интерфейсов, которые входят в одну из следующих групп:

- `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
- `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi.

Если созданный динамический интерфейс входит в одну из перечисленных групп, он автоматически становится активным и начинает пропускать IP-трафик. Дополнительные настройки динамических интерфейсов, аналогичные настройкам статических интерфейсов через файл `iplir.conf`, не требуются. Для каждой группы динамических интерфейсов на ViPNet Coordinator IG создан отдельный журнал IP-пакетов (файл `iplir.conf-<интерфейс или группа интерфейсов>`), в котором регистрируются записи обо всех IP-пакетах, разрешённых и заблокированных на интерфейсах этой группы.

Вы можете просмотреть список активных динамических сетевых интерфейсов:

```
hostname> iplir show adapters groups
```

Активные динамические интерфейсы также отображаются в списке интерфейсов:

```
hostname> iplir show adapters
```

Чтобы изменить настройки журнала IP-пакетов для группы интерфейсов:

1. Остановите службу `iplircfg`:

   ```
   hostname# iplir stop
   ```

2. Откройте конфигурационный файл:

   ```
   hostname# iplir config <группа интерфейсов>
   ```

3. Измените параметры.

4. Запустите службу `iplircfg`:

   ```
   hostname# iplir start
   ```

Описание параметров см. в документе «Справочник команд и конфигурационных файлов».

Использование агрегированных сетевых интерфейсов

Чтобы повысить надежность ваших каналов передачи данных, вы можете объединить несколько физических сетевых интерфейсов ViPNet Coordinator IG в один логический — агрегированный интерфейс. При этом соответствующие каналы связи объединяются на канальном уровне сетевой модели OSI.

Например, вы можете объединить два или три сетевых интерфейса в один агрегированный. Трафик будет передаваться через один из подчинённых физических интерфейсов. Если он выйдет из строя, трафик будет передаваться через другой подчинённый интерфейс.

Чтобы задать распределение нагрузки по подчинённым физическим интерфейсам, выберите один из режимов работы агрегированного интерфейса.

Создание агрегированного интерфейса

1 Для физических интерфейсов, которые вы хотите объединить, установите класс `slave`:

```
hostname# inet ifconfig <имя интерфейса> class slave
```

2 Создайте агрегированный интерфейс:

```
hostname# inet bonding add <номер> mode <режим> slaves <интерфейс 1> [<интерфейс 2>] [<интерфейс N>]
```

, где:

- `<номер>` — номер агрегированного сетевого интерфейса. Возможные значения: 0, 1, 2, 3, 4, 5, 6, 7. Вы можете создать до восьми агрегированных интерфейсов с номерами с именами `bond<номер>`.
- `<режим>` — режим работы агрегированного интерфейса.
- `<интерфейс 1>`, `<интерфейс 2>`, `<интерфейс N>` — имена физических интерфейсов, подчинённых создаваемому агрегированному интерфейсу. При создании агрегированного интерфейса необходимо задать не менее одного подчинённого интерфейса. Ограничения на количество подчинённых интерфейсов в составе агрегированного интерфейса нет.



Примечание. Вы можете добавлять или удалять подчинённые интерфейсы в любой момент времени:

- Добавить подчинённый интерфейс: `hostname# inet ifconfig <агрегированный интерфейс> bonding add <имя подчинённого интерфейса>`
- Удалить подчинённый интерфейс: `hostname# inet ifconfig <агрегированный интерфейс> bonding delete <имя подчинённого интерфейса>`

3 В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 вы можете изменить значение MTU агрегированного интерфейса, чтобы оптимизировать передачу данных через него.

4 Задайте частоту проверки соединения на подчинённых интерфейсах. По умолчанию соединение на подчинённых физических интерфейсах проверяется каждые 0,1 секунды. Вы можете изменить это значение и задать частоту от 1 до 1000 миллисекунд:

```
hostname# inet ifconfig <имя агрегированного интерфейса> bonding miimon <частота в миллисекундах>,
```

где `<имя агрегированного интерфейса>` — `bond{0,1,2,3,4,5,6,7}`.

5 Настройте дополнительные параметры выбранного режима, например для режима `balance-xor` задайте алгоритм вычисления хэш-функции:

```
hostname# inet ifconfig <имя агрегированного интерфейса> bonding xmit-hash-policy layer2
```

6 Назначьте агрегированному интерфейсу динамический или статический IP-адрес:

- Чтобы включить режим автоматического получения параметров от DHCP-сервера:

  ```
  hostname# inet ifconfig <имя агрегированного интерфейса> dhcp
  ```

  Дополнительно см. Настройка получения параметров от DHCP-сервера.

- Чтобы присвоить статический IP-адрес:

  ```
  hostname# inet ifconfig <имя агрегированного интерфейса> address <IP-адрес> netmask <маска подсети>
  ```

  Если до выполнения этой команды агрегированный интерфейс работал в режиме DHCP, данные о DNS- и NTP-серверах, полученные по протоколу DHCP, будут потеряны.

7 Добавьте агрегированный интерфейс в конфигурационный файл `iplir.conf`:

```
hostname# iplir adapter add <имя агрегированного интерфейса> traffic on,
```

где `<имя агрегированного интерфейса>` — `bond{0,1,2,3,4,5,6,7}`.

Если пока не нужно разрешать трафик через агрегированный интерфейс, выполните команду без параметра `traffic on`. Позже вы сможете разрешить прохождение трафика:

```
hostname# iplir adapter traffic <имя агрегированного интерфейса> on
```

По умолчанию агрегированному интерфейсу назначается класс `access`. Чтобы агрегированный интерфейс обрабатывал трафик из нескольких VLAN, назначьте ему класс `trunk`.

8 Последовательно включите все подчинённые физические интерфейсы:

```
hostname# inet ifconfig <подчиненный интерфейс> up
```

9 Включите агрегированный интерфейс:

```
hostname# inet ifconfig <агрегированный интерфейс> up
```

Чтобы изменить режим работы агрегированного интерфейса, удалите его, а затем создайте заново. При изменении параметров агрегированного интерфейса возможно кратковременное пропадание соединения (до 1 секунды).

Режимы работы агрегированного сетевого интерфейса

Таблица 1. Режимы работы агрегированного интерфейса

Режим	Описание
`balance-rr`	Подходит для балансировки нагрузки подчиненных физических интерфейсов и для защиты от сбоев. Применяется в сетях с простой топологией. Исходящие IP-пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные интерфейсы поочередно: первый пакет отправляется через один подчиненный интерфейс, второй пакет — через следующий подчиненный интерфейс и так далее.
`balance-xor`	Предназначен для защиты от сбоев и распределения нагрузки. IP-пакеты отправляются от отправителя к получателю всегда через один и тот же подчиненный интерфейс, для определения которого используется хэш-функция. Алгоритм вычисления хэш-функции можно задать: `inet ifconfig <имя агрегированного интерфейса> bonding xmit-hash-policy <алгоритм>` Вы можете задать один из алгоритмов: • `layer2` — используются MAC-адреса отправителя и получателя, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами; • `layer2+3` — используются MAC-адреса и IP-адреса отправителя и получателя, одинаковыми считаются сетевые узлы с одинаковыми MAC-адресами и IP-адресами; • `layer3+4` — используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии), одинаковыми считаются сетевые узлы с одинаковыми IP-адресами, а также портами TCP или UDP.
`balance-tlb`	Предназначен для балансировки нагрузки на подчиненных физических интерфейсах. Рекомендуется использовать при передаче большого числа IP-пакетов разного размера, когда режимы `balance-rr` и `balance-xor` не распределяют нагрузку равномерно. Ведется подсчет размера исходящих пакетов, переданных через каждый из подчиненных интерфейсов, и на основе этого выбирается интерфейс, через который будет передан пакет, попавший на агрегированный интерфейс. **Примечание.** Для работы агрегированного интерфейса в режиме `balance-tlb` необходимо, чтобы все подчиненные физические интерфейсы были подключены к сети через коммутатор.

Режим	Описание

802.3ad	Предназначен для балансировки нагрузки с использованием протокола LACP. Агрегированный интерфейс работает следующим образом:
	• Среди подчиненных однотипных физических интерфейсов формируются группы — «агрегаторы», скорость передачи данных на интерфейсах которых одинакова (например, группа гигабитных интерфейсов и группа 10-гигабитных интерфейсов). Параметры физических интерфейсов `mtu`, `duplex` и `autoneg`, объединяемых в группу, должны совпадать.
	• Активный агрегатор выбирается в соответствии с режимом выбора, задаваемым:
	`inet ifconfig <имя интерфейса> bonding ad-select <режим>`
	Вы можете выбрать один из режимов выбора:
	`stable` — 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` — 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` — 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.
	• Внутри активного агрегатора подчиненный физический интерфейс, через который отправляются исходящие пакеты, выбирается аналогично режиму `balance-xor`.
	• С другим сетевым оборудованием происходит обмен LACPDU-пакетами с периодичностью, задаваемой:
	`inet ifconfig <имя интерфейса> bonding lacp-rate <slow | fast>`
	В случае выбора параметра `slow` обмен пакетами по протоколу LACP выполняется каждые 30 секунд, в случае выбора параметра `fast` — каждую секунду.
	Обмен пакетами позволяет определить сбой подчиненного интерфейса даже в том случае, если этот интерфейс подключен к другому сетевому узлу не напрямую.
	Примечание. Механизм MC-LAG (MLAG) не поддерживается, поэтому физические порты разных ViPNet Coordinator IG нельзя использовать в одном агрегированном интерфейсе.

Режим	Описание
`active-backup`	Предназначен для защиты от сбоев, но не для балансировки нагрузки на подчиненных физических интерфейсах. Один из подчиненных физических интерфейсов назначается основным (автоматически или явно с помощью команды `inet ifconfig bonding primary`), и все исходящие IP-пакеты отправляются через него. При этом, в случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.
`broadcast`	Предназначен для защиты от сбоев. IP-пакеты, попадающие на агрегированный интерфейс, отправляются через все подчиненные физические интерфейсы одновременно. **Примечание**. Режим `broadcast` требует настройки сетевого оборудования, предотвращающей дальнейшую передачу по сети нескольких копий пакетов.

Настройка получения параметров от DHCP-сервера

При использовании режима автоматического получения параметров от DHCP-сервера сетевой интерфейс получает:

- собственный IP-адрес и маску подсети;
- IP-адреса DNS-серверов;
- IP-адреса NTP-серверов;
- маршруты.



Примечание. Отправка указанных параметров должна быть настроена на DHCP-сервере.

Вы можете отключить получение параметров от DHCP-сервера:

- Чтобы отключить получение IP-адресов DNS-серверов:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp dns off
  ```

- Чтобы отключить получение IP-адресов NTP-серверов:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp ntp off
  ```

- Чтобы отключить получение маршрутов:

  ```
  hostname# inet ifconfig <имя интерфейса> dhcp route off
  ```

Чтобы задать специфичное значение метрики для маршрутов, полученных от DHCP-сервера:

```
hostname# inet ifconfig <имя интерфейса> dhcp route-metric <1-255>
```

Подробнее см. в документе «Справочник команд и конфигурационных файлов».

Вы можете задать ряд параметров, которые будут присваиваться маршрутам DHCP-сервера (см. Настройка маршрутов протоколов DHCP и PPP). Чтобы просмотреть параметры, которые заданы для режима DHCP на всех сетевых интерфейсах, см. Просмотр настроек DHCP в режиме клиента.

Изменение значения MTU для сетевых интерфейсов

По умолчанию для передачи данных через сетевой интерфейс используется размер MTU 1500 байт. Для исполнений ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 вы можете изменить размер MTU, чтобы оптимизировать передачу данных через интерфейс:

```
hostname# inet ifconfig <имя интерфейса> mtu <значение MTU>
```

Значение MTU задаётся в байтах. Допустимый диапазон значений: 1280–9000.



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

Чтобы вернуть значение MTU по умолчанию, в качестве значения MTU укажите `auto`.

При изменении значения MTU учитывайте:

- Значение MTU, заданное для интерфейса класса `trunk`, автоматически применяется ко всем виртуальным интерфейсам класса `vlan`, созданным на этом физическом интерфейсе. Изменять значения MTU для отдельных интерфейсов класса `vlan` нельзя.
- Значение MTU, заданное для агрегированного интерфейса, будет использоваться на всех подчинённых физических интерфейсах класса `slave`. Изменять значения MTU для отдельных интерфейсов класса `slave` нельзя. По умолчанию при создании агрегированного интерфейса для всех подчинённых физических интерфейсов автоматически задаётся значение MTU 1500 байт. Если вы исключаете подчинённый физический интерфейс из агрегированного, для исключённого интерфейса устанавливается значение MTU 1500 байт.

При поступлении на интерфейс фрагментов транзитных IP-пакетов:

1. Из этих фрагментов восстанавливаются транзитные IP-пакеты.
2. Восстановленные IP-пакеты заново фрагментируются в соответствии со значением MTU и отправляются через этот интерфейс.

Просмотр параметров сетевых интерфейсов

Чтобы просмотреть параметры сетевого интерфейса:

```
hostname> inet show interface <имя интерфейса>
```

Если интерфейс не указан, отобразится информация обо всех сетевых интерфейсах.

На экран будет выведена информация:

- IP-адрес и маска подсети;
- MAC-адрес;
- настройки DHCP;
- класс и состояние интерфейса;
- параметры агрегированного интерфейса;
- другие параметры.

Подробное описание всех параметров см. в документе «Справочник команд и конфигурационных файлов».

Для просмотра параметров виртуального интерфейса:

```
hostname> inet show interface <имя интерфейса>:<номер>
```

Настройка Power over Ethernet

Технология Power over Ethernet (PoE) позволяет устройству подавать питание на другие устройства через интерфейсы Ethernet, а также получать питание для собственной работы.

PoE поддерживается в исполнении ViPNet Coordinator IG100 I5.

Вы можете подключить устройства, работающие по технологии PoE, ко всем портам **LAN** на аппаратной платформе ViPNet Coordinator IG. При этом необходимо учитывать ограничения:

Таблица 2. Ограничения по мощности подключаемых устройств

Способ питания ViPNet Coordinator IG	**Максимальная мощность потребления подключённых устройств с PoE**
От блока питания	30 Вт для каждого устройства
От коммутатора по технологии PoE	15 Вт суммарно на все устройства: Одно устройство не выше 3го класса мощности или два устройства не выше 2го класса мощности

В кластере работа PoE не поддерживается.

Настройка питания внешних устройств

1. Подключите одно или несколько устройств с поддержкой PoE к портам **LAN**. Вы также можете подключить устройства после настройки питания.
2. По умолчанию установлено ограничение на подачу питания — 7 Вт на каждый порт (интерфейс).

   Если этой мощности недостаточно для подключённого устройства, измените ограничение:

   ```
   hostname# poe interface <имя интерфейса> limit <ограничение>
   ```

   При этом необходимо учитывать:

   - Если заданное ограничение превышает мощность, выделенную на питание всех устройств (15 Вт или 60 Вт — в зависимости от источника питания ViPNet Coordinator IG), питание не будет подано на устройство.
   - Если потребляемая устройством мощность превысит заданное вами ограничение, сработает защита по току и устройство будет перезагружено.

   > **Примечание.** Погрешность в расчете фактического потребления мощности составляет 3%.

3. Если вы подключили несколько устройств, укажите очерёдность подачи питания:

```
hostname# poe interface <имя интерфейса> priority <приоритет>
```

Например, чтобы питание подавалось сначала на интерфейс `eth2`, а затем — на `eth1`, выполните команды:

```
hostname# poe interface eth2 priority 1
hostname# poe interface eth1 priority 2
```

При этом:

- Если выделенной мощности (15 Вт или 60 Вт) хватит на питание устройства, подключённого к `eth2`, остаток мощности будет передан на `eth1`. Если остатка мощности не хватит для питания устройства, подключённого к `eth1`, оно будет выключено.
- Если выделенной мощности не хватит на питание устройства, подключённого к `eth2`, мощность будет передана на `eth1`.



Внимание! Если ViPNet Coordinator IG питается от блока питания, а порт **WAN** подключён к коммутатору с PoE, то при отключении блока питания мощность, выделенная на питание всех устройств, снизится до 15 Вт. При этом мощность между устройствами будет распределяться в порядке приоритетов, заданных на интерфейсах. Устройства, которым не хватило мощности, будут выключены.

По умолчанию для каждого интерфейса задан приоритет 1. В этом случае питание сначала будет подано на интерфейс с меньшим индексом в имени (например, сначала на `eth1`, затем `eth2`).

4 При включении ViPNet Coordinator IG питание на интерфейсы подаётся после загрузки ПО ViPNet Coordinator IG. Чтобы подключенное устройство загрузилось быстрее, разрешите подачу питания до загрузки ПО:

```
hostname# poe interface <имя интерфейса> faststart on
```

5 Включите подачу питания на интерфейс:

```
hostname# poe interface <имя интерфейса> power on
```

Питание будет подано после определения класса устройства и при условии, что потребление мощности не превышает установленные ограничения. Если устройство не подключено, питание будет подано автоматически при подключении устройства к интерфейсу.



Примечание. Описание световой индикации питания по технологии PoE см. в документе «Описание аппаратных платформ».

Настройка проверки внешних устройств

ViPNet Coordinator IG может автоматически проверять доступность устройств, работающих по технологии PoE. Это позволяет обнаруживать и устранять неполадки в работе устройств. Для этого:

1 Задайте IP-адрес, по которому ViPNet Coordinator IG будет проверять доступность устройства:

```
hostname# poe interface <имя интерфейса> check-ip address <IP-адрес>
```

где <имя интерфейса> — имя интерфейса, к которому подключено устройство с поддержкой PoE.

2 По умолчанию проверка доступности будет выполняться каждые 10 секунд. Чтобы изменить период опроса:

```
hostname# poe interface <имя интерфейса> check-ip frequency <период опроса>
```

Период опроса задаётся в диапазоне от 1 до 120 с.

3 По умолчанию устройство считается недоступным, если опрос IP-адреса (ICMP-запрос) завершился неудачно два раза подряд.

Чтобы изменить число проверок IP-адреса, при достижении которого устройство считается недоступным:

```
hostname# poe interface <имя интерфейса> check-ip failed-attempts <число проверок>
```

Вы можете задать число проверок в диапазоне от 1 до 10.

Примечание. Убедитесь в наличии сетевого фильтра, разрешающего ICMP-соединения. По умолчанию такой фильтр уже задан в межсетевом экране ViPNet Coordinator IG.

---

4 Если устройство недоступно, ViPNet Coordinator IG записывает информацию об этом в системный журнал. В дополнение к этому вы можете настроить перезагрузку устройства в случае его недоступности. Для этого выполните команду:

```
hostname# poe interface <имя интерфейса> check-ip action add restart <интервал>
```

где <интервал> — время в секундах, на которое будет отключено питание от устройства. По истечении этого времени, питание вновь будет подано. Вы можете задать от 1 до 120 с.

Чтобы отключить перезагрузку устройства в случае его недоступности:

```
hostname# poe interface <имя интерфейса> check-ip action del restart
```

5 Включите проверку доступности подключенного устройства:

```
hostname# poe interface <имя интерфейса> check-ip mode on
```

Просмотр настроек PoE

Чтобы просмотреть настройки службы управления питанием PoE, а также информацию о подключенных устройствах с поддержкой PoE:

```
hostname> poe show
```

Описание информации, которая выводится по команде, см. в документе «Справочник команд и конфигурационных файлов».

3

Настройка VPN

Общие принципы настройки VPN 53

Настройка подключения к внешней сети 54

Настройка виртуальных IP-адресов 61

Настройка туннелирования на сетевом уровне 67

Настройка IP-адресов доступа к узлу и их приоритета 71

Настройка TCP-туннеля 73

Настройка туннелирования на канальном уровне по технологии L2OverIP 76

Общие принципы настройки VPN

Настройка VPN выполняется в конфигурационном файле `iplir.conf`. Большинство параметров в этом файле задается автоматически при установке справочников и ключей — параметрам присваиваются значения, заданные администратором при настройке сети ViPNet и отдельных сетевых узлов в ViPNet Prime.

С помощью параметров файла `iplir.conf` вы можете выполнить следующие виды настроек VPN:

- Настройка параметров сетевого подключения координатора.
- Настройка виртуальных IP-адресов.
- Настройка туннелирования на сетевом уровне.
- Настройка IP-адресов доступа к узлу и их приоритета.
- Настройка TCP-туннеля.

Настройка подключения к внешней сети

Чтобы обеспечить возможность подключения к ViPNet Coordinator IG других узлов, находящихся во внешней сети или стоящих за другими межсетевыми экранами, выберите и настройте режим подключения ViPNet Coordinator IG к внешней сети:

- Режим «Со статической трансляцией адресов» используется:
  - если между ViPNet Coordinator IG и внешней сетью установлен межсетевой экран или иное устройство с трансляцией адресов (далее — устройство NAT), на котором можно настроить статические правила трансляции;
  - если ViPNet Coordinator IG имеет непосредственное подключение к внешней сети, то есть может быть доступен напрямую со стороны других сетевых узлов (например, имеет публичный адрес).
- Режим «С динамической трансляцией адресов» используется:
  - если между ViPNet Coordinator IG и внешней сетью установлено устройство NAT, на котором нет возможности настроить статические правила трансляции адресов;
  - если между ViPNet Coordinator IG и внешней сетью установлен другой координатор, выполняющий функции межсетевого экрана.

  Данный режим наиболее универсален, и ViPNet Coordinator IG в этом режиме будет работоспособен и при других способах подключения к сети.

Режим «Со статической трансляцией адресов»

Если ViPNet Coordinator IG установлен за устройством NAT, на котором можно настроить статические правила трансляции, или ViPNet Coordinator IG напрямую подключён к внешней сети, настройте на координаторе режим «Со статической трансляцией адресов».

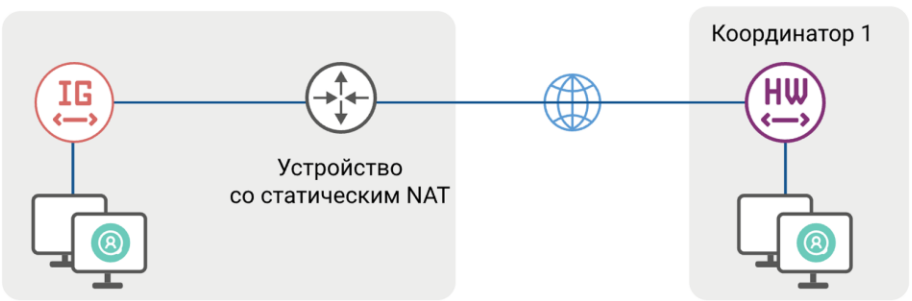


Рисунок 1. Подключение координатора через устройство со статической трансляцией адресов

Перед включением режима «Со статической трансляцией адресов» настройте маршрутизацию на устройство NAT (шлюз по умолчанию или маршруты для удалённых подсетей). Также рекомендуем использовать ViPNet Coordinator IG в качестве сервера соединений для клиентов локальной сети.

На устройстве со статическим NAT настройте следующие правила:

- пропускать UDP-пакеты с трансляцией адреса источника на внешний IP-адрес устройства NAT:
  - адрес источника: IP-адрес доступа ViPNet Coordinator IG;
  - порт источника: диапазон от `port` до `port+255` (`port` — параметр в собственной секции `[id]` файла `iplir.conf` на ViPNet Coordinator IG);
  - адрес назначения: любой;
  - порт назначения: любой;
- пропускать UDP-пакеты с трансляцией адреса назначения на IP-адрес и порт ViPNet Coordinator IG:
  - адрес источника: любой;
  - порт источника: любой;
  - адрес назначения: внешний IP-адрес устройства NAT;
  - порт назначения: см. параметр `port` на Координаторе 1 в секции `[id]` для ViPNet Coordinator IG.

Примечание. Для просмотра файла `iplir.conf` на ViPNet Coordinator IG выполните команду: `hostname> iplir show config`

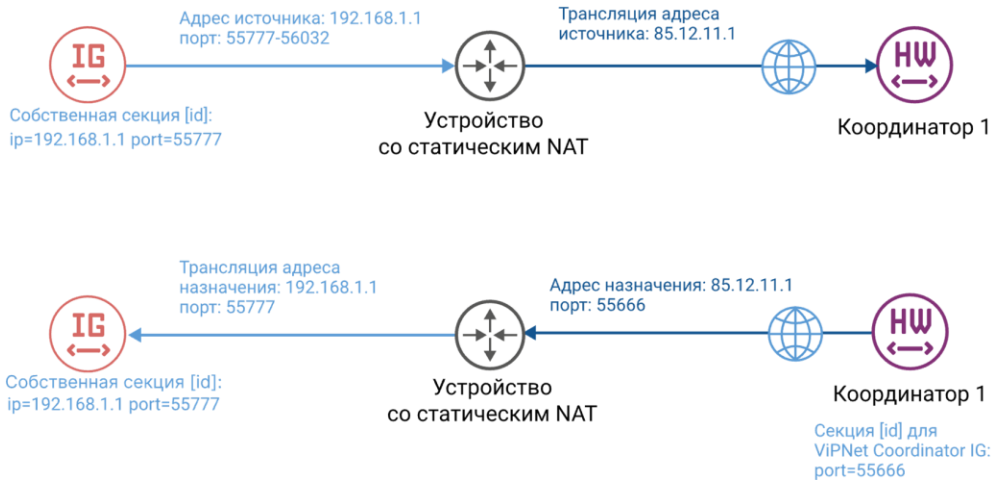


Рисунок 2. Пример работы координатора в режиме «Со статической трансляцией адресов»

На ViPNet Coordinator IG настройте режим «Со статической трансляцией адресов». Вы можете сделать это с помощью команд или через конфигурационный файл `iplir.conf`.

Настройка с помощью команд:

1 Выполните команду:

```
hostname# iplir option mode static
```

2 Перезапустите службу `iplircfg` с помощью команд:

```
hostname# iplir stop
hostname# iplir start
```

Настройка через конфигурационный файл:

1 Завершите работу службы `iplircfg`:

```
hostname# iplir stop
```

2 Откройте конфигурационный файл `iplir.conf` для редактирования:

```
hostname# iplir config
```

3 В собственной секции `[id]` (первая секция):

3.1 Убедитесь, что параметр `usefirewall` отсутствует или установлен в значение `on`.

3.2 Установите параметр `proxyid` в значение `0x00000000`.

4 В секции `[dynamic]` установите параметр `dynamic_proxy` в значение `off`.

5 Сохраните изменения (**Ctrl+O**, затем **Enter**) и закройте редактор (**Ctrl+X**).

6 Запустите службу `iplircfg`:

```
hostname# iplir start
```

IP-адрес устройства NAT и порт доступа автоматически передаются всем остальным узлам, с которыми связан ViPNet Coordinator IG.

Несколько координаторов

Если через устройство NAT к внешней сети подключается ещё один координатор (Координатор 2):

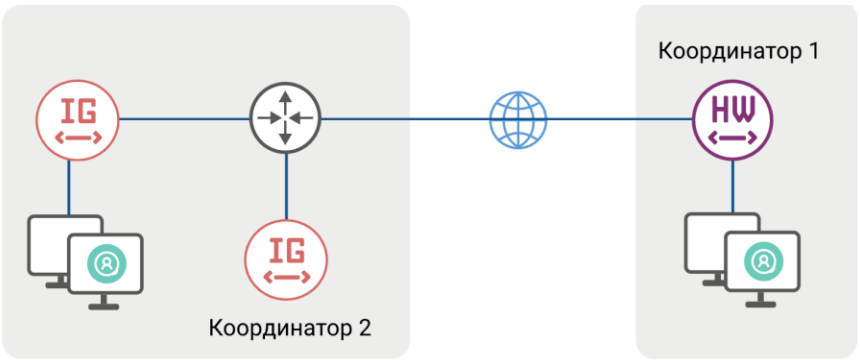


Рисунок 3. Подключение двух координаторов через устройство со статической трансляцией адресов

1 Значение параметра `port` в собственной секции `[id]` файла `iplir.conf` на Координаторе 2 не должно входить в диапазон, используемый на ViPNet Coordinator IG (`port + 255`). Для этого измените значение параметра `port` на Координаторе 2.

2 На устройстве NAT добавьте правила трансляции адресов:

- пропускать UDP-пакеты с трансляцией адреса источника на внешний IP-адрес устройства NAT:
  - адрес источника: IP-адрес доступа Координатора 2;
  - порт источника: диапазон от `port` до `port + 255` (`port` — параметр в собственной секции `[id]` файла `iplir.conf` на Координаторе 2);
  - адрес назначения: любой;
  - порт назначения: любой;
- пропускать UDP-пакеты с трансляцией адреса назначения на IP-адрес и порт Координатора 2:
  - адрес источника: любой;
  - порт источника: любой;
  - адрес назначения: внешний IP-адрес устройства NAT;
  - порт назначения: см. параметр `port` на Координаторе 1 в секции `[id]` для Координатора 2.

Режим «С динамической трансляцией адресов»

Если ViPNet Coordinator IG подключён к внешней сети через устройство NAT, на котором затруднительно настроить статические правила трансляции адресов, настройте на координаторе режим «С динамической трансляцией адресов». Также данный режим используется в случае, если ViPNet Coordinator IG подключён к внешней сети через другой координатор.

Типичные ситуации, когда нет возможности настроить статические правила трансляции:

- устройство NAT принадлежит провайдеру;
- устройство NAT имеет минимум настроек.

Во внешней по отношению к устройству NAT сети должен присутствовать постоянно доступный координатор, выполняющий функцию сервера соединений. Взаимодействие между узлами локальной и внешних сетей будет обеспечиваться через этот сервер соединений.

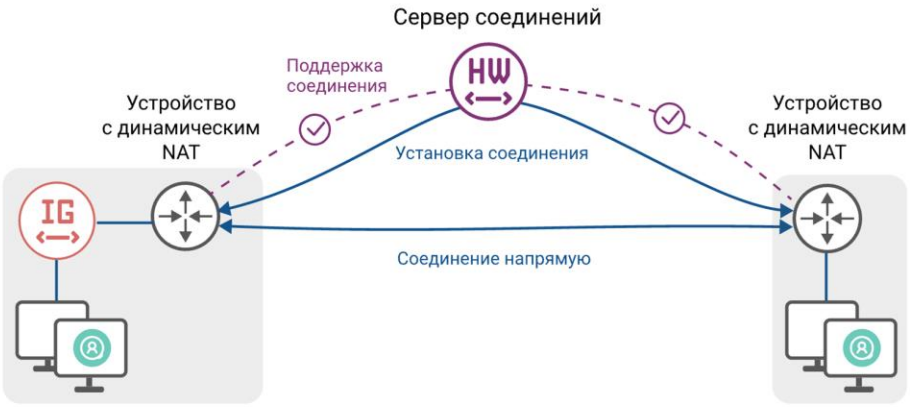


Рисунок 4. Подключение координатора через межсетевой экран с динамической трансляцией адресов

Алгоритм организации соединений между узлами сети ViPNet:

- Каждый узел после подключения к сети периодически отправляет IP-пакеты на свой сервер соединений (для клиентов — это координатор, за которым они зарегистрированы). Период отправки таких IP-пакетов по умолчанию составляет 25 секунд. Этого, как правило, достаточно для работы через большинство устройств NAT. При необходимости вы можете изменить этот период (таймаут).
- После того как связь между узлом и его сервером соединений установлена, узел начинает устанавливать соединение с другим узлом. Он начинает передавать тестовые IP-пакеты удалённому узлу через свой сервер соединений. Одновременно с этим узел передаёт тестовые IP-пакеты на сервер соединений удалённого узла и напрямую на удалённый узел.
- Если тестовые IP-пакеты дошли до удалённого узла, то удалённый узел регистрирует соединение и начинает передавать ответный IP-трафик напрямую. Узел при получении ответного IP-трафика от удалённого узла свой последующий IP-трафик также начинает передавать напрямую.

  Если тестовые IP-пакеты дошли только до сервера соединений удалённого узла, то сервер соединений регистрирует это соединение и отправляет напрямую узлу ответные IP-пакеты удалённого узла.

  То есть с удалённым узлом устанавливается прямое соединение или соединение через его сервер соединений. Если ответный IP-трафик так и не поступил от удалённого узла или его сервера соединений, то узел по-прежнему осуществляет соединение с удалённым узлом через свой сервер соединений.
- Возможность прямого соединения с удалённым узлом, находящимся за устройством с динамической трансляцией сетевых адресов, сохраняется по умолчанию в течение 75 секунд (трёх интервалов отправки IP-пакетов) с момента окончания предыдущего соединения.

Настройка

Вы можете настроить работу ViPNet Coordinator IG в режиме «С динамической трансляцией адресов» с помощью команд или через конфигурационный файл `iplir.conf`.

Настройка с помощью команд:

1. Выберите режим «С динамической трансляцией адресов»:

   ```
   hostname# iplir option mode dynamic <идентификатор узла> [always-use-server]
   ```

   - `<идентификатор узла>` — идентификатор внешнего координатора (сервера соединений). Выбранный сервер соединений должен быть доступен напрямую или через устройство со статической трансляцией адресов.
   - `always-use-server` — необязательный параметр; используется, если необходимо направлять весь трафик с внешними узлами через сервер соединений (может привести к снижению скорости обмена данными между узлами).

   Просмотреть идентификаторы всех связанных узлов вы можете по команде:

   ```
   hostname# iplir node list
   ```

2. Перезапустите службу `iplircfg` с помощью команд:

   ```
   hostname# iplir stop
   hostname# iplir start
   ```

Настройка через конфигурационный файл:

1. Завершите работу службы `iplircfg`:

   ```
   hostname# iplir stop
   ```

2. Откройте конфигурационный файл `iplir.conf` для редактирования:

   ```
   hostname# iplir config
   ```

3. В собственной секции `[id]` (первая секция) убедитесь, что параметр `usefirewall` отсутствует или установлен в значение `on`.

4. В секции `[dynamic]`:

   - параметр `dynamic_proxy` установите в значение `on`;
   - в параметре `forward_id` укажите идентификатор сервера соединений. Указывается в шестнадцатеричном формате с префиксом `0x`, например: `0x15c8000a`.

   Внимание! Выбранный сервер соединений должен быть доступен напрямую или через устройство со статической трансляцией адресов.

   При подключении через устройство с динамическим NAT параметры `firewallip` и `port` секции `[id]` определяются автоматически по информации, полученной от внешних узлов, редактировать их вручную не следует.

5. При необходимости в секции `[dynamic]`:

   - измените значение параметра `timeout` (период отправки IP-пакетов серверу соединений);

- параметр `always_use_server` установите в значение `on`, если требуется направлять весь IP-трафик через сервер соединений. При этом учтите, что передача всего IP-трафика через сервер соединений может привести к снижению скорости обмена данными между узлами.

6 Сохраните изменения (**Ctrl+O**, затем **Enter**) и закройте редактор (**Ctrl+X**).

7 Запустите службу `iplircfg`:

```
hostname# iplir start
```



Примечание. На ViPNet Coordinator IG, который является сервером соединений для узла, работающего в режиме «С динамической трансляцией адресов», в секции `[id]` этого узла параметру `proxyid` будет присвоено значение `0xFFFFFFFE`.

На всех остальных координаторах в секции `[id]` этого узла в параметре `proxyid` будет указан идентификатор узла, выполняющего функции его сервера соединений.

Настройка виртуальных IP-адресов

Общие сведения о виртуальных IP-адресах

При подключении удалённых пользователей к ресурсам локальной сети, а также при организации взаимодействия локальных сетей с использованием технологии VPN может возникать проблема пересечения IP-адресов. Например, два сетевых узла, находящиеся в разных сетях, которые взаимодействуют с помощью VPN, могут иметь одинаковые частные IP-адреса, и в случае обращения по такому адресу возникнет неоднозначность. Технология виртуальных IP-адресов позволяет решить эту проблему без изменения текущей адресной структуры сетей.

Каждый узел сети ViPNet при получении справочников автоматически формирует виртуальные IP-адреса для доступа ко всем защищённым узлам, с которыми у него имеется связь. Если среди них есть координаторы, виртуальные IP-адреса формируются также для всех узлов, которые эти координаторы туннелируют. Каждому реальному IP-адресу узла ставится в соответствие виртуальный IP-адрес. В результате каждый защищённый узел имеет собственный список виртуальных IP-адресов для доступа к узлам сети ViPNet.

Приложения на защищённом узле могут использовать виртуальные IP-адреса для соединения с соответствующими узлами. При отправке IP-пакета VPN-драйвер защищённого узла подменяет виртуальный IP-адрес получателя на реальный и отправляет адресату. В момент приема ответного IP-пакета из сети ViPNet-драйвер передает его приложению после подмены реального IP-адреса отправителя на виртуальный. Это происходит только в случае успешной расшифровки IP-пакета с помощью ключей отправителя, что обеспечивает защиту от подмены адреса отправителя.

Виртуальные IP-адреса для защищённых узлов закрепляются за уникальными идентификаторами узлов ViPNet. Виртуальные IP-адреса для туннелируемых узлов закрепляются за реальными IP-адресами.

При добавлении новых связей с защищёнными узлами, а также новых реальных IP-адресов для узлов, с которыми уже существует связь, защищённый узел присваивает им свободные виртуальные IP-адреса из используемого диапазона виртуальных адресов. При удалении связей между узлами или удалении реальных IP-адресов, виртуальные IP-адреса освобождаются и могут использоваться повторно. Виртуальные IP-адреса, выделенные для туннелируемых узлов, могут измениться при добавлении новых IP-адресов туннелируемых узлов.

Если защищённый узел имеет несколько сетевых интерфейсов или несколько IP-адресов на интерфейсе, то виртуальные адреса для них формируются по правилу: для каждого следующего IP-адреса второй октет виртуального адреса увеличивается на единицу, начиная с нуля, например 11.**0**.0.1, 11.**1**.0.1, 11.**2**.0.1 и далее.

Настройка параметров виртуальных IP-адресов

ViPNet Coordinator IG формирует виртуальные IP-адреса для защищённых узлов и узлов, туннелируемых другими координаторами, с которыми у ViPNet Coordinator IG имеются связи.

По умолчанию начальный IP-адрес для генератора виртуальных IP-адресов — 11.0.0.1 (маска подсети: 255.0.0.0). Автоматическое формирование виртуальных IP-адресов для защищённых узлов и одиночных туннелируемых узлов начинается с этого IP-адреса.

Примечание. Одиночный туннелируемый узел — это узел, IP-адрес которого явно (а не в составе диапазона IP-адресов) указан в настройках туннелирования координатора.

Для диапазонов IP-адресов туннелируемых узлов начальным виртуальным IP-адресом по умолчанию является 12.0.0.1 (маска подсети 255.0.0.0).

Вы можете изменить используемые диапазоны IP-адресов для формирования виртуальных IP-адресов:

Внимание! При изменении начального IP-адреса для генератора виртуальных IP-адресов все виртуальные IP-адреса на ViPNet Coordinator IG будут сформированы заново.

1. Завершите работу управляющей службы:

   ```
   hostname# iplir stop
   ```

2. Откройте файл `iplir.conf` для редактирования:

   ```
   hostname# iplir config
   ```

3. В секции `[virtualip]` задайте диапазон IP-адресов для формирования виртуальных IP-адресов защищённых узлов и одиночных туннелируемых узлов одним из следующих способов:

   - Задайте начальный и конечный IP-адреса диапазона виртуальных IP-адресов в параметрах `startvirtualip` и `maxvirtualip`. Последний октет IP-адресов не должен быть равен 0. При этом `maxvirtualip` должен быть больше `startvirtualip`.
   - Задайте начальный IP-адрес диапазона виртуальных IP-адресов в параметре `startvirtualip`. Значение должно быть меньше 11.0.255.254 (так как начальный IP-адрес 12.0.0.1 задан по умолчанию для формирования виртуальных IP-адресов туннелей). При этом значение параметра `maxvirtualip` останется равным 11.0.255.254. Если значение `startvirtualip` задать в виде `x.0.0.1`, то параметру `maxvirtualip` будет автоматически присвоено значение `x.255.255.254`.
   - Задайте начальный IP-адрес диапазона виртуальных IP-адресов с маской подсети в параметре `startvirtualip` (допустимые маски подсети — /8 или /16, например: `startvirtualip = 11.0.0.1/8`). При этом не присваивайте значение параметру `maxvirtualip`, и сам параметр не будет использоваться в конфигурационном файле, а диапазон виртуальных IP-адресов будет ограничен IP-адресом, указанным в параметре `startvirtualip` с маской подсети /16 (пример: `11.0.0.1/16`).

Внимание! Чтобы избежать ошибок при назначении начальных IP-адресов для генератора виртуальных IP-адресов, следует учитывать:



- Значение первого октета должно быть в диапазоне 1–239.
- Значение второго и третьего октетов должно быть в диапазоне 0–255.
- Значение четвёртого октета должно быть в диапазоне 1–254.

4 Начальный IP-адрес для формирования диапазонов виртуальных IP-адресов туннелируемых узлов задаётся автоматически: `starttunnelvirtualip = <x>.0.0.1`, где `x` больше первого октета `startvirtualip` на 1. Вы можете задать его вручную. Для этого введите значение в параметр `starttunnelvirtualip`. При этом первый октет должен быть больше первого октета `startvirtualip` и не должен быть равен 0, 127, 224-239, 255.

5 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

6 Запустите управляющую службу:

```
hostname# iplir start
```

Следует учитывать, что любой диапазон виртуальных IP-адресов (как диапазон по умолчанию, так и заданный вручную) будет пересекаться с одним из диапазонов реальных IP-адресов интернета. Поэтому при взаимодействии узла с открытыми ресурсами интернета может возникнуть конфликт, если у открытого ресурса IP-адрес совпадёт с виртуальным IP-адресом одного из узлов сети ViPNet. Соединение с таким открытым ресурсом будет невозможно. В этом случае доступ к этому ресурсу можно настроить одним из способов:

- сменить диапазон виртуальных IP-адресов;
- работать с ресурсом через прокси-сервер.

При этом работать с защищёнными узлами через прокси-сервер нельзя. Поэтому при использовании прокси-сервера требуется указать IP-адреса защищённых узлов в качестве исключений.

Настройка видимости узлов

В настройках ViPNet Coordinator IG вы можете задать видимость защищённых узлов и узлов, туннелируемых другим координатором, по реальным или виртуальным IP-адресам. При этом узлы, туннелируемые ViPNet Coordinator IG, будут подключаться к защищённым и туннелируемым узлам других координаторов по тем же IP-адресам, что и ViPNet Coordinator IG. Например, если в настройках ViPNet Coordinator IG задано использование виртуальных IP-адресов для подключения к определённым защищённым узлам, то узлы, туннелируемые этим ViPNet Coordinator IG, также будут подключаться к ним по виртуальным IP-адресам.

По умолчанию на ViPNet Coordinator IG используются следующие настройки видимости:

- защищённые узлы, находящиеся в одном и том же широковещательном сегменте, доступны по реальным IP-адресам;
- туннелируемые узлы (узлы, туннелируемые другими координаторами) доступны по реальным IP-адресам;

- остальные узлы сети ViPNet доступны по виртуальным IP-адресам.

Видимость каждого защищённого узла сети ViPNet определяется с помощью параметров файла `iplir.conf` следующим образом:

1. Если в секции `[id]` узла присутствует параметр `visibility`, то видимость узла определяется значением этого параметра.
2. Если в секции `[id]` узла нет параметра `visibility`, но при этом сеть, которой принадлежит узел, указана в параметре `subnet_real` или `subnet_virtual` секции `[visibility]`, то видимость узла определяется значением этого параметра.
3. В иных случаях видимость узла определяется значением параметра `default` секции `[visibility]`.

То есть индивидуальные настройки видимости узлов приоритетнее настроек видимости сетей, а настройки видимости сетей приоритетнее настроек видимости по умолчанию.

Видимость туннелируемых узлов определяется с помощью параметров файла `iplir.conf` следующим образом:

1. Если в секции `[id]`, которая относится к туннелирующему координатору, присутствует параметр `tunnelvisibility`, то видимость туннелируемых узлов определяется значением этого параметра.
2. Если в секции `[id]`, которая относится к туннелирующему координатору, нет параметра `tunnelvisibility`, то видимость туннелируемых узлов определяется значением параметра `tunneldefault` секции `[visibility]`.

Просмотреть настройки видимости в файле `iplir.conf` вы можете с помощью команды:

```
hostname> iplir show config
```

Настройка видимости защищённых узлов

1. Завершите работу управляющей службы:

   ```
   hostname# iplir stop
   ```

2. Откройте файл `iplir.conf` для редактирования:

   ```
   hostname# iplir config
   ```

3. Чтобы настроить параметры видимости защищённых узлов по умолчанию и параметры видимости сетей, в секции `[visibility]`:
   - установите параметр `default` в одно из значений:
     - `real` — для доступа к узлам используются их реальные IP-адреса;
     - `virtual` (по умолчанию) — для доступа к узлам используются их виртуальные IP-адреса.
   - при необходимости укажите идентификаторы вашей сети ViPNet и доверенных сетей в одном из параметров:

- `subnet_real` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по реальным IP-адресам;
- `subnet_virtual` — идентификаторы сетей ViPNet, для которых необходимо настроить видимость узлов по виртуальным IP-адресам.

Вы можете указать один либо несколько идентификаторов через запятую.

4 Чтобы настроить параметры видимости отдельных защищённых узлов, в соответствующих секциях `[id]` параметр `visibility` установите в одно из значений:

- `real` — всегда обращаться к узлу по его реальному адресу.
- `virtual` — всегда обращаться к узлу по его виртуальному адресу.



Внимание! До изменения видимости защищённого узла, который не находится с ViPNet Coordinator IG в одном широковещательном сегменте, с виртуальной на реальную, выполните команду `inet ping` на виртуальный IP-адрес этого узла. Иначе после изменения видимости доступ к узлу по реальному IP-адресу будет отсутствовать.

До изменения видимости сети ViPNet с виртуальной на реальную, для каждого защищённого узла, который не находится с ViPNet Coordinator IG в одном широковещательном сегменте, выполните команду `inet ping` на виртуальный IP-адрес этого узла. Иначе после изменения видимости сети ViPNet доступ к узлам по реальному IP-адресу, на которые не была выполнена команда `inet ping`, будет отсутствовать.

---

5 Сохраните изменения (**Ctrl+O**, затем **Enter**) и закройте редактор (**Ctrl+X**).

6 Запустите управляющую службу:

```
hostname# iplir start
```

Настройка видимости туннелируемых узлов

1 Завершите работу управляющей службы:

```
hostname# iplir stop
```

2 Откройте файл `iplir.conf` для редактирования:

```
hostname# iplir config
```

3 Чтобы настроить параметры видимости туннелируемых узлов по умолчанию, в секции `[visibility]` установите параметр `tunneldefault` в одно из значений:

- `real` (по умолчанию) — для доступа к туннелируемым узлам используются их реальные IP-адреса.
- `virtual` — для доступа к туннелируемым узлам используются их виртуальные IP-адреса.

4 Чтобы настроить параметры видимости туннелируемых узлов, в секциях `[id]`, которые относятся к туннелирующим координаторам, в параметре `tunnelvisibility` установите одно из значений:

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

5 Сохраните изменения (**Ctrl+O**, затем **Enter**) и закройте редактор (**Ctrl+X**).

6 Запустите управляющую службу:

```
hostname# iplir start
```

Настройка туннелирования на сетевом уровне

Общие сведения о туннелировании

Технология туннелирования применяется в следующих случаях:

- для защиты данных при их передаче на потенциально опасном участке сети;
- для организации доступа к открытому узлу, на котором установка ПО ViPNet невозможна или нежелательна (например, средства промышленной автоматики, устройства телеметрии, серверы DHCP, IP-АТС или аппаратные IP-телефоны, и др.).

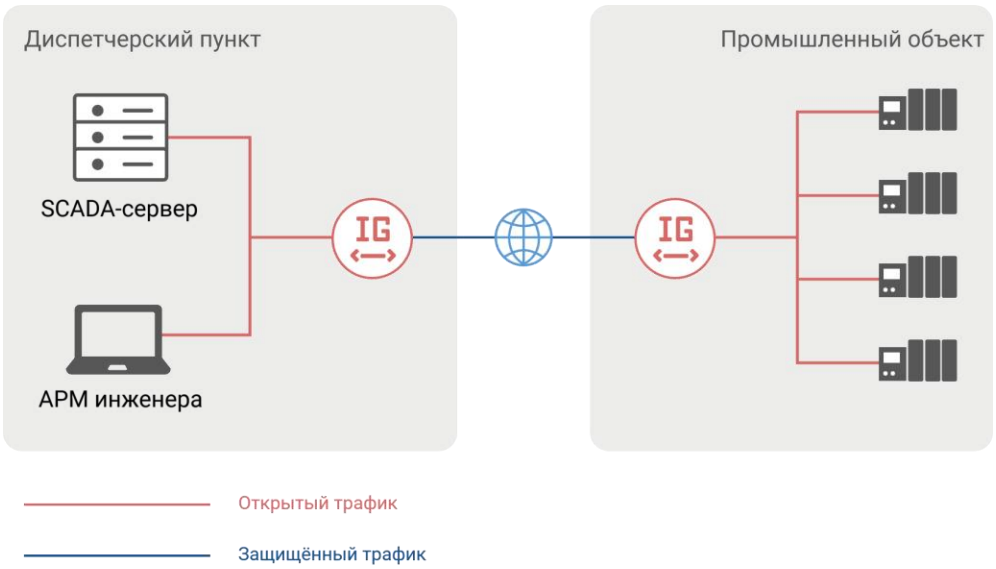


Рисунок 5. Схема туннелирования

Технология туннелирования предполагает направление трафика узла не напрямую на другой узел, а через координатор, где трафик фильтруется и защищается криптографическими методами. Также настройки туннелирования открытых узлов, которые задаёт администратор сети ViPNet, хранятся на координаторах, выполняющих туннелирование этих узлов.

Узлы, которые будут туннелироваться координатором, задаются в ViPNet Prime (см. документ «ViPNet Prime. Руководство администратора», раздел «Создание туннелируемых адресов ресурсов»). Эта информация автоматически передаётся на узлы защищённой сети в составе справочников. Для взаимодействия между узлом защищённой сети и туннелируемым узлом, а также между двумя туннелируемыми узлами, необходимо создать связи между ними в ViPNet Prime.

Если ViPNet Coordinator IG работает в условиях отсутствия связи с ViPNet Prime, вы можете настроить туннелирование локально на ViPNet Coordinator IG (см. Ручная настройка

туннелирования). Затем IP-адреса туннелируемых узлов необходимо задать вручную на каждом связанном координаторе.

Если настройки туннелирования были заданы вручную, а затем поступили из ViPNet Prime, выполняется их слияние:

- Если с настройками туннелирования из ViPNet Prime получены новые IP-адреса туннелируемых узлов, они добавляются в конфигурационный файл `iplir.conf`.
- Если заданные локально IP-адреса туннелируемых узлов отсутствуют в настройках туннелирования, полученных из ViPNet Prime, то эти IP-адреса будут удалены.

После изменения настроек туннелирования может возникнуть конфликт между реальными IP-адресами узлов из широковещательного сегмента вашего ViPNet Coordinator IG и реальными IP-адресами узлов, туннелируемых удалённым координатором, или между реальными IP-адресами туннелируемых узлов. Чтобы устранить возможные конфликты, на координаторе, туннелирующем узлы с конфликтующими IP-адресами, задайте видимость туннелируемых узлов по виртуальным IP-адресам (см. Настройка видимости узлов).

Примеры настройки туннелей см. в документе «Сценарии работы».

Ручная настройка туннелирования

Примечание. Настраивайте туннелирование на координаторе только когда централизованная настройка туннелирования в ViPNet Prime не используется, иначе настройки на координаторе могут быть заменены настройками из ViPNet Prime.

Чтобы настроить туннелирование для открытых узлов, подключённых к ViPNet Coordinator IG, или настроить доступ к туннелируемым узлам удалённого координатора:

1 Завершите работу управляющей службы:

```
hostname# iplir stop
```

2 Откройте конфигурационный файл `iplir.conf` для редактирования:

```
hostname# iplir config
```

3 Выберите режим задания виртуальных IP-адресов для туннелируемых узлов. Для этого в секции `[misc]` установите параметр `tunnel_virt_assignment` в одно из значений:

   - `auto` (по умолчанию) — при задании реальных IP-адресов туннелируемых узлов виртуальные IP-адреса для них назначаются автоматически.

Внимание! Если все возможные адреса из диапазонов виртуальных IP-адресов для туннелируемых узлов заняты, то следующим узлам в качестве виртуальных копируются реальные адреса. При этом режим назначения принудительно переключается в ручной (`manual`).

- `manual` — виртуальные IP-адреса для туннелируемых узлов задаются вручную. При этом реальные IP-адреса туннелируемых узлов могут быть заданы как вручную, так и получены из ViPNet Prime.

4 Для туннелирования открытых узлов, подключённых к ViPNet Coordinator IG, в собственной секции `[id]` (первая секция) измените значение параметра `tunnel`:

- при автоматическом режиме задания виртуальных IP-адресов (см. предыдущий шаг):

  ```
  tunnel = <ip1>-<ip2>
  ```

  где `<ip1>-<ip2>` — диапазон реальных IP-адресов туннелируемых узлов (начальный и конечный IP-адреса диапазона).

  Виртуальные IP-адреса для заданного диапазона будут сформированы автоматически.

  Например, чтобы ViPNet Coordinator IG туннелировал IP-адреса с 192.168.201.5 по 192.168.201.10, а виртуальные IP-адреса для этого диапазона были назначены автоматически, задайте:

  ```
  tunnel= 192.168.201.5-192.168.201.10
  ```

- при ручном режиме задания виртуальных IP-адресов (см. предыдущий шаг):

  ```
  tunnel = <ip1>-<ip2> to <ip3>-<ip4>
  ```

  где `<ip1>-<ip2>` — диапазон реальных IP-адресов туннелируемых узлов (начальный и конечный IP-адреса диапазона),

  `<ip3>-<ip4>` — диапазон виртуальных IP-адресов (начальный и конечный IP-адреса диапазона), которые будут использоваться вместо реальных IP-адресов туннелируемых узлов, если на узле, который к ним обращается, настроена видимость по виртуальным IP-адресам.

  Параметр `<ip4>` можно не указывать, он формируется путем прибавления к `<ip3>` разницы между `<ip2>` и `<ip1>`.

  Внимание! При задании виртуальных IP-адресов в ручном режиме автоматическая проверка повторного использования одних и тех же IP-адресов не производится. Поэтому убедитесь, что задаваемые диапазоны виртуальных IP-адресов не пересекаются.

  Например, чтобы координатор туннелировал IP-адреса с 192.168.201.5 по 192.168.201.10, а виртуальными IP-адресами для этого диапазона были IP-адреса с 192.168.111.5 по 192.168.111.10, задайте:

  ```
  tunnel = 192.168.201.5-192.168.201.10 to 192.168.111.5-192.168.111.10
  ```

  Внимание! На всех туннелируемых узлах сети настройте статические маршруты для защищаемого трафика через ViPNet Coordinator IG или укажите ViPNet Coordinator IG в качестве шлюза по умолчанию.

5 Для настройки доступа к узлам, туннелируемым удалённым координатором, в секции `[id]` соответствующего координатора измените значение параметра `tunnel`:

```
tunnel = <ip1>-<ip2> to <ip3>-<ip4>
```

где <ip1>-<ip2> — диапазон реальных IP-адресов узлов, туннелируемых данным координатором (начальный и конечный IP-адреса диапазона),

<ip3>-<ip4> — диапазон виртуальных IP-адресов (начальный и конечный IP-адреса диапазона), которые используются вместо реальных IP-адресов туннелируемых узлов данного координатора, если на узле, который к ним обращается, настроена видимость по виртуальным IP-адресам.

6 Задайте использование IP-адресов <ip3>-<ip4> на каждом защищённом узле, с которого необходим доступ к туннелируемым узлам.

7 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

8 Запустите управляющую службу:

```
hostname# iplir start
```

Настройка IP-адресов доступа к узлу и их приоритета

Каждый узел ViPNet взаимодействует с другим узлом, с которым у него есть связь, по определённому адресу доступа. Однако нередко некоторые узлы подключены к нескольким независимым каналам связи и имеют несколько адресов доступа, каждый из которых может использоваться для связи с другими узлами.

Приоритеты каналов связи зависят от метрик, настроенных на сетевом узле, которому необходимо получить доступ к защищённому сегменту сети.

Исходя из значений метрик каналов, ViPNet Coordinator IG будет выбирать более приоритетный канал связи. Для этого при включении ViPNet Coordinator IG отправляет служебные сообщения на все известные адреса доступа узлов с определённой задержкой, равной метрике, заданной для этих адресов в миллисекундах. Выбор канала для связи производится с учетом следующего:

- Адрес с наименьшей метрикой считается наиболее приоритетным. Соединение с узлом устанавливается по адресу с наименьшей метрикой всегда, когда этот адрес доступен.
- Если адрес с наименьшей метрикой недоступен или если все метрики равны, то соединение с узлом устанавливается по тому адресу, доступность которого определяется быстрее в результате опроса.
- Если помимо адресов с заданными метриками, есть адреса, для которых метрика установлена в значение `auto` (определяется автоматически), значение `auto` всегда будет на 100 миллисекунд больше максимального значения заданной метрики. То есть канал с автоматически определяемой метрикой всегда будет иметь самый низкий приоритет по сравнению с каналами, для которых метрика задана вручную.
- После установления соединения с узлом определение доступности других его адресов выполняется только при разрыве текущего соединения. Задержка в выборе альтернативного канала связи может составлять от 7 до 70 секунд.

Адреса доступа для узлов, связанных с ViPNet Coordinator IG, настраиваются в соответствующих секциях `[id]` файла `iplir.conf`. Каждый адрес доступа узла указывается в параметре `accessiplist` этой секции, количество данных параметров в секции не ограничено.

Примечание. IP-адреса доступа узла могут быть настроены централизованно в ViPNet Prime. В этом случае они будут указаны в соответствующих секциях `[id]` файла `iplir.conf`. Для таких адресов вы также можете настроить приоритет, изменив соответствующие значения метрик (по умолчанию они определяются автоматически).

Чтобы указать IP-адреса доступа к какому-либо узлу, связанному с ViPNet Coordinator IG, и определить приоритеты этих адресов:

1 Завершите работу управляющей службы:

```
hostname# iplir stop
```

2 Откройте файл `iplir.conf` для редактирования:

```
hostname# iplir config
```

3 В параметрах `accessiplist` секции `[id]` соответствующего узла выполните одно из действий:

- Укажите IP-адреса доступа к узлу и задайте метрики маршрутов для каждого из этих адресов в следующем виде:

  ```
  accessiplist= <IP-адрес узла>, <метрика>
  ```

  При задании значения метрики необходимо учитывать следующее:

  - рекомендуется указывать значения метрик больше максимального времени задержки при прохождении служебного сообщения и ответа на него по соответствующему каналу связи, но не превышающее 9999 миллисекунд;
  - рекомендуемая минимальная разница между метриками — 100 миллисекунд.

- Если вы уже указали IP-адреса доступа ранее или они были получены из ViPNet Prime автоматически, в параметре `accessiplist` задайте метрики маршрутов для этих адресов в соответствии с рекомендациями, описанными выше.

4 Сохраните изменения (**Ctrl+O**, затем нажмите **Enter**) и закройте редактор (**Ctrl+X**).

5 Запустите управляющую службу:

```
hostname# iplir start
```

В результате в параметры `accessiplist` файла `iplir.conf` автоматически будут добавлены реальный IP-адрес сетевого интерфейса узла, через который будут передаваться IP-пакеты для выбранного IP-адреса доступа, условный номер этого интерфейса и тип регистрации данного IP-адреса доступа узла в виде:

```
accessiplist= <IP-адрес узла>, <метрика>, <IP-адрес интерфейса>, <номер интерфейса>, <тип регистрации>
```

Например, запись об автоматическом добавлении IP-адреса 89.135.15.2 с метрикой 1 будет выглядеть следующим образом:

```
accessiplist= 89.135.15.2, 1, 0.0.0.0, 0, auto
```

Подробнее о параметре `accessiplist` см. в документе «Справочник команд и конфигурационных файлов», описание секции `[id]` файла `iplir.conf`.

Настройка TCP-туннеля

При удалённом подключении клиентов к сетям ViPNet может возникать проблема с передачей IP-пакетов по протоколу UDP из-за того, что данный протокол блокируется некоторыми интернет-провайдерами. Но в этих случаях обычно разрешён доступ по протоколу TCP через порты 80 (HTTP) и 443 (HTTPS).

Для решения проблемы доступа можно организовать взаимодействие клиентов с другими узлами сети ViPNet через TCP-туннель, настроенный на сервере соединений этих клиентов. В таком случае ViPNet Coordinator IG будет выступать в качестве сервера TCP-туннелей, а удалённые клиенты (ViPNet-клиенты или другие координаторы) — в качестве клиентов TCP-туннелей.

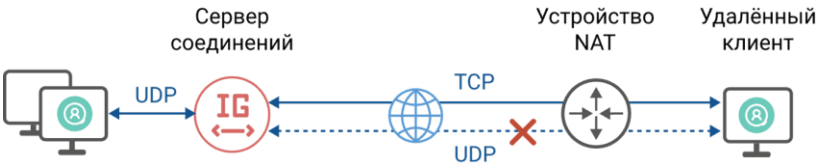


Рисунок 6: Доступ удалённого клиента к сети ViPNet через TCP-туннель

Если клиент TCP-туннеля не может связаться со своим сервером соединений (сервером TCP-туннелей) по протоколу UDP, он автоматически начинает устанавливать с ним соединение через TCP-туннель. Сервер соединений (сервер TCP-туннелей) передаёт полученные от клиента IP-пакеты дальше на узлы назначения по протоколу UDP.

ViPNet Coordinator IG может работать в режиме сервера TCP-туннелей или в режиме клиента TCP-туннеля, подключаясь к своему серверу соединений.

Настройка сервера TCP-туннелей

Примечание. ViPNet Coordinator IG может поддерживать не более 100 соединений через TCP-туннель.

При соединении через TCP-туннель клиентам не будут приходить уведомления в случае рассинхронизации времени.

Условия работы TCP-туннеля

- ViPNet Coordinator IG должен иметь публичный IP-адрес, поскольку для установления TCP-соединения клиент использует именно публичный IP-адрес доступа сервера соединений.
- На ViPNet Coordinator IG должен быть запущен сервер TCP-туннелей и настроен порт для входящих TCP-соединений (см. описание ниже).
- На клиентах TCP-туннеля заданный порт должен совпадать с номером порта, который используется на ViPNet Coordinator IG для TCP-соединений. Номер порта поступает клиенту от

сервера соединений в составе служебной информации. Если служебная информация не поступила, то порт на клиенте можно задать вручную.

Настройка работы TCP-туннеля

1 Убедитесь, что служба `iplircfg` запущена:

```
hostname# failover show info
```

2 Назначьте ViPNet Coordinator IG роль сервера TCP-туннелей (установлена по умолчанию):

```
hostname# iplir tcptunnel role server
```

3 По умолчанию для подключения клиентов TCP-туннелей к ViPNet Coordinator IG задан порт 80, но если в ViPNet Prime задан другой порт, он изменится в настройках ViPNet Coordinator IG. Чтобы просмотреть, какой порт задан:

```
hostname# iplir show tcptunnel-info
```

Порт указан в параметре `TCP server port`.

Если этот порт используется другой службой, измените номер порта:

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

4 Запустите сервер TCP-туннелей:

```
hostname# iplir tcptunnel server on
```

Если номер порта был изменён, то на все клиенты TCP-туннеля будет отправлена информация с новым номером порта для TCP-соединений.

Настроить сервер TCP-туннелей также можно путём редактирования конфигурационного файла `iplir.conf`.

Примечание. В случае если протокол UDP перестал блокироваться, соединение по данному протоколу восстановится при следующих условиях:

- по истечении таймаута отправки служебных IP-пакетов с клиента на сервер соединений (по умолчанию таймаут равен 5 минутам);
- после проверки соединения этого узла с другим;
- после смены IP-адреса узла (например, при изменении точки доступа к интернету).

Настройка клиента TCP-туннеля

Примечание. Работа ViPNet Coordinator IG в качестве клиента TCP-туннеля возможна только при подключении к сети в режиме «С динамической трансляцией адресов» (см. Настройка подключения к внешней сети).

---

1 Убедитесь, что служба `iplircfg` запущена:

```
hostname# failover show info
```

2 Назначьте ViPNet Coordinator IG роль клиента:

```
hostname# iplir tcptunnel role client
```

3 Выберите режим подключения:

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

- `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.

4 Задайте порт для подключения к серверу TCP-туннелей:

```
hostname# iplir tcptunnel client port <порт>
```

Этот порт должен совпадать с номером порта, заданным на сервере TCP-туннелей.

Если порт используется какой-либо другой службой, нужно задать другой порт на клиенте и сервере TCP-туннелей.

5 Включите режим клиента TCP-туннелей:

```
hostname# iplir tcptunnel client on
```

Настроить клиента TCP-туннелей также можно путём редактирования конфигурационного файла `iplir.conf`.

Настройка туннелирования на канальном уровне по технологии L2OverIP

Общие сведения об L2OverIP

ViPNet Coordinator IG поддерживает технологию L2OverIP, которая позволяет организовать защиту удалённых сегментов сети, использующих одно адресное пространство, на канальном уровне модели OSI. В результате сетевые узлы из разных сегментов смогут взаимодействовать друг с другом так, как будто они находятся в одном сегменте с прямой видимостью по MAC-адресам. Такая защита может потребоваться, например, для организации работы территориально распределённых ЦОДов (центров обработки данных), локальные сети которых объединены высокоскоростным каналом связи и представляют собой единый широковещательный домен.

Технология L2OverIP предполагает взаимодействие между узлами нескольких удалённых сегментов сети через ViPNet Coordinator IG, которые установлены на границах этих сегментов. ViPNet Coordinator IG перехватывает Ethernet-кадры, отправленные из его сегмента сети в другой, упаковывает их в IP-пакеты специального формата и передаёт эти IP-пакеты другому ViPNet Coordinator IG по защищённому каналу. ViPNet Coordinator IG, получивший IP-пакеты специального формата, извлекает из них исходные кадры и передаёт получателям в своем сегменте.

С помощью L2OverIP можно объединить несколько сегментов сети:

- сегменты без VLAN, находящиеся за сетевыми интерфейсами класса `access`;
- виртуальная сеть VLAN из одного сегмента и виртуальная сеть VLAN из другого сегмента;
- все виртуальные сети VLAN из одного сегмента со всеми виртуальными сетями другого сегмента (для этого необходимо указать сетевые интерфейсы класса `trunk`, за которыми находятся виртуальные сети VLAN; адреса виртуальных сетей VLAN должны совпадать);
- одна из виртуальных сетей VLAN сегмента и сегмент без VLAN, находящийся за сетевым интерфейсом класса `access`.

При использовании L2OverIP ViPNet Coordinator IG работает как виртуальный сетевой коммутатор, хранящий в памяти таблицу MAC-адресов сетевых узлов, от которых поступает сетевой трафик.

Каждому сегменту сети назначается свой номер порта, который задаётся в настройках L2OverIP. Порт, заданный для собственного сегмента сети, называется локальным. Порты, заданные на ViPNet Coordinator IG в других сегментах, называются удалёнными. Трафик самого ViPNet Coordinator IG всегда относится к порту с номером 0.

L2OverIP можно использовать в кластере (см. Развёртывание кластера). Настройка L2OverIP выполняется на активном узле. При переключении узлов кластера таблица MAC-адресов не

передаётся пассивному узлу. Коммутация кадров восстановится, когда узлы из разных сегментов, взаимодействующие друг с другом, заново отправят ARP-запросы.

Особенности реализации L2OverIP в ViPNet Coordinator IG

- Сегменты сети, объединяемые по L2OverIP, должны быть изолированы друг от друга. Сетевое взаимодействие между ними должно осуществляться только по каналам связи между ViPNet Coordinator IG, установленными на границах объединяемых сегментов.
- Для использования беспроводных интерфейсов в L2OverIP действуют ограничения:
  - нельзя использовать интерфейс модема;
  - интерфейс Wi-Fi можно использовать только со статическим IP-адресом.
- Текущая версия ViPNet Coordinator IG позволяет объединять не более 31 сегмента сети.
- Используйте не более 252 IP-адресов во всех объединяемых сегментах сети. Превышение этого количества может привести к снижению пропускной способности сети в связи с возрастанием служебного трафика в широковещательном домене.
- Поиск IP-пакетов, переданных по L2OverIP, в журнале регистрации IP-пакетов необходимо выполнять по признакам исходных IP-пакетов: IP-адрес источника и получателя, номер TCP- и UDP-порта, интерфейс.

Настройка L2OverIP

При настройке туннелирования на канальном уровне каждый сегмент сети подключается к одному из сетевых интерфейсов ViPNet Coordinator IG, установленному на границе сегмента. Если сегмент сети состоит из нескольких VLAN, они должны быть объединены с помощью коммутатора в транковый порт, к которому подключается один из сетевых интерфейсов ViPNet Coordinator IG (см. документ «Сценарии работы», раздел «Настройка L2OverIP в случае использования VLAN»).

Чтобы настроить L2OverIP, на каждом ViPNet Coordinator IG:

1 Укажите сетевой интерфейс, подключённый к локальному сегменту сети, который требуется объединить с другим сегментом по L2OverIP:

```
hostname# iplir set l2overip interface <имя интерфейса>
```



Примечание. Если требуется объединить отдельную VLAN одного сегмента сети с другим сегментом сети, на ViPNet Coordinator IG, стоящем на границе сегмента с VLAN, укажите в качестве интерфейса виртуальный интерфейс VLAN в формате `<физический интерфейс>.<номер виртуального интерфейса>`.

2 Задайте статический IP-адрес на сетевом интерфейсе, который будет подключён к ViPNet Coordinator IG удалённого сегмента сети (далее — внешний интерфейс):

```
hostname# inet ifconfig <имя внешнего интерфейса> address <IP-адрес> netmask <маска сети>
```

3 Задайте параметры локального сегмента сети — уникальный номер порта сегмента и IP-адрес внешнего интерфейса ViPNet Coordinator IG:

```
hostname# iplir set l2overip local-port <номер порта> <IP-адрес внешнего интерфейса>
```

В качестве номера порта вы можете задать значение из интервала 1–31. Каждому сегменту необходимо назначить свой номер порта.

4 Вы можете изменить время жизни MAC-адреса в таблице MAC-адресов виртуального коммутатора (см. Общие сведения об L2OverIP) при отсутствии трафика от этого адреса. По умолчанию задано значение — 300 секунд. Чтобы изменить его:

```
hostname# iplir set l2overip mac-ttl <время жизни MAC-адреса>
```

Задайте значение из интервала 60–86400.

5 Вы можете изменить режим обработки функцией L2OverIP одноадресных Ethernet-кадров с неизвестным MAC-адресом получателя. По умолчанию такие кадры блокируются. Чтобы изменить режим обработки:

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

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

6 Задайте параметры удалённого сегмента сети — номер порта сегмента и IP-адрес видимости внешнего интерфейса удалённого ViPNet Coordinator IG:

```
hostname# iplir set l2overip remote-port <номер порта> <IP-адрес удалённого ViPNet Coordinator IG>
```

В зависимости от настройки видимости удалённого ViPNet Coordinator IG укажите его реальный или виртуальный IP-адрес. Если ViPNet Coordinator IG имеет более одного адреса видимости для удалённого ViPNet Coordinator IG (секция `[id]` конфигурационного файла `iplir.conf`, соответствующая удалённому координатору, содержит более одного параметра `ip`), настройте видимость удалённого ViPNet Coordinator IG по реальным адресам и укажите его реальный IP-адрес.



Внимание! Если в процессе работы вы поменяете видимость удалённого узла, измените его адрес в настройках L2OverIP:

```
hostname# iplir set l2overip remote-port <номер порта> <новый IP-адрес>
```

После изменения адреса удалённого узла перезапустите службу L2OverIP:

```
hostname# iplir set l2overip mode none
hostname# iplir set l2overip mode switch
```

7 Добавьте фильтры защищённой сети, разрешающие любые соединения по протоколу 97:

```
hostname# firewall vpn add src @local dst @any proto 97 pass
hostname# firewall vpn add src @any dst @local proto 97 pass
```

8 Включите службу L2OverIP:

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

9 Проверьте текущее состояние и настройки L2OverIP:

```
hostname# iplir show l2overip config
```

На узлах локального сегмента сети укажите IP-адрес ViPNet Coordinator IG в качестве шлюза по умолчанию.

Примеры организации защищённого соединения между удалёнными сегментами сети с использованием L2OverIP см. в документе «Сценарии работы», в разделе «Защита соединения между удалёнными сегментами сети на канальном уровне модели OSI».

4

Настройка фильтрации трафика

Настройка сетевых фильтров 81

Настройка фильтрации промышленных протоколов 103

Настройка прокси-сервера 116

Настройка межсетевого экрана 125

Настройка сетевых фильтров

Типы трафика

Фильтрации подвергается весь трафик, который проходит через ViPNet Coordinator IG:

- → открытый трафик — незашифрованный трафик между открытыми (или открытым и защищённым) узлами;
- → защищённый трафик — зашифрованный трафик между узлами сети ViPNet.

Открытый трафик может быть локальным или транзитным:

- локальный трафик — трафик, в котором ViPNet Coordinator IG является получателем или отправителем IP-пакетов;
- транзитный трафик — трафик, в котором ViPNet Coordinator IG не является ни получателем, ни отправителем IP-пакетов.

ViPNet Coordinator IG обрабатывает трафик, разделяя его на следующие типы:

- открытый локальный трафик — между открытым узлом и ViPNet Coordinator IG;
- защищённый трафик — трафик между узлами сети ViPNet;
- туннелируемый трафик — трафик между двумя открытыми (или открытым и защищённым) узлами, зашифрованный в пределах сети ViPNet;

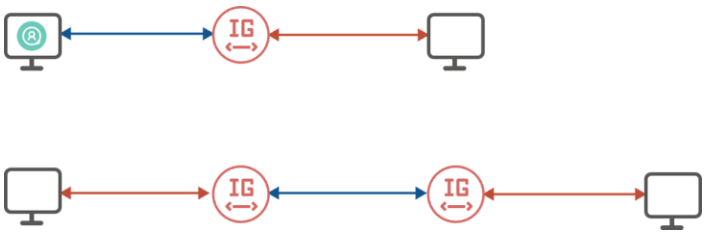


Рисунок 7. Туннелируемый трафик

- открытый транзитный трафик — трафик между открытыми (или открытым и защищённым) узлами, проходящий через координатор, который не является ни отправителем, ни получателем IP-пакетов.



Рисунок 8. Открытый транзитный трафик

Для каждого типа трафика можно настроить соответствующие сетевые фильтры (см. Создание сетевого фильтра).

Принципы фильтрации трафика

- Все входящие и исходящие открытые и защищённые IP-пакеты обрабатываются сетевыми фильтрами в порядке убывания приоритета этих фильтров.
- Если IP-пакет соответствует условию одного из фильтров, он пропускается или блокируется этим фильтром; при этом фильтры с более низким приоритетом не применяются.
- Если IP-пакет был пропущен одним из фильтров, ответные IP-пакеты (включая служебные ICMP-пакеты) в рамках текущего соединения будут пропускаться автоматически.
- Если IP-пакет не был обработан ни одним из фильтров, он блокируется фильтром по умолчанию.

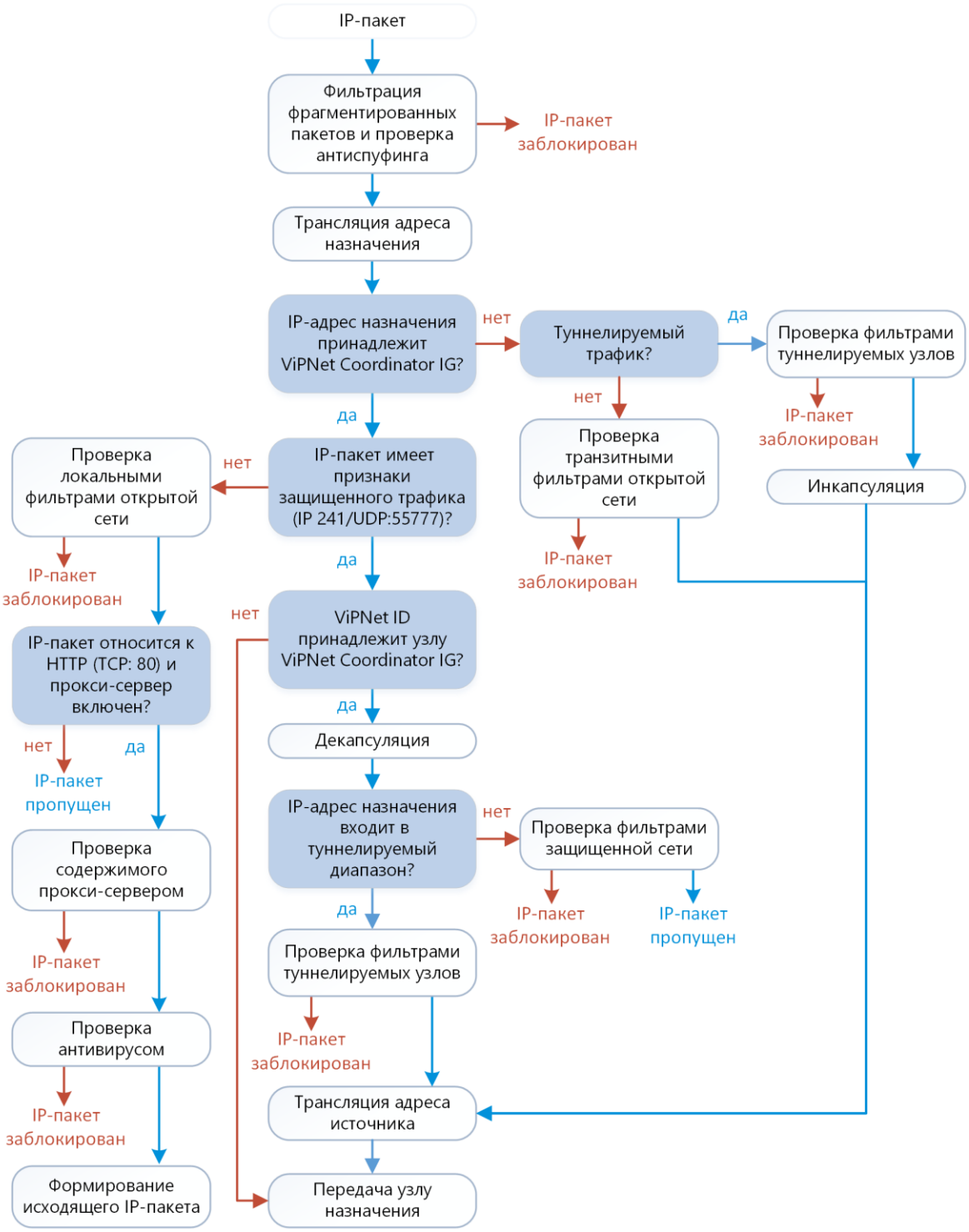


Рисунок 9. Схема фильтрации трафика

IP-пакет, поступивший на сетевой интерфейс ViPNet Coordinator IG, последовательно проходит ряд проверок:

1 IP-пакет проверяется на фрагментацию, если эта проверка включена (см. Настройка дополнительных параметров межсетевого экрана). Если IP-пакет фрагментирован, он блокируется, иначе — передаётся на следующий шаг проверки.

2 IP-пакет обрабатывается правилами антиспуфинга, если он включён (см. Настройка антиспуфинга). В результате IP-пакет блокируется или передаётся на следующий шаг проверки.

3 Случаи, в которых выполняется трансляция IP-адреса назначения (см. Трансляция адреса назначения):

- IP-пакет удовлетворяет условиям правила трансляции адресов.
- Включена обработка прикладного протокола, к которому относится IP-пакет (см. Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP).
- IP-пакет соответствует протоколу HTTP (TCP: 80) и прокси-сервер работает в «прозрачном» режиме. В этом случае с помощью трансляции адреса назначения транзитный трафик перенаправляется на ViPNet Coordinator IG и обрабатывается как локальный трафик открытой сети.

4 Если IP-пакет адресован ViPNet Coordinator IG и имеет признаки защищённого трафика (протокол IP/241 или протокол UDP и порт 55777 или другой порт, настроенный администратором), то в IP-пакете проверяется идентификатор узла ViPNet (ViPNet ID):

- Если ViPNet ID не принадлежит ViPNet Coordinator IG, в IP-пакете преобразуются IP-адреса и порты в соответствии с имеющейся информацией о ближайшей к узлу назначения точке доступа. Затем IP-пакет отправляется в сеть для передачи узлу назначения.
- Если ViPNet ID принадлежит ViPNet Coordinator IG, выполняется расшифровка и декапсуляция IP-пакета. Полученный IP-пакет (исходный IP-пакет) проверяется на принадлежность туннелируемому трафику:
  - Если IP-адрес назначения в исходном IP-пакете входит в туннелируемый диапазон ViPNet Coordinator IG, IP-пакет проверяется фильтрами туннелируемых узлов. В результате IP-пакет блокируется или отправляется на туннелируемый узел после трансляции адреса источника.
  - Если IP-адрес назначения в исходном IP-пакете не входит в туннелируемый диапазон ViPNet Coordinator IG, IP-пакет проверяется фильтрами защищённой сети, после чего блокируется или пропускается.

5 Если IP-пакет адресован ViPNet Coordinator IG и не имеет признаков защищённого трафика, IP-пакет проверяется локальными фильтрами открытой сети. В результате IP-пакет блокируется или проходит следующие проверки:

5.1 Если IP-пакет относится к протоколу HTTP (TCP: 80), он проверяется прокси-сервером на прикладном уровне. Если прокси-сервер выключен или IP-пакет не относится к протоколу HTTP, IP-пакет пропускается.

5.2 После проверки прокси-сервером выполняется антивирусная проверка, если она включена. В результате IP-пакет блокируется или формируется новый исходящий IP-пакет.

6 Если IP-пакет адресован не ViPNet Coordinator IG, а другому узлу, проверяется принадлежность IP-пакета туннелируемому трафику:

- Если IP-адрес отправителя входит в туннелируемый диапазон ViPNet Coordinator IG, а IP-адрес получателя входит в туннелируемый диапазон другого координатора или принадлежит защищённому узлу, IP-пакет проверяется фильтрами туннелируемых узлов. В

результате IP-пакет блокируется или отправляется получателю после процедур инкапсуляции и трансляции адреса источника.

- Если IP-пакет не принадлежит туннелируемому трафику, IP-пакет проверяется транзитными фильтрами открытой сети. В результате IP-пакет блокируется или отправляется получателю после трансляции адреса источника.



Примечание. Если настроена фильтрация промышленных протоколов, то при проверке IP-пакета сетевыми фильтрами (локальными, транзитными, фильтрами защищённой сети или фильтрами туннелируемых узлов) правила фильтрации промышленных протоколов применяются в первую очередь. Подробнее см. Настройка фильтрации промышленных протоколов.

Особенности при настройке фильтрации трафика на ViPNet Coordinator IG:

- TCP-порт 2047 и UDP-порт 2046 являются служебными портами ViPNet Coordinator IG, поэтому входящий открытый трафик, поступающий на эти порты, блокируется без возможности настройки.
- Изменения в конфигурации межсетевого экрана, влияющие на открытый транзитный трафик, начинают действовать сразу, в том числе для уже установленных ранее соединений.

  Изменения в конфигурации межсетевого экрана, влияющие на другие виды трафика, будут действовать только для новых соединений. К уже установленным соединениям изменения не будут применены до истечения времени жизни соединения. Чтобы принудительно применить изменения ко всем соединениям, выполните команду в командном интерпретаторе:

  ```
  hostname# firewall conntrack flush
  ```

Общие сведения о сетевых фильтрах

Типы фильтров

Сетевые фильтры различаются по типу трафика (защищённый, туннелируемый, открытый локальный и транзитный), который они обрабатывают:

- Фильтры защищённой сети. Могут разрешать или блокировать обмен IP-трафиком с защищёнными узлами, с которыми ViPNet Coordinator IG имеет связь.
- Фильтры туннелируемых узлов. Могут разрешать или блокировать IP-пакеты, передаваемые между туннелируемыми узлами и узлами сети ViPNet, с которыми ViPNet Coordinator IG имеет связь.
- Локальные фильтры открытой сети. Могут разрешать или блокировать обмен IP-трафиком ViPNet Coordinator IG с открытыми узлами.
- Транзитные фильтры открытой сети. Могут разрешать либо блокировать обмен IP-трафиком между открытыми (или открытым и защищённым) узлами, проходящий через ViPNet Coordinator IG.

Сетевые фильтры для каждого типа трафика разделяются на:

- Служебные фильтры. Создаются автоматически; имеют самый высокий приоритет и недоступны для изменения.
- Фильтры, поступившие в составе политик безопасности из ViPNet Prime Policy Management. Применяются после служебных фильтров. Недоступны для изменения. В составе политик безопасности, формируемых в ViPNet Prime Policy Management, могут быть и правила трансляции адресов. При получении политики безопасности из ViPNet Prime Policy Management, она немедленно применяется на узле.
- Настраиваемые фильтры. Содержат предустановленные фильтры и фильтры, создаваемые пользователем. Применяются после фильтров, поступивших в составе политик безопасности. Доступны для изменения.
- Блокирующий фильтр по умолчанию. Применяется после всех фильтров. Недоступен для изменения.

Порядок применения фильтров

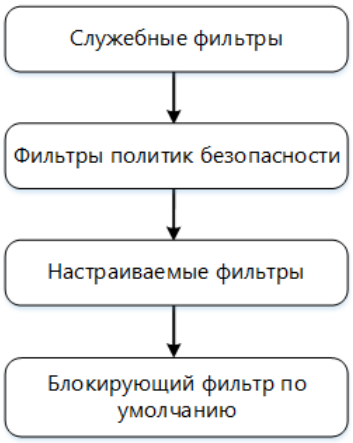


Рисунок 10. Порядок применения фильтров

Параметры фильтров

В настраиваемых сетевых фильтрах вы можете задать:

- адрес отправителя и получателя IP-пакетов, на которые действует фильтр;
- транспортные протоколы, используемые для передачи этих IP-пакетов, например, TCP, UDP, ICMP;
- расписание применения фильтра — ежедневно, еженедельно или по календарю;
- признак регистрации IP-пакетов в журнале IP-пакетов при срабатывании фильтра;
- действие, применяемое к IP-пакетам:
  - пропускать;
  - блокировать;
  - блокировать и отправить ICMP-уведомление.

Подсчёт срабатываний фильтров

В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 для каждого сетевого фильтра ведётся подсчёт срабатываний. Счётчик срабатываний запускается с момента первого включения ViPNet Coordinator IG. Сброс счётчика выполняется в ViPNet Prime. Перезагрузка ViPNet Coordinator IG, обновление ПО или переключение узлов кластера не влияют на подсчёт срабатываний. Просмотр срабатываний фильтров доступен только в веб-интерфейсе.

Группы объектов

Группы объектов позволяют упростить процессы создания и изменения сетевых фильтров и правил трансляции сетевых адресов в ViPNet Coordinator IG. Каждая группа объединяет несколько объектов одного типа (например, IP-адреса или сетевые интерфейсы). Группы можно указывать в параметрах сетевого фильтра или правила трансляции сетевых адресов вместо перечисления отдельных объектов.

В зависимости от типа объединяемых объектов различаются следующие группы:

- Группа сетевых узлов ViPNet — содержит любую комбинацию узлов сети ViPNet, используется в фильтрах защищённой сети и фильтрах туннелируемых узлов.
- Группа IP-адресов — содержит любую комбинацию IP-адресов, диапазонов IP-адресов и доменных имен, используется в фильтрах открытой сети, фильтрах туннелируемых узлов и правилах трансляции сетевых адресов.
- Группа сетевых интерфейсов — содержит любую комбинацию сетевых интерфейсов, используется в фильтрах открытой сети и фильтрах туннелируемых узлов.
- Группа протоколов — содержит любую комбинацию сетевых протоколов и портов, используется в фильтрах открытой и защищённой сетей, фильтрах туннелируемых узлов и правилах трансляции сетевых адресов.
- Группа расписания — содержит любую комбинацию параметров, определяющих время действия сетевого фильтра, используется в фильтрах открытой и защищённой сетей, фильтрах туннелируемых узлов.

Каждая группа объектов относится к одному из следующих видов:

- Системные группы объектов — настроенные по умолчанию группы с фиксированными именами, которые могут использоваться для задания адресов отправителей и получателей IP-пакетов в сетевых фильтрах и правилах трансляции адресов, а также при создании пользовательских групп объектов. Такие группы объектов не отображаются в списках групп (см. Просмотр групп объектов), их нельзя ни изменить, ни удалить.
- Группы объектов из ViPNet Prime Policy Management — группы, получаемые в составе политик безопасности, и используемые в соответствующих фильтрах. Такие группы нельзя ни удалять, ни изменять, ни использовать для задания параметров пользовательских фильтров и групп объектов.

- Пользовательские группы объектов — группы, создаваемые пользователем на узле, а также несколько групп, настроенных по умолчанию. Такие группы можно использовать для задания параметров сетевых фильтров и правил трансляции адресов, а также при создании других пользовательских групп объектов.

Системные группы объектов

В таблице ниже описаны доступные системные группы объектов и указано соответствие имён системных групп объектов ViPNet Coordinator IG в командном интерпретаторе и веб-интерфейсе.

Таблица 3. Системные группы объектов

Имя системной группы объектов	Описание и область применения группы
`allclients` (Все клиенты)	Все клиенты, с которыми у узла есть связь. Можно использовать в фильтрах защищённой сети и фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.
`allcoordinators` (Все координаторы)	Все координаторы, с которыми у узла есть связь. Можно использовать в фильтрах защищённой сети и фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.
`broadcast` (Широковещательные адреса)	Все широковещательные адреса. Можно использовать в фильтрах защищённой сети и фильтрах открытой сети для идентификации широковещательных адресов получателей. Использование других адресов совместно с этой группой недопустимо.
`local` (Мой узел)	Собственный узел ViPNet Coordinator IG. Можно использовать в фильтрах защищённой сети и фильтрах открытой сети для задания адреса отправителя для исходящих соединений узла или адреса получателя для входящих соединений узла. Использование других адресов совместно с этой группой недопустимо.
`remote` (Другие узлы)	Другие узлы (любые, кроме собственного). Можно использовать в фильтрах защищённой сети и фильтрах открытой сети для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла. Использование других адресов совместно с этой группой недопустимо.

Имя системной группы объектов	Описание и область применения группы
`tunneledip` (Туннелируемые IP-адреса)	Все IP-адреса, туннелируемые координатором. Можно использовать в фильтрах туннелируемых узлов для задания адреса отправителя для входящих соединений узла или адреса получателя для исходящих соединений узла.
`multicast` (Групповые адреса)	Диапазон IP-адресов для групповой рассылки (224.0.0.0 – 239.255.255.255). Можно использовать в фильтрах открытой сети для задания адреса получателя. Использование других адресов совместно с этой группой недопустимо.

Кроме того, в сетевых фильтрах и правилах трансляции сетевых адресов может использоваться объект `any`, обозначающий любое значение, то есть:

- для локальных и транзитных фильтров открытой сети — все IP-адреса;
- для фильтров защищённой сети — все VPN-узлы;
- для фильтров туннелируемых узлов — все IP-адреса или все VPN-узлы;
- для протоколов — все протоколы;
- для расписаний — все время (постоянно).

Использование других условий совместно с объектом `any` недопустимо.

Пользовательские группы объектов по умолчанию

По умолчанию в ViPNet Coordinator IG настроены следующие пользовательские группы объектов:

- Группы IP-адресов:
  - `PrivateNetworkIP` (частные IP-адреса) — IP-адреса локальных сетей: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16.
  - `InternetIP` (публичные IP-адреса) — IP-адреса за исключением частных IP-адресов.
  - `HttpProxyUsers` — IP-адреса локальных сетей, которым разрешён доступ к прокси-серверу.



Внимание! Группа объектов `HttpProxyUsers` автоматически создаётся при добавлении сетевых фильтров и правил трансляции, необходимых для работы прокси-сервера, с помощью команды:

```
hostname# service http-proxy fw-rules apply
```

- Группы протоколов (см. Пользовательские группы протоколов по умолчанию).
- Группы расписаний:

- `Workdays` — рабочие дни недели (с понедельника по пятницу).
- `Weekends` — выходные дни недели (суббота и воскресенье).

Создание пользовательской группы объектов

Чтобы создать группу объектов, выполните:

`hostname# firewall <тип объектов> add name @<имя> <состав> [exclude <исключения>]`, где:

- параметр `<тип объектов>` может принимать одно из следующих значений:
  - `ip-object` — IP-адреса или доменные имена;
  - `vpn-object` — узлы сети ViPNet;
  - `interface-object` — сетевые интерфейсы;
  - `service-object` — протоколы;
  - `schedule-object` — расписания;
- имя группы объектов должно быть уникальным, допустимые символы: a–z, A–Z, 0–9, _ и точка;
- в параметрах `<состав>` и `<исключения>` указываются объекты, входящие и не входящие в группу соответственно, причем:
  - IP-адреса и идентификаторы узлов сети ViPNet указываются через запятую или в виде диапазона (подробнее см. в разделах Адрес отправителя и Адрес получателя);
  - сетевые интерфейсы разделяются пробелом, и перед именем каждого сетевого интерфейса необходимо указать слово `interface`;
  - протоколы или расписания указываются в соответствии с синтаксисом, описанным в разделах Протокол и Расписание;
  - количество объектов, входящих в группу, не должно превышать 1000.

Примечание. Если при вводе команды допущена синтаксическая ошибка, то после выполнения такой команды появится сообщение с указанием места ошибки. Исправьте ошибку и выполните команду еще раз.

В результате будет создана группа объектов, и вы сможете использовать ее для задания параметров сетевых фильтров и правил трансляции сетевых адресов.

Примеры создания групп объектов

- 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
  ```

Просмотр групп объектов

Чтобы просмотреть пользовательские группы объектов и группы объектов, полученные из ViPNet Prime Policy Management, выполните одну из команд:

- для просмотра всех групп объектов:

  ```
  hostname> firewall object show
  ```

- для просмотра групп объектов определённого типа:

  ```
  hostname> firewall <тип объектов> show
  ```

  Например, для просмотра всех групп IP-адресов:

  ```
  hostname> firewall ip-object show
  ```

В результате будет выведена таблица, содержащая группы объектов.

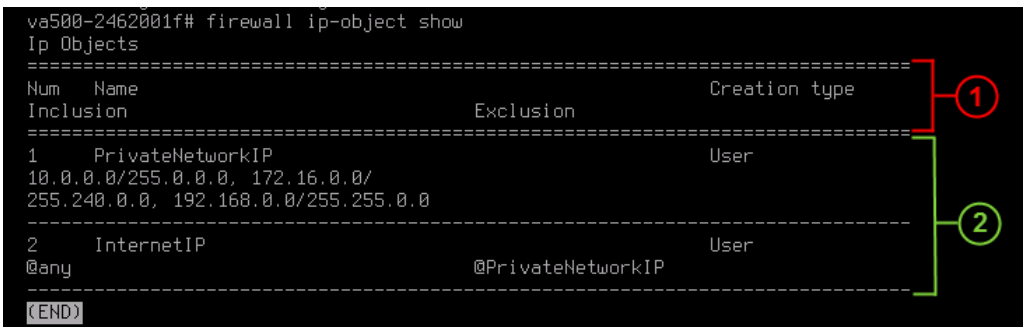


Рисунок 11. Просмотр групп IP-адресов

Цифрами обозначены:

1 Заголовок таблицы, где:
   - `Num` — порядковый номер группы объектов.
   - `Name` — имя группы объектов.
   - `Creation type` — вид группы объектов:
     - для групп из ViPNet Prime Policy Management — `Policy`;
     - для пользовательских групп — `User`.
   - `Inclusion` — состав группы объектов.
   - `Exclusion` — исключения группы объектов.

2 Параметры групп объектов.

Удаление пользовательских групп объектов

Вы можете удалить пользовательскую группу объектов, если она не используется в других группах объектов, сетевых фильтрах или правилах трансляции сетевых адресов.

Для удаления пользовательской группы объектов выполните:

```
hostname# firewall object delete @<имя группы объектов>
```

При попытке удаления пользовательской группы объектов, используемой в другой группе объектов, сетевом фильтре или правиле трансляции сетевых адресов, появится сообщение об ошибке со списком всех групп, фильтров и правил, которые используют данную группу. Удалите эти группы, фильтры и правила, затем выполните команду для удаления группы ещё раз.

Чтобы удалить группу сетевых узлов ViPNet с именем `range_<диапазон узлов>`, которая создается при конвертации правил защищённой сети во время обновления ViPNet Coordinator IG, сначала удалите все сетевые фильтры, в которых содержится эта группа.

Создание сетевого фильтра

Для каждого типа трафика создаются отдельные сетевые фильтры, которые хранятся в соответствующей таблице (см. Просмотр сетевых фильтров).

Чтобы создать сетевой фильтр:

```
hostname# firewall <тип> add [<номер>] [rule <имя>] src <адрес отправителя>
dst <адрес получателя> [<протокол>] [<расписание>] [log {on | off}] <действие>
```

где:

- `<тип>` — тип фильтра:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `vpn` — фильтр защищённой сети;
  - `tunnel` — фильтр туннелируемых узлов.
- `<номер>` — порядковый номер сетевого фильтра в таблице, определяющий его приоритет. Чем меньше номер, тем выше приоритет фильтра (наиболее приоритетный фильтр имеет номер 1). Если заданный номер меньше максимального номера в таблице фильтров, номера фильтров, следующих за новым фильтром, автоматически увеличиваются на единицу (их приоритет понижается).

  Если номер не указан, сетевой фильтр будет последним в таблице, и он будет иметь самый низкий приоритет.
- `<имя>` — имя сетевого фильтра. Если имя состоит из нескольких слов, разделённых пробелом, заключите его в кавычки (например, `rule "number one"`).

  Если имя не указано, сетевой фильтр будет создан без имени.

Примечание. После создания фильтра защищённой сети, локального фильтра открытой сети или фильтра туннелируемых узлов, такой фильтр не будет действовать на уже установленные соединения до истечения времени жизни этих соединений.

Транзитный фильтр открытой сети действует сразу после его создания.

Параметры, определяющие процесс обработки IP-пакетов этим фильтром:

- Адрес отправителя.
- Адрес получателя.
- Протокол.
- Расписание.
- Регистрация IP-пакетов.
- Действие.

Внимание! Максимальное количество сетевых фильтров для вашего исполнения ViPNet Coordinator IG см. в документе «Подготовка к работе» в разделе «Основные отличия аппаратных платформ». Превышение этого количества может значительно снизить производительность ViPNet Coordinator IG.

Если для компьютеров вашей сети вы настроили доступ в интернет через прокси-сервер ViPNet Coordinator IG, то HTTP-трафик не будет обрабатываться транзитными фильтрами открытой сети. В этом случае для фильтрации HTTP-трафика используйте прокси-сервер (см. Настройка правил контент-фильтрации трафика).

Примеры создания сетевых фильтров

- Чтобы разрешить отправку FTP-запросов со своего узла открытому узлу с адресом 192.168.2.4:

```
hostname# firewall local add src @local dst 192.168.2.4 service @FTP pass
```

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

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

- Чтобы создать фильтр защищенной сети, разрешающий отправку IP-пакетов от защищенного узла с идентификатором 0x1a12000a на свой узел:

```
hostname# firewall vpn add src 0x1a12000a dst @local pass
```

- Чтобы создать фильтр, разрешающий отправку открытых транзитных IP-пакетов от узла с адресом 192.168.0.1 на узел с адресом 192.168.30.3 через координатор:

```
hostname# firewall forward add src 192.168.0.1 dst 192.168.30.3 pass
```

- Чтобы создать фильтр, разрешающий отправку IP-пакетов от туннелируемого узла с адресом 192.168.0.1 на защищенный узел с идентификатором 0x1234abab:

```
hostname# firewall tunnel add src 192.168.0.1 dst 0x1234abab pass
```

- Чтобы создать фильтр, разрешающий отправку IP-пакетов от туннелируемого узла с адресом 192.168.0.1 туннелируемому узлу с адресом 192.168.2.3:

```
hostname# firewall tunnel add src 192.168.0.1 dst 192.168.2.3 pass
```

Адрес отправителя

Адрес отправителя IP-пакетов является обязательным параметром сетевого фильтра и описывается лексемой:

```
src <адрес отправителя>
```

Возможные значения адреса отправителя:

- для локальных фильтров открытой сети:
  - IP-адрес или доменное имя узла;



Примечание. При задании адреса отправителя в виде доменного имени на DNS-сервер отправляется соответствующий запрос для разрешения данного имени. DNS-запись и время её жизни (TTL, «Time to live»), полученные в ответ на такой запрос, сохраняются в кеше. По истечении времени её жизни отправляется новый запрос на DNS-сервер для актуализации данных в кеше. Если полученные данные отличаются, происходит перезагрузка сетевых фильтров в драйвере ViPNet.

Если разрешения указанного в сетевом фильтре доменного имени по каким-либо причинам не произошло, то такой фильтр не загружается в драйвер ViPNet до тех пор, пока в результате отправки повторных запросов на DNS-сервер не будет получен корректный ответ.

  - диапазон IP-адресов узлов — два ограничивающие диапазон IP-адреса, разделённые дефисом. При этом значение второго IP-адреса (конца диапазона) должно быть больше первого (начала диапазона), например:

```
src 192.168.1.1-192.168.1.10
```

  - маска подсети — IP-адрес подсети в формате классовой или бесклассовой адресации CIDR (Classless Inter-Domain Routing), например:

```
src 192.168.1.0/24
```
или
```
src 192.168.1.0/255.255.255.0
```

  - доменное имя узла, например:

```
src mydomain.ru
```



Примечание. При необходимости вы можете задать несколько IP-адресов и доменных имён отправителей IP-пакетов в одной лексеме, перечислив их через запятую, например:

```
src 192.168.30.2,192.169.1.1,mydomain.ru
```

  - системная группа объектов `any` (любое значение), `local` (собственный узел) или `remote` (другие узлы) либо одна или несколько пользовательских групп IP-адресов. Имя группы

необходимо дополнить символом «@», несколько групп указываются через запятую. Например:

```
src @IP_group_1,@IP_group_2
```



Внимание! Использование других адресов отправителей IP-пакетов совместно с системными группами объектов `any`, `local` и `remote` недопустимо.

- сетевой интерфейс собственного узла, через который будут проходить IP-пакеты, в следующем виде:

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

- для транзитных фильтров открытой сети: то же, что для локальных фильтров открытой сети, но в таких фильтрах нельзя использовать системные группы объектов `local` и `remote`;
- для фильтров защищённой сети:
  - идентификатор узла сети ViPNet, например:

    ```
    src 0x1a12000a
    ```

  - системные группы объектов `any`, `allcoordinators`, `allclients`, `local` или `remote` либо пользовательские группы узлов ViPNet. Имя группы необходимо дополнить символом «@», несколько групп указываются через запятую. Например:

    ```
    src @allclients,@allcoordinators
    ```

  - идентификатор сети ViPNet, например:

    ```
    src 0x1a12
    ```

Примечание. При задании адреса отправителя для фильтров защищённой сети:



- В одной лексеме можно указать несколько идентификаторов узлов или сетей ViPNet, пользовательских групп узлов ViPNet и системную группу `allcoordinators` или `allclients`, перечислив их через запятую. Например: `src @allcoordinators,0x1a12000a`
- Нельзя указывать IP-адреса, доменные имена, маски адресов и сетевой интерфейс узла.
- Нельзя использовать другие адреса отправителей совместно с группами объектов `any`, `local` и `remote`.
- Фильтры защищённой сети используются только для локального защищённого 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`.

- для фильтров туннелируемых узлов: то же, что для локальных фильтров открытой сети и фильтров защищённой сети, но в таких фильтрах можно использовать только системные группы объектов `any`, `allcoordinators`, `allclients`, `tunneledip`.



Внимание! Если в фильтре туннелируемых узлов в качестве адреса отправителя указан идентификатор защищённого узла, то в качестве адреса получателя в этом фильтре должен быть указан адрес открытого узла, и наоборот.

Адрес получателя

Адрес получателя IP-пакетов является обязательным параметром сетевого фильтра. Синтаксис адреса получателя повторяет синтаксис адреса отправителя, за исключением следующих особенностей:

- Адрес получателя описывается после адреса отправителя лексемой:

  `dst <адрес получателя>`

- Для задания адреса получателя нельзя использовать сетевой интерфейс узла.
- Для задания адреса получателя, помимо пользовательских групп объектов, можно использовать следующие системные группы объектов:
  - Для локальных фильтров открытой сети: `any`, `local`, `remote`, `broadcast`, `multicast`.

    Внимание! Использование других адресов отправителей IP-пакетов совместно с системными группами объектов `any`, `local`, `remote`, `broadcast` и `multicast` недопустимо.

  - Для фильтров защищённой сети: `any`, `allcoordinators`, `allclients`, `local`, `remote`, `broadcast`.

    Примечание. Фильтры защищённой сети используются только для локального защищённого трафика, поэтому 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: `any`, `allcoordinators`, `allclients`, `tunneledip`.

Протокол

Протокол не является обязательным параметром сетевого фильтра.

Протоколы можно указывать, используя:

- Имена протоколов, написанные строчными буквами и разделённые пробелами, например:

  `tcp udp icmp`

  В этом случае также можно задать дополнительные параметры для протоколов, например:

  - для протоколов TCP и UDP: `sport` (порт или диапазон портов источника пакета) и (или) `dport` (порт или диапазон портов назначения пакета). При использовании обоих

параметров сначала необходимо указать параметр `sport`, затем — параметр `dport`. Например: `tcp sport 1024-65535 dport 1024;`

- для протокола ICMP: только параметр `type` (тип пакета) либо параметр `type` вместе с параметром `code` (код пакета). Например: `icmp type 3 code 1`. Если параметр `code` не задан, то под условие будут подпадать все ICMP-пакеты указанного типа;

- номера протоколов. В этом случае для каждого протокола необходимо указать ключевое слово `proto` и его номер. Например, для протоколов TCP, UDP и ICMP: `proto 6 proto 17 proto 1`;



Внимание! При использовании номеров протоколов задать дополнительные параметры протоколов невозможно.

- пользовательские группы протоколов, в том числе заданные по умолчанию, в виде:

  `service @<имя группы>`

  Например: `service @DNS`.

Расписание

Расписание задает время действия сетевого фильтра и не является его обязательным параметром. Описывается одной из следующих лексем:

- `daily <чч:мм>-<чч:мм>` — фильтр действует ежедневно в течение заданного интервала времени. Время указывается в 24-часовом формате: `чч` — часы, `мм` — минуты.
- `weekly [mo] [tu] [we] [th] [fr] [sa] [su] [at <чч:мм>-<чч:мм>]` — фильтр действует еженедельно в заданные дни недели:
  - `mo` — понедельник;
  - `tu` — вторник;
  - `we` — среда;
  - `th` — четверг;
  - `fr` — пятница;
  - `sa` — суббота;
  - `su` — воскресенье.
- `calendar <дд.мм.гггг>-<дд.мм.гггг> [at <чч:мм>-<чч:мм>]` — фильтр действует в заданные даты и интервал времени. Дата указывается в следующем формате:
  - `дд` — день;
  - `мм` — месяц;
  - `гггг` — год.

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

  Для задания расписания можно использовать соответствующие пользовательские группы, в том числе заданные по умолчанию.

Регистрация IP-пакетов

Необязательный параметр. Определяет действия по регистрации IP-пакетов в журнале IP-пакетов при срабатывании сетевого фильтра. Описывается лексемой log {on | off}:

- on — регистрировать IP-пакеты.

  По умолчанию устанавливается для всех фильтров с действием блокировать (drop) и отклонить (reject).

- off — не регистрировать IP-пакеты.

  По умолчанию устанавливается для всех фильтров с действием пропускать (pass).

Подробнее см. Журнал IP-пакетов.



Внимание! Отключение регистрации IP-пакетов в блокирующих сетевых фильтрах может помешать расследованию инцидентов информационной безопасности.

Действие

Действие является обязательным параметром сетевого фильтра и определяет, что делает фильтр с IP-пакетом, соответствующим его условию.

Действие описывается одной из следующих лексем:

- pass — пропустить IP-пакет;
- drop — блокировать IP-пакет;
- reject — отклонить IP-пакет и отправить ICMP-уведомление:
  - reject — отправляет сообщение Destination port unreachable;
  - rej-net-unreachable — отправляет сообщение Destination net unreachable;
  - rej-host-unreachable — отправляет сообщение Destination host unreachable;
  - rej-proto-unreachable — отправляет сообщение Destination protocol unreachable;
  - rej-net-prohibited — отправляет сообщение Network administratively prohibited;
  - rej-host-prohibited — отправляет сообщение Host administratively prohibited;
  - rej-admin-prohibited — отправляет сообщение Communication administratively prohibited;
  - rej-tcp-reset — отправляет сообщение TCP reset (только для TCP-пакетов).

Изменение сетевого фильтра

Вы можете изменить ранее созданный сетевой фильтр, а также его положение в таблице сетевых фильтров (приоритет).

Чтобы добавить в сетевой фильтр новые значения параметров или изменить настройку регистрации IP-пакетов:

1. Выполните команду:

   ```
   hostname# firewall <тип> change append <номер> <параметры>
   ```

   В качестве `<параметры>` вы можете указать: адрес отправителя, адрес получателя, протокол, расписание или параметр регистрации IP-пакетов. Вы можете указать несколько параметров в одной команде.

2. Для подтверждения изменений сетевого фильтра введите `y` в строке `Do you want to perform the action on the above rule? [Yes/No]` и нажмите **Enter**.

Например, чтобы в локальный фильтр открытой сети с номером 1 и параметрами `src 192.168.1.1,2.2.2.2/24 dst @local drop` добавить адрес отправителя 192.168.3.3, выполните команду:

```
hostname# firewall local change append 1 src 192.168.3.3
```

В результате фильтр будет содержать параметры: `src 192.168.1.1,2.2.2.2/24,192.168.3.3 dst @local drop`.

Чтобы изменить приоритет сетевого фильтра:

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

При этом номера фильтров, следующих за изменённым фильтром, автоматически увеличатся на единицу, то есть их приоритет понизится.

Просмотр сетевых фильтров

Чтобы просмотреть сетевые фильтры, заданные на ViPNet Coordinator IG, выполните одну из команд:

- Для просмотра всех сетевых фильтров, включая правила трансляции адресов:

  ```
  hostname> firewall rules show
  ```

- Для просмотра сетевых фильтров определённого типа:

  ```
  hostname> firewall <тип> show
  ```

  где `<тип>`:

  - `local` — локальные фильтры открытой сети;

- `forward` — транзитные фильтры открытой сети;
- `tunnel` — фильтры туннелируемых узлов;
- `vpn` — фильтры защищённой сети.

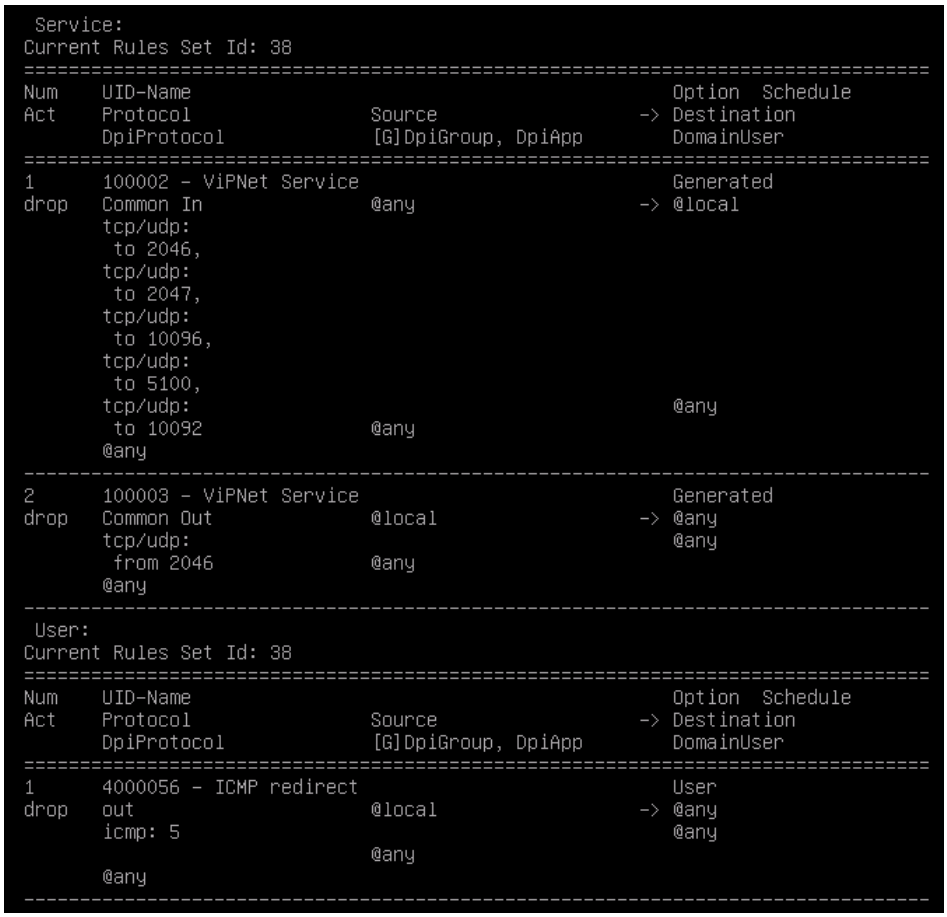


Рисунок 12. Фрагмент списка локальных фильтров открытой сети

- Для просмотра сетевых фильтров с определёнными параметрами:

```
hostname> firewall {<тип> | rules} show <параметры>
```

В качестве параметров можно указать:

- `<номер>` — порядковый номер фильтра в таблице.
- `pass`, `drop`, `reject` — действие фильтра;
- `src <адрес>` — адрес отправителя;
- `dst <адрес>` — адрес получателя;
- `tcp [sport <порт> и/или dport <порт>]`, `udp [sport <порт> и/или dport <порт>]`, `icmp` — протокол, указанный в сетевом фильтре.

При необходимости вы можете указать несколько параметров. Например, для просмотра локального фильтра открытой сети с несколькими адресами отправителей или одним адресом получателя:

```
hostname> firewall local show src 192.168.30.2,192.169.1.1,mydomain.ru dst
192.168.0.1
```

Примечание. Поиск сетевых фильтров для отображения выполняется по строгому совпадению с указанными параметрами. Например, если указан параметр `src 192.168.1.10`, отобразится фильтр, содержащий адрес `src 192.168.1.10`, но не отобразится фильтр, содержащий адрес `src 192.168.1.10-192.168.1.11`.

Подробное описание команды и её вывода см. в документе «Справочник команд и конфигурационных файлов».

Настройка регистрации IP-пакетов при срабатывании фильтров

Каждый сетевой фильтр содержит параметр `log`, который определяет, регистрировать обработанный им IP-пакет в журнале IP-пакетов или нет (см. Регистрация IP-пакетов). Вы можете задать значение параметра `log` при создании сетевого фильтра и изменить его в любое время.

Данный параметр учитывается, только если выбран способ регистрации IP-пакетов по фильтрам (если вы обновили ПО ViPNet Coordinator IG до версии 5.2.0, то по умолчанию будет выбран другой способ регистрации IP-пакетов). Подробнее о способах регистрации IP-пакетов см. Журнал IP-пакетов. При этом настраивать параметр `log` вы можете независимо от используемого способа регистрации IP-пакетов.

Чтобы просмотреть, на каких сетевых фильтрах включена регистрация IP-пакетов:

```
hostname> firewall <тип фильтра> show
```

Если регистрация IP-пакетов включена, перед именем фильтра отображается префикс `[LOG]`.

Вы можете включить регистрацию IP-пакетов сразу для всех настраиваемых фильтров с действиями блокировать (`drop`) и отклонить (`reject`). Для этого выполните команду:

```
hostname# firewall rules log-blocked
This will turn on logging for all user rules with action drop or reject.
Continue? [Yes/No]: y
```

Удаление сетевого фильтра

Чтобы удалить ненужный сетевой фильтр:

- Если вы знаете порядковый номер фильтра:

  ```
  hostname# firewall <тип> delete <номер>
  ```

  Например:

  ```
  hostname# firewall local delete 7
  ```

- Если вы не знаете номер фильтра, то выполните поиск по известным вам параметрам:

  `hostname# firewall <тип> delete <параметр>,`

  где в качестве `<параметр>` можете указать имя, адрес отправителя, адрес получателя, протокол или действие. Вы можете указать несколько параметров. Например, для удаления локальных фильтров открытой сети с адресом отправителя 192.168.20.2:

  `hostname# firewall local delete src 192.168.20.2`

  Внимание! Поиск сетевых фильтров выполняется по строгому совпадению с указанными параметрами.

  Будет выведен список подходящих сетевых фильтров:

  - Если в результате поиска найдено несколько сетевых фильтров:
    - введите номер фильтра из столбца `Num`, чтобы удалить только его;
    - введите `a`, чтобы удалить все фильтры списка;
  - Если найден один фильтр, подтвердите его удаление: введите `y`.

После удаления изменятся номера (приоритеты) фильтров. Номера фильтров с более низким приоритетом уменьшатся на единицу.

Настройка фильтрации промышленных протоколов

Примечание. Фильтрация промышленных протоколов доступна на ViPNet Coordinator IG при наличии лицензии на функцию IPF. Чтобы активировать её, включите эту функцию в настройках координатора в ViPNet Prime.

Общие сведения о фильтрации промышленных протоколов

Вы можете настроить фильтрацию трафика на прикладном уровне для следующих протоколов:

- Modbus:
  - по адресам устройств;
  - по кодам функций;
  - по адресам регистров чтения и записи (для функций, которые работают с регистрами).
- МЭК 60870-5-104:
  - по общим адресам ASDU;
  - по адресам объектов информации;
  - по идентификаторам типов объектов информации.

Для фильтрации промышленного протокола на прикладном уровне необходимо сначала настроить фильтрацию на транспортном уровне. Правила транспортного уровня позволяют задавать:

- объекты промышленной сети, между которыми необходимо разрешить трафик;
- порт, используемый в промышленном протоколе.

Правила транспортного уровня определяют, какой трафик будет передан на обработку правилами прикладного уровня.

При создании правил транспортного уровня автоматически создаются разрешающие служебные фильтры межсетевого экрана, которые применяются к трафику в первую очередь. Это необходимо, чтобы трафик промышленных протоколов не блокировался предустановленными и пользовательскими сетевыми фильтрами и не пропускался без фильтрации на прикладном уровне.

Правила фильтрации промышленных протоколов создаются в составе именованных наборов правил. Каждый набор состоит из двух таблиц:

- Таблица правил транспортного уровня.

- Таблица правил прикладного уровня.

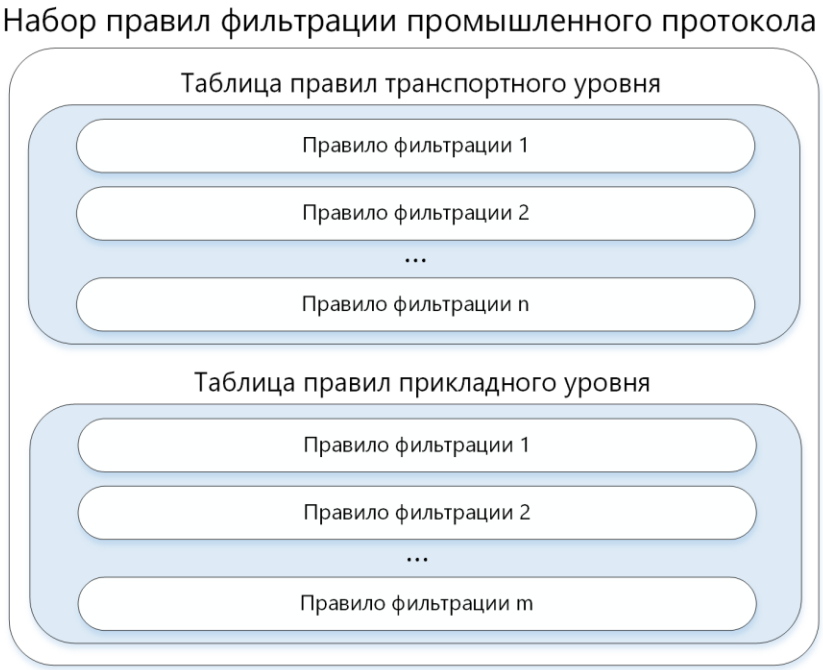


Рисунок 13. Структура набора правил фильтрации промышленного протокола

Основные принципы фильтрации промышленных протоколов

- Входящие IP-пакеты проверяются правилами фильтрации транспортного уровня при условиях:
  - Фильтрация промышленного протокола включена (см. Порядок настройки фильтрации промышленных протоколов).
  - Создан хотя бы один набор правил промышленного протокола (см. Работа с наборами правил фильтрации промышленных протоколов).
- IP-пакет обрабатывается правилами транспортного уровня всех наборов правил в порядке их расположения в таблицах правил.
- Если IP-пакет соответствует условиям правила транспортного уровня, он передаётся на обработку правилами прикладного уровня, которые содержатся в этом же наборе правил.

Примечание. Если PDU пакета содержит несколько пакетов промышленного протокола (далее – прикладные пакеты), они все передаются на проверку правилами прикладного уровня.

Другие правила транспортного уровня к этому IP-пакету уже не применяются.

- Перед обработкой правилами прикладного уровня прикладной пакет проверяется на наличие аномалий. Если аномалия обнаружена, сессия завершается и необработанные прикладные пакеты отбрасываются (критерии аномалий см. ниже).
- Прикладной пакет обрабатывается правилами прикладного уровня в порядке убывания их приоритета (расположения в таблице правил).
- Если прикладной пакет соответствует условиям правила прикладного уровня, он пропускается или блокируется этим правилом.

  Диапазоны значений в правиле фильтрации применяются следующим образом:

  - Разрешающее правило применяется, если диапазон значений в прикладном пакете полностью входит в диапазон значений, заданный в правиле.
  - Запрещающее правило применяется, если диапазон значений в прикладном пакете пересекается с диапазоном значений, заданным в правиле.

  Другие правила прикладного уровня к этому пакету уже не применяются.
- Прикладной пакет, не обработанный ни одним из правил прикладного уровня текущего набора правил, блокируется.
- IP-пакет, не обработанный ни одним из правил транспортного уровня всех наборов правил промышленных протоколов, обрабатывается остальными сетевыми фильтрами, заданными в межсетевом экране.

Принципы фильтрации протокола Modbus на прикладном уровне

- Аномалией в прикладном пакете считается:
  - Идентификатор устройства не входит в диапазон 0–255.
  - Код функций не входит в диапазон 1–127.
  - Номер регистра не входит в диапазон 0–65535.
  - Размер пакета превышает 260 байт.
  - Количество запрашиваемых регистров не входит в диапазоны:
    - 1–125 для функций с кодами: 03, 04;
    - 1–2000 для функций с кодами: 01, 02, 15;
    - 1–123 для функции с кодом 16;
    - 1–125 (чтение) 1–121 (запись) для функции с кодом 23.
- Если в правиле заданы диапазоны устройств, то диапазоны функций интерпретируются как относящиеся к каждому устройству.
- Если в правиле заданы диапазоны функций, то диапазоны регистров интерпретируются как параметры этих функций.
- Фильтрация по регистрам чтения и записи:

- Правило, в котором заданы регистры чтения, но не заданы регистры записи, применяется для функций, запрашивающих чтение регистров (функции с кодами: 01, 02, 03, 04, 23).
- Правило, в котором заданы регистры записи, но не заданы регистры чтения, применяется для функций, запрашивающих запись регистров (функции с кодами: 05, 06, 15, 16, 22, 23).
- Правило, в котором заданы и регистры чтения, и регистры записи, применяется для функций, запрашивающих чтение и запись регистров (функция с кодом 23).
- Правило, в котором не заданы ни регистры чтения, ни регистры записи, применяется для всех функций, независимо от того, запрашивают они доступ к регистрам или нет (фильтрация по регистрам не производится).
- Ответные пакеты не содержат номеров регистров, но к ним применяются как правила без регистров, так и правила с регистрами (регистры не учитываются). При этом, к таким пакетам применяются только разрешающие правила. Если ответный пакет не удовлетворяет ни одному разрешающему правилу, он блокируется.



Примечание. Не создавайте правила, разрешающие пакеты от любых устройств и функций (группа `@any`). Такое правило будет пропускать ответные пакеты даже с неправильными идентификаторами устройств и кодами функций.

- Разрешающее правило применяется, если диапазон регистров функции полностью входит в диапазон регистров правила.
- Запрещающее правило применяется, если диапазон регистров функции пересекается с диапазоном регистров правила.
- Диапазоны регистров правила распространяются на все, указанные в нём функции.

Принципы фильтрации протокола МЭК 60870-5-104 на прикладном уровне

- Аномалией в прикладном пакете считается:
  - Неправильный формат APCI (управляющей информации прикладного протокола). Правильный формат: байт начала, байт длины, 4 байта управления.
  - Идентификатор типа не используется (равен нулю), не входит в диапазон 1–127 или входит в один из диапазонов: 22–29, 41–44, 52–57, 65–69, 71–99, 108–109, 114–119.
  - Общий адрес ASDU не используется (равен нулю) или не входит в диапазоны: 1–255 при длине адреса в 1 байт, 1–65535 при длине адреса в 2 байта.
  - Адрес информационного объекта не входит в диапазоны: 0–255 при длине адреса в 1 байт, 0–65534 при длине адреса в 2 байта, 0–16777215 при длине адреса в 3 байта.
  - Размер APDU превышает максимальный размер, заданный настройками формата протокола (см. Настройка формата протокола МЭК 60870-5-104).

Примечание. Неструктурированный трафик обрабатывается как аномалия.

- Если в правиле заданы диапазоны адресов ASDU, то диапазоны адресов объектов информации интерпретируются как относящиеся к каждому адресу ASDU.
- Если в правиле заданы диапазоны адресов объекта информации, то диапазоны типов объектов информации интерпретируются как параметры этих объектов информации.

Порядок настройки фильтрации промышленных протоколов

1 Включите фильтрацию промышленного протокола:

```
hostname# ipf {modbus | iec104} mode on
```

где,

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

2 Создайте набор правил (см. Работа с наборами правил фильтрации промышленных протоколов).

3 Добавьте правила транспортного уровня в созданный набор правил (см. Настройка правил фильтрации транспортного уровня).

4 При фильтрации МЭК 60870-5-104 настройте формат протокола в соответствии с формуляром, определяющим формат приема/передачи данных в вашей автоматизированной системе (см. Настройка формата протокола МЭК 60870-5-104).

5 Добавьте правила прикладного уровня в созданный набор правил (см. Настройка правил фильтрации прикладного уровня).

Примечание. Чтобы просмотреть состояние фильтрации промышленных протоколов:

```
hostname# ipf show
```

Работа с наборами правил фильтрации промышленных протоколов

Создать набор правил

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

В результате будет создан набор правил, который содержит пустые таблицы транспортного и прикладного уровней. Чтобы добавить правила в эти таблицы, см. Настройка правил фильтрации транспортного уровня и Настройка правил фильтрации прикладного уровня.

Вы можете фильтровать трафик между разными устройствами или сегментами промышленной сети по разным таблицам правил прикладного уровня. Для этого создайте несколько наборов правил.



Примечание. Невозможно создать два и более набора правил, в которых таблицы правил транспортного и прикладного уровней полностью совпадают, даже если эти наборы имеют разные имена. Например, нельзя создать два пустых набора правил.

Переименовать набор правил

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

Удалить набор правил

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

Для подтверждения удаления введите `y`.

Включить или выключить использование набора правил

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

После создания набор правил находится во включённом состоянии.

Просмотреть все наборы правил для определенного протокола

```
hostname> ipf show {modbus | iec104}
```

Настройка правил фильтрации транспортного уровня

Правила фильтрации создаются в рамках определённого набора правил (см. Работа с наборами правил фильтрации промышленных протоколов). Вы можете создать несколько правил в одном наборе.

Создать правило фильтрации

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

где,

- `<имя набора правил>` — имя набора правил, в котором вы хотите создать правило фильтрации.

- <номер правила> — порядковый номер правила в таблице транспортного уровня.
- <тип> — тип трафика, для фильтрации которого предназначено правило:
  - local — локальный трафик открытой сети;
  - forward — транзитный трафик открытой сети;
  - tunnel — туннелируемый трафик;
  - vpn — защищённый трафик.
- <адрес клиента> — адрес узла, который запрашивает TCP-соединение:
  - Для локального, транзитного и туннелируемого трафика — IP-адрес, доменное имя, диапазон IP-адресов, список IP-адресов, список доменных имён, маска адресов подсети, системная группа объектов (any, local или remote), пользовательские группы IP-адресов;
  - Для защищённого трафика (vpn) — идентификатор узла или сети ViPNet, список идентификаторов, системная группа объектов (any, allcoordinators, allclients, local или remote).



Примечание. Правила фильтрации защищённого трафика применяются только к локальному защищённому трафику, поэтому в качестве адреса клиента или адреса сервера укажите группу local.

- <адрес сервера> — адрес узла, который ожидает TCP-соединение. Список возможных значений параметра совпадает с параметром <адрес клиента>.
- <протокол> — транспортный протокол, по которому передаются IP-пакеты. Доступен только протокол TCP.
- <порт> — порт назначения. Вы можете задать список портов или их диапазоны. Не указывайте порты, которые используются другими службами (вы можете посмотреть их в сетевых фильтрах с помощью команды hostname> firewall <тип> show).

По умолчанию задаются следующие значения параметров:

- <номер правила> — последний номер правила в таблице;
- <адрес сервера> — @any;
- <адрес сервера> — @any;
- <протокол> — TCP.

Например, чтобы добавить в набор Modbus с именем Controllers_02 правило для транзитного трафика со следующими значениями параметров: адрес клиента 192.168.0.1, адрес сервера 89.135.15.2, протокол TCP, порт назначения 502:

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

Внимание! К уже установленным соединениям локального Modbus-трафика (открытого и защищенного) изменения в наборе правил (создание, изменение, удаление правила) применяются не сразу, а через одну минуту. В течение этого времени указанный трафик будет заблокирован. Чтобы применить изменения вручную, перезапустите шлюз Modbus:

```
hostname# service mbgw stop
hostname# service mbgw start
```

Изменить или удалить правило фильтрации

- Добавить новые значения для одного или нескольких параметров правила:

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

- Заменить правило целиком:

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

  По умолчанию задаются следующие значения параметров:

  - `<адрес сервера>` — `@any`;
  - `<адрес сервера>` — `@any`;
  - `<протокол>` — `TCP`.

- Удалить правило:

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

Настройка правил фильтрации прикладного уровня

Правила фильтрации создаются в рамках определённого набора правил (см. Работа с наборами правил фильтрации промышленных протоколов).

Внимание! Максимальное количество правил прикладного уровня для вашего исполнения ViPNet Coordinator IG см. в документе «Подготовка к работе» в разделе «Основные отличия аппаратных платформ». Превышение этого количества может значительно снизить производительность ViPNet Coordinator IG.

Для всех поддерживаемых промышленных протоколов правила фильтрации создаются с помощью команды:

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

где,

- `<имя набора правил>` — имя набора правил, в котором вы хотите создать правило.

- <номер правила> — порядковый номер правила, определяющий его приоритет в таблице прикладного уровня. Чем меньше номер, тем выше приоритет правила при обработке трафика (наиболее приоритетный фильтр имеет номер 1). Если заданный номер меньше максимального номера в таблице, номера фильтров, следующих за новым, автоматически увеличиваются на единицу (их приоритет понижается).
- <имя правила> — имя правила фильтрации.
- <параметры прикладного протокола> — параметры промышленного протокола, по которым выполняется фильтрация на прикладном уровне:
  - для протокола Modbus:

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

  - для протокола МЭК 60870-5-104:

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

- pass — пропускать трафик.
- drop — блокировать трафик.

Создать правило фильтрации для протокола Modbus

```
hostname# ipf modbus rules <имя набора правил> rule add [<номер правила>] [name <имя правила>] id <идентификаторы узлов> fc <коды функций> [r <диапазоны регистров чтения>] [w <диапазоны регистров записи>] {pass | drop}
```

где,

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

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

- <диапазоны регистров чтения> — номера регистров чтения. Допустимые значения: числа, диапазоны чисел, входящие в интервал 0–65535.
- <диапазоны регистров записи> — номера регистров записи. Допустимые значения: числа, диапазоны чисел, входящие в интервал 0–65535.

По умолчанию задаются следующие значения параметров:

- <номер правила> — последний номер правила в таблице;
- <диапазоны регистров чтения> — @any;
- <диапазоны регистров записи> — @any.

Примеры см. в разделе Примеры создания правил фильтрации прикладного уровня.



Внимание! К уже установленным соединениям локального Modbus-трафика (открытого и защищенного) изменения в наборе правил (создание, изменение, удаление правила) применяются не сразу, а через одну минуту. В течение этого времени указанный трафик будет заблокирован. Чтобы применить изменения вручную, перезапустите шлюз Modbus:

```
hostname# service mbgw stop
hostname# service mbgw start
```

Создать правило фильтрации для протокола МЭК 60870-5-104



Совет. Перед созданием правил фильтрации настройте формат протокола МЭК 60870-5-104.

```
hostname# ipf iec104 rules <имя набора правил> rule add [<номер правила>] [name <имя правила>] [asdu <общий адрес ASDU>] [ioa <адреса объектов информации>] [iot <идентификаторы типов объектов информации>] {pass | drop}
```

где,

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

  Чтобы задать размер поля, содержащего общий адрес ASDU, см. Настройка формата протокола МЭК 60870-5-104.
- `<адреса объектов информации>` — адреса (идентификаторы) объектов информации. Допустимые значения: числа, диапазоны чисел, входящие в интервал:
  - 0–255 — при размере поля в 1 байт;
  - 0–65535 — при размере поля в 2 байта;
  - 0–16777215 — при размере поля в 3 байта (установлено по умолчанию).

  Чтобы задать размер поля, содержащего адрес объектов информации, см. Настройка формата протокола МЭК 60870-5-104.



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

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

По умолчанию задаются следующие значения параметров:

- `<номер правила>` — последний номер правила в таблице;
- `<общий адрес ASDU>` — `@any`;
- `<адреса объектов информации>` — `@any`;
- `<идентификаторы типов объектов информации>` — `@any`.

Примеры см. в разделе Примеры создания правил фильтрации прикладного уровня.

Изменить, удалить или выключить правило фильтрации

- Изменить приоритет правила:

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

- Добавить новые значения для одного или нескольких параметров правила:

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

  Например, чтобы добавить общий адрес ASDU 1 и адреса объектов информации в диапазоне 15000–16000 в правило с порядковым номером 2, содержащееся в наборе правил МЭК 60870-5-104 с именем `For_rdu`:

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

- Заменить правило целиком:

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

- Удалить правило:

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

- Отключить правило:

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

  После создания все правила фильтрации включены по умолчанию.

Примеры создания правил фильтрации прикладного уровня

Примечание.

- Если в таблице правил прикладного уровня нет разрешающих правил, то трафик, удовлетворяющий условиям правил транспортного уровня, будет заблокирован. Поэтому создавать запрещающие правила имеет смысл только в сочетании с разрешающими.
- В первом примере указаны такие необязательные параметры, как номер и имя правила фильтрации. В последующих примерах эти параметры опущены.

Чтобы разрешить прохождение команд Modbus с кодами функций 1, 3 и 4, запрашивающих чтение регистров с номерами 30–50 от устройств с идентификаторами 2 и 6:

```
hostname# ipf modbus rules ModbusRuleSet1 rule add 1 name Rule_01 id 2,6 fc 1,3-4 r 30-50 pass
```

Чтобы разрешить прохождение команд Modbus с кодами функций 1, 3, 4, запрашивающих чтение регистров 1, 2, 30–50, от любых Modbus-устройств:

```
hostname# ipf modbus rules ModbusRuleSet1 rule add id @any fc 1,3,4 r 1,2,30-50 pass
```

Чтобы запретить прохождение команды Modbus с кодом функции 5, запрашивающей запись регистра 14, от устройства с идентификатором 66:

```
hostname# ipf modbus rules ModbusRuleSet2 rule add id 66 fc 5 w 14 drop
```

Чтобы запретить прохождение команды Modbus с кодом функции 23, запрашивающей чтение регистров 14–20 и запись регистров 14–20, от устройств с идентификаторами 3–15:

```
hostname# ipf modbus rules ModbusRuleSet2 rule add id 3-15 fc 23 r 14-20 w 14-20 drop
```

Чтобы запретить прохождение команд Modbus с кодами функций 5–13, не зависимо от того, запрашивают они доступ к регистрам или нет, от устройств с идентификаторами 3–15 и 18:

```
hostname# ipf modbus rules ModbusRuleSet2 rule add id 3-15,18 fc 5-13 drop
```

Чтобы разрешить прохождение блоков данных со следующими параметрами протокола МЭК 60870-5-104: общие адреса ASDU 1, 3 и 4, адреса объектов информации в диапазоне 10000–15000, идентификатор типов объектов 36:

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

Настройка формата протокола МЭК 60870-5-104

По умолчанию для каждого набора правил фильтрации МЭК 60870-5-104 установлен следующий формат протокола:

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

Вы можете изменить формат протокола МЭК 60870-5-104 для выбранного набора правил фильтрации:

- Изменить размер поля, содержащего общий адрес ASDU:

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

  Возможные значения: 1, 2 байта.

- Изменить размера поля, содержащего адрес объекта информации:

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

  Возможные значения: 1, 2, 3 байта.

- Изменить размера поля, содержащего причину передачи ASDU:

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

Возможные значения: 1, 2 байта.

- Изменить максимальный размер APDU:

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

  Возможные значения: число, входящее в диапазон 2-253 включительно (в байтах).

- Чтобы сбросить настройки формата протокола МЭК 60870-5-104 на значения по умолчанию:

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

Чтобы просмотреть текущие настройки формата протокола МЭК 60870-5-104 для выбранного набора правил:

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

Просмотр правил фильтрации промышленных протоколов

Чтобы просмотреть содержимое набора правил промышленного протокола:

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

Чтобы просмотреть содержимое всех наборов правил промышленного протокола:

```
hostname> ipf show {modbus | iec104}
```

В результате выполнения любой из перечисленных команд на экран выводятся таблицы правил транспортного и прикладного уровней, в которых используются следующие сокращения:

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

Настройка прокси-сервера

Общие сведения о работе прокси-сервера

Прокси-сервер ViPNet Coordinator IG обладает следующими возможностями:

- Кеширование данных для ускорения доступа пользователей к часто запрашиваемым ресурсам.
- «Прозрачный» режим работы, для которого не требуется дополнительная настройка приложений на рабочих местах пользователей.
- Контент-фильтрация HTTP-трафика.
- Проверка HTTP-трафика внешним антивирусом по протоколу ICAP.



Рисунок 14. Схема работы прокси-сервера ViPNet Coordinator IG

Порядок обработки запроса при обращении к интернет-ресурсу:

1 Запрос от клиента прокси-сервера поступает на ViPNet Coordinator IG:
   - Обрабатывается сетевыми фильтрами:
     - если сработал запрещающий сетевой фильтр, то передача IP-пакетов блокируется, в журнал IP-пакетов добавляется запись об этом событии (см. События журнала IP-пакетов);
     - если запрос не попал под действие ни одного из запрещающих сетевых фильтров, он передаётся на прокси-сервер.
   - Если включена контент-фильтрация трафика, то запрос обрабатывается её правилами:
     - если ни одно правило не сработало, то применяется правило по умолчанию (блокирующее или разрешающее);
     - если сработало запрещающее правило по HTTP-методу или MIME-типу, то передача HTTP-трафика блокируется.
   - Если включена антивирусная проверка трафика, данные проверяются на наличие вирусов. Если пользователь попытается отправить файл, в котором был обнаружен вирус, он увидит соответствующее сообщение от антивируса и попытка отправки файла будет заблокирована. Запись об этом событии будет создана в системном журнале.
2 Если запрос не был заблокирован при контент-фильтрации трафика или при проверке антивирусом, он передаётся на интернет-ресурс.
3 Ответ от интернет-ресурса поступает на ViPNet Coordinator IG:

- Обрабатывается сетевыми фильтрами аналогично шагу 1.
- Если включена функция фильтрации содержимого трафика, то ответ обрабатывается её правилами аналогично шагу 1.
- Если включена антивирусная проверка трафика, данные проверяются на наличие вирусов. Если пользователь попытается загрузить файл (в том числе открыть HTML-страницу), в котором был обнаружен вирус, он увидит сообщение от антивируса и попытка загрузки файла будет заблокирована. Запись об этом событии будет создана в системном журнале.

В случае успешного прохождения всех проверок HTTP-трафик от прокси-сервера передаётся пользователю.

Если вы хотите использовать встроенный прокси-сервер для защиты интернет-соединения пользователей вашей локальной сети, настройте основные параметры прокси-сервера. Вы также можете включить антивирусную проверку и контент-фильтрацию трафика.

Режимы работы прокси-сервера:

- Обычный режим — в пользовательских приложениях, например в браузере, требуется настроить подключение: указать IP-адрес и порт прокси-сервера и исключить использование прокси-сервера для локальных адресов, в том числе адресов ViPNet Coordinator IG.
- «Прозрачный» режим — дополнительная настройка приложений не требуется. При этом пользователи не имеют возможности отказаться от использования прокси-сервера. На компьютерах пользователей в качестве шлюза по умолчанию необходимо указать IP-адрес ViPNet Coordinator IG, на котором запущен прокси-сервер.

Настройка основных параметров прокси-сервера

На ViPNet Coordinator IG:

- Выберите внешний сетевой интерфейс прокси-сервера, задайте IP-адреса, на которые прокси-сервер будет принимать запросы от пользователей («прослушивать» их), и IP-адреса локальных сетей, которым разрешено использовать прокси-сервер.
- Настройте и включите DNS-сервер (см. Настройка DNS-сервера).

На стороне пользователя в качестве шлюза по умолчанию задайте IP-адрес интерфейса, на который прокси-сервер принимает запросы от этого пользователя.

1 Завершите работу прокси-сервера:

```
hostname# service http-proxy stop
```

2 Укажите интерфейсы и порты, на которых прокси-сервер будет принимать запросы от пользователей:

- Чтобы добавить интерфейс и порт:

```
hostname# service http-proxy listen-address add <интерфейс> <порт>
```

- Чтобы просмотреть список заданных интерфейсов и портов:

  ```
  hostname# service http-proxy listen-address list
  ```

- Чтобы удалить интерфейс и порт:

  ```
  hostname# service http-proxy listen-address delete <интерфейс>
  ```

3 Укажите внешний интерфейс, который используется для подключения к интернету:

```
hostname# service http-proxy external-address set <интерфейс>
```

- Чтобы просмотреть заданный внешний интерфейс:

  ```
  hostname# service http-proxy external-address show
  ```

- Если интерфейс был указан неправильно, задайте его этой же командой.

4 Если требуется, задайте размер кеша прокси-сервера:

```
hostname# service http-proxy cache <размер>
```

Кеш используется для хранения копии данных, к которым часто обращаются пользователи. Размер кеша указывается в мегабайтах, максимальное значение и значение по умолчанию зависит от аппаратной платформы (подробнее см. описание команды в документе «Справочник команд и конфигурационных файлов»).

5 Чтобы включить или выключить «прозрачный» режим работы прокси-сервера:

```
hostname# service http-proxy transparent-mode {on | off}
```



Примечание. По умолчанию в «прозрачном» режиме работы прокси-сервера к DNS-серверу ViPNet Coordinator IG могут обращаться только защищённые узлы. Если необходимо предоставить доступ к DNS-серверу для открытых узлов, создайте локальный фильтр открытой сети:

```
hostname# firewall local add rule "Allow DNS in" src <IP-адреса открытых
узлов> dst @local udp dport 53 tcp dport 53 pass
```

6 Добавьте сетевые фильтры и правила трансляции, необходимые для работы прокси-сервера:

```
hostname# service http-proxy fw-rules apply
```

При выполнении команды все необходимые сетевые фильтры и правила трансляции будут созданы автоматически.

При выполнении команды также автоматически создаётся пользовательская группа объектов `HttpProxyUsers`, содержащая IP-адреса локальных сетей, для которых разрешено использование прокси-сервера. По умолчанию в эту группу входят те же IP-адреса, что и в пользовательскую группу объектов `PrivateNetworkIP` (10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16).

- Чтобы добавить или удалить IP-адреса из списка локальных сетей, которым разрешено использовать прокси-сервер, измените группу объектов `HttpProxyUsers`. Изменение пользовательских групп объектов возможно только с помощью веб-интерфейса. Подробнее см. документ «Настройка с помощью веб-интерфейса», раздел «Создание и изменение групп объектов».

Примечание. Если для подключения к интернету использует маршрут с несколькими шлюзами (multi-hop route), для корректной работы прокси-сервера создайте локальный фильтр открытой сети:

```
hostname# firewall local add src @local dst @InternetIP tcp dport 80 tcp dport 21 tcp dport 443 pass
```

- Чтобы просмотреть сетевые фильтры и правила трансляции прокси-сервера:

  ```
  hostname# service http-proxy fw-rules show
  ```

- При смене режима работы прокси-сервера, заданного на шаге 5, выполните действия шага 6 заново.

- При отказе от использования прокси-сервера удалите его сетевые фильтры и правила трансляции:

  ```
  hostname# service http-proxy fw-rules delete
  ```

7 Включите автоматический запуск прокси-сервера:

```
hostname# service http-proxy mode on
```

8 Запустите прокси-сервер:

```
hostname# service http-proxy start
```

Настройка правил контент-фильтрации трафика

Прокси-сервер проверяет HTTP-трафик с помощью правил контент-фильтрации. Вы можете настроить блокировку трафика по HTTP-методу запроса к удаленному ресурсу, а также по MIME-типу файла или приложения.

Примечание. При блокировке трафика в браузере отображается веб-страница с соответствующим сообщением, а время блокировки отображается в формате UTC+0.

Контент-фильтрация HTTP-трафика включается автоматически при запуске прокси-сервера.

Для настройки контент-фильтрации:

1 Завершите работу прокси-сервера:

```
hostname# service http-proxy stop
```

2 Чтобы включить или выключить контент-фильтрацию трафика:

```
hostname# service http-proxy content-filter mode {on | off}
```

3 Задайте действие правила по умолчанию для запросов к HTTP-ресурсам:

```
hostname# service http-proxy content-filter default-request-action {pass | drop}
```

указав следующие параметры:

- `pass` — правило по умолчанию пропускает запросы к HTTP-серверам, не попадающие под действие других правил;

- `drop` — правило по умолчанию блокирует запросы к HTTP-серверам, не попадающие под действие других правил.

4 Задайте действие правила по умолчанию для ответов от HTTP-ресурсов:

```
hostname# service http-proxy content-filter default-reply-action {pass | drop}
```

указав следующие параметры:

- `pass` — правило по умолчанию пропускает ответы от HTTP-серверов, не попадающие под действие других правил;
- `drop` — правило по умолчанию блокирует ответы от HTTP-серверов, не попадающие под действие других правил.

5 Чтобы добавить правило контент-фильтрации трафика:

```
hostname# service http-proxy content-filter add [num <номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя> {command <HTTP-метод> | mime-type <mime-тип>} <действие>
```

указав следующие параметры:

- `<номер>` — порядковый номер правила в таблице, определяющий его приоритет. Чем меньше порядковый номер правила, тем выше его приоритет (наиболее приоритетное правило имеет номер 1). Если указанный номер правила меньше последнего номера в таблице, нумерация правил, следующих после нового правила, будет автоматически изменена (их номера будут увеличены на 1).
- `<имя>` — имя правила. Если имя состоит из нескольких слов, разделённых пробелом, заключите его в кавычки (например, `rule "number one"`).



Примечание. Порядковый номер и имя не являются обязательными параметрами правила контент-фильтрации трафика. При создании правила без указания номера ему будет присвоен номер, следующий за номером последнего правила в таблице, и оно будет иметь самый низкий приоритет. При создании правила без указания имени будет создано правило без имени. Создание фильтра с порядковым номером, превышающим максимальный номер в таблице фильтров более чем на 1, запрещено.

- Параметры контент-фильтрации:
  - Адрес отправителя.
  - Адрес получателя.
  - HTTP-метод.
  - MIME-тип.
  - Действие.

6 Чтобы изменить существующее правило контент-фильтрации:

```
hostname# service http-proxy content-filter change num <номер правила> [rule <имя правила>] src <адрес отправителя> dst <адрес получателя> {command <HTTP-метод> | mime-type <mime-тип>} <действие>
```

7 Чтобы удалить правило контент-фильтрации из таблицы правил:

```
hostname# service http-proxy content-filter delete {num <номер> | rule <имя>},
```

- `<номер>` — порядковый номер правила в таблице;
- `<имя>` — имя правила.

8 Чтобы изменить порядок правила контент-фильтрации в таблице правил:

```
hostname# service http-proxy content-filter move {num <номер> | rule <имя>} to <новый номер>,
```

где:

- `<номер>` — порядковый номер правила в таблице, определяющий его приоритет;
- `<имя>` — имя правила;
- `<новый номер>` — новый порядковый номер правила в таблице.

9 Чтобы просмотреть правила контент-фильтрации:

```
hostname# service http-proxy content-filter list
```

10 Запустите прокси-сервер:

```
hostname# service http-proxy start
```

Адрес отправителя

Адрес отправителя является обязательным параметром правила контент-фильтрации:

```
src <адрес отправителя>
```

Возможные значения адреса отправителя:

- IP-адрес, например:

  ```
  src 192.168.1.36
  ```

- адрес подсети в формате классовой адресации, например:

  ```
  src 192.168.1.0/24
  ```

- системная группа объектов `any`, например:

  ```
  src @any
  ```



Внимание! В качестве отправителя всегда указывайте клиента прокси-сервера. Использование доменных имен не допускается.

Адрес получателя

Адрес получателя является обязательным параметром правила контент-фильтрации:

```
dst <адрес получателя>
```

Возможные значения адреса получателя:

- IP-адрес или доменное имя узла;
- системная группа объектов `any`, например:

```
dst @any
```



Внимание! Контент-фильтрация прокси-сервера работает на прикладном уровне модели OSI. Поэтому при использовании в качестве адреса получателя 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».

HTTP-метод

HTTP-метод не является обязательным параметром правила контент-фильтрации:

```
command <HTTP-метод>
```

Вы можете указать любой из методов протокола HTTP/1.0 (но только один):

- HEAD
- GET
- POST
- PUT
- DELETE
- CONNECT
- OPTIONS
- TRACE



Внимание! Вы можете указать HTTP-метод только в том случае, если в правиле контент-фильтрации трафика не был задан MIME-тип.

Правило с заданным HTTP-методом будет действовать в тех случаях, когда прокси-сервер получит от клиента запрос к удалённому HTTP-серверу с этим методом. Например, необходимо запретить заполнение и отправку форм на веб-портал `example.com`, доступный по протоколу HTTP. Для этого необходимо создать правило, которое будет блокировать метод POST для `example.com`:

```
hostname# service http-proxy content-filter add src @any dst example.com command POST drop
```

Чтобы полностью запретить доступ к этому порталу, создайте правило с методом GET:

```
hostname# service http-proxy content-filter add src @any dst example.com command GET drop
```

MIME-тип

Тип содержимого не является обязательным параметром правила контент-фильтрации:

```
mime-type <mime-тип>
```

Вы можете указать любой тип содержимого из поддерживаемых (см. Поддерживаемые MIME-типы), но только один.



Внимание! Вы можете указать MIME-тип только в том случае, если в правиле контент-фильтрации трафика не был задан HTTP-метод.

Правило с заданным MIME-типом будет блокировать трафик, передающий файлы этого типа. Например, чтобы заблокировать загрузку изображений формата PNG:

```
hostname# service http-proxy content-filter add src @any dst @any mime-type image/png drop
```



Примечание. MIME-тип файла может зависеть от настроек удалённого HTTP-сервера, с которого этот файл был загружен. То есть, файл будет иметь тот MIME-тип, который был назначен ему HTTP-сервером.

Действие

Действие является обязательным параметром правила контент-фильтрации:

- `pass` — пропускать HTTP-трафик;
- `drop` — блокировать HTTP-трафик.

Настройка антивирусной проверки трафика



Примечание. Антивирусная проверка трафика поддерживается только в исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1.

Если на ViPNet Coordinator IG запущен прокси-сервер, вы можете настроить антивирусную проверку данных, передаваемых через него по HTTP в обоих направлениях: из интернета к пользователю и от пользователя в интернет, например при добавлении вложения в сообщение электронной почты с помощью веб-интерфейса. Проверка выполняется внешним антивирусом по протоколу ICAP.



Внимание! Время на ICAP-сервере должно быть синхронизировано с ViPNet Coordinator IG.

1 Остановите работу прокси-сервера:

```
hostname# service http-proxy stop
```

2 Выключите антивирусную проверку трафика прокси-сервером:

```
hostname# service http-proxy antivirus mode off
```

3 Задайте IP-адрес ICAP-сервера внешнего антивируса для проверки входящего трафика:

```
hostname# service http-proxy antivirus server-url add respmod
icap://<адрес>[:<порт>]/[<путь>]
```

где:

- `<адрес>` — IP-адрес или доменное имя;
- `<порт>` — номер порта;
- `<путь>` — путь на ICAP-сервере.

Например:

```
hostname# service http-proxy antivirus server-url add respmod
icap://192.168.1.45:1344/respmod.
```

Если порт не указан, будет использоваться порт 1344.

4 Задайте IP-адрес ICAP-сервера внешнего антивируса для проверки исходящего трафика:

```
hostname# service http-proxy antivirus server-url add reqmod
icap://<адрес>[:<порт>]/[<путь>]
```

5 Создайте разрешающие фильтры межсетевого экрана для работы прокси-сервера:

```
hostname# service http-proxy fw-rules apply
```

6 Задайте режим пропуска трафика при недоступности ICAP-сервера:

```
hostname# service http-proxy antivirus bypass on
```

7 Включите антивирусную проверку трафика прокси-сервером:

```
hostname# service http-proxy antivirus mode on
```

8 Запустите прокси-сервер:

```
hostname# service http-proxy start
```

Настройка межсетевого экрана

Обработка фрагментированных пакетов

ViPNet Coordinator IG при шифровании трафика добавляет к каждому IP-пакету служебный заголовок (выполняет инкапсуляцию), вследствие чего размер сформированного пакета может получиться больше заданного в MTU и потребует фрагментации. В свою очередь, некоторые сервисы не позволяют фрагментировать свои пакеты (например, видео-трафик), используя флаг Don't fragment (DF). В любом случае, обработка фрагментированных пакетов снижает пропускную способность сети, так как два пакета вместо одного суммарно длиннее и их обработка требует больше ресурсов. В ViPNet Coordinator IG предусмотрены средства решения этой проблемы.

Установка TCP-соединения

На этапе установки соединения по протоколу TCP сервер и клиент обмениваются значениями MSS (максимальная длина сегмента), которые основаны на MTU их сетевых интерфейсов. В итоге принимается минимальное из двух значений. В результате инкапсуляции IP-пакета ViPNet Coordinator IG учитывает размер, на который был увеличен IP-пакет после инкапсуляции, и уменьшает значение MSS с учётом этих данных.

Также вы можете настроить дополнительное уменьшение размера MSS с помощью команды `iplir option mss-decrease`.

Обработка IP-пакетов с флагом Don't fragment (DF)

Рассмотрим случай, когда ViPNet Coordinator IG туннелирует сетевые узлы, которые отправляют через него IP-пакеты с размером, не превышающим размер MTU, заданный на внешнем сетевом интерфейсе ViPNet Coordinator IG. При шифровании трафика размер IP-пакета может превысить MTU, и в этом случае IP-пакет будет фрагментирован.

Если же такой IP-пакет имеет флаг DF, запрещающий фрагментацию, то, в зависимости от его размера, будет выполнен один из сценариев:

- Если размер IP-пакета после инкапсуляции не превышает MTU, то ViPNet Coordinator IG его пропустит и сбросит флаг DF (который не восстановится при последующей декапсуляции).
- Если размер IP-пакета после инкапсуляции превышает MTU, то ViPNet Coordinator IG его отбросит (при этом в журнале IP-пакетов появится запись о блокировке с кодом события 97) и отправит ICMP-сообщение о необходимости фрагментации IP-пакета (ICMP type 3, code 4) его отправителю. В зависимости от настройки отправителя IP-пакетов необходимо выполнить одно из действий:
    - Если отправитель IP-пакетов с флагом DF не получает (не обрабатывает) такие ICMP-сообщения, то ему необходимо самостоятельно уменьшить размер IP-пакетов.

- Если отправитель IP-пакетов с флагом DF принимает и корректно обрабатывает ICMP-сообщения ICMP type 3, code 4 (в соответствии с RFC 4459), то такой трафик будет пропущен.

Блокировка входящих фрагментированных пакетов

Фрагментированные IP-пакеты используются как средство сетевой атаки «отказ в обслуживании» (DDoS). В качестве меры защиты от такой атаки на межсетевом экране включено блокирование всех входящих фрагментированных IP-пакетов на всех сетевых интерфейсах. Чтобы выключить такую блокировку, см Настройка дополнительных параметров межсетевого экрана.

Настройка антиспуфинга

ViPNet Coordinator IG может блокировать входящие IP-пакеты от отправителей, IP-адреса которых недопустимы на данном сетевом интерфейсе. Антиспуфинг работает как для открытого, так и для защищённого трафика. При этом открытые IP-пакеты, полученные в результате декапсуляции защищённых IP-пакетов, не проверяются антиспуфингом, так как уже не относятся к сети отправителя. Эти IP-пакеты, как и обычные открытые IP-пакеты, после проверки антиспуфингом обрабатываются сетевыми фильтрами.

Основная задача антиспуфинга — защита от сетевых атак, называемых спуфингом. При спуфинге злоумышленник посылает на какой-либо сетевой узел IP-пакет, в котором в качестве адреса отправителя указан не адрес этого злоумышленника, а адрес другого узла, которому разрешено соединение с узлом получателя. Таким образом можно отправить открытый пакет из интернета через координатор, задав в качестве адреса отправителя адрес частной внутренней сети, которая подключена к данному координатору. Правила антиспуфинга позволяют исключить такую возможность.

1 По умолчанию антиспуфинг выключен. Проверьте его текущее состояние:

```
hostname# firewall settings show
Antispoofing     off
...
```

2 Если антиспуфинг выключен, включите его для повышения безопасности сети:

```
hostname# firewall settings antispoofing on
```

При этом на основе таблицы маршрутизации автоматически задаются правила антиспуфинга.



Внимание! При использовании сложных схем маршрутизации на узле (с метриками маршрутов или асимметричными маршрутами) функция антиспуфинга может работать некорректно.

Правила антиспуфинга применяются для открытого транзитного трафика:

- Для всех сетевых интерфейсов, кроме интерфейса, соответствующего маршруту по умолчанию, блокируются IP-пакеты, адреса отправителей которых не совпадают с адресами, маршрутизируемыми через данный интерфейс.
- Для сетевого интерфейса, соответствующего маршруту по умолчанию, блокируются IP-пакеты, адреса отправителей которых совпадают с зарегистрированными маршрутами других интерфейсов.

Пример настройки антиспуфинга

Таблица 4. Таблица маршрутизации на сетевом узле

Сетевой адрес	Маска подсети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	10.0.8.1	10.0.8.54	20
10.0.8.0	255.255.255.0	On-link	10.0.8.54	276
10.0.8.54	255.255.255.255	On-link	10.0.8.54	276
10.0.8.255	255.255.255.255	On-link	10.0.8.54	276
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.48.0	255.255.255.0	On-link	192.168.48.1	276
192.168.48.1	255.255.255.255	On-link	192.168.48.1	276
192.168.48.255	255.255.255.255	On-link	192.168.48.1	276
192.168.59.0	255.255.255.0	On-link	192.168.59.1	276
192.168.59.1	255.255.255.255	On-link	192.168.59.1	276
192.168.59.255	255.255.255.255	On-link	192.168.59.1	276
224.0.0.0	224.0.0.0	On-link	127.0.0.1	306
224.0.0.0	224.0.0.0	On-link	10.0.8.54	276
224.0.0.0	224.0.0.0	On-link	192.168.48.1	276
224.0.0.0	224.0.0.0	On-link	192.168.59.1	276
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	10.0.8.54	276
255.255.255.255	255.255.255.255	On-link	192.168.48.1	276
255.255.255.255	255.255.255.255	On-link	192.168.59.1	276

Сетевой узел имеет четыре интерфейса, один из которых с адресом 127.0.0.1 (loopback).

При включении антиспуфинга на узле будут заданы следующие правила:

- На интерфейсе с адресом 192.168.48.1 разрешены входящие пакеты только от узлов с IP-адресами 192.168.48.0/24.
- На интерфейсе с адресом 192.168.59.1 разрешены входящие пакеты только от узлов с IP-адресами 192.168.59.0/24.
- На интерфейсе с адресом 10.0.8.54 разрешены все входящие пакеты, кроме пакетов от узла с IP-адресами 192.168.48.0/24, 192.168.59.0/24.

Настройка дополнительных параметров межсетевого экрана

Чтобы настроить параметры межсетевого экрана:

```
hostname# firewall settings <параметр> <значение>
```

Список доступных параметров:

- `antispoofing` — антиспуфинг:
  - `on` — включить;
  - `off` — выключить (по умолчанию);
- `block-fragmented-packets` — блокирование входящих фрагментированных IP-пакетов на всех сетевых интерфейсах:
  - `on` — включить (по умолчанию);
  - `off` — выключить;



Примечание. В некоторых прикладных протоколах, например SIP, используются IP-пакеты с большим размером блока данных, которые могут быть фрагментированы при передаче. Для работы таких протоколов отключайте блокирование фрагментированных IP-пакетов.

- `connection-ttl-ip` — время жизни соединений по протоколу IP при отсутствии в них активности, в секундах (по умолчанию — 300);
- `connection-ttl-tcp` — время жизни соединений по протоколу TCP при отсутствии в них активности, в секундах (по умолчанию — 1800);
- `connection-ttl-udp` — время жизни соединений по протоколу UDP при отсутствии в них активности, в секундах (по умолчанию — 300);
- `max-connections` — максимальное количество одновременно установленных соединений (транзитных, служебных и управляющих) в зависимости от исполнения ViPNet Coordinator IG;

Чтобы просмотреть значения параметров:

```
hostname# firewall settings show
```

5

Настройка правил трансляции адресов

Трансляция сетевых адресов (NAT) 130

Создание правила трансляции адресов 133

Просмотр, изменение, удаление правил трансляции сетевых адресов 135

Трансляция сетевых адресов (NAT)

Трансляция сетевых адресов (NAT) — механизм преобразования IP-адресов одной сети в IP-адреса другой сети. Технология трансляции сетевых адресов описана в RFC 2663 (IP Network Address Translator Terminology and Considerations).

ViPNet Coordinator IG может выполнять:

- Трансляцию адреса источника (маскарадинг (masquerading) или динамическую трансляцию).

  В этом случае при прохождении через координатор IP-пакетов от отправителей с частными IP-адресами в них заменяется адрес отправителя на внешний (реальный) адрес координатора. При получении ответных пакетов в них подменяется IP-адрес получателя обратно на частный IP-адрес, и в таком виде пакет доставляется в частную сеть.

  Используется для подключения локальной сети к интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг интернета количество публичных IP-адресов. В результате локальные сети, использующие частные IP-адреса, получают доступ к ресурсам интернета.

- Трансляцию адреса назначения (перенаправление портов (port forwarding) или статическую трансляцию).

  В этом случае IP-пакеты, приходящие из интернета на определенный порт внешнего адреса координатора, перенаправляются на указанный адрес внутренней сети путем подмены в них адреса получателя, а у ответных пакетов от узла внутренней сети подменяется адрес отправителя.

  Используется для организации доступа к ресурсам локальной сети из интернета. В результате локальные сети, использующие частные адреса, могут быть доступны пользователям интернета по публичным IP-адресам.

- Одновременную трансляцию сетевых адресов источника и назначения.

  Используется в сложных схемах маршрутизации трафика.

Трансляция сетевых адресов выполняется координатором, только если настроены соответствующие правила. Координатор должен иметь как минимум два сетевых интерфейса:

- внешний — имеет публичный IP-адрес и обеспечивает доступ в интернет;
- внутренний — имеет частный IP-адрес.



Внимание! Правила трансляции сетевых адресов, описанные в данном разделе, относятся только к открытому трафику. Для защищённого трафика действуют автоматические механизмы трансляции сетевых адресов, параметры которых не могут быть изменены.

Трансляция адреса назначения

Трансляция адреса узла назначения применяется для организации доступа из интернета к серверам локальной сети, не имеющим публичного IP-адреса. Правило трансляции адреса назначения ставит в соответствие частным IP-адресам локальных сетевых узлов публичный IP-адрес координатора. Таким образом, по публичному IP-адресу внешние пользователи могут получить доступ к ресурсам локальной сети.

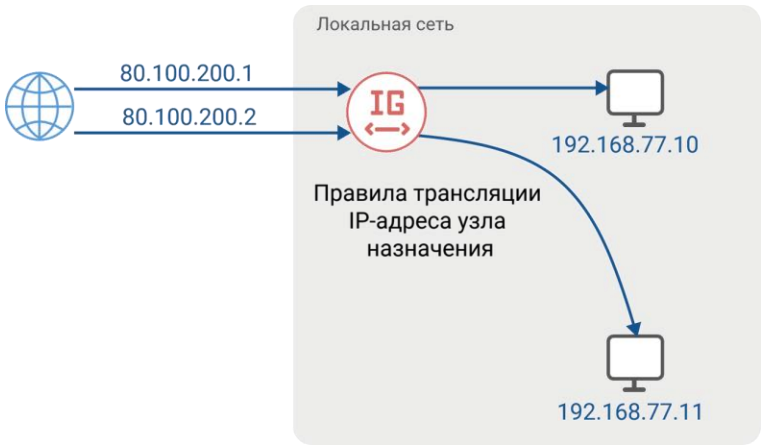


Рисунок 15. Доступ к внутренним ресурсам при помощи трансляции IP-адресов узлов назначения

Если для публичного IP-адреса координатора задано правило трансляции адреса назначения, то при обращении к этому IP-адресу из интернета будут выполняться преобразования:

- Во входящих IP-пакетах от внешнего узла координатор подменяет адрес получателя (публичный IP-адрес координатора) локальным IP-адресом в соответствии с правилом. Затем пакет передаётся через внутренний сетевой интерфейс на узел локальной сети, которому адресован пакет.
- При прохождении ответных IP-пакетов (в рамках уже созданной сессии) координатор производит обратную замену IP-адресов. Адрес отправителя (IP-адрес локального узла) подменяется публичным IP-адресом внешнего сетевого интерфейса координатора. Затем ответный пакет отправляется узлу в интернете.

  Таким образом, при передаче в интернете IP-пакет выглядит так, будто отправитель и получатель этого пакета имеют публичные IP-адреса.

Внимание! При трансляции адреса узла назначения инициировать соединение может только внешний сетевой узел. Чтобы локальный сетевой узел мог также иметь доступ в интернет (двусторонний NAT), необходимо в дополнение к правилу трансляции адреса узла назначения задать также правило трансляции адреса источника.

Трансляция адреса источника

Трансляция адреса источника предназначена для организации доступа узлов локальной сети в интернет. Правило трансляции адреса источника ставит в соответствие нескольким частным IP-адресам локальных сетевых узлов публичный IP-адрес координатора. Таким образом, узлы локальной сети могут устанавливать соединения с узлами в интернете от имени публичного IP-адреса координатора.



Рисунок 16. Организация доступа в интернет при помощи трансляции IP-адреса источника

Если на координаторе настроено правило трансляции адреса источника, то транзитные IP-пакеты, проходящие через координатор из локальной сети в интернет, будут преобразованы:

- В момент передачи IP-пакета из локальной сети в интернет координатор преобразует IP-адрес (или IP-адрес и порт) отправителя пакета для протоколов TCP и UDP. Для пакетов протокола ICMP преобразуется адрес отправителя, остальные параметры запоминаются. При этом частный IP-адрес отправителя заменяется на публичный IP-адрес внешнего сетевого интерфейса координатора, обеспечивающего доступ во внешнюю сеть. При дальнейшей передаче в интернете пакет имеет публичный IP-адрес отправителя. Номера портов отправителя (для протоколов TCP и UDP) и запоминаемые параметры (для протокола ICMP) пакетов имеют уникальные значения для всех исходящих IP-соединений внешнего сетевого интерфейса координатора. После преобразования пакет отправляется адресату в интернете.
- При прохождении ответных IP-пакетов ViPNet Coordinator IG производит обратное преобразование указанных параметров. То есть в момент передачи ответного IP-пакета координатор заменяет в нем IP-адрес получателя на частный IP-адрес узла локальной сети, которому адресован ответный пакет. Преобразование происходит на основании уникальных номеров портов, присвоенных исходящим пакетам (для протоколов TCP и UDP), и запоминаемых параметров исходящих пакетов (для протокола ICMP). Номера портов (для протоколов TCP и UDP) также преобразуются в свои истинные значения. Затем ответные пакеты передаются через внутренний сетевой интерфейс узлу локальной сети, которому адресован пакет.

Примечание. Для всех протоколов, кроме TCP, UDP и ICMP, преобразуются только IP-адреса. Для протоколов с частичным преобразованием трансляция адреса источника не будет работать, если несколько узлов локальной сети одновременно инициируют соединение с одним и тем же IP-адресом публичной сети.

Создание правила трансляции адресов

Примечание. Правила трансляции адресов работают только при наличии транзитных фильтров открытой сети, пропускающих трафик от узлов, к которым они будут применяться.

Чтобы создать правило трансляции адресов, выполните команду:

`hostname# firewall nat add [<номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя> [<протокол>] [<расписание>] change {src <адрес отправителя> | dst <адрес получателя>}`, указав следующие параметры:

- Порядковый номер правила в таблице, определяющий его приоритет. Чем меньше порядковый номер правила, тем выше его приоритет (наиболее приоритетное правило имеет номер 1). При создании правила с порядковым номером, меньшим максимального номера в таблице правил, номера правил, следующих за этим правилом, автоматически увеличиваются на единицу (то есть их приоритет понижается).
- Имя правила. Если имя состоит из нескольких слов, разделенных пробелом, заключите его в кавычки (например, `rule "number one"`).

  Примечание. При создании правила трансляции адресов можно не указывать его номер. В этом случае правилу будет присвоен номер, следующий за номером последнего правила в таблице, и оно будет иметь самый низкий приоритет.
  Имя правила можно не указывать, правило будет создано без имени.

- Параметры, определяющие обработку трафика:
  - адрес отправителя и адрес получателя являются обязательными параметрами правила и задаются в виде IP-адреса или доменного имени узла, диапазона IP-адресов узлов, списка IP-адресов или доменных имен узлов, маски адресов подсети, доменного имени сети, одной или нескольких пользовательских групп IP-узлов;
  - протокол и расписание являются необязательными параметрами правила и задаются так же, как для сетевых фильтров;
  - действие правила в виде одной из лексем:
    - для трансляции адреса источника: `change src {<адрес> | auto}`, указав адрес (внешний адрес координатора или адрес из другой сети), на который будет заменяться адрес отправителя пакетов, либо параметр `auto`, чтобы адрес отправителя автоматически заменялся на публичный адрес внешнего сетевого интерфейса координатора.

Примечание. При использовании в `change src` IP-адреса, не принадлежащего ViPNet Coordinator IG, на сетевом устройстве, расположенным за ViPNet Coordinator IG, настройте обратную маршрутизацию на ViPNet Coordinator IG (или на другое устройство, например для балансировки) для корректной обработки ответного трафика.

Если на сетевом устройстве нельзя настроить обратную маршрутизацию, используйте в `change src` только IP-адреса, принадлежащие ViPNet Coordinator IG, или автоматическое определение адреса исходящего интерфейса (`auto`).

- для трансляции адреса и/или порта назначения: `change dst <адрес>:[<порт>]`, указав адрес и/или порт узла локальной сети, которому будут перенаправляться пакеты.

Примечание. Созданное правило трансляции сетевых адресов будет работать для новых соединений. Для уже установленных соединений правило будет работать после истечения времени жизни соединения. Чтобы принудительно применить правило трансляции сетевых адресов, выполните сброс соединений:

```
hostname# firewall conntrack flush
```

Примеры создания правил трансляции адресов

- Чтобы при отправке пакета узлом с адресом 10.0.0.1 внешнему узлу с адресом 185.37.128.163 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 185.37.128.163 change src auto
  ```

- Чтобы во входящих пакетах на публичный IP-адрес координатора от внешнего узла mydomain.ru адрес получателя подменялся на 10.0.0.7, создайте правило трансляции адреса назначения:

  ```
  hostname# firewall nat add src mydomain.ru dst 192.0.2.1 change dst 10.0.0.7
  ```

- Чтобы во входящих пакетах на публичный IP-адрес и порт 8080 координатора от внешнего узла mydomain.ru адрес получателя подменялся на 10.0.0.7 и порт 8080, создайте правило трансляции адреса назначения:

  ```
  hostname# firewall nat add src mydomain.ru dst 192.0.2.1 tcp dport 8080 change dst
  10.0.0.7:8080
  ```

Просмотр, изменение, удаление правил трансляции сетевых адресов

Вы можете просмотреть, изменить или удалить правила трансляции сетевых адресов, заданные на ViPNet Coordinator IG.

Чтобы просмотреть правила, выполните одну из команд:

- для просмотра всех правил:

  ```
  hostname> firewall nat show
  ```

- для просмотра правил с конкретными параметрами:

  ```
  hostname> firewall nat show <параметр>,
  ```

  указав в качестве параметра порядковый номер, имя, адрес отправителя, адрес получателя или протокол. При необходимости вы можете указать несколько параметров.

Примечание. Поиск правил трансляции сетевых адресов выполняется по строгому совпадению с указанными параметрами.

В результате выполнения команды будет отображена таблица, содержащая правила трансляции сетевых адресов.

```
 User:
=============================================================================
Num   Name                                          Option       Schedule
Act   Protocol                Source              > Destination
=============================================================================
1                                                   User
NAT   @any                    172.20.0.77         > @any
                              Change: auto
-----------------------------------------------------------------------------
```

Рисунок 17. Просмотр правил трансляции сетевых адресов

Таблица содержит следующие столбцы:

- `Num` — порядковый номер правила, определяющий его приоритет.
- `Name` — имя правила.
- `Option` — категория правила: для правил из ViPNet Prime Policy Management — `Policy`, для правил пользователя — `User`.
- `Schedule` — расписание применения правила.
- `Act` — действие правила (`NAT`).
- `Source` — адрес источника до или после трансляции.

- `Destination` — адрес назначения до или после трансляции.
- `Protocol` — протокол.



Внимание! Если из ViPNet Prime Policy Management поступили правила трансляции сетевых адресов, в которых указан порт, но не указан протокол, они будут применены для протоколов TCP и UDP. Чтобы не открывать лишние порты, укажите протоколы для этих правил в ViPNet Prime Policy Management и отправьте политики еще раз.

Изменение и удаление правил трансляции сетевых адресов выполняется аналогично изменению и удалению сетевых фильтров:

```
hostname# firewall nat change append <номер> <параметры>
```

```
hostname# firewall nat delete <параметры>
```

Подробнее см. в разделах Изменение сетевого фильтра и Удаление сетевого фильтра.

6

Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP

О прикладных протоколах 138

Настройка параметров обработки прикладных протоколов 140

О прикладных протоколах

Прикладные протоколы обеспечивают работу пользовательских сетевых сервисов, например, IP-телефонии, DNS, FTP. При использовании данных служб IP-адреса часто передаются в теле сообщения прикладного протокола. Эта особенность может повлиять на доступность сервисов в защищённой сети с виртуальной адресацией или трансляцией сетевых адресов. Кроме того, некоторые прикладные протоколы, помимо управляющего соединения, открывают для передачи данных дополнительные соединения. Поскольку параметры таких соединений заранее неизвестны, невозможно создать сетевой фильтр, разрешающий только необходимый трафик.

ViPNet Coordinator IG может выполнять роль шлюза прикладного уровня, что позволяет решить перечисленные проблемы, обеспечивая:

- Подмену IP-адресов в теле сообщения прикладного протокола на виртуальные IP-адреса.
- Подмену IP-адреса в теле сообщения протокола FTP при трансляции адреса источника или назначения в транзитном FTP-трафике.
- Создание временных сетевых фильтров, пропускающих IP-пакеты дополнительных соединений, которые используются прикладным протоколом.

Примечание. Для разрешения управляющего соединения между узлами создайте сетевой фильтр вручную.

Вы можете настроить обработку прикладных протоколов для открытого и туннелируемого трафика. Список поддерживаемых прикладных протоколов см. ниже.

ViPNet Coordinator IG поддерживает также обработку промышленных прикладных протоколов, что позволяет фильтровать трафик между промышленными устройствами на прикладном уровне. Подробнее см. Настройка фильтрации промышленных протоколов. Фильтрация трафика промышленных протоколов доступна для открытого, туннелируемого и защищённого трафика.

Поддерживаемые прикладные протоколы

- DNS — для доступа к сетевым узлам по доменным именам.
- FTP — для передачи файлов между FTP-клиентом и FTP-сервером.

  Команды FTP-протокола EPRT и EPSV, используемые некоторыми FTP-клиентами, не поддерживаются ViPNet Coordinator IG.
- SIP — для организации сеансов связи (мультимедийных конференций, телефонных соединений) и распределения мультимедийной информации.

  Не поддерживаются SIP-клиенты и телекоммуникационные серверы, использующие при подключении протокол TLS, SIP-клиенты, использующие «компактные поля» (compact headers), а также SIP-клиенты, использующие сжатие данных в сообщениях SIP.

- H.323 — для передачи мультимедийных данных в IP-сетях (IP-телефония, видео- и аудиоконференции).

  При использовании IP-телефонов Yate не поддерживается виртуальная видимость IP-адресов. RTCP-трафик между IP-телефонами Polycom может работать некорректно при виртуальной видимости IP-адресов.

- SCCP — для передачи сообщений между Skinny-клиентами (проводными и беспроводными IP-телефонами Cisco) и сервером голосовой почты (Cisco Unity Connection и Cisco CallManager).

  Передача мультимедийных данных с использованием протокола SCCP возможна, если сервер голосовой почты туннелируется координатором ViPNet Coordinator IG.



Примечание. ViPNet Coordinator IG также поддерживает обработку прикладного протокола Cisco NetMeeting для организация видеоконференций, но только при использовании видимости по реальным IP-адресам между клиентским ПО Cisco Meeting App в сети ViPNet и туннелируемым сервером Cisco Meeting Server.

- Промышленные протоколы:
  - Modbus — для взаимодействия электронных устройств на промышленных объектах.
  - МЭК 60870-5-104 — для контроля и управления территориально распределёнными процессами в электроэнергетике.

Настройка параметров обработки прикладных протоколов

По умолчанию в ViPNet Coordinator IG включена обработка всех поддерживаемых прикладных протоколов, кроме промышленных протоколов.

Примечание.

- Настройка обработки промышленных протоколов выполняется отдельно (см. Настройка фильтрации промышленных протоколов).
- Трафик обрабатываемого прикладного протокола не должен проходить через трансляцию сетевых адресов. Это ограничение не распространяется на FTP-трафик и трафик промышленных протоколов. Для маршрутизации обратного трафика от туннелируемых узлов укажите координатор в качестве шлюза по умолчанию для таких узлов.
- Для туннелируемых узлов по умолчанию созданы фильтры, разрешающие передачу трафика по любым IP-адресам, протоколам и портам. Если вы настраиваете обработку прикладных протоколов в туннелируемом трафике, то в целях безопасности рекомендуется удалить эти фильтры и создать фильтры, разрешающие соединения между конкретными узлами по транспортным протоколам и портам, заданным в параметрах настройки прикладных протоколов.

Чтобы просмотреть текущие настройки обработки прикладных протоколов:

```
hostname> alg show
```

В результате отобразится таблица:

```
SERVICE       PROTOCOL      PORTS                      ON/OFF

=========     =========     ====================       =====

FTP           TCP           21                         ON

DNS           UDP           53                         ON

H323          TCP           1720                       ON

H323          UDP           1719                       ON

SCCP          TCP           2000                       ON

MODBUS        TCP                                      OFF

IEC104        TCP                                      OFF

SIP           TCP           5060,5080                  ON

SIP           UDP           5060,5080                  ON
```

где:

- `Service` — прикладной протокол.
- `Protocol` — транспортный протокол, используемый прикладным протоколом.
- `Ports` — порты, используемые прикладным протоколом.
- `On/Off` — состояние обработки: `on` — включена, `off` — выключена.

Чтобы изменить параметры обработки прикладного протокола:

```
hostname# alg module <прикладной протокол> process <транспортный протокол> <порт> on
```

где:

- `<прикладной протокол>` — `dns`, `ftp`, `h323`, `sccp` или `sip`;
- `<транспортный протокол>` — `tcp` или `udp`;

  Выбор транспортного протокола поддерживается не для всех прикладных протоколов. Например, для FTP нельзя задать протокол UDP, а для DNS — TCP.
- `<порт>` — порт, диапазон портов либо список, состоящий из портов или их диапазонов, разделённых запятой.

Например, если для обработки данных, передаваемых по протоколу SIP, используются не только стандартные порты, но и дополнительные: 10000 и 21–65 для протокола UDP, добавьте их:

```
hostname# alg module sip process udp 10000,21-65 on
```



Внимание! Заданные параметры обработки должны соответствовать параметрам, указанным в настройках соответствующих приложений (FTP-клиент, DNS-клиент, SIP-клиент и так далее).

После изменения настроек обработки прикладных протоколов (в том числе, включения или выключения) перезапустите приложение (например, DNS-, FTP-, SIP-клиент) или устройство (например, SIP-телефон).

Чтобы выключить обработку прикладного протокола:

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

Особенности обработки прикладных протоколов DNS, FTP, SIP и H.323

Обработка протокола DNS

В сетях ViPNet приложения могут использовать виртуальные IP-адреса, реально не существующие в сети и уникальные на каждом сетевом узле, что позволяет избежать конфликтов при наличии пересекающихся адресов в разных сетях.

Чтобы узлы внутренней сети ViPNet могли обращаться к удалённым узлам ViPNet по доменным именам через туннелируемый DNS-сервер, требуются дополнительные настройки на DNS-сервере и узлах сети ViPNet:

1. На DNS-сервере настройте поддержку динамического изменения DNS-записей. Как правило, по умолчанию DNS-серверы не поддерживают эту настройку.
2. Для клиентов, к которым будут обращаться по доменному имени:
   2.1 В ViPNet Prime укажите корпоративный DNS-сервер.
   2.2 На самих клиентах настройте автоматическую регистрацию на DNS-сервере.
3. На туннелирующем координаторе включите обработку протокола.

Обработка протокола FTP

При передаче файлов между клиентом и сервером по протоколу FTP устанавливается как минимум два TCP-соединения:

- для отправки команд на сервер и получения ответов от него — управляющее TCP-соединение;
- для передачи данных — дополнительное TCP-соединение.

TCP-соединения по протоколу FTP устанавливаются в следующем порядке:

1. Клиент создаёт управляющее TCP-соединение с сервером со своего порта из диапазона 1024-65535 на 21-й порт сервера.
2. В зависимости от выбранного режима передачи данных, клиент отправляет по управляющему соединению:
   - в активном режиме — номер порта, открытого клиентом для получения данных с сервера;
   - в пассивном режиме — запрос на номер порта сервера, к которому будет подключаться клиент.
3. Соединение устанавливается одним из двух способов:
   - в активном режиме — сервер создаёт дополнительное соединение для передачи данных на указанный клиентом порт;
   - в пассивном режиме — сервер по управляющему соединению передаёт клиенту номер порта, к которому клиент создаёт дополнительное соединение.

Таким образом, в активном режиме соединение для передачи данных создаёт сервер, а в пассивном — клиент.

Чтобы использовать протокол FTP:

1. Разрешите управляющее соединение. Для этого создайте сетевой фильтр, разрешающий исходящее TCP-соединение на 21-й порт FTP-сервера.
2. При использовании активного режима передачи данных разрешите дополнительное соединение. Для этого включите обработку протокола FTP, которая автоматически добавит необходимый сетевой фильтр.

Для разрешения дополнительного соединения в пассивном режиме работы настройки не требуются.

Обработка протокола SIP

При передаче мультимедийных данных по протоколу SIP создаётся управляющее и дополнительное соединение (RTP-сессия). Медиа-потоки в дополнительных соединениях могут передаваться между SIP-клиентами напрямую (т.н. режим Direct Call или Peer-to-Peer RTP) или через сервер телефонии.

Чтобы настроить связь между SIP-клиентами:

1. Убедитесь, что включена обработка протокола SIP.
2. Если хотя бы один SIP-клиент является открытым узлом, убедитесь, что для всех защищённых узлов настроена видимость по реальным IP-адресам.
3. Создайте сетевые фильтры, разрешающие управляющие соединения. Сетевые фильтры должны пропускать трафик между SIP-клиентами и сервером телефонии по транспортным протоколам и портам, заданным в параметрах обработки прикладных протоколов (по умолчанию TCP и UDP с портами 5060 и 5080):
   - Если все SIP-клиенты туннелируются координаторами, создайте фильтры туннелируемых узлов.
   - Если хотя бы одно SIP-устройство является открытым узлом, создайте транзитные фильтры.



Примечание. Некоторые SIP-клиенты, например SIP-клиент компании Zoiper, могут устанавливать соединения TCP и UDP не через порт 5060, а через динамический порт, выбранный произвольно из определенного диапазона. Поэтому если хотя бы один из SIP-клиентов является открытым узлом, возможность использования динамических портов необходимо отключить в настройках SIP-клиента.

4. Настройте создание сетевых фильтров для разрешения RTP-сессий:
   - По умолчанию создаются фильтры, разрешающие RTP-трафик между SIP-клиентами и сервером телефонии. Для этого проверяется совпадение IP-адреса создаваемой RTP-сессии с одним из IP-адресов сигнальной сессии.
   - Если на сервере телефонии настроен режим передачи RTP-трафика между SIP-клиентами напрямую (без участия сервера телефонии), выполните:

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

     После этого разрешающие фильтры будут создаваться без проверки принадлежности RTP-сессии к сигнальной сессии.



Внимание! Сетевые фильтры, которые создаются для режима прямого соединения между SIP-клиентами, будут разрешать RTP-сессии между любыми IP-адресами. Поэтому не рекомендуется использовать этот режим, если ViPNet Coordinator IG размещён на границе защищаемой сети.

5 Чтобы настройки вступили в силу, закройте все открытые соединения:

```
hostname# firewall conntrack flush
```

Обработка протокола H.323

В наборе протоколов H.323 используются сигнальные протоколы H.225 и H.245. Для передачи медиа-потоков используется RTP. При включении обработки H.323 автоматически создаются временные сетевые фильтры, разрешающие сигнальные H.245-сессии и дополнительные RTP-сессии. При этом, чтобы разрешить сигнальные H.225-сессии, необходимо создать разрешающие сетевые фильтры вручную.

Терминалы H.323 (IP-телефоны) могут устанавливать связь друг с другом напрямую или с участием контроллера зоны (gatekeeper). В зависимости от наличия контроллера зоны и режимов его работы может потребоваться настройка создания временных сетевых фильтров, разрешающих H.245- и RTP-сессии.

Чтобы настроить связь между IP-телефонами по протоколу H.323:

1 Убедитесь, что включена обработка протокола H.323.

2 При использовании IP-телефонов Yate настройте видимость туннелируемых узлов по реальным IP-адресам.

3 Создайте сетевые фильтры, разрешающие сигнальные H.225-сессии между H.323-устройствами. Сетевые фильтры должны пропускать трафик по транспортным протоколам и портам, заданным в параметрах обработки прикладных протоколов (по умолчанию UDP 1719 и TCP 1720):

   - Если H.323-устройства туннелируются координаторами, создайте фильтры туннелируемых узлов.
   - Если хотя бы одно H.323-устройство является открытым узлом, создайте транзитные фильтры.

4 Настройте автоматическое создание сетевых фильтров, разрешающих дополнительную сигнальную H.245-сессию, а также RTP-сессию:

   В зависимости от настроек H.323-телефонии потоки сигнальных H.225- и H.245-сессий могут проходить через контроллер зоны или напрямую между IP-телефонами.

   - Если пути прохождения H.225-потока и H.245-потока отличаются, например:

     ```
     H.225: IP-телефон -> контроллер зоны -> IP-телефон
     H.245: IP-телефон -> IP-телефон
     RTP: IP-телефон -> IP-телефон
     ```

     выполните команду:

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

   - Если пути прохождения RTP-потока и родительского H.245-потока отличаются, например:

     ```
     H.225: IP-телефон -> контроллер зоны -> IP-телефон
     H.245: IP-телефон -> контроллер зоны -> IP-телефон
     RTP: IP-телефон -> IP-телефон
     ```

выполните команду:

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

- Если H.225-, H.245- и RTP-сессии проходят между IP-телефонами напрямую, например:

  ```
  H.225: IP-телефон -> IP-телефон
  H.245: IP-телефон -> IP-телефон
  RTP: IP-телефон -> IP-телефон
  ```

  менять настройки по умолчанию не требуется (`direct-h245 on` и `direct-media on`).



Примечание. В некоторых IP-телефонах (например, Yate) отсутствует H.245-сессия. Если пути прохождения RTP-потока и родительского H.225-потока отличаются, выполните команду:

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

Иначе, оставьте настройки по умолчанию.

Подробнее о работе этих команд см. в документе «Справочник команд и конфигурационных файлов».

5 Чтобы настройки вступили в силу, закройте все открытые соединения:

```
hostname# firewall conntrack flush
```

Синхронизация сессий прикладных протоколов в кластере

При переключении узлов кластера прерываются все открытые к этому моменту соединения. Чтобы соединения не прерывались, вы можете использовать функцию синхронизации открытых соединений (см. Развёртывание кластера). Но для синхронизации сессий прикладных протоколов необходимо выполнить дополнительную настройку. Это можно сделать, как на этапе развёртывании кластера, так и его использования:



Примечание. Для промышленных прикладных протоколов синхронизация сессий не поддерживается.

1 Завершите работу системы защиты от сбоев:

```
hostname# failover stop
```

2 Откройте файл `failover.ini` для изменения:

```
hostname# failover config edit
```

3 В секции `[misc]` задайте параметры:

- `syncconnections = yes`
- `syncalgtcp = yes`

Примечание. Параметры `syncconnections` и `syncalgtcp` необходимо задать со значением `yes` на обоих узлах кластера.

4 Сохраните изменения (**Ctrl+O**, затем **Enter**) и закройте редактор (**Ctrl+X**).

5 Запустите систему защиты от сбоев:

```
hostname# failover start
```

Чтобы выключить синхронизацию сессий прикладных протоколов, измените значение параметра `syncalgtcp` на `no`.

7

Настройка сетевых служб

Настройка DHCP-сервера 148

Настройка DHCP-relay 150

Настройка DNS-сервера 152

Настройка NTP-сервера 154

Настройка точки доступа к сети Wi-Fi 157

Настройка шлюза Modbus 159

Настройка интерфейса GPIO 163

Настройка DHCP-сервера

В состав ViPNet Coordinator IG входит DHCP-сервер. Он динамически назначает IP-адреса сетевым узлам (DHCP-клиентам). Также DHCP-сервер может передать дополнительные параметры — IP-адреса шлюза по умолчанию, DNS-, NTP-сервера и другие.

DHCP-сервер может обслуживать DHCP-клиентов, которые находятся:

- в одной сети с DHCP-сервером, в том числе в сегментах сети, объединённых по L2OverIP;
- в удалённых подсетях с помощью агента DHCP-relay.

Чтобы настроить DHCP-сервер:

1 Включите сетевой интерфейс, на котором будет работать DHCP-сервер:

```
hostname# inet ifconfig <интерфейс> up
```

2 Задайте этот интерфейс для работы DHCP-сервера:

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



Примечание. Можно указать Ethernet-, VLAN-, Wi-Fi или агрегированный интерфейс, у которого настроен статический IP-адрес.

Если вы указали `wlan0`, настройте точку доступа к сети Wi-Fi.

3 Задайте диапазон IP-адресов, выделяемых клиентам:

```
hostname# inet dhcp server add range <начальный IP-адрес> <конечный IP-адрес>
{interface <интерфейс> | remote subnet <подсеть> mask <маска>}
```

Диапазон IP-адресов должен принадлежать сети интерфейса или заданной подсети (при указании `remote subnet`). IP-адрес интерфейса не должен входить в этот диапазон.



Примечание. DHCP-сервер может выделять клиентам любые диапазоны IP-адресов. Если локальная сеть маршрутизируется в интернет, используйте диапазоны, которые установлены стандартом для частных сетей: `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`.

4 Задайте дополнительные параметры:

- IP-адрес шлюза по умолчанию:

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

  IP-адрес шлюза должен принадлежать сети интерфейса и не должен входить в диапазон IP-адресов, выделяемых клиентам. В случае указания `remote subnet` IP-адреса шлюза должен принадлежать к указанной подсети `<subnet>`.

- IP-адрес DNS-сервера:

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

- IP-адрес NTP-сервера:

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

Например, чтобы задать адрес DNS-сервера 192.168.15.41 для клиентов другой сети с адресом 192.168.1.0/24:

- Задайте `eth0` в качестве сетевого интерфейса, на котором DHCP-сервер будет обрабатывать запросы от агента DHCP-relay, работающего в удалённой подсети 192.168.1.0/24:

  ```
  hostname# inet dhcp server add relay-interface eth0 remote subnet 192.168.1.0 mask
  255.255.255.0
  ```

- Задайте адрес DNS-сервера 192.168.15.41 для клиентов сети 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
  ```

5. Проверьте настройки DHCP-сервера:

   ```
   hostname# inet show dhcp server
   ```

6. Включите автоматический запуск DHCP-сервера:

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

   По умолчанию автоматический запуск DHCP-сервера выключен.

7. Запустите DHCP-сервер:

   ```
   hostname# inet dhcp server start
   ```

Чтобы просмотреть список клиентов DHCP-сервера:

`hostname# inet show dhcp server lease [{last | all | full}]`, где:

- `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.

Если несколько клиентов получили одинаковые IP-адреса, возможно, у них совпадает идентификатор DHCP-клиента (UID). Чтобы избежать этого, в сетевых настройках клиентов задайте MAC-адрес в качестве идентификатора DHCP.

Настройка DHCP-relay

ViPNet Coordinator IG можно использовать в качестве агента DHCP-relay. Он принимает от узлов DHCP-запросы и передаёт их DHCP-серверу. Ответы, полученные от DHCP-сервера, агент DHCP-relay перенаправляет сетевым узлам.



Внимание! Для приема и перенаправления DHCP-запросов через DHCP-relay необходимо, чтобы DHCP-сервер поддерживал Option 82 Suboption 5.

Агент DHCP-relay используется, когда сетевые узлы не могут обращаться напрямую к DHCP-серверу. Например, в разветвлённой сети из нескольких подсетей, в которых нет своего DHCP-сервера.

Агент DHCP-relay может работать с несколькими локальными сетями. Это могут быть как сети, подключённые к разным физическим сетевым интерфейсам ViPNet Coordinator IG, так и виртуальные локальные сети, подключённые к одному физическому интерфейсу. Вы можете настроить несколько копий DHCP-relay, которые будут иметь различные слушающие, внешние интерфейсы и IP-адреса DHCP-серверов.

Узлы, которые будут обращаться к DHCP-серверу через ViPNet Coordinator IG, могут быть защищёнными и открытыми. DHCP-сервер может быть защищённым, открытым или туннелируемым узлом.

Если агент DHCP-relay перенаправляет запросы на DHCP-сервер, который туннелируется другим координатором, настройте между координаторами видимость по реальным IP-адресам (см. Настройка видимости узлов). Если между ними настроена видимость по виртуальным адресам, ответы от DHCP-сервера будут отправляться на реальный адрес ViPNet Coordinator IG, выступающего в качестве агента DHCP-relay, и не будут доставлены.

Чтобы запустить DHCP-relay:

1. Задайте список сетевых интерфейсов, через которые DHCP-relay должен получать DHCP-запросы от клиентов. Чтобы добавить интерфейс в список:

   ```
   hostname# inet dhcp relay [<номер копии>] add listen-interface <имя интерфейса>
   ```

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

   На каждом добавляемом сетевом интерфейсе должен быть задан статический IP-адрес, принадлежащий адресному пространству соответствующей подсети. Сетевой интерфейс, который используется для соединения с удаленным сервером может также получать IP-адрес по DHCP.

2. Задайте внешний DHCP-сервер для перенаправления DHCP-запросов клиентов и сетевой интерфейс ViPNet Coordinator IG для доступа к удаленному серверу:

   ```
   hostname# inet dhcp relay [<номер копии>] add external-interface <имя интерфейса>
   server <IP-адрес внешнего DHCP-сервера>
   ```



Внимание! В случае если по событию DGD произойдет переключение внешних сетевых интерфейсов, то служба DHCP-relay, использующая один из этих интерфейсов в качестве внешнего, будет недоступна.

3 Укажите сетевой интерфейс ViPNet Coordinator IG, который должен использоваться для доступа к резервному DHCP-серверу, если он есть в сети:

```
hostname# inet dhcp relay [<номер копии>] add backup-interface <имя интерфейса> server <IP-адрес сервера>
```

4 Включите автоматический запуск DHCP-relay при загрузке ViPNet Coordinator IG:

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

По умолчанию автоматический запуск DHCP-relay выключен.

5 Запустите DHCP-relay:

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

6 Посмотрите настройки DHCP-relay и его текущее состояние:

```
hostname# inet show dhcp relay [<номер копии>]
```



Примечание. Чтобы впоследствии завершить работу DHCP-relay и одновременно сбросить все его настройки, а также выключить автоматический запуск при загрузке ViPNet Coordinator IG:

```
hostname# inet dhcp relay reset
```

Настройка DNS-сервера

DNS-сервер преобразует доменные имена в IP-адреса в ответ на запросы сетевых узлов (DNS-клиентов).

Локальный DNS-сервер перенаправляет поступающие к нему DNS-запросы на вышестоящие DNS-серверы и передает полученные ответы DNS-клиентам. По умолчанию локальный DNS-сервер преобразует доменные имена с использованием корневых DNS-серверов из домена `root-servers.net`. Этот список можно дополнить DNS-серверами пересылки (forwarders).



Внимание! В качестве DNS-серверов пересылки используйте доверенные DNS-серверы из сети ViPNet. Ответы на запросы DNS-клиентов, приходящие не от доверенных DNS-серверов, могут быть скомпрометированы.

Список дополнительных DNS-серверов:

- Можно получить от внешнего DHCP-сервера.

  На сетевом интерфейсе должен быть установлен режим автоматического получения параметров от DHCP-сервера, а DHCP-сервер должен отправлять информацию о DNS-серверах.

  Если режим DHCP установлен на нескольких интерфейсах ViPNet Coordinator IG, то результат обработки собственных DNS-запросов и запросов DNS-клиентов не определен, так как неизвестно, какой интерфейс будет включен первым и какой список DNS-серверов пересылки получит ViPNet Coordinator IG.

  Настраивайте получение информации о DNS-серверах только на одном интерфейсе. Данные об адресах DNS-серверов поступают автоматически, откажитесь от их получения:

  ```
  hostname# inet ifconfig <интерфейс> dhcp dns off
  ```

- Задать вручную.



Внимание! Если DNS-серверы пересылки недоступны, но при этом доступны корневые DNS-серверы, DNS-клиенты будут получать ответы на свои запросы с задержкой.

Команды для работы с локальным DNS-сервером

- Указать IP-адреса узлов и подсетей, узлам которых разрешены запросы к DNS-серверу:

  ```
  hostname# inet dns clients add {<IP-адрес> | <IP-адрес/длина маски>}
  ```

  По умолчанию DNS-запросы к серверу разрешены для любых узлов.

- Посмотреть список IP-адресов, которым разрешены DNS-запросы к серверу:

  ```
  hostname# inet dns clients list
  ```

- Удалить IP-адреса из списка адресов, которым разрешены DNS-запросы к серверу:

```
hostname# inet dns clients delete {<IP-адрес> | <IP-адрес/длина маски>}
```

- Добавить IP-адрес DNS-сервера, на который ViPNet Coordinator IG будет перенаправлять DNS-запросы:

  ```
  hostname# inet dns forwarders add <IP-адрес>
  ```

  Если необходимо перенаправлять DNS-запросы для определенных зон, то добавьте для каждой такой зоны IP-адрес DNS-сервера пересылки с указанием параметра `<for-zone>`:

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

- Посмотреть список DNS-серверов пересылки:

  ```
  hostname# inet dns forwarders list
  ```

- Удалить DNS-сервер из списка:

  ```
  hostname# inet dns forwarders delete <IP-адрес>
  ```

  Для удаления из списка DNS-сервера пересылки, заданного для определенной зоны, укажите параметр `<for-zone>`:

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



Примечание. При добавлении двух и более DNS-серверов пересылки, серверы, добавленные без указания имени зоны, имеют приоритет и будут использоваться для перенаправления всех DNS-запросов вне зависимости от наличия серверов пересылки для отдельных зон. При этом появится сообщение:

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

При изменении конфигурации внешних DNS-серверов перезапустите локальный DNS-сервер:

```
hostname# inet dns stop
hostname# inet dns start
```

- Включить или выключить автоматический запуск DNS-сервера при загрузке ViPNet Coordinator IG:

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

  Текущее состояние задано при установке справочников и ключей.

- Запустить или остановить DNS-сервер:

  ```
  hostname# inet dns {start | stop}
  ```

- Посмотреть текущие параметры DNS-сервера:

  ```
  hostname# inet show dns
  ```

Настройка NTP-сервера

В состав ViPNet Coordinator IG входит локальный NTP-сервер. Он используется для синхронизации времени на ViPNet Coordinator IG и на других сетевых узлах (NTP-клиентах).

По умолчанию локальный NTP-сервер синхронизирует время с публичными NTP-серверами:

- `ntp1.vniiftri.ru`;
- `ntp2.vniiftri.ru`;
- `ntp.ix.ru`.

Вы можете добавить синхронизацию времени с другими NTP-серверами (публичными или корпоративными).

Дополнительные NTP-серверы:

- Можно получить от внешнего DHCP-сервера.

  На сетевом интерфейсе должен быть установлен режим автоматического получения параметров от DHCP-сервера и DHCP-сервер должен отправлять информацию о NTP-серверах.

  Если режим DHCP установлен на нескольких сетевых интерфейсах ViPNet Coordinator IG, то результат синхронизации времени на ViPNet Coordinator IG и на NTP-клиентах не определён, так как неизвестно, какой сетевой интерфейс будет включён первым и какой список дополнительных NTP-серверов получит ViPNet Coordinator IG.

  Настраивайте получение адресов NTP-серверов только на одном интерфейсе и откажитесь от их получения при настройке других интерфейсов, на которых включён режим DHCP:

  ```
  hostname# inet ifconfig <интерфейс> dhcp ntp off
  ```

- Добавить вручную.

Дополнительный NTP-сервер может находиться как в защищённой, так и в открытой сети:

- Если дополнительный NTP-сервер — узел защищённой сети, видимый по реальному адресу, то в файле `iplir.conf` в секции `[id]` для этого узла установите параметр `visibility` в значение `real`. Описание секции и параметра см. в документе «Справочник команд и конфигурационных файлов», в разделе «Файл iplir.conf».
- Если дополнительный NTP-сервер — узел открытой сети, добавьте разрешающий фильтр открытой сети для входящего трафика от NTP-сервера:

  ```
  hostname# firewall local add src @any dst @local udp dport 123 pass
  ```

Команды для работы с локальным NTP-сервером

- Просмотреть список NTP-серверов:

  ```
  hostname# inet ntp list
  ```

- Добавить адрес дополнительного NTP-сервера:

```
hostname# inet ntp add {server | peer} {<IP-адрес> | <доменное имя>}
```

- `server` — если NTP-сервер только рассылает данные о времени;
- `peer` — если NTP-сервер рассылает и получает данные о времени.

- Отключить использование NTP-серверов, заданных по умолчанию, и использовать только дополнительные NTP-серверы:

```
hostname# inet ntp use-default off
```



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

- Разрешить переход в изолированный (orphan) режим при потере соединения с внешними NTP-серверами:

```
hostname# inet ntp orphan on <stratum>
```

`<stratum>` — уровень внешнего NTP-сервера (от 1 до 10). Если со всеми внешними NTP-серверами меньше указанного уровня не удаётся установить соединение в течение 5 минут, то локальный NTP-сервер переходит в изолированный режим. По умолчанию значение `<stratum>` равно 5. Значение `stratum` задаётся в настройках NTP-сервера.



Примечание. Разрешите переход локального NTP-сервера в изолированный режим, если ViPNet Coordinator IG используется в качестве NTP-сервера для внутренней сети. Иначе клиенты ViPNet Coordinator IG не будут получать информацию о точном времени при потере соединения ViPNet Coordinator IG с внешними NTP-серверами, так как в этом случае локальный NTP-сервер будет считаться недостоверным.

- Удалить адрес дополнительного NTP-сервера:

```
hostname# inet ntp delete {server | peer} {<IP-адрес> | <доменное имя>}
```

- Включить автоматический запуск локального NTP-сервера при загрузке ViPNet Coordinator IG:

```
hostname# inet ntp mode on
```

Текущее состояние задано при установке справочников и ключей.

- Запустить или остановить NTP-сервер:

```
hostname# inet ntp {start | stop}
```



Примечание. NTP-серверы, указанные по доменному имени, будут доступны, только если запущен DNS-сервер.

Информация о попытках подключения к NTP-серверам записывается в системный журнал.

- Просмотреть текущие параметры и состояние локального NTP-сервера:

```
hostname# inet show ntp
```



Внимание! Если время на вышестоящем NTP-сервере будет изменено более чем на 1000 секунд вперёд или назад, это может привести к аварийному завершению работы локального NTP-сервера. Запустите NTP-сервер:

```
hostname# inet ntp start
```

Настройка точки доступа к сети Wi-Fi

Примечание.

- Использование ViPNet Coordinator IG в качестве точки доступа Wi-Fi возможно только в исполнениях со встроенным модулем Wi-Fi.
- Беспроводные сети, такие как Wi-Fi и 3G/4G, менее надежны, чем проводные. Воздействие различного рода помех на беспроводные сети может приводить к потерям среди IP-пакетов и снижению скорости передачи данных.
- ViPNet Coordinator IG может также работать в качестве клиента сети Wi-Fi (см. Подключение к сети Wi-Fi). Использование ViPNet Coordinator IG одновременно в качестве клиента и точки доступа Wi-Fi не поддерживается.

Чтобы настроить работу ViPNet Coordinator IG в качестве точки доступа Wi-Fi:

1 Отключите сетевой интерфейс `wlan0`:

```
hostname# inet wifi mode off
```

2 Переключите `wlan0` в режим точки доступа:

```
hostname# inet wifi role access-point
```

3 Задайте имя вашей сети Wi-Fi и способ аутентификации пользователей в сети:

- Если аутентификация в сети не требуется:

  ```
  hostname# inet wifi access-point authentication open
  ```

  По запросу введите имя сети.

- Если для аутентификации требуется использовать пароль, выберите режим аутентификации WPA-PSK или WPA2-PSK:

  ```
  hostname# inet wifi access-point authentication {wpa-psk | wpa2-psk}
  ```

  По запросу введите имя сети и пароль. Заданный пароль сообщите пользователям вашей сети Wi-Fi.

4 Точка доступа поддерживает стандарты:

- IEEE 802.11b — 2,4 ГГц, скорость соединения до 11 Мбит/с.
- IEEE 802.11g — 2,4 ГГц, скорость соединения до 54 Мбит/с (установлен по умолчанию).

Вы можете изменить стандарт связи:

```
hostname# inet wifi access-point hwmode {b | g}
```

5 Задайте номер используемого канала Wi-Fi:

```
hostname# inet wifi access-point channel <номер канала>
```

По умолчанию используется канал номер 1, допустимы номера от 1 до 11.

6 Назначьте интерфейсу `wlan0` статический IP-адрес:

```
hostname# inet ifconfig wlan0 address <IP-адрес> netmask <маска подсети>
```

7 Включите `wlan0`:

```
hostname# inet wifi mode on
```

8 Настройте параметры DHCP-сервера для интерфейса `wlan0` (см. Настройка DHCP-сервера).

9 Для связи с устройствами, которые подключены к сети Wi-Fi, и устройствами, подключенными к сети Ethernet, создайте транзитные фильтры открытой сети, разрешающие прохождение IP-пакетов между этими сетями.

Вы можете настроить запись уровня сигнала Wi-Fi в системный журнал с помощью команды:

```
hostname# inet wifi log signal <периодичность>
```

где `<периодичность>` — интервал времени, через который уровень сигнала будет записываться в журнал (в минутах). Чтобы выключить запись уровня сигнала, введите `off` вместо интервала времени.

Настройка шлюза Modbus

Примечание. Шлюз Modbus поддерживается во всех исполнениях ViPNet Coordinator IG10 и ViPNet Coordinator IG100. Для использования шлюза Modbus включите эту функцию в настройках координатора в ViPNet Prime. Это можно сделать при наличии лицензии на шлюз Modbus.

Вы можете настроить шлюз Modbus на каждом из последовательных интерфейсов ViPNet Coordinator IG.

Настройка

1 Задайте произвольное имя шлюза, укажите последовательный интерфейс и TCP-порт, на которых он будет работать:

```
hostname# service mbgw add name <имя шлюза> serial <последовательный интерфейс> port <TCP-порт>
```

Список доступных последовательных интерфейсов зависит от вашего исполнения ViPNet Coordinator IG. Если интерфейс уже используется другим шлюзом Modbus, он не отображается в списке. Для просмотра последовательных интерфейсов см. ниже раздел «Просмотр настроек».

По умолчанию заданы следующие настройки шлюза Modbus:

- Режим работы: TCP to RTU;
- Время ожидания запроса: 1500 мс;
- Время ожидания ответа: 1500 мс;
- Скорость TTY: 115200 бод;
- Контроль чётности: even;
- Задержка до отправки: 100 мс (для интерфейса с типом RS-485);
- Задержка после отправки: 0 мс (для интерфейса с типом RS-485);
- Шлюз Modbus отключён.

2 Чтобы изменить настройки, заданные по умолчанию:

2.1 Остановите работу шлюза Modbus, если он включён:

```
hostname# service mbgw name <имя шлюза> stop
```

2.2 Чтобы выбрать режим работы RTU to TCP:

```
hostname# service mbgw name <имя шлюза> type rtu-to-tcp
```

2.3 Чтобы изменить время ожидания запроса от ведущего Modbus-устройства:

```
hostname# service mbgw name <имя шлюза> request-timeout <интервал>
```

2.4 Чтобы изменить время ожидания ответа от ведомого Modbus-устройства:

```
hostname# service mbgw name <имя шлюза> response-timeout <интервал>
```

2.5 Чтобы изменить скорость последовательного интерфейса:

```
hostname# service mbgw name <имя шлюза> baudrate <скорость>
```

2.6 Чтобы изменить режим работы с битом контроля чётности последовательного интерфейса:

```
hostname# service mbgw name <имя шлюза> parity <режим>
```

Возможные значения:

- `off` — режим, при котором проверка бита чётности не производится;
- `even` — режим, при котором биты данных и бит чётности всегда должны составлять чётное число единиц;
- `odd` — режим, при котором биты данных и бит чётности всегда должны составлять нечётное число единиц;
- `mark` — режим, при котором бит чётности всегда принимает значение 1;
- `space` — режим, при котором бит чётности всегда принимает значение 0;
- `none` — режим, при котором бит чётности отсутствует.

3 Если необходимо, чтобы шлюз Modbus включался автоматически при загрузке ViPNet Coordinator IG:

```
hostname# service mbgw name <имя шлюза> mode on
```

4 Если выбран режим работы RTU to TCP, настройте маршрутизацию для Modbus-устройства, подключённого к ViPNet Coordinator IG по последовательной линии связи:

```
hostname# service mbgw name <имя шлюза> routing add <адрес устройства> ip <IP-адрес>
[port <TCP-порт>] [description <комментарий>] [request-timeout <интервал>]
[response-timeout <интервал>]
```

где:

- `<адрес устройства>` — адрес устройства Modbus, которое необходимо маршрутизировать в сети Ethernet (SlaveID). Вы можете задать несколько адресов и (или) их диапазонов через запятую.
- `<IP-адрес>` — IP-адрес шлюза Modbus.
- `<комментарий>` — произвольный комментарий (без пробелов) для описания подключения к Modbus-устройству.

Если необязательные параметры не указаны, используются значения, заданные для шлюза Modbus (TCP-порт, время ожидания запроса от ведущего устройства и время ожидания ответа от ведомого устройства).

Чтобы изменить маршрут, используйте команду:

```
hostname# service mbgw name <имя шлюза> routing change <адрес устройства> [ip
<IP-адрес>] [port <TCP-порт>] [description <комментарий>] [request-timeout
<интервал>] [response-timeout <интервал>]
```

Чтобы удалить маршрут:

```
hostname# service mbgw name <имя шлюза> routing delete <адрес устройства>
```

5 Запустите шлюз Modbus:

```
hostname# service mbgw name <имя шлюза> start
```

Примечание. Шлюз Modbus доступен по IP-адресам всех сетевых интерфейсов ViPNet Coordinator IG и заданному TCP-порту. Чтобы разрешить или ограничить доступ к шлюзу Modbus, используйте сетевые фильтры.

Изменение настроек

Чтобы выбрать другой последовательный интерфейс или TCP-порт, на котором должен работать шлюз Modbus:

1. Остановите работу шлюза Modbus:

   ```
   hostname# service mbgw name <имя шлюза> stop
   ```

2. Измените параметр:

   - Чтобы выбрать другой последовательный интерфейс:

     ```
     hostname# service mbgw name <имя шлюза> serial <последовательный интерфейс>
     ```

     Нельзя выбрать интерфейс, который уже используется другим шлюзом Modbus.

     Примечание. Чтобы освободить последовательный интерфейс, занятый шлюзом Modbus:

     1. Остановите работу этого шлюза: `hostname# service mbgw name <имя шлюза> stop`
     2. Удалите шлюз Modbus с последовательного интерфейса: `hostname# service mbgw delete name <имя шлюза>`

   - Чтобы указать другой TCP-порт:

     ```
     hostname# service mbgw name <имя шлюза> port <TCP-порт>
     ```

     Нельзя выбрать TCP-порт, который уже используется другим шлюзом Modbus или занят другой службой.

3. Запустите шлюз Modbus:

   ```
   hostname# service mbgw name <имя шлюза> start
   ```

Для изменения других настроек шлюза Modbus см. выше подраздел **Настройка**, шаг 2.

Примечание. Команды остановки, запуска и настройки автоматического запуска вы можете выполнять без указания имени шлюза Modbus. В этом случае команда будет выполнена в отношении всех шлюзов Modbus.

Просмотр настроек

- Чтобы просмотреть настройки одного шлюза Modbus:

  ```
  hostname> service mbgw name <имя шлюза> show
  ```

- Чтобы просмотреть настройки всех шлюзов Modbus:

  ```
  hostname> service mbgw show
  ```

- Чтобы просмотреть список маршрутизируемых устройств шлюза Modbus, работающего в режиме RTU to TCP:

  ```
  hostname> service mbgw name <имя шлюза> routing show
  ```

- Чтобы просмотреть информацию обо всех последовательных интерфейсах, а также какие шлюзы Modbus на них настроены:

  ```
  hostname> inet serial show
  ```

Устранение неполадок

Ошибки и другие события в работе шлюзов Modbus записываются в системный журнал. По умолчанию в журнал записываются: критические события, ошибки, предупреждения и важные события.

Если этой информации недостаточно для определения причин неполадок в работе шлюза Modbus, измените уровень важности событий, записываемых в системный журнал:

1. Остановите работу одного или всех шлюзов Modbus:

   ```
   hostname# service mbgw [name <имя шлюза>] stop
   ```

2. Измените уровень важности событий одного или всех шлюзов Modbus:

   ```
   hostname# service mbgw [name <имя шлюза>] syslog-level <уровень важности>
   ```

   Возможные значения:

   - `0` — критические события (critical);
   - `1` — ошибки (error);
   - `2` — предупреждения (warning);
   - `3` — важные события (notice);
   - `4` — информационные события (info);
   - `5` — отладочные события (debug).

   Каждый последующий уровень включает в себя предыдущие. По умолчанию задан уровень `3`.

3. Запустите один или все шлюзы Modbus:

   ```
   hostname# service mbgw [name <имя шлюза>] start
   ```

Внимание! В случае возникновения нештатных условий эксплуатации, которые повлекли за собой перезагрузку ViPNet Coordinator IG или подключённых к нему устройств или узлов, проверьте работоспособность Modbus-соединений с этими устройствами и узлами. Если связь не восстановилась, перезапустите шлюзы Modbus:

```
hostname# service mbgw stop
hostname# service mbgw start
```

Настройка интерфейса GPIO

На корпусе ViPNet Coordinator IG расположен интерфейс GPIO, который вы можете использовать для решения следующих задач безопасности АСУ ТП:

- Подключение датчика вскрытия внешнего шкафа.
- Подключение внешней кнопки для перевода ViPNet Coordinator IG в специальный режим функционирования.
- Сигнализация о событиях, отслеживаемых ViPNet Coordinator IG.
- Отправка сигналов о режиме работы ViPNet Coordinator IG в кластере.

Подробнее о настройке интерфейса GPIO для решения этих задач см. в документе «Сценарии работы» в разделе «Использование интерфейса GPIO».

Чтобы выполнить настройку интерфейса GPIO:

1 Остановите службу `piomonitord`, которая обрабатывает сигналы интерфейса GPIO:

```
hostname# service piomonitor stop
```

2 Задайте активный уровень сигнала для контакта GPIO, который будет определять срабатывание обработчика:

```
hostname# service piomonitor set <имя_контакта> activelevel { 0 | 1 }
```

где:

- `<имя_контакта>` — наименование контакта GPIO (`In` или `Out`), для которого необходимо задать активный уровень сигнала;
- `0` — обработчик будет срабатывать при изменении уровня сигнала на контакте GPIO с 1 на 0;
- `1` — обработчик будет срабатывать при изменении уровня сигнала на контакте GPIO с 0 на 1.

3 В зависимости от решаемой задачи, настройте обработку сигналов для входного контакта GPIO:

- Чтобы настроить обработку сигнала от внешнего устройства для перевода ViPNet Coordinator IG в специальный режим работы, если ViPNet Coordinator IG инициализирован как межсетевой экран типа «Д», выполните команду:

  ```
  hostname# service piomonitor set In emergency {button | switch}
  ```

  где:

  - `button` — если внешнее устройство, которое вы используете для перевода ViPNet Coordinator IG в специальный режим работы, — кнопка;
  - `switch` — если внешнее устройство, которое вы используете для перевода ViPNet Coordinator IG в специальный режим работы, — двухпозиционный переключатель.

- Чтобы настроить пользовательскую обработку входящего сигнала от внешнего устройства:

`hostname# service piomonitor set In custom {button | switch}`, где:

- `button` — если внешнее устройство, которое вы используете, — кнопка;
- `switch` — если внешнее устройство, которое вы используете, — двухпозиционный переключатель.

- Чтобы настроить обработку сигнала от датчика вскрытия внешнего шкафа:

  `hostname# service piomonitor set In tamper`

4. В зависимости от решаемой задачи, настройте обработку сигналов для выходного контакта GPIO:

   - Чтобы настроить отправку на выходной контакт GPIO сигнала, соответствующего текущему режиму работы ViPNet Coordinator IG в кластере:

     `hostname# service piomonitor set Out cluster`

   - Чтобы настроить отправку на выходной контакт GPIO сигнала, соответствующего одному из событий, отслеживаемых ViPNet Coordinator IG:

     `hostname# service piomonitor set Out event {on | off} {custom | restricted | service | emergency | tamper}`

     где:

     - `custom` — сигнализация о любых необрабатываемых сигналах, поступающих на входящий контакт GPIO;
     - `restricted` — сигнализация о переходе в режим ограниченного функционирования;
     - `service` — сигнализация о переходе ViPNet Coordinator IG в режим регламентного обслуживания;
     - `emergency` — сигнализация о переходе ViPNet Coordinator IG в специальный режим;
     - `tamper` — сигнализация о срабатывании датчика вскрытия внешнего шкафа.

5. Чтобы включить автозапуск службы `piomonitord` при загрузке ViPNet Coordinator IG:

   `hostname# service piomonitor mode on`

6. По завершении настройки, запустите службу `piomonitord`:

   `hostname# service piomonitor start`

Чтобы проверить настройки службы `piomonitord`:

`hostname> service piomonitor show`

8

Настройка маршрутизации

Общие сведения о маршрутизации 166

Принципы маршрутизации 167

Просмотр таблиц маршрутизации 171

Настройка статической маршрутизации 173

Настройка маршрутов протоколов DHCP и PPP 177

Настройка OSPF 182

Настройка BGP 192

Настройка функции MultiWAN 207

Общие сведения о маршрутизации

ViPNet Coordinator IG поддерживает маршрутизацию IP-трафика в сетях со сложной структурой. Маршрутизация — процесс выбора маршрута следования IP-пакета, передаваемого в сети от одного узла другому. Он выбирается из подмножества маршрутов, имеющихся в таблице маршрутизации ViPNet Coordinator IG.

Маршруты могут быть:

- статические — добавляются в таблицу маршрутизации вручную;
- динамические — добавляются в таблицу маршрутизации с помощью алгоритмов на основе информации о топологии и состоянии сети, предоставляемой протоколами динамической маршрутизации.

Динамическая маршрутизация позволяет:

- автоматически формировать таблицу маршрутизации;
- автоматически выбирать по определенным критериям лучший маршрут из нескольких доступных, в том числе, при сбое других маршрутизаторов в сети;
- распределять нагрузку IP-трафика, передаваемого в сети.

ViPNet Coordinator IG может маршрутизировать IP-трафик с использованием следующих видов маршрутов:

- статических, в том числе на основе маршрутов с несколькими шлюзами;
- получаемых по протоколам DHCP и PPP;
- динамических, формируемых протоколами OSPF, BGP (поддерживается только ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1).

Принципы маршрутизации

В ViPNet Coordinator IG для хранения маршрутов используются:

- Таблица маршрутизации по умолчанию (Main) — содержит:
  - статические маршруты, заданные вручную (Static).
  - маршруты в подсети, к которым подключены сетевые интерфейсы (Connected);
  - маршруты, полученные по протоколам DHCP, PPP, OSPF и BGP.
- Пользовательские таблицы маршрутизации — содержат только статические маршруты, заданные вручную, и используются для создания политик маршрутизации (см. Настройка функции MultiWAN).

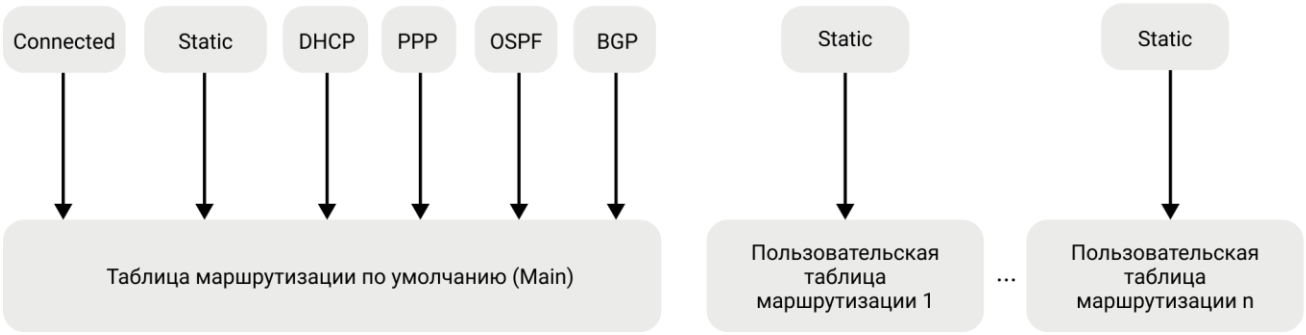


Рисунок 18. Формирование таблиц маршрутизации

В маршрутизации трафика участвуют не все маршруты, содержащиеся в таблице маршрутизации, а только лучшие маршруты в каждую сеть (подробнее см. «Формирование списка лучших маршрутов» ниже).

Характеристики маршрутов

- Источник получения маршрута: Connected, Static, PPP, DHCP, OSPF, BGP — определяет, каким образом был получен маршрут.
- Административная дистанция — определяет приоритет маршрута от каждого источника. Учитывается, когда в таблице маршрутизации есть несколько маршрутов в одну и ту же сеть:
  - Чем меньше административная дистанция, тем более приоритетным считается маршрут.
  - Административная дистанция задаётся для каждого статического маршрута.
  - Административная дистанция маршрутов протокола PPP отдельно не задаётся и равна дистанции маршрутов протокола DHCP.
  - Административная дистанция маршрутов протоколов OSPF и BGP задаётся не для конкретного маршрута, а для всех маршрутов протокола.
  - Административная дистанция статических маршрутов не может совпадать с дистанцией, заданной для маршрутов протоколов OSPF и BGP.

Примечание. Для каждого типа маршрутов задана административная дистанция по умолчанию:

- для статических маршрутов — 10;
- для маршрутов протоколов DHCP и PPP — 70;
- для маршрутов протокола OSPF — 110;
- для маршрутов протокола iBGP — 200;
- для маршрутов протокола eBGP — 20.

Для первых двух типов маршрутов вы можете изменять значение административной дистанции.

- Метрика — определяет приоритет маршрутов протоколов DHCP, PPP и OSPF. Чем меньше метрика, тем выше приоритет маршрута.
  - Для маршрутов протокола DHCP метрики указываются вручную, причём на каждом сетевом интерфейсе, на котором включен режим DHCP и настроен параметр получения маршрутов от DHCP-сервера. Таким образом, если на разные сетевые интерфейсы будут получены одинаковые маршруты в одну и ту же сеть, то будет выбран маршрут с наименьшей метрикой.
  - Для маршрутов протокола PPP метрика также может быть задана вручную в том случае, если ViPNet Coordinator IG подключён к нескольким сетям, одной из которых является сеть 3G/4G, а в другой установлен DHCP-сервер. Если метрики для маршрутов протоколов DHCP и PPP не были заданы, используется метрика по умолчанию.
  - Для маршрутов протокола OSPF метрика (стоимость) вычисляется автоматически.
- Вес — определяет долю IP-трафика, который будет проходить по маршруту через указанный шлюз. Используется в статических маршрутах и multipath-маршрутах протокола BGP. Вес задаётся для шлюза. Позволяет настроить балансировку передаваемого IP-трафика между несколькими шлюзами, когда часть IP-пакетов направляется на один шлюз, а часть — на другой.

Политики маршрутизации

Выбор, по какой таблице маршрутизировать трафик, определяется активной политикой маршрутизации. В качестве активной политики вы можете выбрать:

- Политику маршрутизации по умолчанию — выбрана автоматически после инициализации ViPNet Coordinator IG. Политика использует маршруты из таблицы маршрутизации по умолчанию (Main). Настройка политики недоступна.
- Одну из пользовательских политик маршрутизации — создаются пользователем. С помощью таких политик вы можете разделить IP-трафик по признакам и маршрутизировать его по разным таблицам маршрутизации (см. Настройка функции MultiWAN).

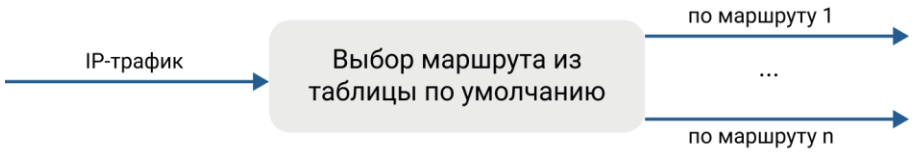


Рисунок 19. Маршрутизация при политике по умолчанию

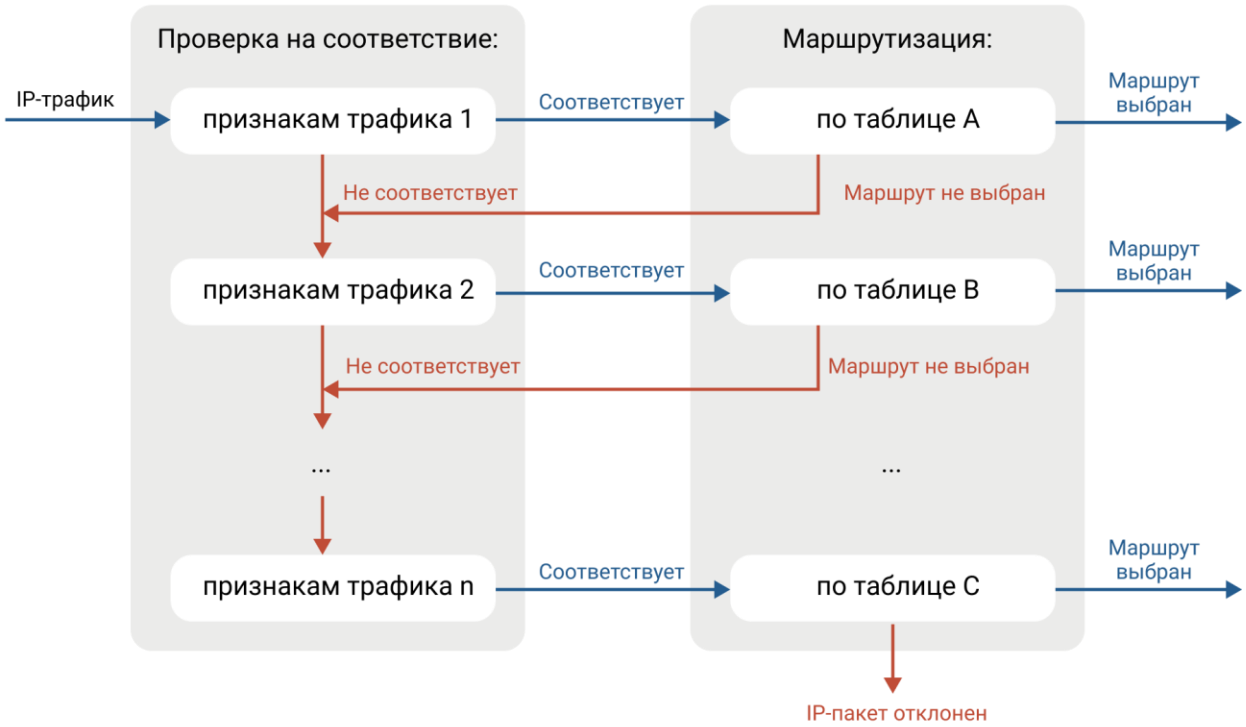


Рисунок 20. Маршрутизация при пользовательской политике

Пользовательская политика маршрутизации состоит из правил маршрутизации. Для каждого правила задаются:

- Приоритет — определяет в каком порядке правила будут применяться к трафику.
- Признаки трафика — задают условия, которым должен соответствовать трафик. Если признаки не указаны, правило распространяется на весь трафик.
- Таблица маршрутизации, по которой должен обрабатываться трафик, соответствующий заданным признакам трафика. Можно указать пользовательскую таблицу или таблицу по умолчанию.

Принципы маршрутизации при использовании пользовательской политики:

- IP-пакет последовательно проходит проверку правилами маршрутизации в соответствии с их приоритетом.
- Если IP-пакет соответствует всем признакам, заданным в правиле, он будет обработан по указанной таблице маршрутизации.
- Если IP-пакет не соответствует хотя бы одному из признаков правила, он передаётся на проверку следующему по приоритету правилу маршрутизации.

Формирование списка лучших маршрутов

В маршрутизации участвуют только лучшие статические и динамические маршруты в каждую сеть. Остальные маршруты в таблице игнорируются. Лучшие маршруты определяются в каждой таблице маршрутизации по следующим правилам:

- Из нескольких маршрутов в одну сеть лучшим признаётся маршрут с меньшей административной дистанцией, даже если маршруты получены из разных источников (Static, DHCP, PPP, OSPF, BGP). Например, имеется два маршрута в сеть 10.0.5.0 с маской 255.255.255.0. Для первого маршрута задана административная дистанция — 10, для второго — 30. В результате в маршрутизации будет участвовать первый маршрут. Если дистанции маршрутов, полученных из одного источника, равны, будут участвовать оба маршрута.
- Из нескольких маршрутов с разными префиксами (например, 10.0.0.0/8 и 10.0.0.0/16) лучшими признаются все маршруты.

Выбор маршрута из списка лучших

В процессе маршрутизации для каждого IP-пакета выбирается маршрут из списка лучших маршрутов. При наличии нескольких маршрутов в нужную сеть применяются правила:

- Из нескольких лучших маршрутов DHCP в одну сеть будет выбран маршрут с наименьшей метрикой. Если метрики равны, маршруты будут выбраны в соответствии со стратегией ECMP (equal-cost multi-path routing).
- Из нескольких лучших маршрутов в одну сеть с разным префиксом (маской подсети) будет выбран маршрут с наиболее длинным префиксом.
- Маршруты от одного источника в одну и ту же сеть объединяются в один маршрут с несколькими шлюзами (multi-hop route):
  - Статические маршруты — по признаку одинаковых административных дистанций маршрутов.
  - Маршруты DHCP и PPP — по признаку одинаковых метрик маршрутов.
  - Маршруты OSPF и BGP — маршрутизаторами OSPF и BGP.

  При просмотре такие маршруты отображаются в виде одного маршрута с несколькими шлюзами:

```
10.100.2.0/24 [30/23]     (weight 1) via 10.1.30.202, eth1
                          (weight 1) via 10.1.31.201, eth2
```



Внимание! Если хотя бы один из шлюзов объединённого маршрута multi-hop route выйдет из строя, работоспособность маршрута не гарантируется.

Просмотр таблиц маршрутизации

Чтобы просмотреть список всех маршрутов в таблице маршрутизации по умолчанию (Main):

```
hostname> inet show routing
```

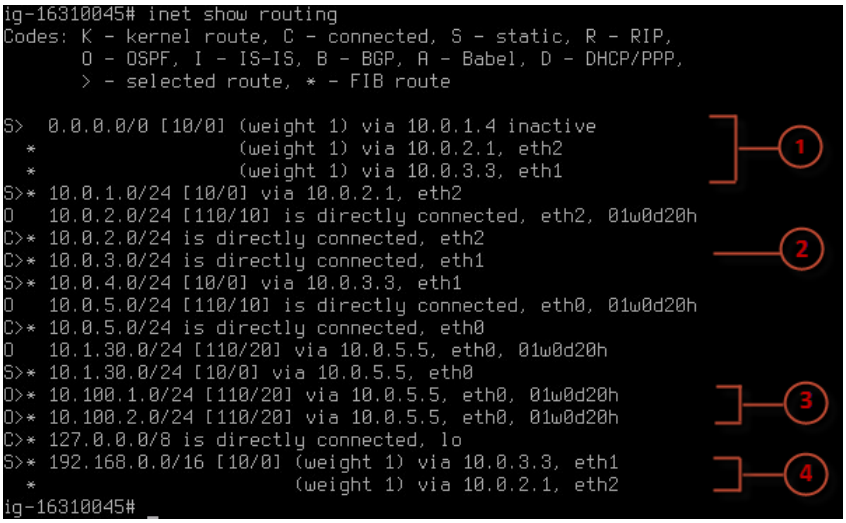


Рисунок 21. Просмотр таблицы маршрутизации

Цифрами на рисунке обозначены:

1 Статический маршрут по умолчанию. Выбран как лучший. Объединяет три маршрута, поэтому включает в себя три шлюза. Каждому шлюзу назначен вес, поэтому в процессе маршрутизации будет осуществляться балансировка нагрузки.

Примечание. Если маршрут по умолчанию не задан, отображается соответствующее предупреждение. В этом случае создайте статический маршрут по умолчанию.

---

2 Маршрут в подсеть 10.0.3.0 с маской 255.255.255.0, к которой подключен один из интерфейсов ViPNet Coordinator IG. Выбран как лучший.

3 Маршруты в подсети 10.100.1.0 и 10.100.2.0 с маской 255.255.255.0, полученные по протоколу OSPF. Выбраны как лучшие.

4 Статический маршрут в подсеть 192.168.0.0 с маской 255.255.0.0. Выбран как лучший. Объединяет два маршрута, поэтому включает в себя два шлюза. Каждому шлюзу назначен вес, поэтому в процессе маршрутизации будет осуществляться балансировка нагрузки.

Каждый раз перед списком маршрутов выводится список возможных атрибутов, которые могут присваиваться для маршрутов, и их расшифровка. В таблице ниже приведены пояснения по данным атрибутам.

Таблица 5. Атрибуты маршрутов

Атрибут	Расшифровка в командном интерпретаторе	Пояснение
C	connected	Маршрут в подсеть, к которой подключен один из интерфейсов ViPNet Coordinator IG
S	static	Статический маршрут
O	OSPF	Маршрут протокола OSPF
B	BGP	Маршрут протокола BGP
D	DHCP/PPP	Маршрут протокола DHCP или PPP-сервером
>	selected route	Лучший маршрут — отображается, если в таблице есть несколько маршрутов в одну и ту же сеть с разной административной дистанцией
*	FIB route	Маршрут, признанный лучшим и участвующий в маршрутизации

Примечание. В таблице маршрутизации могут присутствовать другие атрибуты, кроме описанных в таблице выше. Эти атрибуты зарезервированы для других протоколов маршрутизации и в текущей версии ViPNet Coordinator IG не используются.

Чтобы просмотреть определённые типы маршрутов из таблицы маршрутизации по умолчанию:

```
hostname> inet show routing {static table default | dhcp | ospf | bgp}
```

где:

- `static table default` — просмотр статических маршрутов;
- `dhcp` — просмотр маршрутов протоколов DHCP и PPP;
- `ospf` — просмотр маршрутов протокола OSPF;
- `bgp` — просмотр маршрутов протокола BGP.

Чтобы просмотреть содержимое пользовательской таблицы маршрутизации:

```
hostname> inet show routing static table {<номер таблицы> | name <имя таблицы>}
```

где:

- `<номер таблицы>` — номер пользовательской таблицы маршрутизации;
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации.

Настройка статической маршрутизации

Если ViPNet Coordinator IG функционирует в сети, конфигурация которой не меняется или в которой используется минимальное количество путей для доставки IP-пакетов, то вы можете настроить маршрутизацию на ViPNet Coordinator IG с помощью статических маршрутов. Статическая маршрутизации может потребоваться, когда нет возможности использовать маршрутизаторы, работающие по протоколам динамической маршрутизации, или в следующих случаях:

- Чтобы направлять часть IP-трафика по конкретным маршрутам (например, есть требование направлять IP-трафик по самому надежному каналу связи) или через конкретный шлюз.
- Нужен статический маршрут по умолчанию, если работа по протоколам динамической маршрутизации невозможна.
- Чтобы распределять передачу IP-трафика по нескольким маршрутам.

Создание статических маршрутов

Вы можете добавить статические маршруты в таблицу маршрутизации по умолчанию или создать пользовательские таблицы маршрутизации. Пользовательские таблицы используются для создания политик маршрутизации (см. Принципы маршрутизации).

- Чтобы добавить маршрут по умолчанию в таблицу маршрутизации по умолчанию:

  ```
  hostname# inet route add default next-hop <IP-адрес шлюза> [distance <1-255> [weight <1-255>]]
  ```

- Чтобы добавить статический маршрут в таблицу маршрутизации по умолчанию:

  ```
  hostname# inet route add <IP-адрес назначения> [netmask <маска>] next-hop <IP-адрес шлюза> [distance <1-255> [weight <1-255>]]
  ```



Совет. Если вам требуется добавить один статический маршрут с несколькими шлюзами, создайте несколько статических маршрутов в одну и ту же сеть с одинаковой административной дистанцией, указав в каждом по одному шлюзу. В результате эти маршруты будут просуммированы и объединены в один с несколькими шлюзами. Как правило, такие маршруты требуются для балансировки нагрузки, поэтому в маршрутах также должен быть задан вес шлюзам (см. ниже).

- Чтобы добавить маршрут в пользовательскую таблицу маршрутизации (см. Настройка функции MultiWAN):

  ```
  hostname# 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>]]
  ```

Если указанной таблицы маршрутизации не существует, она будет создана с заданными именем и номером.

Во всех командах вы можете задать необязательные параметры: `distance` — административную дистанцию маршрута и `weight` — вес шлюза.

Административная дистанция задаётся, чтобы назначить приоритет маршруту. Если вы не укажете значение административной дистанции, то оно будет задано автоматически: `distance=10`. Если вы укажете административную дистанцию, и её значение будет совпадать со значением административной дистанции, заданной протоколам динамической маршрутизации, появится сообщение, что маршрут не может быть добавлен. В этом случае создайте маршрут с другим значением административной дистанции.

Вес задается в маршруте для шлюза. Его требуется задавать в том случае, если создаётся несколько маршрутов в одну сеть с разными шлюзами, между которыми требуется производить балансировку нагрузки. Подробнее см. раздел Настройка балансировки IP-трафика.

Если маршрут, добавленный в таблицу маршрутизации по умолчанию, будет определён как лучший, то он будет участвовать в маршрутизации IP-трафика.

Для использования пользовательских таблиц маршрутизации создайте политику маршрутизации и активируйте её (см. Настройка функции MultiWAN).

Удаление статических маршрутов

Вы можете удалить маршрут по умолчанию или статический маршрут:

- Чтобы удалить маршрут по умолчанию из таблицы маршрутизации по умолчанию:

  ```
  hostname# inet route delete default next-hop <IP-адрес шлюза>
  ```

- Чтобы удалить статический маршрут из таблицы маршрутизации по умолчанию:

  ```
  hostname# inet route delete <IP-адрес назначения> [netmask <маска подсети>] next-hop
  <IP-адрес шлюза>
  ```

- Чтобы удалить маршрут из пользовательской таблицы маршрутизации:

  ```
  hostname# inet route delete {<IP-адрес назначения> [netmask <маска подсети>] | default}
  next-hop <IP-адрес шлюза> table <номер таблицы> [name <имя таблицы>]
  ```

Если при вводе команды вы не указали маску подсети или IP-адрес шлюза, и в процессе проверки будет установлено, что в таблице маршрутизации есть несколько маршрутов в указанную сеть, то на экран будет выведен список этих маршрутов. Для удаления всех выбранных маршрутов введите `y` и нажмите **Enter**. Аналогичная ситуация возникнет при удалении маршрута с несколькими шлюзами.

После удаления маршрута будет выбран новый лучший маршрут в ту же сеть.

Примечание. Если требуется удалить все статические маршруты, включая все маршруты по умолчанию, воспользуйтесь командой:

```
hostname# inet route clear [table {<номер таблицы> | name <имя таблицы>}]
```

Просмотр статических маршрутов

Чтобы просмотреть список всех статических маршрутов, содержащихся в таблице маршрутизации по умолчанию и в пользовательских таблицах маршрутизации:

```
hostname> inet show routing static
```

В списке для каждого маршрута указаны: IP-адрес назначения, маска сети, шлюз, административная дистанция маршрута и вес шлюза.

Настройка балансировки IP-трафика

Если вы хотите ускорить процесс отправки IP-пакетов в сеть назначения, вы можете создать несколько статических маршрутов в данную сеть через разные шлюзы и настроить балансировку IP-трафика между этими маршрутами. Это позволит в процессе разных TCP-соединений отправлять часть IP-пакетов по одному маршруту, часть — по другому, что повысит скорость передачи IP-пакетов в сеть назначения. Балансировка IP-трафика настраивается с помощью одного из параметров маршрутов — веса (`weight`). При этом все маршруты, которые будут участвовать в балансировке IP-трафика, должны иметь одинаковую административную дистанцию, то есть иметь одинаковый приоритет.

Примечание. При маршрутизации маршруты в одну сеть назначения и с одинаковой дистанцией объединяются в один маршрут с несколькими шлюзами (multi-hop route). При просмотре таблицы маршрутизации они отображаются как один маршрут с несколькими шлюзами (см. Принципы маршрутизации).

Для настройки балансировки IP-трафика:

1. Создайте нужное количество маршрутов с одинаковым адресом назначения и с разными шлюзами.
2. Задайте каждому маршруту одинаковую административную дистанцию.
3. Задайте в каждом маршруте вес шлюзу. IP-трафик будет распределяться между шлюзами в соответствии с соотношением их весов. Например:
   - если вы создаёте 2 маршрута и в каждом маршруте вес шлюза равен 1, то IP-трафик будет разделён между этими маршрутами поровну, то есть 50% IP-трафика будет передаваться по одному маршруту, 50% — по второму;
   - если вы создаёте 3 маршрута, и в первом маршруте вес шлюза равен 1, во втором — вес шлюза равен 2, в третьем — вес шлюза равен 3, то по второму маршруту будет

передаваться в два раза больше IP-трафика, чем по первому, по третьему — в три раза больше, чем по первому.

Пример команд для создания статических маршрутов с весом шлюзов равным 1:

```
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
```



Примечание. Если в процессе создания маршрута вы не укажете вес шлюза, то шлюзу автоматически будет назначен вес равный 1. Вы не можете задать вес равный 0.

Балансировка IP-трафика будет осуществляться только если созданные маршруты признаны лучшими (см. Принципы маршрутизации).

Настройка маршрутов протоколов DHCP и PPP

Если на каком-либо сетевом интерфейсе ViPNet Coordinator IG включен режим DHCP и настроено автоматическое получение маршрутов (см. Настройка сетевых интерфейсов Ethernet), то в процессе маршрутизации будут использоваться эти маршруты. В этом случае настройте дополнительные параметры:

1. Настройте административную дистанцию для протокола DHCP. Это позволит определить приоритет маршрутов DHCP-сервера среди всех маршрутов в таблице маршрутизации по умолчанию (статических маршрутов, маршрутов протокола OSPF, если такие есть).
2. Если режим DHCP включен на нескольких сетевых интерфейсах, настройте метрики протокола DHCP на каждом сетевом интерфейсе, на котором включен этот режим. Это позволит определить приоритет среди маршрутов DHCP-сервера в одну и ту же сеть, полученных с разных сетевых интерфейсов.

Если ViPNet Coordinator IG подключен к сети 3G/4G и получает информацию для маршрута по умолчанию от PPP-сервера провайдера (см. Подключение к мобильной сети 3G/4G), и при этом он также подключен к другой сети и получает в ней маршрутную информацию от DHCP-сервера, то в этом случае задайте метрику для PPP-протокола. Это позволит определить, какой маршрут по умолчанию (сформированный на основе шлюза по умолчанию от PPP-сервера или предоставленный DHCP-сервером) является приоритетным. Административная дистанция для этого протокола не задается и равна дистанции для протокола DHCP.

Настройка административной дистанции для маршрутов DHCP-протокола

Если на ViPNet Coordinator IG настроено взаимодействие с DHCP-сервером, от которого поступают маршруты, а также настроена статическая маршрутизация (см. Настройка статической маршрутизации) или динамическая маршрутизация (см. Настройка OSPF), то задайте административную дистанцию для маршрутов протокола DHCP. Административная дистанция определит приоритет данных маршрутов среди всех остальных, и в случае, если будет обнаружено несколько маршрутов в одну и ту же сеть из разных источников, будет выбран тот маршрут, у которого выше приоритет. Чем меньше значение административной дистанции, тем выше приоритет маршрута.

В настройках ViPNet Coordinator IG вы можете:

- Задать административную дистанцию для маршрутов, поступающих от DHCP-сервера:

```
hostname# inet dhcp client route-distance <1-255>
```

Эта дистанция будет определять приоритет всех маршрутов DHCP-сервера, независимо от того, на какой сетевой интерфейс они поступили.

- Задать административную дистанцию для маршрутов по умолчанию вместе с общей административной дистанцией для всех маршрутов DHCP-сервера:

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

  где `default-route <1-255>` — значение административной дистанции для маршрутов по умолчанию.

  Эта дистанция будет определять приоритет только маршрутов по умолчанию. Если дистанция не задана, то у маршрутов по умолчанию дистанция и приоритет будет таким же, как и у других маршрутов DHCP-сервера.

При необходимости перед или после настройки административной дистанции вы можете посмотреть, на каких сетевых интерфейсах включен режим DHCP и какая административная дистанция задана. Подробнее см. раздел Просмотр настроек DHCP в режиме клиента.

Настройка метрики для маршрутов DHCP-протокола

Если на ViPNet Coordinator IG режим DHCP включен на нескольких сетевых интерфейсах, то может сложиться ситуация, когда с этих интерфейсов поступят разные маршруты от DHCP-сервера в одну и ту же сеть. В этом случае требуется определить, какой маршрут является лучшим, чтобы использовать его при маршрутизации трафика. Параметром, позволяющим выбрать наилучший маршрут, выступает метрика маршрута. Её можно задать на каждом сетевом интерфейсе, на котором включен режим DHCP, чтобы определить приоритет маршрутов DHCP-сервера на разных сетевых интерфейсах. Чем меньше значение метрики, тем выше приоритет маршрута. Если на разных сетевых интерфейсах заданы одинаковые метрики, то поступившие маршруты в одну и ту же сеть будут объединены в один маршрут с несколькими шлюзами.

В ViPNet Coordinator IG вы можете задать или удалить метрику для маршрутов DHCP-сервера на конкретном сетевом интерфейсе (далее — специфичная метрика). Если специфичная метрика не задана, то вместо неё используется метрика по умолчанию.

- Чтобы добавить специфичную метрику на сетевом интерфейсе:

  `hostname# inet ifconfig <имя интерфейса> dhcp route-metric <1-255>`

Примечание. Задать специфичную метрику для протокола DHCP вы можете на сетевых интерфейсах следующих типов:

- Ethernet (см. Настройка сетевых интерфейсов Ethernet).
- VLAN.
- Wi-Fi (wlan) (см. Подключение к сети Wi-Fi).
- Агрегированный интерфейс.

Если режим DHCP включен только на одном сетевом интерфейсе, то настройка специфичной метрики не требуется, поскольку для группы маршрутов в рамках одного сетевого интерфейса она всегда будет одинаковой.

- Чтобы удалить метрику, заданную на сетевом интерфейсе:

```
hostname# inet ifconfig <имя интерфейса> dhcp route-metric none
```

После удаления метрики на этом интерфейсе будет использоваться метрика по умолчанию.

При необходимости перед или после настройки метрик вы можете посмотреть, на каких сетевых интерфейсах включен режим DHCP и какие метрики заданы. Подробнее см. раздел Просмотр настроек DHCP в режиме клиента.

Настройка метрики для маршрутов PPP-протокола

Если ViPNet Coordinator IG подключен к мобильной сети, (см. Подключение к мобильной сети 3G/4G) то при первом соединении с сервером мобильного оператора ViPNet Coordinator IG получает от него по протоколу PPP IP-адрес шлюза по умолчанию, на основе которого создается маршрут по умолчанию.

Примечание. Вы можете выключить получение IP-адреса шлюза по умолчанию от сервера мобильного оператора с помощью команды `hostname# inet usb-modem route off` (см. Подключение к мобильной сети 3G/4G).

Если кроме подключения к сети 3G/4G, ViPNet Coordinator IG также подключен к другим сетям, в которых информация об адресах и маршрутах распространяется DHCP-сервером, то он также будет получать маршруты по умолчанию по протоколу DHCP. Если требуется, чтобы маршрут по умолчанию PPP-протокола имел приоритет выше, чем маршруты по умолчанию DHCP-протокола, и использовался в процессе маршрутизации, требуется задать метрику для протокола PPP (далее — специфичную метрику). Причем она должна быть меньше метрики DHCP-протокола на каждом сетевом интерфейсе, на которых они заданы. Если специфичная метрика не будет задана, то вместо нее будет использоваться метрика по умолчанию (см. Изменение метрики по умолчанию для маршрутов протоколов DHCP и PPP). В этом случае маршруты по умолчанию PPP- и DHCP-протокола будут иметь одинаковый приоритет.

- Чтобы добавить специфичную метрику для протокола PPP:

```
hostname# inet usb-modem route-metric <1-255>
```

Примечание. Данную операцию вы можете выполнить только при следующих условиях:

- выключено использование модема;
- разрешено применение маршрута по умолчанию от PPP-сервера оператора.

- Чтобы удалить специфичную метрику для протокола PPP:

  ```
  hostname# inet usb-modem route-metric none
  ```

  После удаления метрики для протокола PPP будет использоваться метрика по умолчанию.

Изменение метрики по умолчанию для маршрутов протоколов DHCP и PPP

Если для маршрутов протоколов DHCP и PPP не задавались специфичные метрики, то для определения приоритета маршрутов будет использоваться метрика по умолчанию (первоначально — 70).

Чтобы изменить метрику:

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

Просмотр настроек DHCP в режиме клиента

Вы можете просмотреть следующие параметры DHCP в режиме клиента:

- административная дистанция, которая задана для маршрутов, поступающих от DHCP-сервера (см. Настройка административной дистанции для маршрутов DHCP-протокола);
- метрика по умолчанию (см. Настройка метрики для маршрутов DHCP-протокола);
- сетевые интерфейсы, на которых включен режим DHCP;
- специфичные метрики на сетевых интерфейсах, если такие заданы;
- разрешение на автоматическое получение IP-адресов, адресов DNS- и NTP-серверов.

Чтобы посмотреть указанные настройки:

```
hostname> inet show dhcp client
```

В результате выполнения команды указанные настройки будут отражены в следующем виде:

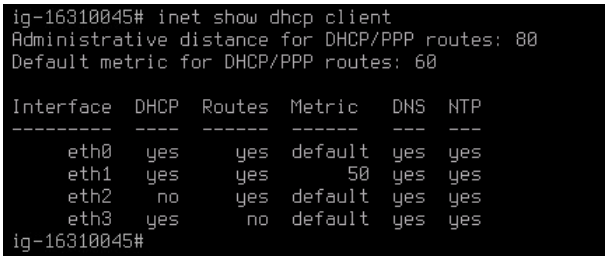


Рисунок 22. Просмотр настроек DHCP-режима

Просмотр маршрутов DHCP/PPP-протокола

Чтобы просмотреть список маршрутов, полученных от DHCP/PPP-сервера:

```
hostname> inet show routing dhcp
```

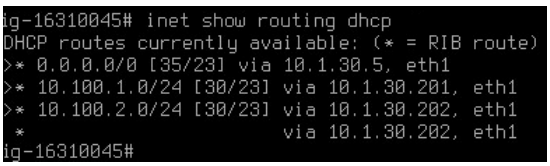


Рисунок 23. Просмотр маршрутов DHCP-сервера

В списке для каждого маршрута указаны: атрибут, IP-адрес назначения, маска сети, шлюз и имя сетевого интерфейса, на который поступил маршрут. Если маршрут определён как лучший маршрут в сеть, перед ним указан атрибут «*».

Настройка OSPF

Настройка динамической маршрутизации по протоколу OSPF имеет смысл в том случае, если в сети, в которой установлен ViPNet Coordinator IG, одновременно выполняются следующие условия:

- используются другие OSPF-маршрутизаторы, и они напрямую связаны с ViPNet Coordinator IG;
- используется протокол OSPF версии 2;
- поддерживается многоадресное вещание (multicast);
- по требованиям безопасности вашей организации разрешена передача IP-трафика по протоколу OSPF между сетевыми узлами.

В процессе настройки маршрутизации по протоколу OSPF вам потребуется:

- включить использование протокола OSPF;
- указать сети, к которым подключён ViPNet Coordinator IG и которые будут участвовать в маршрутизации по протоколу OSPF, и области маршрутизации;
- создать ряд сетевых фильтров.

Если ViPNet Coordinator IG непосредственно связан с другими координаторами, рекомендуется в конфигурационном файле `iplir.conf` в секциях `[id]`, соответствующих этим координаторам, указать в параметре `accessiplist` метрику `1`. В этом случае при наличии нескольких альтернативных маршрутов защищённый трафик всегда будет передаваться по кратчайшему маршруту — через соседний координатор.

При необходимости вы также можете настроить Настройка перераспределения маршрутов.

Общие сведения о протоколе OSPF

Протокол OSPF — внутренний шлюзовой протокол (Interior Gateway Protocol, IGP), используется для распространения данных маршрутизации внутри одной автономной системы.

Реализация протокола OSPF в ViPNet Coordinator IG имеет ограничения: из RFC 2328 не поддерживаются:

- изменение пропускной способности reference-bandwidth — cost, auto-cost;
- настройка метрик маршрутов;
- перераспределение (redistribute) маршрутов, кроме заданных статически и полученных по DHCP;
- настройка параметров взаимодействия соседних маршрутизаторов — HelloInterval и DeadInterval;
- другие типы областей (area type), кроме backbone и standard;
- настройка типа сети (network types), — задан тип Broadcast;

- фильтрация по политике импорта и экспорта маршрутов;
- виртуальные каналы (Virtual Links).

OSPF-маршрутизация работает следующим образом:

1. OSPF-маршрутизаторы устанавливают связь друг с другом посредством многоадресной (multicast) рассылки.
2. OSPF-маршрутизаторы начинают обмениваться сообщениями типа LSA (Link State Advertisements), в которых передают информацию о состоянии каналов связи с помощью однонаправленной (unicast) рассылки.
3. При получении LSA-сообщения информация из него заносится в базу данных (link state database). Если LSA-сообщение содержит новую информацию о канале связи по сравнению с той, которая содержится в базе данных, то оно передаётся маршрутизаторам-соседям.
4. На каждом маршрутизаторе по алгоритму Дейкстры (SPF algorithm) вычисляется множество кратчайших маршрутов ко всем сетям назначения и их стоимость. Таким образом, каждый OSPF-маршрутизатор имеет собственное представление о состоянии каналов связи и топологии сети, но при этом все маршрутизаторы используют одну базу данных состояний каналов связи для вычисления кратчайших маршрутов.

Межсетевая среда, в которой находятся OSPF-маршрутизаторы, представляется как совокупность областей маршрутизации, соединённых друг с другом через некоторую базовую область.

Выделяют следующие типы областей маршрутизации:

- Базовая или область 0 (backbone area) — с ней должны быть соединены все остальные области автономной системы.
- Стандартная (standard area) — граничит как с другими областями, так и с другими автономными системами.
- Стандартная тупиковая (stub area) — граничит только с другими областями.
- Полностью тупиковая (totally stubby area) — граничит только с одной областью.
- Не полностью тупиковая (not-so-stubby area) — стандартная тупиковая область, которая может взаимодействовать с другими автономными системами с помощью пограничных маршрутизаторов (ABR).

Каждый OSPF-маршрутизатор входит в определённую область маршрутизации и обменивается информацией только с маршрутизаторами, входящими в эту же область. При этом обмен идет не напрямую, а через посредника — маршрутизатор, выбранный главным в этой области. Информация между разными областями передаётся через маршрутизатор, который располагается на границе этих областей. Если автономная система взаимодействует с другой автономной системой, то информация передаётся через маршрутизатор, который располагается на границе систем. Такой подход позволяет уменьшить объём рассылаемых LSA-сообщений, тем самым уменьшить нагрузку на маршрутизаторы и повысить скорость построения таблиц маршрутизации.

Выделяют следующие типы маршрутизаторов:

- Внутренний (internal router, IR) — все его сетевые интерфейсы находятся в одной области.

- Назначенный (designated router, DR) — выбран главным среди всех внутренних маршрутизаторов в одной области.
- Резервный назначенный (backup designated router, BDR) — берёт на себя функции главного в случае, если главный маршрутизатор вышел из строя.
- Межобластной граничный (area border router, ABR) — соединяет несколько областей OSPF одной автономной системы.
- Граничный маршрутизатор автономной системы (autonomous system boundary router, ASBR) — граничит с другой автономной системой, работающей по другому протоколу динамической маршрутизации (IGRP, EIGRP, IS-IS, RIP, BGP, Static).

Примечание. Для проверки подлинности маршрутов, полученных с других устройств по протоколу OSPF, мы рекомендуем настроить аутентификацию на маршрутизаторах.

Протокол OSPF поддерживает два способа аутентификации:

- простая аутентификация на пароле (simple password authentication). Одинаковый пароль настраивается на интерфейсах, через которые передаётся информация по протоколу OSPF. Пароль передаётся в открытом виде.
- криптографическая аутентификация (cryptographic authentication). Общий секретный ключ и идентификатор ключа настраиваются на интерфейсах, через которые передаётся информация по протоколу OSPF. Ключ передаётся в зашифрованном виде (используется алгоритм хэширования md5).

Аутентификация настраивается для соседних маршрутизаторов. По умолчанию протокол OSPF не использует аутентификацию.

Настройка протокола OSPF

Для настройки протокола OSPF:

1 Включите использование протокола:

```
hostname# inet ospf mode on
```

2 Укажите сеть, в которой осуществляется обмен информацией по протоколу OSPF:

```
hostname# inet ospf network add <IP-адрес назначения> netmask <маска сети> area
<0-4294967295>
```

К данной сети должен быть подключен сетевой интерфейс ViPNet Coordinator IG.

С помощью параметра `area` задайте область маршрутизации, в которую входит ViPNet Coordinator IG (см. Общие сведения о протоколе OSPF).

Примечание. Вы можете указать не более 128 сетей, в которых осуществляется обмен информацией по протоколу OSPF.

---

3 Для защиты от получения ложной информации от других устройств по протоколу OSPF, настройте аутентификацию. По умолчанию обмен информацией по протоколу OSPF происходит без аутентификации.



Внимание! Настройки аутентификации на маршрутизаторах, которые обмениваются информацией, должны быть одинаковыми.

3.1 Включите аутентификацию в выбранной области маршрутизации:

- Аутентификация на простом пароле:

  ```
  hostname# inet ospf area <area> auth on pswd
  ```

- Криптографическая аутентификация:

  ```
  hostname# inet ospf area <area> auth on md5,
  ```

  где `<area>` — область маршрутизации.

3.2 Установите пароль (при аутентификации на пароле) или добавьте ключ (при криптографической аутентификации) на интерфейсе, за которым находится область маршрутизации:

- Установка пароля:

  ```
  hostname# inet ospf interface <интерфейс> password
  ```

- Добавление ключа:

  ```
  hostname# inet ospf interface <интерфейс> keys add <keyid>
  ```



Примечание. На каждом интерфейсе вы можете создать не более 255 ключей с уникальным `keyid` и только один пароль.

4 Создайте на ViPNet Coordinator IG следующие фильтры открытой сети:

- Фильтры, разрешающие входящий однонаправленный (unicast) и многоадресный (multicast) IP-трафик по протоколу OSPF от всех соседних OSPF-маршрутизаторов, с которыми взаимодействует ViPNet Coordinator IG:

  ```
  hostname# firewall local add 1 rule "Allow OSPF unicast" src <IP-адрес OSPF-маршрутизатора> dst @local service @OSPF pass
  ```

  ```
  hostname# firewall local add 2 rule "Allow OSPF multicast" src <IP-адрес OSPF-маршрутизатора> dst @multicast service @OSPF pass
  ```

  Фильтры должны быть созданы для каждого соседнего OSPF-маршрутизатора в области, в которой находится ViPNet Coordinator IG.



Примечание. В фильтрах вместо service @OSPF вы можете указать proto 89.

- Фильтр, разрешающий исходящий трафик ViPNet Coordinator IG по протоколу OSPF на любой IP-адрес назначения:

```
hostname# firewall local add 3 rule "Allow OSPF outcoming" src @local dst @any
service @OSPF pass
```

Подробнее о создании сетевых фильтров см. в разделе Создание сетевого фильтра.

5 Если между координаторами сети ViPNet установлены связи на уровне пользователей (в том числе между координатором и ViPNet xFirewall), разрешите трафик протокола OSPF в защищенной сети:

```
hostname# firewall vpn add 1 rule "Allow OSPF outcoming" src @local dst @any service
@OSPF pass
```

```
hostname# firewall vpn add 2 rule "Allow OSPF incoming" src @any dst @local service
@OSPF pass
```



Внимание! Если вы не настроите указанные фильтры, то ViPNet Coordinator IG не сможет работать по протоколу OSPF (см. Общие сведения о протоколе OSPF).

Впоследствии вы можете отказаться от использования протокола OSPF для маршрутизации:

```
hostname# inet ospf mode off
```

Если в подсети прекращено использование протокола OSPF, удалите ее:

```
hostname# inet ospf network delete <IP-адрес назначения> netmask <маска подсети> area
<0-4294967295>
```

Чтобы отключить аутентификацию для области маршрутизации, выполните:

```
hostname# inet ospf area <area> auth off
```

При необходимости удалите пароль или ключ для аутентификации:

- Удаление пароля:

  ```
  inet ospf interface <интерфейс> password remove
  ```

- Удаление одного ключа:

  ```
  inet ospf interface <интерфейс> keys remove <keyid>
  ```

- Удаление всех ключей, добавленных для интерфейса:

  ```
  inet ospf interface <интерфейс> keys remove all
  ```

Настройка перераспределения маршрутов

Протокол OSPF может перераспределять маршруты, заданные статически или полученные по протоколу DHCP. Это может понадобиться, если в подсетях разветвленной сети используются разные виды маршрутов.

Рассмотрим пример:

- Главный офис и филиал входят в одну автономную систему. Используют маршрутизацию по протоколу OSPF.

- Сеть партнера является другой автономной системой. Использует статическую маршрутизацию (Static). На маршрутизаторе настроены статические маршруты для сетей главного офиса и филиала.
- IG-1 расположен на границе автономных областей и является граничным маршрутизатором.
- На IG-1 настроены статические маршруты в сеть партнера.

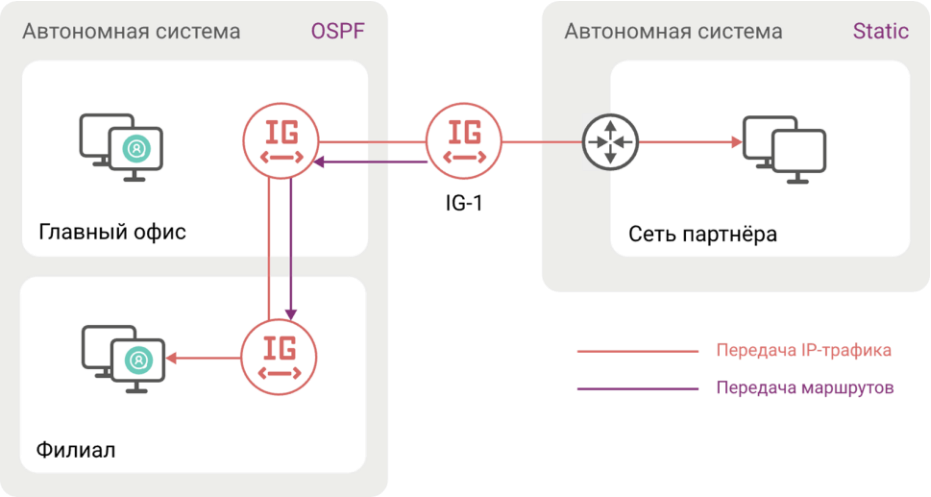


Рисунок 24. Перераспределение маршрутов

Чтобы узлы сети филиала могли обмениваться IP-трафиком с узлами сети партнера, вместо настройки статических маршрутов на оборудовании сетей главного офиса и филиала включите перераспределение статических маршрутов на IG-1:

```
hostname# inet ospf redistribute add static
```

IG-1 передаст статические маршруты в автономную систему офиса и узлы сети филиала смогут обмениваться IP-трафиком с узлами сети партнера.

Примечание.

- Статический маршрут по умолчанию не перераспределяется.
- Если в сети партнера используются динамические маршруты от DHCP-сервера, перераспределение включается командой `inet ospf redistribute add dhcp`. Также на граничном маршрутизаторе должно быть настроено получение маршрутов от DHCP-сервера сети партнера.

Просмотр настроек протокола OSPF

Вы можете просмотреть следующие параметры протокола OSPF:

- статус использования протокола OSPF: включен или выключен;
- список сетей, в которых ViPNet Coordinator IG выполняет маршрутизацию по протоколу OSPF (IP-адреса, маски и области);

- статус перераспределения маршрутов: доступно или недоступно.

Чтобы посмотреть указанные настройки, выполните команду:

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

```
hw> inet ospf show configuration
OSPF protocol autostart is on
OSPF protocol has been enabled
OSPF networks defined:
Destination      Netmask          OSPF Area      Authentication
-----------      -------          ---------      --------------
172.18.0.0       255.255.255.0    1              No

Interface:       OSPF priority    Password       Keyid
---------        -------------    --------       -----
eth0:            1                No             No
eth1:            1                No             No
eth2:            1                No             No
OSPF router id is 53.0.53.0
Redistribution of static routes is disabled.
Redistribution of DHCP routes is disabled.
```

Рисунок 25. Просмотр настроек протокола OSPF

Настройка протокола OSPF в сетях со множественным доступом

ViPNet Coordinator IG выполняет фильтрацию трафика между узлами сегмента локальной сети и внешними сетями. Вы можете сделать сегмент локальной сети частью сети со множественным доступом, входящей в область с маршрутизацией по протоколу OSPF. Когда в сети со множественным доступом становится больше двух маршрутизаторов, необходимо, для сокращения служебного трафика между маршрутизаторами, выбрать среди них назначенный маршрутизатор DR и резервный назначенный маршрутизатор BDR. Выбор роли DR или BDR происходит на основании параметров приоритета `priority` или идентификатора `router-id` маршрутизаторов:

- маршрутизатор с наивысшим значением приоритета становится DR;
- маршрутизатор с наивысшим значением приоритета из оставшихся становится BDR;
- маршрутизатор с приоритетом 0 не может стать DR или BDR;
- если у маршрутизаторов одинаковые приоритеты, то маршрутизатор с наивысшим идентификатором становится DR, а с наивысшим из оставшихся — BDR;
- появление в сети со множественным доступом нового маршрутизатора с более высоким приоритетом, чем у текущего DR, не влияет на роли текущих DR и BDR;
- процедура выбора нового DR или BDR запускается, если текущий DR или BDR выходят из строя.

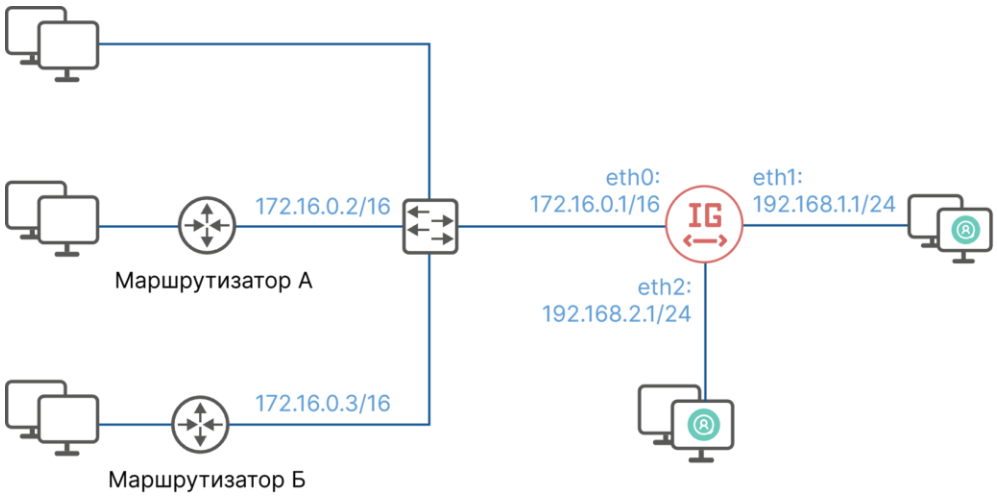


Рисунок 26. ViPNet Coordinator IG в сети со множественным доступом

Приоритет является параметром интерфейса ViPNet Coordinator IG. По умолчанию на всех интерфейсах ViPNet Coordinator IG установлен приоритет — 1. Вы можете изменить значение приоритета интерфейса ViPNet Coordinator IG на целое число из диапазона от 0 до 255:

```
hostname# inet ospf priority <значение приоритета> interface <имя интерфейса>
```

Идентификатор ViPNet Coordinator IG представляет собой число в формате адреса протокола IPv4, которое однозначно идентифицирует ViPNet Coordinator IG в пределах одной автономной области. По умолчанию идентификатор равен максимальному значению IP-адреса из назначенных на интерфейсах ViPNet Coordinator IG. Вы можете изменить значение идентификатора:

```
hostname# inet ospf router-id <адрес IPv4>
```

Внимание! Если в сети со множественным доступом у двух маршрутизаторов будут одинаковые идентификаторы `router-id`, то такие маршрутизаторы не смогут установить отношения соседства.

Чтобы посмотреть текущие значения параметров `priority` и `router-id` ViPNet Coordinator IG:

```
hostname# inet ospf show configuration
```

Просмотр состояния каналов связи между маршрутизаторами

Кроме настроек протокола OSPF вы также можете просмотреть информацию о состоянии каналов связи между всеми маршрутизаторами, работающими по протоколу OSPF. Она содержится в базе данных (link state database) (см. Общие сведения о протоколе OSPF) и синхронизируется на всех OSPF-маршрутизаторах. Именно на ее основе вычисляются динамические маршруты протокола OSPF. Для просмотра информации базы данных состояний каналов связи:

```
hostname> inet ospf show database
```

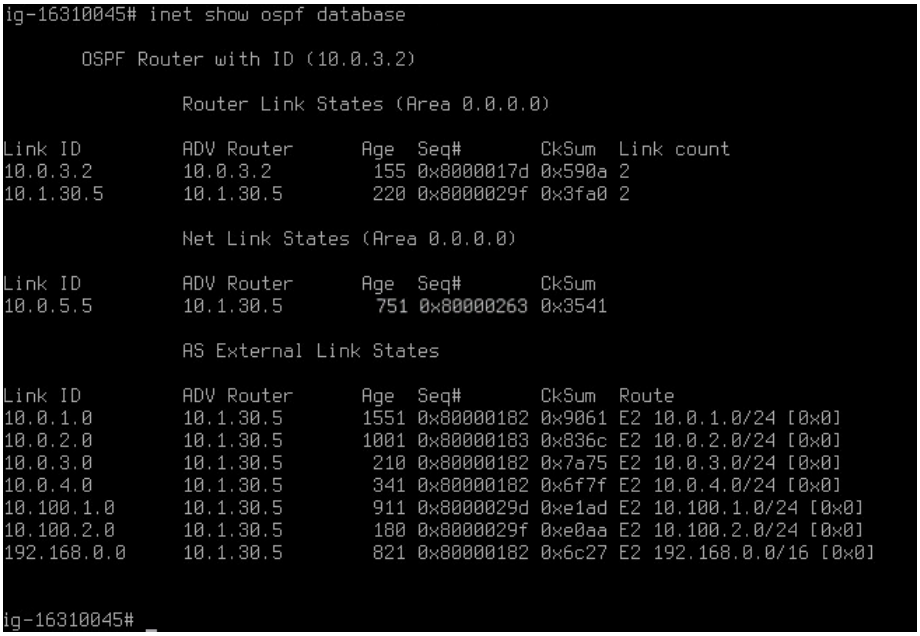


Рисунок 27. Просмотр базы данных состояний связи

Просмотр информации о соседних маршрутизаторах

В составлении маршрутов по протоколу OSPF участвуют все OSPF-маршрутизаторы, находящиеся в области маршрутизации ViPNet Coordinator IG. При необходимости вы можете просмотреть сведения об OSPF-маршрутизаторах, которые являются соседними для ViPNet Coordinator IG:

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

В результате выполнения команды отобразится информация обо всех соседних OSPF-маршрутизаторах:

По каждому маршрутизатору отображается следующая информация:

- уникальный идентификатор OSPF-маршрутизатора, под которым он известен другим маршрутизаторам при работе по протоколу OSPF;
- приоритет маршрутизатора;
- тип маршрутизатора (см. Общие сведения о протоколе OSPF) (в случае, приведенном на рисунке, маршрутизатор-сосед является назначенным, на что указывает значение `DR` в поле `State`);
- интервал простоя маршрутизатора, по истечении которого он будет считаться неактивным (выключенным);
- IP-адрес маршрутизатора, по которому он доступен для обмена информацией по протоколу OSPF;
- IP-адрес активного сетевого интерфейса маршрутизатора;

- другие параметры.

Просмотр маршрутов, сформированных по протоколу OSPF

Чтобы просмотреть список динамических маршрутов, сформированных по протоколу OSPF:

```
hostname> inet show routing ospf
```

В результате отобразятся списки маршрутов в трех разделах:

В каждом из разделов отображаются следующие маршруты:

- `OSPF network routing table` — маршруты, которые были сформированы по OSPF-протоколу в той области маршрутизации, к которой подключен ViPNet Coordinator IG. Если ViPNet Coordinator IG является межобластным маршрутизатором (ABR) (см. Общие сведения о протоколе OSPF), то в этом разделе будут присутствовать маршруты из всех областей, которые он объединяет.
- `OSPF router routing table` — маршруты до соседних OSPF-маршрутизаторов, которые находятся в области маршрутизации ViPNet Coordinator IG и выполняют перераспределение маршрутов (см. Настройка перераспределения маршрутов).
- `OSPF external routing table` — маршруты в другие автономные системы, поступившие при перераспределении от соседних OSPF-маршрутизаторов.

Настройка BGP

Примечание.

- Протокол BGP поддерживается только в исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1.
- BGP-маршруты не синхронизируются между узлами кластера.

Общие сведения о протоколе BGP

BGP (Border Gateway Protocol) — протокол динамической маршрутизации, предназначенный для обмена маршрутами между автономными системами (AS). AS — это совокупность IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с интернетом.

Маршрутизатор ViPNet Coordinator IG поддерживает протокол BGP для обмена маршрутами с соседними маршрутизаторами, а также для передачи параметров, позволяющих выбрать лучшие маршруты.

Таблица 6. Порядок выбора лучшего маршрута

№	Параметр маршрута	Критерий выбора	Анонсирование
1	Вес (`weight`)	Выбирается маршрут с наибольшим весом	Нет
2	Значение `local preference`	Выбирается маршрут с наибольшим значением	Только внутри AS
3	Локальный или внешний	Локальные маршруты имеют приоритет	Нет
4	Длина (`AS-path`)	Выбирается маршрут наименьшей длины	Да
5	Происхождение (`Origin`)	Маршруты, полученные через IGP имеют приоритет	Да
6	Значение `MED`	Выбирается маршрут с наименьшим `MED`	Только внутри AS и в соседнюю AS
7	eBGP или iBGP	Маршруты eBGP имеют приоритет	Нет
8	Значение `Router ID`	Выбирается маршрут с наименьшим `Router ID`	Нет
9	Адрес соседа	Выбирается маршрут с наименьшим адресом	Нет

Настройка соседей

1 Включите BGP:

```
hostname# inet bgp on
```

2 Задайте номер AS:

```
hostname# inet bgp router as <as-number>
```

где `<as-number>` — номер вашей AS (целое число из диапазона 1–4294967295).

3 Чтобы изменить идентификатор маршрутизатора `Router ID`, заданный автоматически:

```
hostname# inet bgp router id <a.b.c.d>
```

где: `<a.b.c.d>` — идентификатор маршрутизатора в формате A.B.C.D (может принимать значения от 0.0.0.1 до 255.255.255.255);

4 Настройте соседей:

4.1 Чтобы добавить соседа:

`hostname# inet bgp neighbor add <IP-address> remote-as <as-number> [port <portnumber>]`, где:

- `<IP-address>` — IP-адрес соседа;
- `<as-number>` — номер AS соседа (целое число из диапазона 1–4294967295);
- `<portnumber>` — номер TCP-порта соседа для установления BGP-сессии. По умолчанию используется порт 179.

4.2 Чтобы изменить TCP-порт соседа:

`hostname# inet bgp neighbor <IP-address> set port <portnumber>`, где:

- `<IP-address>` — IP-адрес выбранного соседа;
- `<portnumber>` — порт для установления BGP-сессии.

4.3 Чтобы настроить TTL одним из способов для соседа:

- Включите или выключите TTL-Security:

  `hostname# inet bgp neighbor <IP-address> set ttl-security {<hops>|off}`, где:

  - `<IP-address>` — IP-адрес соседа;
  - `<hops>` — максимальное число переходов до соседа;
  - `off` — отключить TTL-Security.

- Включите или выключите eBGP-multihop:

  `hostname# inet bgp neighbor <IP-address> set ebgp-multihop {<ttl>|off}`, где:

  - `<IP-address>` — IP-адрес соседа;
  - `<ttl>` — значение TTL для исходящих пакетов BGP-сессии;
  - `off` — отключить eBGP-multihop.

4.4 Чтобы настроить MD5-аутентификацию с соседом, включите её и задайте пароль. (такой же пароль установите на соседе):

```
hostname# inet bgp neighbor <IP-address> set password
```

где `<IP-address>` — IP-адрес соседа.

4.5 Чтобы удалить соседа:

```
hostname# inet bgp neighbor <IP-address> delete
```

где `<IP-address>` — IP-адрес соседа.

5 Чтобы вывести список соседей и параметров доступа к ним:

```
hostname# inet bgp show neighbors list
```

6 Чтобы вывести список всех BGP-сессий:

```
hostname# inet bgp show summary
```

7 Чтобы перезапустить BGP-сессии с выбранным соседом или всеми соседями:

`hostname# inet bgp clear {all | <IP-address>}`, где:

- `<IP-address>` — IP-адрес соседа, BGP-сессия с которым будет перезапущена;
- `all` — перезапустить BGP-сессии со всеми соседями.

8 Чтобы сбросить настройки BGP:

```
hostname# inet bgp router reset
```

9 Чтобы выключить BGP:

```
hostname# inet bgp off
```

Анонсирование подсетей и перераспределение маршрутов

Настроенный по умолчанию маршрутизатор ViPNet Coordinator IG не распространяет информацию об известных ему подсетях и маршрутах. При этом он может получать ее от соседей и пересылать дальше, не передавая информацию о собственных подсетях. Чтобы передавать ее, настройте:

- Прямое анонсирование подсетей из заданного списка.
- Перераспределение маршрутов, полученных от соседей. Вы можете использовать карты маршрутов (route maps) для фильтрации и модификации распространяемых маршрутов.

Для маршрута по умолчанию также можно использовать механизм анонсирования default-originate. При этом:

- анонсирование настраивается для выбранного соседа;
- маршрут по умолчанию не попадает в BGP-таблицу;
- не требуется наличие статического маршрута в таблице маршрутизации.

Чтобы настроить анонсирование подсетей и перераспределение маршрутов:

1 Добавьте анонсируемые подсети. Для каждой подсети, которую вы хотите анонсировать, выполните:

`hostname# inet bgp network add <subnet> netmask <netmask>`, где:

- `<subnet>` — адрес IPv4 unicast-подсети, число в виде 4 октетов в формате A.B.C.D;
- `<netmask>` — маска подсети, число в виде 4 октетов в формате W.X.Y.Z.

2 Чтобы удалить подсеть из списка анонсируемых:

`hostname# inet bgp network delete <subnet> netmask <netmask>`, где:

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

3 Чтобы включить перераспределение статических или подключенных маршрутов:

`hostname# inet bgp network redistribute {connected | static} on`, где:

- `connected` — перераспределять подключенные маршруты;
- `static` — перераспределять статические маршруты.

4 Чтобы назначить карту маршрутов для фильтрации или модификации распространяемых маршрутов:

`hostname# inet bgp network redistribute {connected | static} route-map name <name>`, где:

- `connected` — применять карту к подключенным маршрутам;
- `static` — применять карту к статическим маршрутам;
- `name` — имя карты маршрутов.



Примечание. Вы можете назначить карту маршрутов только маршрутам, для которых было включено перераспределение на шаге 4.

5 Включите анонсирование маршрута по умолчанию. Для каждого соседа, которому вы хотите анонсировать маршрут, выполните:

`hostname# inet bgp neighbour <IP-адрес> set default-originate on`

где `<IP-адрес>` — IP-адрес соседа;

6 Чтобы просмотреть настройки анонсирования подсетей и перераспределения маршрутов:

`hostname# inet bgp show network`

Настройка фильтров и префикс-листов маршрутов

По умолчанию ViPNet Coordinator IG принимает все маршруты от своих соседей и распространяет им свои маршруты, признанные лучшими. Для фильтрации входящих и исходящих маршрутов используются:

- Префикс-листы — фильтрация маршрутов осуществляется с учетом их назначения. Префикс-лист — это нумерованный список правил, которыми проверяется маршрут в порядке

увеличения их номеров (до первого совпадения). При соответствии маршрута правилу к нему применяется заданное действие и дальнейшая проверка маршрута прекращается. При создании правил в префикс-листах вы можете настроить проверку на точное совпадение с префиксом, либо проверку попадания в диапазон, определяемый длиной префикса.

- AS-path-фильтры — маршруты фильтруются с учетом порядка прохождения маршрута через автономные системы. AS-path-фильтр — это нумерованный список регулярных выражений, которыми проверяется параметр AS-path. Если AS-path в маршруте удовлетворяет условиям регулярного выражения из списка, то к маршруту применяется действие, заданное в фильтре.

Настройка префикс-листов

Чтобы создать и настроить префикс-лист:

1 Добавьте новый префикс-лист:

```
hostname# inet prefix-list add <name>
```

где `<name>` — имя префикс-листа.

2 Настройте правила для созданного префикс-листа:

2.1 Чтобы добавить правило в префикс-лист:

`hostname# inet prefix-list <name> [seq <num>] {permit | deny} {<subnet> [le <len>] [ge <len>] | any}`, где:

- `<name>` — имя префикс-листа;
- `<num>` — порядковый номер правила в префикс-листе;
- `permit` — разрешает маршрут при соответствии префикса подсети маршрута правилу;
- `deny` — блокирует маршрут при соответствии префикса подсети маршрута правилу;
- `<subnet>` — префикс unicast-подсети в формате CIDR;
  - `le` — задает условие «меньше или равно» при проверке префикса;
  - `ge` — задает условие «больше или равно» при проверке префикса;
  - `<len>` — длина префикса; целое число от 0 до 32;
  - `any` — любой префикс, эквивалент 0.0.0.0 le 32.

2.2 Чтобы удалить правило из префикс-листа:

`hostname# inet prefix-list <name> clear seq <num>`, где:

- `<name>` — имя префикс-листа;
- `<num>` — порядковый номер правила в префикс-листе.

3 Чтобы удалить префикс-лист:

```
hostname# inet prefix-list delete <name>
```

где `<name>` — имя префикс-листа.

4 Назначьте префикс-листы выбранным соседям:

4.1 Чтобы назначить префикс-лист выбранному соседу:

`hostname# inet bgp neighbor <ip-address> set prefix-list <name> {in | out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `<name>` — имя префикс-листа;
- `in` — префикс-лист будет применяться к входящим маршрутам;
- `out` — префикс-лист будет применяться к исходящим маршрутам.

4.2 Чтобы отключить использование префикс-листа для выбранного соседа:

`hostname# inet bgp neighbor <ip-address> remove prefix-list {in | out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `in` — отключить использование префикс-листа к входящим маршрутам;
- `out` — отключить использование префикс-листа к исходящим маршрутам.

Настройка AS-path-фильтров

Чтобы создать и настроить AS-path-фильтры:

1 Добавьте новый AS-path-фильтр:

`hostname# inet bgp as-path-filter add <name>`

где `<name>` — имя AS-path-фильтра.

2 Настройте для созданного AS-path-фильтра списки регулярных выражений:

2.1 Чтобы добавить регулярное выражение в AS-path-фильтр:

`hostname# inet bgp as-path-filter <name> [seq <num>] {permit | deny}`, где:

- `<name>` — имя AS-path-фильтра;
- `<num>` — порядковый номер регулярного выражения в фильтре;
- `permit` — разрешает маршрут при удовлетворении значения AS-path условиям регулярного выражения;
- `deny` — блокирует маршрут при удовлетворении значения AS-path условиям регулярного выражения.

2.2 Чтобы удалить регулярное выражение из AS-path-фильтра:

`hostname# inet bgp as-path-filter <name> clear seq <num>`, где:

- `<name>` — имя AS-path-фильтра;
- `<num>` — порядковый номер регулярного выражения в фильтре.

3 Чтобы удалить AS-path-фильтр:

`hostname# inet bgp as-path-filter delete <name>`

где `<name>` — имя AS-path-фильтра.

4 Назначьте AS-path-фильтры выбранным соседям:

4.1 Чтобы назначить AS-path-фильтр выбранному соседу:

`hostname# inet bgp neighbor <ip-address> set as-path-filter <name> {in | out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `<name>` — имя AS-path-фильтра;
- `in` — фильтр будет применяться к входящим маршрутам;
- `out` — фильтр будет применяться к исходящим маршрутам.

4.2 Чтобы отключить использование AS-path-фильтра для выбранного соседа:

`hostname# inet bgp neighbor <ip-address> remove as-path-filter {in | out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `in` — отключить использование фильтра к входящим маршрутам;
- `out` — отключить использование фильтра к исходящим маршрутам.

Просмотр информации о префикс-листах и AS-path-фильтрах

- Чтобы вывести список префикс-листов или содержимое выбранного префикс-листа:

  `hostname# inet prefix-list show [<name>]`

  где `<name>` — имя префикс-листа. Если параметр `<name>` не задан, то выведется список всех префикс-листов.

- Чтобы вывести список AS-path-фильтров или содержимое выбранного фильтра:

  `hostname# inet bgp show as-path-filter [<name>]`

  где `<name>` — имя AS-Path-фильтра. Если параметр `<name>` не задан, то выведется список всех AS-path-фильтров.

- Чтобы вывести назначенные на соседей префикс-листы, фильтры и карты маршрутов:

  `hostname# inet bgp show neighbors filters [<ip-address>]`

  где `<ip-address>` — IP-адрес соседа. Если параметр `<ip-address>` не задан, то будет выведен список всех соседей.

Настройка карт маршрутов

ViPNet Coordinator IG поддерживает карты маршрутов (route maps) — наборы правил, позволяющие фильтровать принимаемые или передаваемые маршруты, а также изменять их атрибуты. Вы можете создавать карты маршрутов и использовать их при настройке перераспределения маршрутов.

С помощью карт маршрутов вы можете настраивать следующие параметры передаваемых маршрутов:

- значение `next-hop`
- вес маршрута (`weight`);
- метрика маршрута (`MED`);
- значение `local preference`;

- AS-path;
- комьюнити (community).

Принципы обработки карт маршрутов

Карты маршрутов состоят из блоков (последовательности правил), которые определяют порядок обработки маршрута и проверяются до первого совпадения. Маршруты, которые не прошли карту маршрутов, отбрасываются. При описании блоков используются следующие условия проверки:

- Действие — определяет действие с маршрутом, соответствующим условиям блока: разрешить (permit) либо блокировать (deny).
- Match — условие совпадения маршрутов. Если в блоке задано нескольких условий, то действие будет применено к маршруту при совпадении хотя бы одного из условий.
- Set — изменение параметров маршрута. В разрешающем блоке определяет, как изменятся параметры маршрута при его соответствии блоку.
- On-match — указывает о необходимости перехода в другой блок карты маршрутов.

Настройка комьюнити-листов

Параметр community — это 32-битное целое число, используемое для маркировки маршрутной информации. Маршруту можно сопоставить несколько community, на основе которых можно задавать правила фильтрации, балансировки трафика и распределения нагрузки.

Комьюнити-лист (community list) представляют собой последовательности разрешенных или запрещенных community. Если в одной последовательности содержится несколько community, то действие блока будет применено к маршрутам, содержащим все community. ViPNet Coordinator IG поддерживает следующие зарезервированные (well-known) комьюнити:

Таблица 7. Перечень поддерживаемых well-known комьюнити

Название	hex-обозначение	Обозначение ASN:NN	Источник
internet	0x00000000	0:0	Cisco
graceful-shutdown	0xFFFF0000	65535:0	RFC-8326
accept-own	0xFFFF0001	65535:1	RFC-7611
llgr-stale	0xFFFF0006	65535:6	draft-uttaro-idr-bgp-persistence-04
no-llgr	0xFFFF0007	65535:7	draft-uttaro-idr-bgp-persistence-04
blackhole	0xFFFF029A	65535:666	RFC-7999
no-export	0xFFFFFF01	65535:65281	RFC-1997
no-advertise	0xFFFFFF02	65535:65282	RFC-1997
local-AS	0xFFFFFF03	65535:65283	RFC-1997
no-peer	0xFFFFFF04	65535:65284	RFC-3765

Чтобы создать и настроить комьюнити-лист:

1 Создайте комьюнити-лист:

```
hostname# inet bgp community-list add <name>
```

где <name> — имя комьюнити-листа.

2 Добавьте в него правила:

```
hostname# inet bgp community-list <name> [seq <num>] {permit|deny} <community-line>,
```

где:

- <name> — имя комьюнити-листа;
- <num> — указывает точный номер правила в списке;
- permit — устанавливает проверку совпадения комьюнити;
- deny — устанавливает проверку отсутствия комьюнити;
- <community-line> — строка текста от 3 до 256 символов, которая может содержать:
  - одно или более комьюнити в формате AA:NN, разделенные пробелом (строка не может начинаться с пробела);
  - одно или более well-known комьюнити: internet, no-export, no-advertise, local-AS.

3 Чтобы впоследствии удалить добавленное правило:

```
hostname# inet bgp community-list <name> clear seq <num>
```

, где:

- <name> — имя комьюнити-листа;
- <num> — номер правила.

4 Чтобы вывести перечень комьюнити-листов:

```
hostname# inet bgp show community-list
```

5 Чтобы вывести правила, входящие в комьюнити-лист:

```
hostname# inet bgp show community-list <name>
```

где <name> — имя комьюнити-листа.

6 Чтобы удалить комьюнити-лист:

```
hostname# inet bgp community-list delete <name>
```

где <name> — имя комьюнити-листа.

Настройка карт маршрутов

Чтобы создать и настроить карту маршрутов:

1 Создайте карту маршрутов:

```
hostname# inet route-map add <name>
```

где <name> — имя карты.

2 Добавьте в карту маршрутов блоки правил и настройте их:

2.1 Чтобы добавить блок правил:

`hostname# inet route-map <name> {permit|deny} <seq>`, где:

- `<name>` — имя карты маршрутов;
- `permit` — устанавливает для блока действие «разрешить»;
- `deny` — устанавливает для блока действие «запретить»;
- `<seq>` — номер блока в карте маршрутов.

2.2 Чтобы удалить блок:

`hostname# inet route-map <name> clear <seq>`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов.

2.3 Чтобы добавить в блок проверку совпадения с выбранным префикс-листом:

`hostname# inet route-map <name> <seq> match prefix-list <prefix-list-name>`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<prefix-list-name>` — имя префикс-листа.

2.4 Чтобы добавить в блок проверку совпадения с выбранным AS-path-фильтром:

`hostname# inet route-map <name> <seq> match as-path <as-path-filter-name>`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<as-path-filter-name>` — имя AS-path-фильтра.

2.5 Чтобы добавить в блок проверку совпадения с выбранным комьюнити-листом:

`hostname# inet route-map <name> <seq> match community <community-list-name> [exact-match]`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<community-list-name>` — имя комьюнити-листа;
- `exact-match` — задает необходимость точного совпадения комьюнити в маршруте и комьюнити-листе.

2.6 Чтобы задать изменение параметра `next-hop` в маршруте:

`hostname# inet route-map <name> <seq> set next-hop <IP-address>`, где:

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<IP-address>` — новое значение параметра `next-hop`.

2.7 Чтобы задать изменение веса маршрута:

`hostname# inet route-map <name> <seq> set weight <weight>`, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <weight> — вес маршрута.

2.8 Чтобы задать изменение параметра MED:

hostname# inet route-map <name> <seq> set metric <metric>, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <metric> — новое значение параметра MED.

2.9 Чтобы задать изменение параметра local-preference:

hostname# inet route-map <name> <seq> set local-preference <local-preference>, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <local-preference> — новое значение параметра local-preference.

2.10 Чтобы задать для выбранного блока дополнение параметра AS-path:

hostname# inet route-map <name> <seq> set as-path-prepend <string>, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <string> — строка, содержащая номера AS, разделенные пробелом.

2.11 Чтобы задать для выбранного блока обновление списка комьюнити в маршруте:

hostname# inet route-map <name> <seq> set community {[additive] <community-line>| none}, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;
- <community-line> — строка, содержащая номера комьюнити, разделенные пробелом. Может содержать одно или несколько комьюнити в формате AA:NN, а также well-known комьюнити: internet, no-export, no-advertise, local-AS;
- [additive] — задает необходимость дополнения существующего списка комьюнити строкой <community-line>;
- none — удалить все комьюнити из маршрута.

2.12 Чтобы задать директиву перехода к другому блоку при совпадении условий:

hostname# inet route-map <name> <seq> on-match {next|goto <number>}, где:

- <name> — имя карты маршрутов;
- <seq> — номер блока в карте маршрутов;

- `<number>` — номер блока в карте маршрутов, к которому нужно перейти при совпадении условий;
- `<next>` — перейти к следующему блоку при совпадении условий.

3 Чтобы удалить существующую карту маршрутов:

```
hostname# inet route-map delete <name>
```

где `<name>` — имя карты маршрутов.

4 Чтобы вывести список карт маршрутов, или данные об использовании выбранной карты маршрутов:

`hostname# inet route-map show [<name> [usage]]`, где:

- `<name>` — имя карты маршрутов;
- `usage` — вывести перечень объектов, в которых используется карта маршрутов.

5 Чтобы назначить карту маршрутов для обработки маршрутной информации, распространяемой между ViPNet Coordinator IG и выбранным соседом:

`hostname# inet bgp neighbor <ip-address> set route-map <name> {in|out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `<name>` — имя карты маршрутов;
- `in` — применять карту маршрутов к входящим маршрутам;
- `out` — применять карту маршрутов к исходящим маршрутам.

6 Чтобы отключить использование карты маршрутов для обработки маршрутной информации, распространяемой между ViPNet Coordinator IG и выбранным соседом:

`hostname# inet bgp neighbor <ip-address> remove route-map {in|out}`, где:

- `<ip-address>` — IP-адрес соседа;
- `in` — отключить использование карты маршрутов для входящих маршрутов;
- `out` — отключить использование карты маршрутов для исходящих маршрутов.

Настройка распространения маршрутов внутри AS

Взаимодействие соседей внутри одной AS (iBGP-соседей) отличается от взаимодействия соседей из разных AS (eBGP-соседей) и имеет особенности:

- Параметры маршрутов (в том числе `next-hop`) не изменяются.
- Если маршрут получен от iBGP-соседа, то он может передаваться только eBGP-соседу.

В некоторых топологиях автономных систем эти особенности препятствуют распространению маршрутов внутри одной AS, а также прохождению трафика через транзитную AS. Чтобы

обеспечить распространение маршрутов внутри автономной системы, используются следующие механизмы:

- Возможность модифицировать параметр `next-hop` для iBGP-соседей без использования карт маршрутов. Это обеспечивается включением опции `next-hop-self` и назначается для iBGP-соседей в соответствии с настройками соседства.
- Изменение логики работы ViPNet Coordinator IG с iBGP-соседями таким образом, что им передаются маршруты, полученные от других iBGP-соседей. Такой механизм называется отражение маршрутов (Route Reflection), при этом ViPNet Coordinator IG выступает в роли RR-сервера, распространяющего маршруты, а его iBGP-соседи — в роли RR-клиентов. Сервер и его клиенты образуют RR-кластер, обладающий уникальным идентификатором (Cluster ID). AS, в которой используется отражение маршрутов, может состоять из нескольких RR-кластеров, обладающих различными правилами обработки маршрутной информации.

Настройка next-hop-self

Чтобы включить возможность модификации параметра `next-hop` для iBGP-соседа:

```
hostname# inet bgp neighbor <IP-адрес> set next-hop-self on
```

где `<IP-адрес>` — IP-адрес iBGP-соседа.

Настройка Route Reflection

Чтобы настроить отражение маршрутов:

1. Задайте идентификатор RR-кластера `Cluster ID`:

   `hostname# inet bgp route-reflector cluster-id {<a.b.c.d>|auto}`, где:

   - `<a.b.c.d>` — идентификатор RR-кластера, число в виде 4 октетов в формате A.B.C.D;
   - `auto` — идентификатор RR-кластера будет назначен автоматически.

2. Добавьте iBGP-соседей в список клиентов Route Reflection:

   - Чтобы добавить IP-адрес iBGP-соседа в список клиентов:

     ```
     hostname# inet bgp route-reflector client add <IP-address>
     ```

     где `<IP-address>` — IP-адрес iBGP-соседа.

   - Чтобы удалить адрес iBGP-соседа из списка клиентов:

     ```
     hostname# inet bgp route-reflector client delete <IP-address>
     ```

     где `<IP-address>` — IP-адрес iBGP-соседа.

3. Чтобы включить применение карты маршрутов к отраженным маршрутам:

   ```
   hostname# inet bgp route-reflector outbound-policy on
   ```

4. Чтобы вывести текущие настройки Route Reflection:

   ```
   hostname# inet bgp show route-reflector
   ```

Поддержка ECMP и UCMP

Протокол BGP может обеспечить балансировку трафика между шлюзами доступа с помощью механизмов ECMP (Equal Cost Multi Path) и UCMP (Unequal Cost Multi Path). Балансировка осуществляется при наличии нескольких эквивалентных (multipath) маршрутов в таблице маршрутизации.

По умолчанию при наличии нескольких шлюзов доступа для трафика выбирается лучший маршрут в соответствии с правилами выбора маршрута (см. Общие сведения о протоколе BGP). При этом весь трафик идет через шлюз, соответствующий лучшему маршруту и балансировка трафика не выполняется.

Поддержка ECMP позволяет встраивать несколько эквивалентных маршрутов, полученных по протоколу BGP, в таблицу маршрутизации. При этом каждому из соседей будет передан только один маршрут. Маршруты считаются эквивалентными при совпадении их параметров.



Внимание! Длина `AS-path` меняется при распространении маршрутной информации, поэтому, если используется проверка AS-path, вес маршрутов из одной AS может отличаться. Чтобы использовать ECMP, отключите проверку `AS-path` при встраивании маршрутов.

Чтобы отключить проверку `AS-path` при встраивании эквивалентных маршрутов:

```
hostname# inet bgp router bestpath as-path-relax on
```

Поддержка UCMP предполагает добавление в маршрут расширенного комьюнити `Link bandwidth`. При получении нескольких эквивалентных маршрутов они добавляются в таблицу маршрутизации с весом, пропорциональным значению `Link bandwidth`.



Внимание! Использование UCMP возможно, только если маршрутизаторы соседей поддерживают обработку комьюнити `Link bandwidth`.

Чтобы настроить режим обработки эквивалентных маршрутов с расширенным комьюнити `Link bandwith`:

`hostname# inet bgp router bestpath bandwith {ignore|skip|min|default}`, где:

- `ignore` — значение `Link bandwidth` будет проигнорировано, все эквивалентные маршруты будут встроены с весом 1;
- `skip` — маршруты из набора эквивалентных маршрутов без `Link bandwidth` будут проигнорированы и не будут встроены в таблицу маршрутизации;
- `min` — маршруты из набора эквивалентных маршрутов без `Link bandwidth` будут встроены в таблицу маршрутизации с весом 1;
- `default` — возвращает поведения по умолчанию: если хотя бы один маршрут из набора эквивалентных маршрутов будет без `Link bandwidth`, маршруты будут встроены в таблицу маршрутизации с весом 1.

Чтобы просмотреть настройки выбора лучшего маршрута:

```
hostname# inet bgp show bestpath
```

Настройка функции MultiWAN

Если для доступа ViPNet Coordinator IG в интернет используется несколько шлюзов (провайдеров), то вы можете настроить политики маршрутизации для различных случаев. Например, для распределения нагрузки между каналами связи или для резервирования каналов при использовании нескольких интернет-провайдеров на случай отказа одного из них.

Для этих целей в ViPNet Coordinator IG реализована технология MultiWAN, позволяющая настроить поведение ViPNet Coordinator IG в случае недоступности одного из интернет-шлюзов. Эта технология представлена в ViPNet Coordinator IG следующими функциями:

- Пользовательские таблицы маршрутизации (см. Создание статических маршрутов). С их помощью вы можете задать различные маршруты для различных ситуаций. Например, основную таблицу маршрутизации и дополнительную таблицу маршрутизации на случай, если шлюз основного провайдера станет недоступен и потребуется перенаправить трафик через шлюз альтернативного провайдера.
- Политики маршрутизации (см. Настройка политик маршрутизации). С их помощью вы можете задать условия, при которых трафик будет перенаправляться по заданным таблицам маршрутизации.
- Проверка состояния шлюзов (Dead Gateway Detection, DGD) (см. Настройка проверки состояния шлюзов (DGD)). С помощью этой функции вы можете задавать выполнение политики маршрутизации в зависимости от доступности или недоступности шлюза.

Ограничения при настройке MultiWAN

- Добавляйте маршруты только в пользовательские таблицы маршрутизации, а таблицу по умолчанию изменяйте лишь в крайнем случае.
- Не добавляйте в пользовательские таблицы маршрутизации маршруты, противоречащие маршрутам в таблице по умолчанию.
- Не используйте маршруты, получаемые по протоколам DHCP и OSPF (чтобы отключить автоматическое получение маршрутов по DHCP: `hostname# inet ifconfig <интерфейс> dhcp route off`). Такие маршруты записываются в таблицу по умолчанию и будут задействованы с высшим приоритетом. Поэтому канал с динамической маршрутизацией всегда будет основным.
- Перед активацией политики маршрутизации убедитесь, что она настроена корректно и не нарушит связь ViPNet Coordinator IG с узлом, с которого вы настраиваете ViPNet Coordinator IG.
- Не используйте в качестве интернет-шлюза узел ViPNet, иначе при проверке состояния шлюза (DGD) он может ошибочно определиться как нерабочий.
- После добавления проверки шлюза по протоколу TCP и портам 80 и 443 необходимо создать разрешающий сетевой фильтр: источник — `@local`, назначение — IP-адрес шлюза, порты назначения — 80 и 443.

Основные сценарии использования функции MultiWAN см. документе «Сценарии работы», в разделе «Использование функции MultiWAN для резервирования каналов связи».

Настройка политик маршрутизации

Примечание. Принципы использования политик маршрутизации см. в разделе Принципы маршрутизации.

Для применения пользовательской политики маршрутизации необходимо добавить в неё правила маршрутизации и выбрать её в качестве активной.

Каждое правило состоит из условий, которые применяются к трафику (признаки трафика), и действия, которое выполняется, если трафик соответствует условиям.

Чтобы создать правило маршрутизации или добавить условия применения к уже существующему правилу:

```
hostname# inet policy rule add <имя политики> <приоритет> match {address {from | to} <IP-адрес/маска> | {inbound-interface | outbound-interface} <интерфейс> | dscp <значение метки DSCP>}
```

- В параметре `<имя политики>` задайте имя создаваемой политики маршрутизации или укажите имя существующей политики.
- В параметре `<приоритет>` задайте приоритет правила маршрутизации в диапазоне 1024–2048. Чем меньше значение, тем выше приоритет. Если правило с указанным приоритетом уже существует, условие применения правила будет добавлено в это правило.
- После ключевого слова `match` задайте условия применения правила маршрутизации (признаки трафика):
  - `address from <IP-адрес/маска>` — IP-пакеты получены от указанной подсети;
  - `address to <IP-адрес/маска>` — IP-пакеты отправлены в указанную подсеть;
  - `inbound-interface` — IP-пакеты поступили на указанный интерфейс;
  - `outbound-interface` — IP-пакеты отправлены с указанного интерфейса;
  - `dscp <значение метки DSCP>` — IP-пакеты с меткой DSCP (Differentiated Services Code Point).

После создания правила маршрутизации с условиями применения, необходимо задать действие для этого правила (см. ниже).

Чтобы задать действие для существующего правила или создать правило маршрутизации, применяемое для всего IP-трафика:

```
hostname# inet policy rule add <имя политики> <приоритет> {table {<номер таблицы> | name <имя таблицы> | default} | block}
```

- В параметре `<имя политики>` укажите имя существующей политики маршрутизации или задайте имя создаваемой политики.

- В параметре `<приоритет>` укажите приоритет существующего правила маршрутизации, чтобы задать его действие, или задайте приоритет для создания нового правила маршрутизации, которое будет применяться ко всему IP-трафику. Приоритет задаётся в диапазоне 1024–2048.
- Задайте действие правила:
  - Чтобы обрабатывать IP-пакет по пользовательской таблице маршрутизации, укажите:

    `table {<номер таблицы> | name <имя таблицы>}`
  - Чтобы обрабатывать IP-пакет по таблице маршрутизации по умолчанию, укажите:

    `table default`
  - Чтобы заблокировать IP-пакет, укажите:

    `block`



Внимание! Чтобы не нарушить прохождение IP-трафика между локальными сетями (сетевыми интерфейсами ViPNet Coordinator IG), в каждую пользовательскую политику маршрутизации добавьте правило для всего трафика (без признаков) с таблицей маршрутизации по умолчанию. Только эта таблица содержит маршруты в локальную сеть (`connected`). При этом мы рекомендуем присвоить такому правилу наивысший приоритет в политике и очистить таблицу по умолчанию от статических и динамических маршрутов.

Чтобы активировать пользовательскую политику маршрутизации:

```
hostname# inet policy active <имя политики>
```

Чтобы активировать политику маршрутизации по умолчанию:

```
hostname# inet policy active default
```



Примечание. Чтобы узнать, какая политика маршрутизации действует в настоящий момент времени:

```
hostname# inet show policy rule active
```

Примеры

- Чтобы добавить в политику `policy1` правило высшего приоритета, которое будет передавать IP-пакеты от подсети 192.168.1.0/30 на обработку по таблице маршрутизации `table1`:

  ```
  hostname# inet policy rule add policy1 1024 match address from 192.168.1.0/30
  hostname# inet policy rule add policy1 1024 table name table1
  ```
- Чтобы добавить в политику `policy2` правило с приоритетом 1025, которое будет передавать все IP-пакеты на обработку по таблице маршрутизации по умолчанию (Main):

  ```
  hostname# inet policy rule add policy2 1025 table default
  ```
- Чтобы добавить в политику `policy2` правило с приоритетом 1026, которое будет блокировать IP-пакеты, поступающие на сетевой интерфейс `eth1`:

  ```
  hostname# inet policy rule add policy2 1026 match inbound-interface eth1
  hostname# inet policy rule add policy2 1026 block
  ```
- Чтобы добавить в правило с приоритетом 1024 дополнительное условие применения — обработку IP-пакетов с меткой DSCP со значением `0x80`:

```
hostname# inet policy rule add policy1 1024 match dscp 0x80
```

Настройка проверки состояния шлюзов (DGD)

1 Запустите службу DGD:

```
hostname# inet dgd mode on
```

2 Для каждого шлюза настройте проверку его состояния с помощью отправки запросов на тестовый IP-адрес или IP-адрес шлюза:

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

- В параметре `<имя шлюза>` задайте произвольное имя шлюза, которое будет использоваться при настройке DGD.
- Укажите IP-адрес шлюза в параметре `<адрес шлюза>` или имя сетевого интерфейса ViPNet Coordinator IG в параметре `<интерфейс>` — если интерфейс, через который доступен шлюз, получает IP-адрес по DHCP/PPP.
- В параметре `<тестовый адрес>` укажите IP-адрес сетевого узла, по которому будет проверяться доступность шлюза. Если значение не задано, в качестве тестового IP-адреса будет использоваться IP-адрес шлюза. Несколько шлюзов могут иметь один и тот же тестовый IP-адрес.



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

- `check` — включить проверку состояния шлюза.
- `no-check` — выключить 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.

3 Если вы настроили 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
```

4 Добавьте правило проверки состояния шлюза, при выполнении которого будет действовать определённая политика маршрутизации:

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

- В параметре `<имя правила>` задайте уникальное имя правила проверки состояния шлюза.
- В параметре `<имя шлюза>` укажите имя шлюза, заданное на шаге 2.
- Выберите условие применения правила:

- `up` — правило будет применяться, если шлюз доступен.
- `down` — правило будет применяться, если шлюз недоступен.

Созданное правило не будет использоваться, пока не задано действие правила (см. шаг 5).

Вы можете добавить несколько условий в одно правило (например, чтобы правило выполнялось, когда один шлюз доступен, а другой не доступен). Для этого выполните повторно данную команду с указанием того же имени правила, но другого имени шлюза.

5 Задайте действие правила, созданного на предыдущем шаге:

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

- В параметре `<имя правила>` укажите имя правила проверки состояния шлюза.
- В параметре `<приоритет>` задайте приоритет правила: от 1 до 255. Чем меньше значение, тем выше приоритет правила.
- Выберите действие, которое будет выполняться при соблюдении всех условий правила, заданных на предыдущем шаге:
  - `log command <текст сообщения>` — записать событие с текстом `<текст сообщения>` в системный журнал.
  - `route command policy active <имя политики>` — активировать политику маршрутизации с именем `<имя политики>`.
  - `route command policy active default` — активировать политику маршрутизации по умолчанию.



Примечание. События переключения политики маршрутизации, а также изменение доступности шлюзов записываются в системный журнал. Примеры записей см. в приложении События системного журнала и журнала аудита.

6 Чтобы настроить общие параметры для проверки доступности шлюзов:

```
hostname# inet dgd configuration {default | interval-time <интервал> | response-time
<время> | retries-count <число проверок> | syslog-level <уровень важности>}
```

- `interval-time <интервал>` — задать время в секундах, через которое производится проверка соединения с тестовым IP-адресом шлюза. Возможные значения: 1–120.
- `response-time <время>` — задать время в секундах, в течение которого ожидается ответ от тестового IP-адреса шлюза. Возможные значения: 1–120.
- `retries-count <число проверок>` — задать число проверок IP-адреса шлюза, при достижении которого шлюз считается нерабочим. Возможные значения: 1–10.
- `syslog-level <уровень важности>` — изменить уровень важности событий, записываемых в системный журнал. Возможные значения: 0–4.
- `default` — сброс параметров на значения по умолчанию:
  - `interval-time` — 3 секунды;
  - `response-time` — 3 секунды;
  - `retries-count` — 3 проверки;

- `syslog-level` — 3-й уровень (информационные сообщения).

7 Чтобы просмотреть параметры проверки доступности шлюзов и состояние шлюзов:

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

Полный список команд по настройке проверки состоянию шлюзов см. в документе «Справочник команд и конфигурационных файлов».



9

Настройка системных параметров

Настройка даты и времени 214

Переключение режимов работы межсетевого экрана 215

Просмотр активных сессий пользователей 216

Установка допустимого времени неактивности сессии пользователя 217

Настройка расписания перезагрузки 218

Просмотр лицензии 219

Просмотр серийного номера 220

Использование резервного раздела 221

Сброс к заводским настройкам 222

Настройка даты и времени

Внимание!



- Если дата или время отличаются на узлах сети ViPNet, защищённые соединения между ними могут блокироваться. Рекомендуем настраивать синхронизацию системного времени по протоколу NTP.
- Если вы измените время более чем на сутки, ViPNet Coordinator IG будет блокировать весь сетевой трафик. Чтобы возобновить обработку трафика, перезагрузите ViPNet Coordinator IG.

Чтобы настроить дату и время вручную:

1 Посмотрите текущие дату и время:

```
hostname# machine show date
```

2 Чтобы изменить часовой пояс:

```
hostname# machine set timezone {<Континент/Пояс> | <UTC>}
```

Название континента и часового пояса должны начинаться с прописной буквы. Например, чтобы установить часовой пояс Москвы:

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

Чтобы просмотреть список всех часовых поясов, введите команду без параметра.

3 Чтобы изменить дату и время:

```
hostname# machine set date <YYYY-MM-DD> <hh:mm:ss>,
```

где `YYYY` — год, `MM` — месяц, `DD` — день, `hh` — часы, `mm` — минуты, `ss` — секунды.

Например:

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

При работе в кластере настраивайте системную дату, время и часовой пояс только на активном узле кластера. Параметры времени и часового пояса на пассивном узле кластера синхронизируются с активным узлом и недоступны для изменения.

Переключение режимов работы межсетевого экрана

Если ViPNet Coordinator IG инициализирован как межсетевой экран типа «Д», он может работать в следующих режимах:

- Штатный. Работают все функции ViPNet Coordinator IG. Недоступно: обновление справочников и ключей, обновление ПО, управление копиями конфигураций VPN, импорт настроек.
- Регламентного обслуживания. Предназначен для обновления справочников и ключей, обновления ПО, управления копиями конфигураций VPN, импорта настроек, а также регламентного обслуживания защищаемых узлов.
- Специальный. Предназначен для чрезвычайных ситуаций в работе системы. Межсетевой экран по умолчанию настроен пропускать любой сетевой трафик. Обновление справочников и ключей, обновление ПО, управление копиями конфигураций VPN, импорт настроек недоступны.

Каждому из режимов соответствует свой набор сетевых фильтров. Все ваши действия с пользовательскими сетевыми фильтрами (создание, изменение, удаление) применяются только для текущего режима работы межсетевого экрана. Предустановленные сетевые фильтры для каждого из режимов работы приведены в приложении.

Текущий режим работы вы можете узнать по команде:

```
hostname> machine mode show
```



Внимание! Не переключайте режим работы ViPNet Coordinator IG одновременно разными способами. Иначе, это может нарушить работоспособность ViPNet Coordinator IG. Способы переключения режимов работы см. в документе «Подготовка к работе», в разделе «Режимы работы».

Чтобы переключить режим работы ViPNet Coordinator IG:

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

где:

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

Просмотр активных сессий пользователей

Чтобы просмотреть активные сессии пользователей, выполните команду:

```
hostname# who
Interface  Role     User                                    Idle
-------------------------------------------------------------------
CLI        Auditor  user (you)                          00:00:00
CLI        Admin    center/admin                        00:00:08
WebUI      Admin    Petrov.Petr                         00:00:20
WebUI      Admin    Konstantin.Vasiliev                 00:01:48
```

Значение в поле `Idle` показывает время неактивности пользователя в сессии. Когда это значение превышает допустимое время неактивности сессии, сессия автоматически закрывается.

Установка допустимого времени неактивности сессии пользователя

Допустимое время неактивности сессии пользователя определяет период, по истечении которого сессия будет завершена, если пользователь не выполнял управляющих запросов. Этот параметр одинаков для сессий всех пользователей и синхронизируется между узлами кластера. Значение по умолчанию — 600 секунд.

Для просмотра допустимого времени неактивности сессии выполните:

```
hostname# machine session-inactivity-timeout show
```

Для изменения допустимого времени неактивности сессии выполните:

```
hostname# machine session-inactivity-timeout set <время>,
```

где `<время>` — время неактивности в интервале 60–54000 секунд.

Настройка расписания перезагрузки

1. Включите автоматическую перезагрузку по расписанию:

   ```
   hostname# machine reboot-schedule on
   ```

   По умолчанию перезагрузка по расписанию выключена.

2. Выполните одну из команд:

   - Если необходимо настроить перезагрузку в определенный день недели:

     ```
     hostname# machine reboot-schedule time <время> day <день>
     ```

     Вы можете указать только один день недели (`sunday`, `monday`, `tuesday`, `wednesday`, `thursday`, `friday` или `saturday`).

   - Если необходимо настроить ежедневную перезагрузку:

     ```
     hostname# machine reboot-schedule time <время>
     ```

   Время указывается в формате `hh:mm`, где `hh` — часы (24-часовой формат), `mm` — минуты.

Чтобы просмотреть текущие настройки автоматической перезагрузки:

```
hostname> machine reboot-schedule show
```

Чтобы перезагрузить ViPNet Coordinator IG вручную:

```
hostname> machine reboot
```

Настройка перезагрузки в кластере

Расписание перезагрузки (дата и время) не синхронизируется между узлами кластера.

Настройку автоматической перезагрузки выполняйте в следующем порядке:

1. Настройте расписание перезагрузки на активном узле кластера.
2. Дождитесь, когда данные на активном и пассивном узле синхронизируются (по умолчанию — 60 секунд).
3. Подключитесь к пассивному узлу и проверьте настройки автоматической перезагрузки. Автоматическая перезагрузка должна быть включена.

   Если настройки не синхронизировались, проверьте их чуть позже.
4. Настройте время и дату перезагрузки на пассивном узле. Чтобы не допустить одновременной перезагрузки обоих узлов кластера, устанавливайте время перезагрузки на узлах с разницей не менее 30 минут.

Просмотр лицензии

Лицензии определяют функциональные характеристики ViPNet Coordinator IG. Чтобы просмотреть сведения об установленных лицензиях:

```
hostname> license

License object              Version          Status           Expiration date

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

IPF                         5.9              active           2024-05-13

VPN                         5.9              active           2024-05-13

Failover                    5.9              active           2024-05-13

Modbus Gateway              5.9              active           2024-05-13

Coordinator IG100           5.99             active           2024-05-13
```

По команде выводятся сведения:

- `License object` — тип объекта лицензирования:
  - `<Исполнение ViPNet Coordinator IG>` — основной объект.
  - `VPN` — VPN.
  - `Failover` — система защиты от сбоев.
  - `IPF` — фильтрация промышленных протоколов (Modbus и МЭК 60870-5-104) на прикладном уровне.
  - `Modbus Gateway` — шлюз Modbus.
- `Version` — максимальная версия ПО ViPNet Coordinator IG, поддерживаемая лицензией.
- `Status` — состояние объекта лицензирования:
  - `active` — действует.
  - `expired` — не действует.
- `Expiration date` — время окончания действия объекта лицензирования в формате `YYYY-MM-DD`.

Просмотр серийного номера

Серийный номер ViPNet Coordinator IG отображается при выполнении команды:

```
hostname> version
```

Также вы можете получить серийный номер по SNMP (см. OID .1.3.6.1.4.1.10812.1.10.1 в VIPNET-MIB).

Серийный номер будет отсутствовать, если вы выполнили обновление ПО ViPNet Coordinator IG с версии 5.1.0 или ниже. В этом случае вы можете записать серийный номер в память ViPNet Coordinator IG с помощью команды:

```
hostname> serial <серийный номер>
```

В качестве параметра `<серийный номер>` введите серийный номер, указанный на этикетке вашего ViPNet Coordinator IG.

Вы также можете записать серийный номер через веб-интерфейс (см. документ «Настройка с помощью веб-интерфейса», раздел «Просмотр серийного номера»).

Использование резервного раздела

Критически важные файлы ПО ViPNet Coordinator IG автоматически копируются в резервный раздел (`/mnt/reserv`) незагрузочного диска в следующих случаях:

- Успешная проверка целостности файлов при установке ПО, обновлении ПО или загрузке ViPNet Coordinator IG.
- Успешное выполнение команды `machine self-test`.
- Обновление справочников и ключей.
- Изменение пароля локальной учётной записи (`user` или `admin`).

Резервные копии файлов используются при восстановлении, если обнаружено нарушение целостности файлов ПО (см. Контроль целостности файлов ПО).

В кластере резервные копии файлов синхронизируются между узлами.

Сброс к заводским настройкам

Примечание. Сброс к заводским настройкам возможен только в исполнении ViPNet Coordinator IG1000 Q1. Для других исполнений доступна возможность восстановления ПО.

Выполните сброс к заводским настройкам, если вы не можете пройти аутентификацию в ViPNet Coordinator IG, например по причине:

- истёк срок действия ключей или лицензии в момент, когда не было связи с ViPNet Prime;
- некорректно обновлены справочники и ключи;
- утрачен пароль администратора;
- программный сбой, неправильная настройка ПО или аппаратной платформы;
- замена батарейки на аппаратной платформе.

Внимание! При сбросе к заводским настройкам будут удалены ключи. После этого потребуется инициализация ViPNet Coordinator IG с помощью дистрибутива ключей (см. документ «Подготовка к работе», раздел «Инициализация»).

Чтобы выполнить сброс к заводским настройкам:

1. Включите ViPNet Coordinator IG.
2. В окне загрузки:
   - при подключении с помощью монитора и клавиатуры выберите **Factory reset** и нажмите **Enter**;
   - при подключении через консольный порт выберите **Factory reset/Serial console** и нажмите **Enter**.

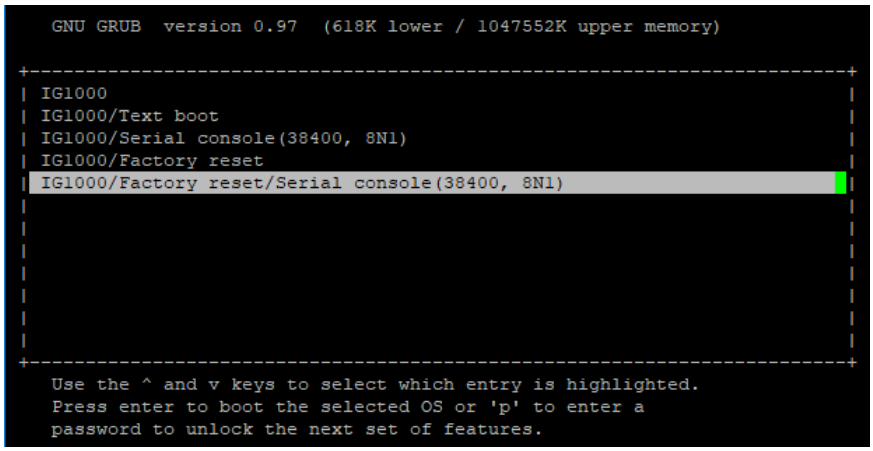


Рисунок 28. Сброс к заводским настройкам

3. В строке `Are you sure you want to execute this command and delete key? [Delete/No]` введите `Delete` и нажмите **Enter**.

Примечание. В течение 30 секунд вы можете отменить сброс к заводским настройкам. Для этого нажмите **Ctrl+C**.

4 Нажмите **Enter** для перезагрузки ViPNet Coordinator IG.

После сброса к заводским настройкам выполните инициализацию ViPNet Coordinator IG (см. «Подготовка к работе», раздел «Инициализация»). Если у вас есть резервная копия индивидуальной конфигурации (файл `*.ecf`), вы можете использовать её для восстановления настроек в ходе инициализации или после.

10

Настройка параметров безопасности

Управление локальными учётными записями 225

Обновление справочников и ключей 230

Просмотр сведений о ключе защиты обновлений и ключах обмена 231

Обновление ключей по истечении срока их действия 234

Настройка оповещения об истечении срока действия ключей 235

Перевыпуск ключей локального SSH-сервера 236

Настройка подключения с помощью веб-интерфейса 237

Смена типа межсетевого экрана с сохранением сетевых фильтров 240

Контроль целостности файлов ПО 241

Управление локальными учётными записями

Блокирование и разблокирование учётных записей

Вы можете заблокировать локальную учётную запись пользователя ViPNet Coordinator IG, удалив его пароль и сертификат (если используется способ аутентификации по сертификату).

Примечание.

- Локальная учётная запись `user` блокируется автоматически после инициализации ViPNet Coordinator IG.
- При использовании кластера из ViPNet Coordinator IG ознакомьтесь с разделом Особенности управления учетными записями в кластере.

Если настроена аутентификация по паролю

Вы можете заблокировать и разблокировать только учётную запись аудитора `user`:

- Чтобы заблокировать учётную запись `user`, удалите пароль:

  ```
  hostname# user reset passwd
  ```

- Чтобы разблокировать учётную запись `user`, задайте для неё новый пароль:

  ```
  hostname# user passwd
  ```

Чтобы заблокировать возможность доступа администратора под локальной учётной записью `admin` (например, в случае компрометации):

1. Войдите под централизованной учётной записью (учётная запись в ViPNet Prime), которая имеет роль администратора в ViPNet Coordinator IG.
2. Измените пароль локальной учётной записи `admin`.

Если настроена аутентификация по сертификату

Сертификат пользователя используется для аутентификации при подключении к ViPNet Coordinator IG с помощью консоли. При подключении через веб-интерфейс (HTTP/HTTPS) сертификат используется только для аутентификации пользователя с централизованной учётной записью.

При подключении по SSH и HTTP/HTTPS для аутентификации пользователя с локальной учётной записью используется пароль вместо сертификата. Поэтому для блокировки локальной учётной записи `user` необходимо удалить не только сертификат пользователя, но и пароль. Если удалить только сертификат, у пользователя останется возможность доступа по SSH и HTTP/HTTPS, и

наоборот. Для локальной учётной записи `admin` удалить пароль нельзя, можно только изменить его.

Чтобы заблокировать учётную запись `user`:

1. Удалите пароль:

   ```
   hostname# user reset passwd
   ```

2. Удалите сертификат:

   ```
   hostname# user certificate delete
   ```

Чтобы разблокировать учётную запись `user`:

1. Задайте для неё новый пароль:

   ```
   hostname# user passwd
   ```

2. Издайте новый сертификат.

Чтобы заблокировать возможность доступа администратора под локальной учётной записью `admin` (например, в случае компрометации):

1. Войдите под централизованной учётной записью с ролью администратора в ViPNet Coordinator IG.
2. Измените пароль администратора.
3. Удалите сертификат администратора:

   ```
   hostname# admin certificate delete
   ```

Чтобы восстановить возможность доступа администратора под локальной учётной записью `admin`:

1. Сообщите ему новый пароль учётной записи `admin`.
2. Издайте новый сертификат.

Изменение паролей

Для локальной учётной записи `admin` пароль задаётся при инициализации ViPNet Coordinator IG. Чтобы изменить его:

```
hostname# admin passwd
```

Локальная учётная запись `user` заблокирована после инициализации ViPNet Coordinator IG. Чтобы разблокировать её, см. Блокирование и разблокирование учётных записей. После этого аудитор сможет войти под учётной записью `user` и изменить пароль самостоятельно:

```
hostname> user passwd
```

Примечание. Если вы используете кластер из ViPNet Coordinator IG, ознакомьтесь с разделом Особенности управления учетными записями в кластере.

Издание сертификатов

Примечание. Если вы используете кластер из ViPNet Coordinator IG, ознакомьтесь с разделом Особенности управления учетными записями в кластере.

Сертификаты используются для аутентификации пользователей ViPNet Coordinator IG, если в ViPNet Prime отключена аутентификация по паролю. Подробнее см. в документе «Подготовка к работе» в разделе «Способы аутентификации».

На ViPNet Coordinator IG вы можете издать сертификат для пользователей с локальной учётной записью `user` или `admin`.

Издание сертификата пользователя необходимо:

- Для замены текущего сертификата:
  - до истечения срока действия текущего сертификата пользователя;
  - в случае компрометации ключа, связанного с сертификатом пользователя.

  Новый сертификат вы можете записать на USB-токен пользователя, где хранится текущий сертификат. При этом текущий сертификат удаляется.
- Перед отключением аутентификации по паролю в ViPNet Prime.

Внимание! Если для пользователя ViPNet Coordinator IG не будет издан сертификат до отключения аутентификации по паролю в ViPNet Prime, то после этого он не сможет пройти аутентификацию локально. В таком случае вы можете войти под централизованной учётной записью и издать сертификат для пользователя с локальной учётной записью.

Чтобы издать сертификат пользователя:

1. Войдите в ViPNet Coordinator IG под локальной учётной записью `admin` или централизованной учётной записью с ролью администратора.
2. Издайте сертификат с помощью одной из команд:
   - для пользователя с учётной записью `admin`:

     ```
     hostname# admin certificate create
     ```
   - для пользователя с учётной записью `user`:

     ```
     hostname# user certificate create
     ```
3. Если вы вошли под одной учётной записью и издаёте сертификат для пользователя с другой учётной записью, отключите свой USB-токен и подключите токен пользователя, для которого нужно издать сертификат, и нажмите **Enter**.
4. Подтвердите очистку памяти USB-токена — в строке `Upon executing the command, you will lost all current token data. Continue? [Yes/No]:` введите `y` и нажмите **Enter**.
5. Введите PIN-код администратора USB-токена (см. документацию на USB-токен):

```
Enter admin-token pincode: ********
```



Внимание! Если вы введёте некорректный PIN-код администратора USB-токена несколько раз подряд, он будет заблокирован (максимальное количество попыток ввода см. в документации на USB-токен). После этого вы больше не сможете записать сертификат на этот USB-токен.

6 Введите и подтвердите новый PIN-код пользователя USB-токена (этот PIN-код будет использоваться для доступа к сертификату при аутентификации на ViPNet Coordinator IG):

```
Enter new user-token pincode: ********
Confirm new user-token pincode: ********
Certificate has been successfully created.
```

Особенности управления учетными записями в кластере

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

Сертификаты пользователей — индивидуальны для каждого узла кластера и не передаются между узлами кластера. Действия по изданию или удалению сертификата необходимо выполнять на обоих узлах кластера. При этом для записи каждого сертификата пользователя необходимо использовать отдельный USB-токен.

Предотвращение подбора пароля

Для предотвращения подбора пароля реализована прогрессивная задержка ввода пароля, а также оповещение о попытках подбора пароля:

- Каждая неудачная попытка ввода пароля увеличивает счётчик ошибок аутентификации на единицу. Счётчик ошибок аутентификации индивидуален для каждой учётной записи.
- После трёх неудачных попыток ввода пароля, следующий ввод станет доступным через три секунды. Каждая последующая неудачная попытка ввода:
  - увеличивает задержку;
  - считается попыткой подбора пароля.
- Каждая ошибка аутентификации регистрируется в системном журнале, а попытка подбора пароля — в журнале СКЗИ.

- Счётчик ошибок аутентификации сбрасывается после успешного ввода пароля или после десяти неудачных попыток подряд.
- Счётчик попыток подбора пароля является общим для всех локальных учётных записей и отображается (если он больше нуля) при каждой успешной аутентификации, например:

```
login: admin
Password:
Last login: Thu Sep 26 19:32:09 +05 2024 on ttyLP0
...
------------------------------------------------------------------
Password guessing attempts registered: 5
------------------------------------------------------------------
```

- Счётчик попыток подбора пароля может быть сброшен только вручную администратором с локальной или централизованной учётной записью:

```
hostname# admin clear-auth-warning
Password guessing counter was cleared.
```

Обновление справочников и ключей

Если администратор защищённой сети добавляет или удаляет связи вашего ViPNet Coordinator IG с другими узлами защищённой сети, новые справочники и ключи обмена будут переданы с ViPNet Prime на ViPNet Coordinator IG.

Согласуйте с администратором защищённой сети дату и время изменения связей с учётом особенностей:

- Если ViPNet Coordinator IG используется как межсетевой экран типа «Д», необходимо переключить его в режим регламентного обслуживания перед обновлением справочников и ключей (см. Переключение режимов работы межсетевого экрана). Иначе справочники и ключи не будут обновлены. Администратор защищённой сети может сделать это удалённо с помощью ViPNet Prime Policy Management.
- Если уровень загрузки процессора ViPNet Coordinator IG близок к 100%, то во время обновления справочников и ключей возможны потери IP-пакетов и снижение производительности. Обновляйте справочники и ключи, когда нагрузка на ViPNet Coordinator IG минимальна. Вы можете посмотреть уровень загрузки процессора с помощью команды:

  ```
  hostname> failover show info
  ```

Информация о принятых обновлениях ключей записывается в журнал СКЗИ (см. Журналы аудита и СКЗИ).

Для просмотра информации об установленных ключах обмена см. Просмотр сведений о ключе защиты обновлений и ключах обмена.

Просмотр сведений о ключе защиты обновлений и ключах обмена

Ключ защиты обновлений

Чтобы просмотреть сведения о ключе защиты обновлений узла и криптодрайвере:

```
hostname> iplir show key-info
NSK information:
        Uid:639F3772BE9A2BD3EF9FE9324B32D419
                Software-specified key ID: bc5c9cef-47c9-4b31-a51c-93548e5d092f
                Key algorithm: The Magma key algorithm
                Key expiration date: 2023-04-15
                Key effective date: 2022-01-20
                My network ID: 383d
                My host ID: 110
                My host name: IG100-2c6700b7
                My host variant: 0
                Message count on NSK: 36
Driver information:
        Support systems:
                ItcsCdCryptSystemGost | status: ItcsCdCryptSystemReady
                ItcsCdCryptSystemFips | status: ItcsCdCryptSystemPrngInitRequire
                ItcsCdCryptSystemCustom | status: ItcsCdCryptSystemUnavailable
        Support crypto suites:
                G28147_CFB_WITH_IMIT
                G28147_CTR_WITH_IMIT_CMACKDF
                ITCS_AES256_CFB_WITH_IMIT
                G28147_CTR_WITH_IMIT (for IPLir 4.1)
                G3412_MAGMA_AEAD
                G3412_KUZNYECHIK_CTR_WITH_CMAC ( CTR + CMAC)
                AES128_GCM_CMACKDF ( IPLir 6.1)
```

```
AES128_CTR_WITH_CMAC_CMACKDF ( CTR + CMAC for IPLir 6.1)
AES128_CFB_WITH_CMAC_CMACKDF ( CFB + CMAC for IPLir 6.1)
```

Отображаются сведения:

- о ключе защиты обновлений узла:
  - `Uid` — идентификатор;
  - атрибуты ключа:
    - `Software-specified key ID` — идентификатор ключа, задаваемый приложением;
    - `Key algorithm` — алгоритм шифрования;
    - `Key expiration date` — дата окончания периода действия ключа;
    - `Key effective date` — дата начала периода действия ключа;
    - `My network ID` — идентификатор собственной сети;
    - `My host ID` — идентификатор собственного узла;
    - `My host name` — имя собственного узла;
    - `My host variant` — вариант собственного узла;
    - `Message count on NSK` — порядковый номер сообщения на ключе.
- о криптодрайвере:
  - поддерживаемые системы и их статус;
  - поддерживаемые алгоритмы шифрования.

Ключи обмена

Чтобы просмотреть сведения обо всех ключах обмена, полученных с ViPNet Prime:

```
hostname> iplir show exchange-keys
 Peer      Variant     StartDate     ExpiryDate                  KeyID
------------------------------------------------------------------------------
231323E1     1        2020-11-08    2021-11-09 (30 days)  123-123-123-123-321
23132341     3        2020-02-05    2022-02-06 (30 days)  321-123-123-123-321
Warning starts displaying in 7 days before expiry date.
```

Отображаются сведения:

- `Peer` — идентификатор узла.
- `Variant` — номер варианта ключа связанного узла (номер варианта увеличивается при каждой смене ключа).
- `StartDate` — дата начала действия ключа.
- `ExpiryDate` — дата окончания действия ключа.

- `KeyID` — идентификатор ключа в ViPNet Prime.

Чтобы просмотреть сведения о ключах обмена, срок действия которых истёк или скоро истечёт:

```
hostname> iplir show exchange-keys warning
```

Обновление ключей по истечении срока их действия

Ключи имеют ограниченный срок действия:

- ключ защиты обновлений — 15 месяцев;
- ключи обмена — 15 месяцев;
- ключ и соответствующий ему сертификат пользователя — 12 месяцев.

Истечение срока действия ключа защиты обновлений и ключей обмена не накладывает ограничений на работу ViPNet Coordinator IG. Но мы рекомендуем обновить ключи, чтобы гарантировать защиту трафика между узлами.

Истечение срока действия сертификата пользователя заблокирует ему доступ к ViPNet Coordinator IG через консоль, если в защищённой сети используется аутентификация по сертификату.

По умолчанию за 30 дней до истечения срока действия ключа появляется сообщение:

- `WARNING: Node security keys expire. Validity period < 30 day(s)` — срок действия ключа защиты обновлений истечёт через 30 дней.
- `WARNING: Exchange keys expire. Validity period < 30 day(s)` — срок действия ключа обмена истечёт через 30 дней.
- `WARNING: Your authentication key expire. Validity period < 30 day(s)` — срок действия сертификата пользователя истечёт через 30 дней.

Оповещение отображается после успешной аутентификации в командном интерпретаторе или веб-интерфейсе. Если вы увидели сообщение о скором истечении срока действия:

- ключа защиты обновлений или ключа обмена — сообщите об этом администратору защищённой сети. Он сформирует новый ключ и вышлет его на ViPNet Coordinator IG.

  Внимание!

  - Если ViPNet Coordinator IG используется как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания перед обновлением ключей. Иначе ключи не будут обновлены. Администратор защищённой сети может сделать это с помощью ViPNet Prime Policy Management.
  - Не обновляйте ключи, если уровень загрузки процессора приближается к 100%. Иначе во время обновления возможны потери IP-пакетов и снижение производительности. Чтобы проверить уровень загрузки процессора, выполните: `failover show info`.
  - После обновления ключей обмена создайте резервную копию конфигурации, так как использовать ранее созданные резервные копии будет невозможно.

- сертификата пользователя — издайте новый сертификат.

Вы можете настроить оповещение об истечении срока действия ключей и сертификата.

Настройка оповещения об истечении срока действия ключей

По умолчанию оповещение срабатывает за 30 дней до истечения срока действия:

- ключа защиты обновлений;
- ключа обмена;
- сертификата пользователя.

Это позволяет обновить ключи или сертификат до истечения их срока действия.

Чтобы изменить период оповещения:

```
hostname# iplir warning-threshold <период оповещения>
```

где `<период оповещения>` — количество дней в интервале 7–365.

Например, чтобы оповещение отображалось за две недели до окончания срока действия:

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

Перевыпуск ключей локального SSH-сервера

Удаленное подключение к ViPNet Coordinator IG обеспечивает локальный SSH-сервер. Если вам необходимо заменить ключи SSH-сервера, например, в вашей компании изменилась политика безопасности, выполните:

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

Старый ключ будет удален и сгенерирован новый.

Для просмотра информации о ключах локального SSH-сервера, выполните:

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

Настройка подключения с помощью веб-интерфейса

Примечание. Веб-интерфейс доступен только в исполнениях ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.

Подключение к ViPNet Coordinator IG с помощью веб-интерфейса обеспечивает служба `WebUI`. По умолчанию служба использует протокол HTTPS (TCP-порт 8080) и самоподписанный сертификат, который генерируется при инициализации ViPNet Coordinator IG.

Вы можете:

- перевыпустить самоподписанный сертификат, например, если закончился срок его действия;
- использовать сертификат, изданный в удостоверяющем центре (далее — УЦ);
- изменить TCP-порт 8080;
- переключить работу службы `WebUI` на HTTP.

Перевыпуск самоподписанного сертификата

Выполните команду:

```
hostname# webui recreate-cert [bits <длина ключа> digest {sha256 | sha384 | sha512} span <срок действия> [subj <subject>]]
```

Если ввести команду без параметров, будут использоваться значения, как при инициализации ViPNet Coordinator IG:

- длина ключа — 2048 бит;
- алгоритм хэширования — sha256;
- срок действия — 1825 дней;
- имя субъекта — имя узла.

Подробнее об использовании параметра `<subject>` см. в документе «Справочник команд и конфигурационных файлов».

Настройка использования сертификата, изданного удостоверяющим центром

Для издания сертификата в УЦ необходимо создать запрос на сертификат и передать его в УЦ. Вы можете создать запрос на сертификат в ViPNet Coordinator IG или с помощью стороннего ПО. Если запрос на сертификат создан с помощью стороннего ПО, начните настройку с шага 3.

1 Создайте запрос на сертификат:

```
hostname# service cert request create name <имя сертификата> bits {2048 | 3072 | 4096} digest {sha256 | sha384 | sha512} [subj <subject>]
```

Длину ключа, алгоритм хэширования и дополнительные параметры задайте в соответствии с политиками безопасности вашей организации. Подробнее об использовании параметра `<subject>` см. в документе «Справочник команд и конфигурационных файлов».

В процессе выполнения команды будут запрошены личные данные, необходимые для создания сертификата (страна, город, организация и т.д.).

После выполнения команды будет создан файл запроса и закрытый ключ.

2 Подключите USB-носитель к ViPNet Coordinator IG и экспортируйте запрос на сертификат:

```
hostname# service cert request export <файл запроса>
```

3 Отправьте файл запроса в УЦ вместе с требованиями:

- УЦ должен использовать алгоритм хэширования SHA-2.
- Сертификат должен быть подписан с использованием алгоритма RSA.
- Файл сертификата должен быть в кодировке DER или Base64.

4 Получите в УЦ сертификат и скопируйте его на USB-носитель.

Примечание. Если запрос на сертификат был создан с помощью стороннего ПО, скопируйте на USB-носитель закрытый ключ и сертификат.

Поддерживаются файлы с расширениями PEM и CER. В контейнере PEM (`*.pem`) используется стандарт PKCS#12.

---

5 Подключите USB-носитель с сертификатом к ViPNet Coordinator IG.

6 Импортируйте сертификат или ключ с сертификатом в ViPNet Coordinator IG:

```
hostname# service cert import
```

7 Выберите импортированный сертификат для использования службой `WebUI`:

```
hostname# webui https-cert <имя файла сертификата>
```

8 Перезапустите службу `WebUI`:

```
hostname# webui restart
```

Изменение TCP-порта

1 Задайте TCP-порт, который будет использоваться для доступа к веб-интерфейсу:

```
hostname# webui port <номер TCP-порта>
```

2 В сетевом фильтре `Allow ViPNet WebGUI` укажите новый номер TCP-порта:

2.1 Удалите существующий фильтр:

```
hostname# firewall vpn delete tcp dport 8080
```

2.2 Добавьте новый фильтр:

```
hostname# firewall vpn add rule "Allow ViPNet WebGUI" src <ViPNet ID узла | группа ViPNet ID узлов> dst @local tcp dport <номер TCP-порта> pass
```

3 Перезапустите службу `WebUI`:

```
hostname# webui restart
```

Теперь для подключения к ViPNet Coordinator IG с помощью веб-интерфейса в адресной строке браузера вводите новый номер TCP-порта:

```
https://<IP-адрес ViPNet Coordinator IG>:<номер TCP-порта>
```

Переключение на протокол HTTP

Чтобы переключить работу службы `WebUI` на HTTP:

```
hostname# webui protocol http
```

Смена типа межсетевого экрана с сохранением сетевых фильтров



Внимание! В процессе смены типа межсетевого экрана ViPNet Coordinator IG не выполняет свои целевые функции, поэтому убедитесь, что временная неработоспособность ViPNet Coordinator IG не приведет к нарушению работы промышленной сети и подключенного к ней оборудования.

Тип межсетевого экрана задаётся в ViPNet Prime. Затем эта информация попадает в ViPNet Coordinator IG вместе с дистрибутивом ключей при инициализации. Смена типа межсетевого экрана может быть выполнена удалённо из ViPNet Prime. При этом необходимо учитывать:

- при смене типа с «А/Б» на «Д» все настройки сетевых фильтров удаляются, а вместо них устанавливаются сетевые фильтры по умолчанию для типа «Д».
- при смене типа с «Д» на «А/Б» все настройки сетевых фильтров, выполненные в штатном режиме работы, переносятся в тип «А/Б». Сетевые фильтры из режима регламентного обслуживания и специального режима удаляются.

Чтобы сохранить настройки сетевых фильтров при смене типа межсетевого экрана с «А/Б» на «Д», вы можете использовать ViPNet Prime Policy Management:

1. Совместно с администратором защищённой сети подготовьте политику в ViPNet Prime Policy Management, включив в неё:
   - все сетевые фильтры, которые вы хотите перенести;
   - режим работы межсетевого экрана — штатный.
2. Из ViPNet Prime на ViPNet Coordinator IG отправьте обновление справочников, в котором задан тип «Д» межсетевого экрана, и время применения обновления справочников `t+40` минут, где `t` — ваше текущее время.
3. Из ViPNet Prime Policy Management отправьте политику, подготовленную на шаге 1, с временем применения `t+60` минут.

Контроль целостности файлов ПО

Целостность критически важных файлов ПО ViPNet Coordinator IG регулярно проверяется встроенными скриптами. В ходе проверки контролируются:

- Исполняемые и конфигурационные файлы.
- Файлы справочников и ключи.

Указанные файлы защищены контрольными суммами, которые хранятся в файлах с расширением `crg`. Проверка целостности заключается в вычислении текущей контрольной суммы файла и её сравнении с контрольной суммой из файла `*.crg`. Несовпадение контрольных сумм считается нарушением целостности файла.

Каждый файл `*.crg` содержит также собственную контрольную сумму. Проверка контрольной суммы файла `*.crg` выполняется перед проверкой целостности остальных файлов, контрольная сумма которых в нём указана.

Нарушением целостности файлов также считается отсутствие хотя бы одного конфигурационного файла или файла с контрольными суммами.

Проверка целостности файлов выполняется в следующих случаях:

- Установка ПО ViPNet Coordinator IG.
- Обновление ПО ViPNet Coordinator IG.
- Загрузка ПО ViPNet Coordinator IG.
- Периодическая проверка с интервалом 12 часов (в этом случае конфигурационные файлы, а также справочники и ключи не проверяются).



Примечание. При каждой периодической проверке в системный журнал вносится запись, содержащая время и результаты этой проверки. Чтобы просмотреть информацию о последней периодической проверке, выполните:

```
hostname> admin show check integrity status
```

Если команда выполнена до первой периодической проверки целостности файлов, то появится сообщение об отсутствии результатов проверки целостности: `No integrity check information`.

При локальном подключении к ViPNet Coordinator IG вы можете проверить целостность файлов вручную, в рамках регламентного контроля:

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

При несовпадении контрольных сумм в ходе периодической проверки ViPNet Coordinator IG автоматически перезагружается.

При несовпадении контрольных сумм в ходе установки, обновления или загрузки ПО выполняются действия:

- Если для повреждённого файла имеется резервная копия, файл автоматически восстанавливается и ViPNet Coordinator IG перезагружается.
- Если исполняемый файл восстановить не удалось, то загрузка ViPNet Coordinator IG завершается. Выполните восстановление ПО или обратитесь в ИнфоТеКС.
- Если конфигурационный файл восстановить не удалось, ViPNet Coordinator IG перезагружается в режим ограниченного функционирования, в котором администратор с локальной учётной записью `admin` может выполнить следующие действия:
  - Подключиться к ViPNet Coordinator IG с помощью консоли.
  - Просмотреть события журналов для определения причин сбоя.
  - Изменить параметры конфигурационных файлов, за исключением настроек сетевых интерфейсов.
  - Восстановить настройки из резервной копии.
  - Перезагрузить ViPNet Coordinator IG.
  - Выполнить сброс к заводским настройкам — только для серверных исполнений ViPNet Coordinator IG.
  - Выполнить восстановление ПО — только для промышленных исполнений ViPNet Coordinator IG.

11

Обеспечение отказоустойчивости

Настройка системы защиты от сбоев 244

Просмотр информации о работе системы защиты от сбоев 258

Подключение к источнику бесперебойного питания 262

Настройка системы защиты от сбоев

Назначение системы защиты от сбоев

Система защиты от сбоев предназначена для контроля работоспособности ПО ViPNet Coordinator IG и создания отказоустойчивого решения на базе двух ViPNet Coordinator IG. Система может работать в одиночном режиме или в режиме кластера.

Параметры работы системы защиты от сбоев задаются в файле `failover.ini`. Подробнее см. «Справочник команд и конфигурационных файлов», раздел «Файл failover.ini».

Работа системы защиты от сбоев в одиночном режиме

По умолчанию система защиты от сбоев работает в одиночном режиме и обеспечивает:

- контроль собственной работоспособности;
- контроль работоспособности запущенных служб и драйверов ViPNet Coordinator IG, ведение статистики использования системных ресурсов;
- контроль сбоев при обработке IP-пакетов VPN-драйвером.

В состав системы защиты от сбоев входят watchdog-драйвер `itcswd` и служба `failoverd`. При загрузке системы сначала запускается watchdog-драйвер, а затем служба `failoverd`, которая запускает остальные службы и драйверы. Watchdog-драйвер `itcswd` и служба `failoverd` работают в фоновом режиме.

Watchdog-драйвер контролирует работоспособность службы `failoverd`. Если в настройках включен механизм регистрации служб и драйверов, `failoverd` периодически посылает драйверу сообщения для подтверждения своей работоспособности. Если по истечении определенного времени от службы не будет получено ни одного сообщения, драйвер инициирует перезагрузку системы. Подробнее см. в документе «Справочник команд и конфигурационных файлов», в описании секции `[misc]` файла `failover.ini`.

Служба `failoverd` контролирует работоспособность остальных служб и драйверов ViPNet Coordinator IG. В процессе своей работы каждая из них периодически посылает службе `failoverd` сообщения для подтверждения своей работоспособности. Если по истечении определенного времени от какой-либо службы не будет получено ни одного сообщения или от VPN-драйвера будет получено сообщение с кодом ошибки обработки IP-пакетов, служба `failoverd` считает, что произошел сбой и пытается завершить работу этой службы. Если завершить работу корректно не удается, служба `failoverd` производит принудительный перезапуск. Если после пяти перезапусков подряд, работу контролируемой службы восстановить не удалось, она считается неработоспособной, и `failoverd` инициирует перезапуск системы.

Работа системы защиты от сбоев в режиме кластера

Система защиты от сбоев позволяет объединить два ViPNet Coordinator IG с одинаковой аппаратной платформой в кластер горячего резервирования. Кластер состоит из двух узлов:

- активный узел — выполняет функции ViPNet Coordinator IG;
- пассивный узел — находится в режиме ожидания.

В случае нарушения работоспособности активного узла, пассивный узел переключается в активный режим и выполняет функции сбойного узла, а сбойный узел переходит в пассивный режим.

Интерфейсы кластера

При описании кластера используются следующие понятия:

- Резервируемый интерфейс — сетевой интерфейс узла кластера, который резервируется на другом узле кластера.
- Интерфейс кластера — резервируемый интерфейс активного узла кластера.

  Каждый интерфейс кластера имеет один IP-адрес, по которому кластер доступен для других узлов. Этот IP-адрес всегда принадлежит узлу, работающему в данный момент в активном режиме. Резервируемые интерфейсы узла, работающего в пассивном режиме, не имеют IP-адресов, по которым другие узлы могли бы установить соединение с кластером. При переключении узлов кластера, резервируемые интерфейсы узла, который переходит в активный режим, получают IP-адреса интерфейсов кластера.
- Интерфейс синхронизации — сетевой интерфейс узла кластера, который подключен напрямую к интерфейсу другого узла кластера, и используется для передачи данных между узлами кластера.

  Через интерфейс синхронизации передаются:

  - Пакеты синхронизации, содержащие информацию о текущем режиме работы каждого узла кластера. Обмен пакетами синхронизации позволяет избежать ситуации, когда оба узла кластера работают в активном режиме (например, в случае практически одновременного запуска).
  - Копии принятых и готовых к отправке MFTP-конвертов.
  - Копии конфигурационных файлов и журналов. Перечень файлов, подлежащих передаче, задаётся в секции `[sendconfig]` конфигурационного файла `failover.ini` (подробнее см. в документе «Справочник команд и конфигурационных файлов»).
  - Справочники и ключи.

  Примечание. Конфигурационный файл `iplir.conf-<интерфейс>` и журнал IP-пакетов интерфейса синхронизации с активного узла кластера на пассивный не передаются.

  Каждая группа данных передаётся путём копирования во временный каталог с последующей проверкой, что все файлы группы успешно переданы.



Рисунок 29. Схема кластера

Алгоритм работы кластера

В процессе работы кластера пассивный узел контролирует работоспособность активного узла кластера, а активный узел контролирует работоспособность своих интерфейсов.

Алгоритм проверки работоспособности активного узла кластера:

1. Пассивный узел периодически проверяет присутствие в сети интерфейсов с IP-адресами активного узла кластера. Для этого используются ARP-запросы в режиме Duplicate address detection.
2. Если ни один из резервируемых интерфейсов активного узла не отвечает на запросы, счётчик сбоев увеличивается на единицу. Если хотя бы один интерфейс ответил на запрос, счётчик сбоев сбрасывается.
3. При достижении счётчиком порогового значения активный узел считается неработоспособным, и пассивный узел переходит в активный режим.

Примечание. Пассивный узел также следит за состоянием интерфейса синхронизации. Это позволяет обнаружить потерю питания на активном узле и быстрее переключить кластер.

1. При потере сигнала на интерфейсе синхронизации пассивный узел проверяет присутствие в сети интерфейсов с IP-адресами активного узла кластера.
2. Если ни один из резервируемых интерфейсов активного узла не отвечает, пассивный узел переходит в активный режим сразу, без использования счётчика сбоев.

Алгоритм проверки работоспособности интерфейсов активного узла кластера:

1. Активный узел периодически анализирует IP-трафик, проходящий через каждый из своих резервируемых интерфейсов.

2 Если за определённый период времени не зафиксировано ни одного отправленного и принятого IP-пакета, выполняется дополнительная проверка — через каждый интерфейс посылаются эхо-запросы заданным объектам сети (например маршрутизаторам).

3 При отсутствии ответов на эхо-запросы, счётчик отказов для соответствующего интерфейса увеличивается на единицу. Если получен хотя бы один ответ или зафиксирован трафик на интерфейсе, счётчик сбрасывается.

4 При достижении счётчиком порогового значения интерфейс считается неработоспособным, и активный узел переключается в пассивный режим, а пассивный узел становится активным.



Примечание. При потере физического соединения на интерфейсе активного узла кластера, для которого настроен параметр `testdevice` (см. Развёртывание кластера), переключение узлов происходит сразу, без проверки трафика.

Подробнее об алгоритмах работы кластера см. в документе «Сценарии работы», в разделе «Организация кластера горячего резервирования».

Для опроса IP-адресов активного узла и обмена данными между активным и пассивным узлом на обоих узлах кластера автоматически создаются разрешающие сетевые фильтры.

Выполнение команд в кластере

Все команды выполняются на активном узле кластера. Если команда предназначена для выполнения на пассивном узле или может выполняться на обоих узлах кластера, об этом указано в особенностях выполнения команды в «Справочнике команд и конфигурационных файлов».

Развёртывание кластера



Примечание. Использование ViPNet Coordinator IG в составе кластера доступно при наличии лицензии на функцию Failover. Чтобы активировать её, включите эту функцию в настройках координатора в ViPNet Prime.

Подготовка

1 Убедитесь, что оба ViPNet Coordinator IG, из которых будет организован кластер, имеют одинаковую аппаратную платформу и версию ПО (для этого используйте команду `version`).

2 Отключите от локальной сети оба ViPNet Coordinator IG, которые будут входить в состав кластера. Это позволит избежать проблем в работе локальной сети и рассылке справочников и ключей в сети ViPNet.

3 Установите на оба ViPNet Coordinator IG один и тот же дистрибутив ключей (см. документ «Подготовка к работе», раздел «Ввод в эксплуатацию»).

   - Если на одном из ViPNet Coordinator IG уже установлены другие ключи, удалите их с помощью команды `admin remove keys` и выполните инициализацию ViPNet Coordinator IG.

- Если в защищённой сети используется аутентификация пользователей по сертификату, используйте разные USB-токены при инициализации каждого ViPNet Coordinator IG. Таким образом у локального администратора `admin` будет два USB-токена с сертификатом, — по одному для аутентификации на каждом узле кластера.
- При инициализации откажитесь от проверки связи с узлом ViPNet, так как ViPNet Coordinator IG отключён от сети.

4 Выберите сетевые интерфейсы, которые будут использоваться в качестве резервируемых интерфейсов. Вы можете использовать проводные, беспроводные, виртуальные и VLAN-интерфейсы. Все резервируемые интерфейсы не могут быть беспроводными, хотя бы один из них должен быть проводной.

5 Убедитесь, что в настройках проводных резервируемых интерфейсов установлен класс `access` и данные интерфейсы включены (для просмотра используйте команду `inet show interface <имя интерфейса>`).

Не важно, какие IP-адреса заданы на резервируемых интерфейсах. Когда ViPNet Coordinator IG станет активным узлом кластера, его интерфейсам будут присвоены IP-адреса, заданные в настройках кластера. А на пассивном узле кластера IP-адреса будут удалены.

6 На каждом ViPNet Coordinator IG:

6.1 Выберите сетевой интерфейс, который будет использоваться в качестве интерфейса синхронизации. Соедините интерфейсы синхронизации обоих ViPNet Coordinator IG напрямую с помощью Ethernet-кабеля.

6.2 Настройте интерфейс синхронизации: задайте статический IP-адрес, установите класс `access` и включите интерфейс (см. Настройка сетевых интерфейсов Ethernet). Запрещено использовать дополнительные IP-адреса (alias) и агрегированные интерфейсы (bond).

IP-адреса интерфейсов синхронизации обоих ViPNet Coordinator IG должны принадлежать одной сети и не должны совпадать с IP-адресами других узлов сети ViPNet, иначе трафик, идущий на эти адреса, будет блокироваться. Если необходимо использовать одинаковые адреса, настройте видимость соответствующих узлов по виртуальным адресам.

7 Выберите один или несколько стабильных объектов сети (например, маршрутизатор), которые будут использоваться для проверки работоспособности интерфейсов активного узла кластера.

8 Выберите ViPNet Coordinator IG, который после запуска системы защиты от сбоев должен запуститься в качестве активного узла кластера, и настраивайте его первым. Выбор — на ваше усмотрение. Вы можете настраивать оба ViPNet Coordinator IG параллельно до момента запуска системы защиты от сбоев.

Примечание. Настройку сетевых служб необходимо выполнять после развёртывания кластера и запуска системы защиты от сбоев. Настройка выполняется на активном узле кластера.

Настройка

Для развёртывания кластера выполните следующие действия на каждом из ViPNet Coordinator IG:

1 Завершите работу системы защиты от сбоев:

```
hostname# failover stop
```

2 Откройте файл `failover.ini` для редактирования:

```
hostname# failover config edit
```

3 Для каждого резервируемого интерфейса задайте следующие параметры в секции `[channel]` (если для нужного интерфейса секция отсутствует, создайте её):

Примечание.



- Для каждой пары резервируемых интерфейсов, подключённых к одной сети, значения параметров секции `[channel]` должны совпадать. То есть секции `[channel]` должны заполняться одинаково на обоих узлах кластера.
- Примеры настройки конфигурационного файла `failover.ini` см. в документе «Сценарии работы» в разделе «Организация кластера».

- `device` — имя сетевого интерфейса.

  На обоих узлах кластера для доступа к одной и той же сети должны использоваться сетевые интерфейсы с одинаковыми именами.

- `activeip` — IP-адрес с префиксом маски, которые присваиваются сетевому интерфейсу, когда узел работает в активном режиме. Для интерфейса с динамическим IP-адресом, в том числе для беспроводного интерфейса, вместо IP-адреса укажите ключевое слово `dynamic`.

- `testip` — IP-адрес маршрутизатора или другого стабильного объекта сети, к которому будут посылаться эхо-запросы для проверки работоспособности интерфейса. IP-адрес должен находиться в одной подсети с IP-адресом из параметра `activeip`.

Примечание.



- 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.
- Для модема в качестве значения параметра `testip` мы рекомендуем указывать IP-адрес стабильного узла во внешней сети, например, DNS-сервера Yandex (`77.88.8.8`).

При необходимости для каждого резервируемого интерфейса вы можете 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 строки:

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

Внимание! Если в кластере используется функция L2OverIP (см. Настройка туннелирования на канальном уровне по технологии L2OverIP) и требуется проверять состояние его интерфейса, то в качестве тестового IP-адреса для этого интерфейса необходимо задать адрес из локального сегмента, а также выключить блокирование одноадресных Ethernet-кадров с неизвестным MAC-адресом получателя командой `iplir set l2overip unsolicited-frames broadcast`. Настоятельно не рекомендуется указывать для рабочего интерфейса L2OverIP тестовый IP-адрес в удалённом сегменте.

- `testdevice` — имя сетевого интерфейса, для которого необходимо контролировать состояние физического соединения. При потере физического соединения на указанном интерфейсе будет выполнено переключение узлов кластера. Использование `testdevice` позволяет быстрее переключать узлы кластера при физической потере соединения.

  В качестве сетевого интерфейса в параметре `testdevice` вы можете указать только физический интерфейс. Не допускается задавать беспроводные, виртуальные, агрегированные или VLAN интерфейсы, а также `localhost`. При этом вы можете указать физический интерфейс, который задан как trunk-интерфейс для VLAN.

  Параметр `testdevice` необязательный. В каждой секции `[channel]` вы можете задать только один параметр `testdevice`.

Внимание!

- Не изменяйте значение параметра `testdevice`, когда служба `failoverd` запущена в режиме кластера. Иначе это будет воспринято системой как потеря физического соединения и приведёт к переключению узлов кластера.
- В параметре `testdevice` указывайте только те сетевые интерфейсы, состояния которых действительно должны контролироваться для работоспособности кластера.

- `ident` — текстовая строка, идентифицирующая сетевой интерфейс. Для интерфейсов, подключённых к одним и тем же сетям, параметры `ident` должны совпадать. По этому параметру система защиты от сбоев определяет интерфейсы, которые выполняют одинаковые функции на узлах кластера.
- `checkonlyidle` — указание на необходимость проверки только неактивных интерфейсов. Возможные значения:
  - `yes` (по умолчанию) — активный узел посылает эхо-запросы на интерфейсы, адреса которых указаны в параметрах `testip`, только если за период опроса IP-адресов на данных интерфейсах не было ни входящих, ни исходящих пакетов;
  - `no` — эхо-запросы на интерфейсы, адреса которых указаны в параметрах `testip`, посылаются всегда.
- `channelgroup` — текстовая строка, идентифицирующая группу сетевых интерфейсов на узле кластера, которые используются в функции MultiWAN (см. Настройка функции MultiWAN). Если на узле кластера настроено резервирование канала доступа в интернет, то для сетевых интерфейсов основного и резервного каналов должно быть задано одинаковое значение `channelgroup` в секциях `[channel]`. Система защиты от сбоев будет считать интерфейс работоспособным пока работает хотя бы один интерфейс с таким же параметром `channelgroup`. Иначе, при недоступности основного канала доступа в

интернет, узлы кластера переключатся раньше, чем будет задействован резервный канал доступа в интернет.

- `usevirtualmac` — использование виртуальных MAC-адресов для сетевых интерфейсов кластера, заданных в данной секции `[channel]`. Не поддерживается для беспроводных интерфейсов. Возможные значения:
  - `yes` — использовать виртуальные MAC-адреса для сетевых интерфейсов;
  - `no` (по умолчанию) — не использовать виртуальные MAC-адреса для сетевых интерфейсов.

  Включение данной функции позволит ускорить восстановление связи с координатором после переключения узлов кластера. Виртуальные MAC-адреса для сетевых интерфейсов кластера генерируются на основе значения параметра `virtualmacprefix` в секции `[network]` (см. описание параметра в документе «Справочник команд и конфигурационных файлов»).

Примечание.

- Для работы этой функции необходимо настроить коммутационное оборудование таким образом, чтобы разрешить использование двух MAC-адресов для одного Ethernet-порта. Убедитесь, что настройки port-security коммутационного оборудования не блокируют смену MAC-адресов сетевых интерфейсов кластера.
- Если вы используете в качестве резервируемых интерфейсов кластера виртуальные интерфейсы, то параметр `usevirtualmac` необходимо настраивать для соответствующих им родительских интерфейсов.

Внимание! Перед выполнением следующего шага, вернитесь к началу текущего шага и настройте параметры для следующего резервируемого интерфейса.

4 Для всех исполнений ViPNet Coordinator IG100 и ViPNet Coordinator IG1000 вы можете включить синхронизацию открытых соединений (не поддерживается для беспроводных интерфейсов). Для этого в секции `[misc]` добавьте параметр `syncconnections` и укажите его значение:

- `yes` — синхронизация открытых соединений включена. В этом случае при переключении узлов кластера соединения, открытые на активном узле до момента переключения, продолжат работу на пассивном узле после его переключения в активный режим.

  Синхронизация открытых соединений не поддерживается в отношении следующих типов соединений:
  - открытые сессии разрешения доменных имен;
  - защищённые соединения по TCP-туннелям;
  - локальные соединения (открытые и защищённые соединения, в которых ViPNet Coordinator IG является источником или назначением);
  - соединения, использующие прикладные протоколы (см. Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP).

Чтобы включить синхронизацию сессий прикладных протоколов DNS, FTP, H.323, SCCP, SIP, добавьте вместе с параметром `syncconnections` параметр: `syncalgtcp = yes`.

- соединения, использующие промышленные прикладные протоколы.

- `no` — синхронизация открытых соединений выключена (аналогично отсутствию параметра `syncconnections`).

Для включения синхронизации открытых соединений и синхронизации сессий прикладных протоколов параметры `syncconnections` и `syncalgtcp` должны иметь значение `yes` на обоих узлах кластера.

5 В секции `[sendconfig]` задайте параметры для синхронизации настроек между узлами кластера:

- `device` — имя интерфейса синхронизации.
- `activeip` — IP-адрес интерфейса синхронизации другого узла кластера.

6 При использовании модема или модуля Wi-Fi в качестве резервируемого интерфейса мы рекомендуем увеличить значение параметра `channelretries` в секции `[network]`:

```
channelretries = 20
```

Параметр `channelretries` определяет количество неудачных попыток опроса IP-адресов, указанных в параметрах `testip`, после которых интерфейс считается неработоспособным. Увеличив значение параметра до 20, вы снизите риск переключения активного узла кластера при кратковременных разрывах связи в сетях 3G/4G или Wi-Fi.

7 При необходимости измените другие параметры секций `[sendconfig]` и `[network]`. Описание параметров секций см. в документе «Справочник команд и конфигурационных файлов».

8 Сохраните изменения (**Ctrl+O**, затем **Enter**) и закройте редактор (**Ctrl+X**).

Примечание. Примеры настройки конфигурационного файла `failover.ini` см. в документе «Сценарии работы», в разделе «Организация кластера».

---

9 Переведите систему защиты от сбоев в режим кластера:

```
hostname# failover config mode cluster
```

10 Подключите ViPNet Coordinator IG к локальной сети.

- Если интерфейс Wi-Fi используется в качестве резервируемого интерфейса, настройте подключение к сети Wi-Fi. При этом укажите одну и ту же точку доступа для обоих узлов кластера.
- Если модем используется в качестве резервируемого интерфейса, настройте подключение к мобильной сети. Вы можете подключить узлы кластера к сетям разных операторов мобильной связи.

11 Убедитесь, что настройки коммутационного оборудования соответствуют требованиям раздела Работа кластера с коммутационным оборудованием.

12 Проверьте связь с каждым IP-адресом, заданным в параметре `testip` секции `[channel]` файла `failover.ini`:

```
hostname# inet ping <IP-адрес>
```



Внимание! Отсутствие связи со всеми IP-адресами, указанными в параметрах `testip` хотя бы одной секции `[channel]`, может привести к циклическому переключению узлов кластера после запуска системы защиты от сбоев.

13 Запустите систему защиты от сбоев:

```
hostname# failover start
```

ViPNet Coordinator IG, на котором система защиты от сбоев будет запущена первой, начнёт работать как активный узел кластера. Вы можете принудительно задать режим работы каждого узла кластера при запуске системы защиты от сбоев:

```
hostname# failover start {active | passive}
```

Если активный узел кластера уже запущен, перед запуском системы защиты от сбоев на втором узле кластера, сначала проверьте доступность активного узла:

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

В случае успешной проверки будет выведен список активных сетевых интерфейсов кластера, описанных параметрами `device` и `activeip` секции `[channel]` конфигурационного файла `failover.ini`, и соответствующих им MAC-адресов, например:

```
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
```



Внимание! Не изменяйте параметры сетевых интерфейсов, задействованных в работе кластера, если система защиты от сбоев запущена в режиме кластера. Иначе это может вызвать сбои в работе кластера.

После запуска системы защиты от сбоев на обоих узлах кластера, кластер начнёт свою работу. При этом на каждом узле кластера будут автоматически созданы нередактируемые сетевые фильтры, необходимые для корректной работы системы защиты от сбоев с выбранными параметрами (см. Сетевые фильтры по умолчанию).



Примечание. Система защиты от сбоев не контролирует работоспособность интерфейса синхронизации. Чтобы проверить его состояние, выполните команду:

```
hostname> failover show info
```

Если на экран выводится информация о состоянии обоих узлов кластера, значит интерфейсы работают исправно. Иначе, проверьте физическое соединение кабеля с интерфейсом.

Подключение к пассивному узлу кластера

В некоторых случаях необходимо удалённо подключиться к пассивному узлу кластера, например, чтобы просмотреть его состояние, если не настроен мониторинг кластера по SNMP (см. Мониторинг кластера):

1. Подключитесь как администратор к активному узлу кластера.
2. Перейдите в режим настройки:

   ```
   hostname> enable
   ```

3. Подключитесь к пассивному узлу кластера по IP-адресу его интерфейса синхронизации:

   ```
   hostname# inet ssh host <IP-адрес> user <пользователь> [port <порт>]
   ```

   в качестве параметра `<пользователь>` укажите:

   - `admin` — администратор пассивного узла кластера;
   - `user` — аудитор пассивного узла кластера, если его учётная запись была разблокирована ранее (см. Блокирование и разблокирование учётных записей).

Запуск и завершение работы системы защиты от сбоев

Чтобы запустить систему защиты от сбоев на одиночном узле, выполните:

```
hostname# failover start
```

Чтобы запустить систему защиты от сбоев на узле кластера, выполните:

- в режиме активного узла:

  ```
  hostname# failover start active
  ```

- в режиме пассивного узла:

  ```
  hostname# failover start passive
  ```



Внимание! Если при запуске системы защиты от сбоев не был указан параметр `active` или `passive`, то она будет запущена в том режиме, в котором находилась до завершения работы.

Перед запуском системы защиты от сбоев в активном или пассивном режиме убедитесь в том, что другой узел кластера работает в противоположном режиме. Запуск обоих узлов кластера в активном режиме вызовет конфликт IP-адресов.

Чтобы завершить работу системы защиты от сбоев, выполните:

```
hostname# failover stop
```

Переключение системы защиты от сбоев в одиночный режим

1. На каждом из узлов кластера выполните:

   ```
   hostname# failover config mode single
   ```

2. Отключите один из узлов кластера от локальной сети, чтобы избежать конфликтов при получении справочников и ключей.

3. Убедитесь, что IP-адреса сетевых интерфейсов второго узла кластера заданы верно, так как при переключении системы защиты от сбоев в одиночный режим параметры сетевых интерфейсов в файле `failover.ini` игнорируются.

4. В зависимости от дальнейших планов по использованию кластера выполните следующие действия:

   - Если вы больше не планируете использовать кластер, удалите ключи с узла, который был отключён от локальной сети:

     ```
     hostname# admin remove keys
     ```

     Если вы хотите в дальнейшем использовать этот ViPNet Coordinator IG как одиночный узел, установите новый дистрибутив ключей.

   - Если вы планируете возобновить работу кластера:

     - Выполните необходимые настройки для развёртывания кластера. В частности, убедитесь, что в конфигурационном файле `failover.ini` заданы IP-адреса всех сетевых интерфейсов кластера.
     - Подключите к локальной сети отключенный узел кластера.

Замена неисправного узла кластера

В случае неисправности активный узел кластера переключается в пассивный режим. Для замены неисправного узла кластера на новый:

1. Выполните резервное копирование конфигурации активного узла кластера на USB-носитель (см. Резервное копирование индивидуальной конфигурации).

Примечание. Для настройки нового узла кластера потребуются:

- IP-адрес интерфейса синхронизации, который был установлен на неисправном узле.
- IP-адрес интерфейса синхронизации активного узла кластера.



IP-адреса вы можете получить на активном узле кластера.

Чтобы узнать IP-адрес интерфейса синхронизации сбойного узла:

```
hostname> failover show config
```

IP-адрес указан в секции `[sendconfig]` в параметре `activeip`.

Чтобы узнать IP-адрес интерфейса синхронизации активного узла:

```
hostname> inet show interface <имя интерфейса>
```

2 Убедитесь, что новый ViPNet Coordinator IG, который будет входить в состав кластера, отключён от локальной сети.

3 Восстановите резервную копию конфигурации активного узла на новый узел кластера (см. Восстановление из резервной копии индивидуальной конфигурации). При этом используйте алгоритм восстановления с помощью инициализации ViPNet Coordinator IG.

4 После перезагрузки нового узла кластера завершите работу системы защиты от сбоев:

```
hostname# failover stop
```

5 Задайте IP-адрес интерфейса синхронизации, который был установлен на неисправном узле кластера:

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

6 Откройте конфигурационный файл `failover.ini` для редактирования:

```
hostname# failover config edit
```

7 Замените значение параметра `activeip` секции `[sendconfig]` на IP-адрес интерфейса синхронизации активного узла кластера.

8 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

9 Если на новом узле кластера включена функция плановой перезагрузки, измените время перезагрузки:

```
hostname# machine reboot-schedule time <время> [day <день>]
```

Время перезагрузки узлов кластера должно отличаться не менее чем на 30 минут.

10 Выключите новый узел кластера.

11 На активном узле кластера проверьте параметр `activeip` секции `[sendconfig]`:

```
hostname> failover show config
```

Параметр `activeip` должен соответствовать IP-адресу интерфейса синхронизации нового узла кластера.

12 Подключите новый узел кластера к локальной сети, а интерфейсы синхронизации обоих узлов кластера соедините между собой.

13 Включите новый узел кластера.

14 Убедитесь, что новый узел перешёл в пассивный режим и стал доступен. Для этого на активном узле кластера выполните:

```
hostname> failover show info
```

Работа кластера с коммутационным оборудованием

Настройки коммутационного оборудования (коммутаторы и маршрутизаторы), к которому подключается кластер, могут влиять на его работу. Поэтому при их совместном использовании убедитесь, что на коммутационном оборудовании:

- пропускаются эхо-запросы ICMP с IP-адресов активного узла до всех узлов с IP-адресами, заданными в параметрах `testip` секции `[channel]` конфигурационного файла `failover.ini`, и ответы на них;
- отключена функция Proxy ARP и пропускаются ARP-запросы от пассивного узла до активного узла и ответы на них.

Эти рекомендации касаются всех сетевых интерфейсов ViPNet Coordinator IG, для которых в файле `failover.ini` существует секция `[channel]`.

Просмотр информации о работе системы защиты от сбоев

Текущее состояние системы защиты от сбоев

Просмотр информации о текущем состоянии системы защиты от сбоев:

```
hostname> failover show info
```

По команде отображаются:

- `Versions` — версии ПО ViPNet Coordinator IG и системы защиты от сбоев;
- `ID` — идентификатор и имя узла ViPNet;
- `workstation time` — локальное время на узле ViPNet;
- `failover mode` — режим работы системы защиты от сбоев:
  - `single` — одиночный режим;
  - `active` — режим активного узла кластера;
  - `passive` — режим пассивного узла кластера.
- `failover uptime` — время непрерывной работы системы защиты от сбоев;
- `total cpu` — общая загруженность процессора;
- `total memory` — общий объём памяти;
- `available memory` — объём доступной памяти;
- сведения о текущем состоянии служб failover, iplir, mftp, webgui, controld, aad, external-controld, licd, piomonitor (см. Список служб ПО ViPNet Coordinator IG):
  - состояние службы:
    - `initializing` — загружается;
    - `works` — работает;
    - `stopped` — работа завершена;
    - `unknown` — неизвестно (например, если произошел сбой в работе службы, была произведена попытка её перезапуска, и данных о её состоянии пока нет);
  - сведения о ресурсах процессора, используемых службой.

Примечание. При работе ViPNet Coordinator IG в составе кластера статистика использования системных ресурсов и текущее состояние служб ViPNet Coordinator IG отображаются для обоих узлов кластера (в столбце `local` — для узла, на котором выполнена команда, в столбце `remote` — для второго узла кластера, см. пример ниже)

Одиночный режим

```
Versions: ViPNet 5.2.0(150), daemon 1.5 (1)
Workstation configured for ID 15EA000B (Coordinator_IG)
The workstation works in a single mode of protection against failures
Workstation time (utc: 1406806848) Wed Jul 31 15:40:48 2025
failover mode                * single
failover uptime              * 0d 0:14
total cpu                    * 3%
total memory                 * 251664 Kb
available memory             * 61576 Kb
failover state               * works
failover cpu                 * 3%
iplir state                  * works
iplir cpu                    * 7%
mftp state                   * works
mftp cpu                     * 1%
webgui state                 * works
webgui cpu                   * 7%
usbmodem state               * stopped
controld state               * works
controld cpu                 * 0%
aad state                    * works
aad cpu                      * 0%
external-controld state      * works
external-controld cpu        * 0%
licd state                   * works
licd cpu                     * 0%
piomonitor state             * stopped
ipf state                    * works
ipf cpu                      * 1%
```

Режим кластера

```
Versions: ViPNet 5.2.0 (30), daemon 1.5 (1)
Workstation configured for ID 29A0022 (Coordinator_IG)
Workstation works in a cluster mode of protection against failures
Workstation time (utc: 1204638024) Thu Jul 27 17:35:30 2025
                             * local             * remote
failover mode                * single            * passive
failover uptime              * 3d 5:26           * 0d 0:14
total cpu                    * 3%                * 0%
total memory                 * 251708 kB         * 251708 kB
available memory             * 66556 kB          * 66556 kB
failover state               * works             * works
failover cpu                 * 3%                * 0%
iplir state                  * works             * works
iplir cpu                    * 7%                * 0%
mftp state                   * works             * works
mftp cpu                     * 1%                * 0%
webgui state                 * works             * stopped
webgui cpu                   * 7%                * 0%
```

```
usbmodem state                * stopped           * stopped
controld state                * works             * works
controld cpu                  * 0%                * 0%
aad state                     * works             * works
aad cpu                       * 0%                * 0%
external-controld state       * works             * works
external-controld cpu         * 0%                * 0%
licd state                    * works             * works
licd cpu                      * 0%                * 0%
piomonitor state              * stopped           * stopped
ipf state                     * works             * works
ipf cpu                       * 1%                * 0%
```

Если служба `failoverd` не работает, выводится только информация о её режиме:

```
The failover system is in the single mode
```

Журнал переключений

События о работе системы защиты от сбоев в режиме кластера регистрируются службой `failoverd` в журнале переключений. Среди таких событий:

- `<BOOT>` — запуск службы `failoverd` при загрузке ViPNet Coordinator IG;
- `<P_START>` — ручной запуск службы `failoverd` в режиме пассивного узла;
- `<A_START>` — ручной запуск службы `failoverd` в режиме активного узла;
- `<SWITCH>` — переход узла из пассивного в активный (или наоборот).

Чтобы просмотреть записи в журнале переключений узла, выполните:

```
hostname> failover view <дд.мм.гггг[.чч.мм.сс]> <дд.мм.гггг[.чч.мм.сс]>,
```

указав начало и конец интересующего интервала времени. Например:

```
failover view 08.03.2025.00.00.00 23.03.2025.16.37.00
```

Выводится следующая информация:

- версии ПО ViPNet Coordinator IG и службы `failoverd`;
- идентификатор и имя узла;
- указание на работу системы защиты от сбоев в режиме кластера;
- локальные дата и время на узле;
- список записей за выбранный интервал времени (дата, время, идентификатор и описание события).

Данная информация выводится в следующем формате:

```
View journal of failover switching
Versions: ViPNet 4.5.1 (40258), daemon 1.5 (1)
Workstation configured for ID 2CEC000A (IG100i1-1)
```

```
The workstation works in a cluster mode of protection against failures
Workstation time (utc: 1406806848) Sat Jan 15 17:31:45 2022

13 Jan 2022 12:51:42     <P_START> Start failover daemon in passive mode
14 Jan 2022 12:27:27     <A_START> Start failover daemon in active mode
14 Jan 2022 14:10:35     <A_START> Start failover daemon in active mode
14 Jan 2022 15:30:46     <BOOT> Boot the system
15 Jan 2022 11:09:07     <SWITCH> Switch server from passive mode to active mode
```

Если за указанный интервал времени не произошло ни одного события, выводится сообщение:

```
There are no records in journal of switchings
```

Подключение к источнику бесперебойного питания

Внимание!

- Подключение к источнику бесперебойного питания (далее — ИБП) поддерживается только в исполнении ViPNet Coordinator IG1000 Q1.
- ViPNet Coordinator IG поддерживает только ИБП производства APC, подключаемые через USB-порт, например APC Smart-UPS.

При подключении ViPNet Coordinator IG к ИБП:

1. ViPNet Coordinator IG получает питание от аккумуляторной батареи ИБП.
2. Если заряд аккумуляторной батареи достигает критически низкого уровня (этот уровень зависит от параметров, заданных на ИБП: `battery.charge`, `battery.charge.low`, `battery.runtime` и `battery.runtime.low`):
   - 2.1 ИБП посылает сигнал ViPNet Coordinator IG по интерфейсному кабелю об истощении батареи.
   - 2.2 ViPNet Coordinator IG получает сигнал и начинает выключаться. При этом он передаёт на ИБП информацию, что для выключения потребуется не менее 180 секунд. Получив эти данные, ИБП корректирует расход оставшегося заряда батареи, чтобы ViPNet Coordinator IG успел штатно завершить работу.

     В результате ViPNet Coordinator IG успевает выключиться до полного разряда батареи и потери данных не происходит.
3. Если подача электроэнергии восстанавливается до достижения батареей критически низкого уровня заряда, ViPNet Coordinator IG снова начинает получать питание от электросети.

К одному ИБП можно подключить несколько ViPNet Coordinator IG. Устройство, к которому подключён интерфейсный кабель ИБП, является главным (primary), остальные — подчинёнными (secondary). Главное устройство взаимодействует непосредственно с ИБП и отвечает за своевременное оповещение по сети подчинённых устройств. Оно должно быть доступно подчинённым по одному из своих IP-адресов.

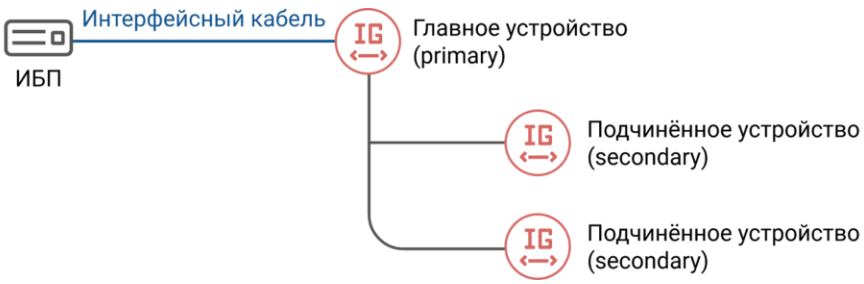


Рисунок 30. Схема подключения к ИБП

Чтобы подключить к ИБП несколько ViPNet Coordinator IG, необходимо настроить каждый из них в соответствии с его ролью (primary или secondary).

На ViPNet Coordinator IG с ролью primary:

1. Подключите интерфейсный кабель ИБП.
2. Включите взаимодействие с ИБП:

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

3. Установите режим главного устройства:

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

4. Запустите взаимодействие с ИБП:

   ```
   hostname# ups start
   ```

5. Проверьте взаимодействие с ИБП:

   ```
   hostname# ups show status
   ```

   Если взаимодействие установлено, отобразится информация о текущем состоянии ИБП.



Внимание! Если вы переподключили интерфейсный кабель ИБП, то для восстановления взаимодействия ViPNet Coordinator IG с ИБП выполните последовательно команды `ups stop` и `ups start`.

На ViPNet Coordinator IG с ролью secondary:

1. Включите взаимодействие с ИБП:

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

2. Установите режим подчинённого устройства:

   ```
   hostname# ups set mode slave <master_IP>
   ```

   ViPNet Coordinator IG, выступающий в роли primary, должен быть доступен с данного ViPNet Coordinator IG по этому IP-адресу.

   При подключении к ИБП кластера в качестве IP-адреса главного устройства укажите адрес интерфейса синхронизации узла с этой ролью.

3. Запустите взаимодействие с ИБП:

   ```
   hostname# ups start
   ```

4. Проверьте взаимодействие с ИБП:

   ```
   hostname# ups show status
   ```

   Если взаимодействие установлено, отобразится информация о текущем состоянии ИБП, подключённого к ViPNet Coordinator IG в роли primary.

Если к ИБП подключается кластер, то один узел будет главным, а другой — подчинённым. При этом другие устройства к ИБП подключать запрещено.

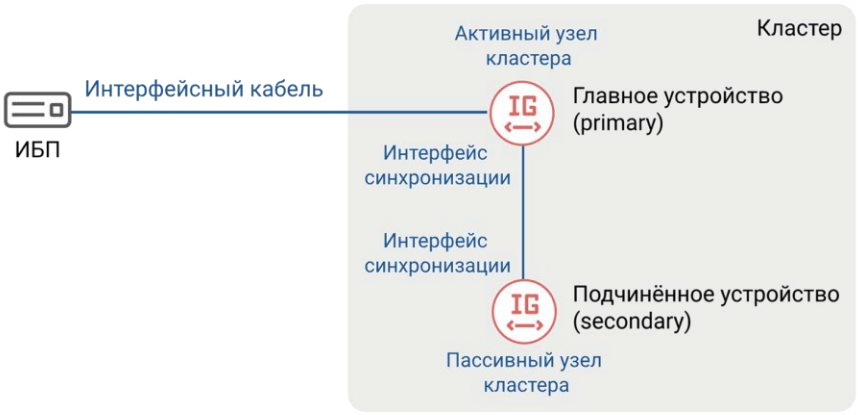


Рисунок 31. Схема подключения кластера к ИБП

12

Настройка транспортного сервера MFTP

Назначение транспортного сервера MFTP 266

Настройка протоколирования событий транспортного сервера MFTP 267

Назначение транспортного сервера MFTP

Транспортный сервер MFTP предназначен для передачи транспортных конвертов MFTP между связанными узлами сети ViPNet, поддерживающими работу с дистрибутивом ключей `dst`. Сервер MFTP обеспечивает удалённое обновление на узлах сети:

- Справочников и ключей.
- ПО ViPNet.
- Политик безопасности из ViPNet Prime Policy Management.



Внимание!

- Исполнения ViPNet Coordinator IG10 не поддерживают функцию транспортного сервера MFTP. Это значит, что транспортные конверты MFTP они не принимают.
- Исполнения ViPNet Coordinator IG100 могут передавать транспортные конверты только зарегистрированным за ними клиентам (не более 10 клиентов). При этом на клиентах не будут поддерживаться такие возможности как деловая почта, файловый обмен и ViPNet Connect.
- Необходимо учитывать, что ViPNet Coordinator IG любых исполнений не поддерживает передачу транспортных конвертов другим координаторам и расположенным за ними клиентам. Для этого используйте ViPNet Coordinator HW.

Транспортный сервер MFTP реализован службой `mftpd`. Конверты MFTP — это файлы с данными, которыми обмениваются между собой приложения, входящие в состав ПО ViPNet версий 4.x. Транспортный сервер передаёт конверты в соответствии с адресами получателей, указанными в заголовках конвертов, по каналу MFTP: узел-отправитель устанавливает TCP-соединение с узлом-получателем, проводится взаимная аутентификация узлов и осуществляется передача конвертов.

Подробнее о настройке сервера MFTP и ведении его журналов см. документ «Справочник команд и конфигурационных файлов», раздел «Файл mftp.conf».

Настройка протоколирования событий транспортного сервера MFTP

Служба `mftpd` записывает информацию о событиях, происходящих в процессе работы транспортного сервера MFTP, в системный журнал.

Чтобы изменить параметры записи событий:

1. Завершите работу службы `mftpd`:

   ```
   hostname# mftp stop
   ```

2. Откройте файл `mftp.conf` для редактирования:

   ```
   hostname# mftp config
   ```

3. В секции `[debug]` при необходимости измените значения следующих параметров:

   - `debuglevel` — уровень важности событий, записываемых в журнал. Возможные значения: от `1` до `4` (по умолчанию `3`). Чем выше уровень важности, тем более подробная информация записывается в журнал. Значение параметра `-1` выключает ведение журнала.

     Не рекомендуется задавать уровень важности выше `3` для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов ИнфоТеКС.

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

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

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

4. Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

5. Запустите службу `mftpd`:

   ```
   hostname# mftp start
   ```

13

Резервное копирование и восстановление настроек

Способы резервирования и восстановления настроек 269

Управление копиями конфигурации VPN 270

Управление индивидуальной конфигурацией 273

Управление универсальной конфигурацией 279

Способы резервирования и восстановления настроек

Вы можете сохранить настройки ViPNet Coordinator IG, чтобы иметь возможность восстановить их в будущем или перенести часть настроек на другой координатор.

Совокупность настроек называется копией конфигурации ViPNet Coordinator IG.

Таблица 8. Виды копий конфигурации ViPNet Coordinator IG

Вид копии конфигурации	Назначение	Создание	Хранение
Копия конфигурации VPN	Быстрое переключение между конфигурациями VPN и межсетевого экрана	Вручную	Память ViPNet Coordinator IG
Индивидуальная конфигурация	Восстановление настроек ViPNet Coordinator IG	Автоматически и вручную	Сервер ViPNet Prime, USB-носитель или сетевой узел
Универсальная конфигурация	Перенос настроек с одного ViPNet Coordinator IG на другой	Вручную	USB-носитель или сетевой узел

Управление копиями конфигурации VPN

Копия конфигурации VPN — совокупность настроек VPN, сетевых интерфейсов, системы защиты от сбоев, транспортного сервера MFTP, шлюза Modbus, а также сетевые фильтры.

Создание копии конфигурации VPN

1 Завершите работу служб `iplircfg`, `failoverd` и `mftpd`:

```
hostname# iplir stop
hostname# failover stop
hostname# mftp stop
```

2 Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания:

```
hostname# machine mode set service
```

3 Выполните команду:

```
hostname# vpn config save <имя>
```

и укажите имя копии конфигурации VPN, используя только буквы латинского алфавита, цифры, символы: «-» и «_».

4 Если копия конфигурации VPN с выбранным именем уже существует, будет предложено её перезаписать:

```
Config with name'<имя копии конфигурации VPN>' (version <версия ViPNet Coordinator IG>)
already exists! Overwrite it?
```

- Чтобы подтвердить перезапись, введите `y` и нажмите **Enter**.
- Чтобы создать конфигурацию с другим именем, введите `n` и нажмите **Enter**.

5 Запустите службы:

```
hostname# iplir start
hostname# failover start
hostname# mftp start
```

6 Если установлен режим межсетевого экрана типа «Д», переключите ViPNet Coordinator IG обратно в штатный режим работы:

```
hostname# machine mode set normal
```

Просмотр списка копий конфигурации VPN

Чтобы просмотреть список ранее созданных копий конфигурации VPN:

```
hostname# vpn config list
```

Формат отображения списка сохраненных копий: `"Name", Version, Type, saved on Date at Time, loaded at Date-load at Time-load`, где:

- `Name` — имя копии конфигурации VPN.
- `Version` — версия ПО ViPNet Coordinator IG, в которой была создана копия конфигурации VPN (может отсутствовать).
- `Type` — вид копии конфигурации VPN: `full` (полная) или `part` (частичная).
- `Date`, `Time` — дата и время создания копии конфигурации VPN.
- `Date-load`, `Time-load` — дата и время загрузки копии конфигурации VPN.

Если копия конфигурации VPN уже использовалась для восстановления настроек ViPNet Coordinator IG, дата и время использования отображаются после даты и времени создания копии конфигурации VPN (после `loaded`). Если копия конфигурации VPN ни разу не использовалась, после даты и времени создания будет указано `never loaded`.

Восстановление настроек из копии конфигурации VPN

1. Завершите работу служб `iplircfg`, `failoverd` и `mftpd`:

   ```
   hostname# iplir stop
   hostname# failover stop
   hostname# mftp stop
   ```

2. Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания:

   ```
   hostname# machine mode set service
   ```

3. Загрузите конфигурацию:

   ```
   hostname# vpn config load <имя копии конфигурации> [<версия ViPNet Coordinator IG>],
   ```

   указав имя копии конфигурации VPN и версию ViPNet Coordinator IG, в которой она была создана. Если имя копии конфигурации VPN состоит из нескольких слов, заключите его в кавычки.

4. Будет предложено сохранить все текущие настройки ViPNet Coordinator IG:

   ```
   Save current configuration?
   Continue [Yes/No]?
   ```

- Чтобы сохранить все текущие настройки, введите `Y` и нажмите **Enter**. Затем укажите имя соответствующей копии конфигурации VPN.
- Чтобы не сохранять текущие настройки ViPNet Coordinator IG, введите `n` и нажмите **Enter**. Для подтверждения действия введите фразу `Yes, do as I say`. Если копия конфигурации VPN создана в более новой версии ПО, подтвердите загрузку настроек.

5 Дождитесь завершения восстановления настроек.

6 Запустите службы:

```
hostname# iplir start
hostname# failover start
hostname# mftp start
```

7 Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», переключите его обратно в штатный режим работы:

```
hostname# machine mode set normal
```

Удаление копии конфигурации VPN

Чтобы удалить ненужные копии конфигурации VPN:

```
hostname# vpn config delete <имя копии конфигурации> [<версия ViPNet Coordinator IG>],
```

указав имя копии конфигурации VPN и версию ПО ViPNet Coordinator IG, в которой она была создана.

Чтобы не писать имя копии конфигурации VPN полностью или удалить сразу несколько копий конфигурации VPN, имена которых содержат определенные символы, вместо имени укажите маску имени, используя символ `*`.

Например, чтобы удалить все копии конфигурации VPN, созданные автоматически в августе 2025 года:

```
hostname# vpn config delete rollback-2025-08-*
```

Если несколько копий конфигурации VPN имеют имя, соответствующее указанной маске, то будет отображено количество таких копий конфигурации VPN:

```
<количество копий конфигурации VPN> configs match that pattern. Delete? [Yes/No]
```

Выполните одно из действий:

- Чтобы подтвердить удаление всех копий конфигурации VPN, введите `y` и нажмите **Enter**.
- Чтобы отменить удаление всех копий конфигурации VPN, введите `n` и нажмите **Enter**.

Чтобы удалить копии конфигурации VPN, созданные в определенной версии VPN-компонента ViPNet Coordinator IG, укажите номер этой версии:

```
hostname# vpn config delete rollback-2025-08-* 4.5.2
```

Управление индивидуальной конфигурацией

Индивидуальная конфигурация позволяет осуществлять возврат настроек ViPNet Coordinator IG к состоянию, которое было на момент создания этой конфигурации.

Индивидуальная конфигурация может использоваться:

- Для восстановления настроек ViPNet Coordinator IG в случае сбоя или некорректного обновления ПО.
- При замене неисправного ViPNet Coordinator IG, в том числе в составе кластера (см. Замена неисправного узла кластера).

При экспорте файл индивидуальной конфигурации (`*.ecf`) зашифровывается на ключе обмена, который используется для защиты соединения ViPNet Coordinator IG с ViPNet Prime. Чтобы восстановить настройки из файла индивидуальной конфигурации, на ViPNet Coordinator IG должен быть установлен тот же ключ обмена, который использовался при экспорте. Если ключ обмена был обновлён на ViPNet Coordinator IG, создайте новую резервную копию индивидуальной конфигурации.

Индивидуальная конфигурация содержит:

- настройки защищённой сети;
- настройки сетевых интерфейсов;
- настройки PoE;
- настройки маршрутизации и статические маршруты, если такие созданы;
- сетевые фильтры и правила трансляции адресов;
- режим работы межсетевого экрана;
- правила фильтрации промышленных протоколов;
- настройки параметров обработки прикладных протоколов;
- настройки шлюза Modbus и интерфейса GPIO;
- настройки системы защиты от сбоев;
- настройки транспортного сервера MFTP;
- журналы и настройки протоколирования;
- настройки дополнительных служб (DHCP-сервера и других);
- настройки туннелирования;
- текущие ключи для соединений по протоколу SSH.

Резервное копирование индивидуальной конфигурации

Резервное копирование индивидуальной конфигурации может быть выполнено:

- Автоматически — на сервер ViPNet Prime один раз в сутки.
- Вручную — на сервер ViPNet Prime или USB-носитель.



Примечание.

- При управлении ViPNet Coordinator IG с помощью веб-интерфейса вы можете создать резервную копию на свой сетевой узел. Подробнее см. документ «Настройка с помощью веб-интерфейса», раздел «Резервное копирование индивидуальной конфигурации». При этом резервное копирование на USB-носитель, подключённый к ViPNet Coordinator IG, будет недоступно.
- На время резервного копирования создаётся сетевой фильтр, разрешающий подключение к серверу ViPNet Prime, и останавливаются службы `vpn` и `mftp`. По завершении копирования фильтр будет удалён, а службы будут запущены заново.

Независимо от того, как была создана резервная копия, на сервере ViPNet Prime хранится только последняя копия конфигурации — каждая последующая копия затирает предыдущую. По умолчанию автоматическое резервное копирование выключено.

Шаблон имени файла индивидуальной конфигурации: `<имя сетевого узла>-<время создания файла>.ecf`.

Формат времени создания файла: `YYYYMMDDTHHMMSSZ`, где `YYYY` — год, `MM` — месяц, `DD` — день, `HH` — час, `MM` — минуты, `SS` — секунды. Время записывается в системе UTC.

Автоматическое резервное копирование

Чтобы настроить автоматическое резервное копирование:

1 Включите резервное копирование:

```
hostname# machine backup on
```

2 По умолчанию резервное копирование выполняется в случайное время из интервала 21.00–23.00. Вы можете изменить время резервного копирования одним из способов:

- Укажите точное время:

  ```
  hostname# machine backup schedule <время>
  ```

  Время задаётся в формате: `hh:mm`, где, `hh` — часы (24-часовой формат), `mm` — минуты.

- Укажите интервал времени:

  ```
  hostname# machine backup schedule <начало интервала>-<конец интервала>
  ```

  Формат: `hh:mm-hh:mm`

Время следующего резервного копирования выбирается случайным образом из указанного диапазона с округлением минут.

Чтобы просмотреть настройки резервного копирования:

```
hostname> machine show backup
```

На экран будут выведены:

- Статус автоматического резервного копирования: включено, выключено или недоступно.
- Информация о последнем резервном копировании на сервер ViPNet Prime.
- Время следующего автоматического резервного копирования.

Резервное копирование вручную

Чтобы однократно создать резервную копию на сервере ViPNet Prime или USB-носителе, выполните:

```
hostname# machine backup export {server | usb)
```

Восстановление из резервной копии индивидуальной конфигурации



Внимание! Восстановление настроек из резервной копии индивидуальной конфигурации возможно, если с момента создания этой копии на ViPNet Coordinator IG не были обновлены ключи обмена.

Алгоритм восстановления настроек зависит от состояния ViPNet Coordinator IG:

- В работоспособном состоянии ViPNet Coordinator IG вы можете восстановить настройки без удаления справочников и ключей.
- Если работоспособность ViPNet Coordinator IG нарушена, необходимо удалить справочники и ключи, затем восстановить настройки в ходе инициализации ViPNet Coordinator IG.

Оба алгоритма описаны ниже.

Если копия индивидуальной конфигурации хранится на сервере ViPNet Prime, скачайте её для восстановления настроек ViPNet Coordinator IG.

Восстановление настроек в работоспособном состоянии

1. Запишите копию индивидуальной конфигурации (файл `*.ecf`) на USB-носитель.
2. Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания:

   ```
   hostname# machine mode set service
   ```

3 Запустите импорт настроек:

```
hostname# machine config import
```

4 Подключите USB-носитель к ViPNet Coordinator IG и нажмите **Enter**.

5 Если на USB-носителе будет обнаружен только один файл `*.ecf` (и нет файлов `*.vbe`), он будет выбран автоматически. Если обнаружено несколько файлов конфигурации, в строке `Found several appliance configuration files` введите номер файла (`*.ecf`) из списка и нажмите **Enter**.

6 Дождитесь сообщения `Settings successfully imported. You may remove the USB drive.`

7 Отключите USB-носитель от ViPNet Coordinator IG.

8 Перезагрузите ViPNet Coordinator IG:

```
hostname# machine reboot
```

Восстановление настроек, когда работоспособность ViPNet Coordinator IG нарушена

1 Получите у администратора защищённой сети новый дистрибутив ключей для вашего ViPNet Coordinator IG.

Примечание. Если у вас есть старый дистрибутив ключей (полученный ранее), вы можете использовать его, если выполняются условия:

- Дистрибутив ключей был создан после того, как ViPNet Coordinator IG был впервые введён в эксплуатацию и подключён к ViPNet Prime.
- С момента создания этого дистрибутива ключей на ViPNet Coordinator IG не был обновлён ключ обмена для связи с ViPNet Prime и не был изменён способ аутентификации. Дату последней установки (обновления) ключа обмена вы можете просмотреть по команде `iplir show key-info` (см. атрибут `Key effective date`).

---

2 Запишите на USB-носитель:

- копию индивидуальной конфигурации (файл `*.ecf`);
- дистрибутив ключей (файл `*.ds5`).

3 Если ViPNet Coordinator IG не находится в режиме инициализации, удалите ключи на ViPNet Coordinator IG:

```
hostname# admin remove keys
```

В строке `Are you sure you want to execute this command? Continue? [Yes/No]` введите `Yes`.

4 Дождитесь приглашения ко вводу имени пользователя и начните инициализацию ViPNet Coordinator IG:

4.1 Выполните все шаги раздела «Начало инициализации» (см. документ «Подготовка к работе», раздел «Инициализация»).

4.2 Выполните шаги 1–4 раздела «Установка дистрибутива ключей» (см. документ «Подготовка к работе», раздел «Инициализация»).

5 Выберите загрузку конфигурации — в строке `Select the setup method` введите `2`.

6 Убедитесь, что USB-носитель с файлом индивидуальной конфигурации подключён к ViPNet Coordinator IG, и нажмите **Enter**.

- Если на USB-носителе будет обнаружен только один файл `*.ecf` (и нет файлов `*.vbe`), он будет выбран автоматически.
- Если обнаружено несколько файлов конфигурации, в строке `Found several appliance configuration files` введите номер файла (`*.ecf`) из списка.

  Если найдено больше 20 файлов, список выводится постранично.

7 Дождитесь сообщения `Host configuration successfully deployed.`

8 Отключите USB-носитель от ViPNet Coordinator IG.

9 Настройки аутентификации (включая пароль и сертификат локального администратора) восстановлены из файла индивидуальной конфигурации. В строке `Local authentication settings were imported from appliance configuration file. Overwrite them? [Yes/No]` введите:

- `Yes` — если вы хотите задать новый пароль или заменить сертификат;
- `No` — если вы хотите использовать пароль и сертификат, восстановленные из индивидуальной конфигурации.

10 Если на предыдущем шаге вы выбрали `Yes`:

10.1 В строке `Enter new admin password` задайте новый пароль, который будет использоваться для аутентификации локального администратора. Если используется аутентификация по сертификату, заданный пароль будет использоваться при доступе по SSH и HTTP/HTTPS. Подробнее см. документ «Подготовка к работе», раздел «Способы аутентификации».

В строке `Confirm new admin password` введите этот же пароль ещё раз.

10.2 Если в дистрибутиве ключей указано, что используется аутентификация по сертификату, появится сообщение `Insert token and press Enter`.

10.2.1 Подключите USB-токен, на который будет записан новый сертификат локального администратора, или на котором уже есть действующий сертификат, который вы хотите использовать для аутентификации локального администратора. Нажмите **Enter**.

10.2.2 В строке `Do you want to initialize token? [Yes/No]` введите `Yes` — для инициализации USB-токена и записи нового сертификата; или `No` — чтобы использовать текущий сертификат и PIN-код на USB-токене.



Внимание! В ходе инициализации USB-токена все данные на нём будут удалены.

10.2.3 Если вы выбрали инициализацию USB-токена, в строке `Enter admin-token pincode` введите PIN-код администратора USB-токена (см. документацию на USB-токен).



Внимание! Если вы введёте некорректный PIN-код администратора USB-токена несколько раз подряд, он будет заблокирован (максимальное количество попыток ввода см. в документации на USB-токен). После этого вы больше не сможете записать сертификат на этот USB-токен.

Затем в строке `Enter new user-token pincode` задайте PIN-код пользователя USB-токена и подтвердите его. Этот PIN-код будет использоваться локальным администратором при аутентификации на ViPNet Coordinator IG.

10.2.4 Если вы отказались от инициализации USB-токена, в строке `Enter user-token pincode` введите текущий PIN-код пользователя USB-токена. Сертификат из USB-токена запишется в память ViPNet Coordinator IG и будет использоваться для аутентификации локального администратора.

11 В строке `For the proper application of the recovered settings, you must reboot IG appliance. Do you want to reboot now? [Yes/No]` введите `Yes`. ViPNet Coordinator IG начнёт перезагрузку.

12 Если при инициализации вы использовали старый дистрибутив ключей, обеспечьте обновление справочников и ключей из ViPNet Prime.

Управление универсальной конфигурацией

Универсальная конфигурация позволяет переносить настройки с одного ViPNet Coordinator IG на другой. Оба ViPNet Coordinator IG должны быть одного исполнения, но могут отличаться версией ПО. Перенос настроек возможен с версии ПО, не ниже 4.3.2.

При экспорте настроек ViPNet Coordinator IG версии 5.2.0 универсальная конфигурация будет содержать следующие группы настроек:

- настройки межсетевого экрана (сетевые фильтры для всех режимов работы, правила трансляции адресов, группы объектов);
- настройки шлюзов Modbus;
- правила фильтрации промышленных протоколов;
- настройки интерфейса GPIO;
- настройки сетевых интерфейсов;
- таблицы и политики статической маршрутизации.

Файл универсальной конфигурации (`*.vbe`) зашифровывается на пароле, который задаётся при экспорте конфигурации.

Особенности импорта настроек

- При импорте настроек вы можете выбрать, какие группы настроек импортировать, а какие нет.
- Настройки, выбранные для импорта, можно добавить к текущим настройкам на ViPNet Coordinator IG или заменить их. Возможность добавления настроек доступна не для всех групп.
- Если конфигурация была создана в ViPNet Coordinator IG, работающем как межсетевой экран типа «Д»:
  - в ViPNet Coordinator IG с типом «Д» импортируются сетевые фильтры для всех режимов;
  - в ViPNet Coordinator IG с типом «А/Б» импортируются сетевые фильтры только из того режима, в котором эта конфигурация была создана.
- Если конфигурация была создана в ViPNet Coordinator IG, работающем как межсетевой экран типа «А/Б», сетевые фильтры импортируются в штатный режим работы независимо от типа межсетевого экрана на вашем ViPNet Coordinator IG.
- При импорте настроек шлюза Modbus:
  - Если конфигурация была создана в ViPNet Coordinator IG, поддерживающем только один шлюз Modbus:

- при выборе замены настроек, они переносятся на первый последовательный интерфейс подходящего типа (RS-232 или RS-485) с присвоением имени шлюза `modbus1`;
- при выборе добавления настроек, они переносятся на свободный последовательный интерфейс подходящего типа с присвоением имени шлюза `modbus1` или `modbus2`. Если свободного интерфейса нет, настройки не переносятся.

  - Если конфигурация была создана в ViPNet Coordinator IG, поддерживающем несколько шлюзов Modbus:
    - при выборе замены настроек, они переносятся на соответствующие последовательные интерфейсы подходящего типа без замены имён шлюзов;
    - при выборе добавления настроек, они переносятся на свободные последовательные интерфейсы подходящего типа с присвоением имени шлюза `modbus<свободный порядковый номер>`. Если свободного интерфейса нет, настройки не переносятся.
  - Если добавляемый маршрут содержит адрес Modbus-устройства, для которого уже заданы маршруты, такой маршрут не будет добавлен.

- При импорте правил фильтрации промышленных протоколов:
  - Если имя добавляемого набора правил совпадает с именем существующего набора правил, такой набор правил будет добавлен с дополнительным суффиксом в имени.
  - Если содержимое добавляемого набора правил совпадает с существующим набором правил, такой набор не будет добавлен.

Экспорт универсальной конфигурации

Чтобы экспортировать универсальную конфигурацию на USB-носитель:

1 Выполните:

```
hostname# machine config export usb
```

2 Добавьте описание конфигурации:

2.1 В строке `Do you want to add configuration description [Yes/No]` введите `y` и нажмите **Enter**.

2.2 В строке `Description` введите текст описания (до 512 символов UTF-8) и нажмите **Enter**.

3 В строке `Enter password for encryption` введите пароль, на котором будет зашифрован файл конфигурации, и нажмите **Enter**. Разрешённые символы: `A-Z`, `a-z`, `0-9`, специальные символы. Длина пароля — от 8 до 31 символа.

4 При появлении сообщения `Insert USB drive with at least 1.7 MB free space and press Enter` подключите USB-носитель к ViPNet Coordinator IG и нажмите **Enter**.

5 Дождитесь завершения экспорта и отключите USB-носитель.

Шаблон имени файла универсальной конфигурации: `<имя сетевого узла>-<время создания файла>.vbe`.

Формат времени создания файла: `YYYYMMDDTHHMMSSZ`, где `YYYY` — год, `MM` — месяц, `DD` — день, `HH` — час, `MM` — минуты, `SS` — секунды. Время записывается в системе UTC.

Импорт настроек универсальной конфигурации

Вы можете импортировать настройки:

- когда на ViPNet Coordinator IG уже установлены справочники и ключи;
- или в ходе инициализации ViPNet Coordinator IG.



Примечание. Если на ViPNet Coordinator IG установлены справочники и ключи, но его работоспособность нарушена, импортируйте настройки в ходе инициализации ViPNet Coordinator IG. Чтобы переключить ViPNet Coordinator IG в режим инициализации, удалите справочники и ключи:

```
hostname# admin remove keys
```

Импорт настроек на ViPNet Coordinator IG с установленными справочниками и ключами

1 Запишите файл универсальной конфигурации (файл `*.vbe`) на USB-носитель.

2 Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания:

```
hostname# machine mode set service
```

3 Запустите импорт настроек:

```
hostname# machine config import
```

4 Подключите USB-носитель к ViPNet Coordinator IG и нажмите **Enter**.

5 Введите номер файла универсальной конфигурации из списка обнаруженных на USB-носителе и нажмите **Enter**.

6 В строке `Enter configuration password` введите пароль, на котором зашифрован файл универсальной конфигурации, и нажмите **Enter**.

7 Выберите импортируемые настройки:



Примечание. Если у вас одно из исполнений ViPNet Coordinator IG10, и вы хотите импортировать все настройки, рекомендуется сделать это в два этапа: сначала импортируйте одну часть настроек (например, шаги 7.1–7.3), затем после шага 10 повторите сценарий импорта (3–11), но на шаге 7 импортируйте оставшуюся часть настроек (7.4–7.6).

7.1 Чтобы импортировать настройки межсетевого экрана, в строке `Firewall [Yes/No]` введите `y` и нажмите **Enter**.

Выберите способ импорта: `a` — добавить или `r` — заменить, и нажмите **Enter**.

7.2 Чтобы импортировать настройки и маршруты шлюзов Modbus, в строке `Modbus Gateway [Yes/No]` введите `y` и нажмите **Enter**.

Выберите способ импорта маршрутов для Modbus-устройств: `a` — добавить или `r` — заменить, и нажмите **Enter**.

7.3 Чтобы импортировать правила фильтрации промышленных протоколов, в строке `Industrial protocol filtration settings [Yes/No]` введите `y` и нажмите **Enter**.

Выберите способ импорта: `a` — добавить или `r` — заменить, и нажмите **Enter**.

7.4 Чтобы импортировать настройки интерфейса GPIO, в строке `General-purpose input/output settings (GPIO) [Yes/No]` введите `y` и нажмите **Enter**.

7.5 Чтобы импортировать настройки сетевых интерфейсов, в строке `Network-interface settings [Yes/No]` введите `y` и нажмите **Enter**.

7.6 Чтобы импортировать таблицы и политики статической маршрутизации, в строке `Static routing settings [Yes/No]` введите `y` и нажмите **Enter**.

Выберите способ импорта: `a` — добавить или `r` — заменить, и нажмите **Enter**.

8 Дождитесь сообщения `Settings successfully imported. You may remove the USB drive.`

9 Отключите USB-носитель от ViPNet Coordinator IG.

10 Перезагрузите ViPNet Coordinator IG:

```
hostname# machine reboot
```

11 Если установлен режим межсетевого экрана типа «Д», переключите ViPNet Coordinator IG обратно в штатный режим работы:

```
hostname# machine mode set normal
```

Импорт настроек при инициализации ViPNet Coordinator IG

1 Получите у администратора защищённой сети новый дистрибутив ключей для вашего ViPNet Coordinator IG.

Примечание. Если у вас есть старый дистрибутив ключей (полученный ранее), вы можете использовать его, если выполняются условия:

- Дистрибутив ключей был создан после того, как ViPNet Coordinator IG был впервые введён в эксплуатацию и подключён к ViPNet Prime.
- С момента создания этого дистрибутива ключей на ViPNet Coordinator IG не был обновлён ключ обмена для связи с ViPNet Prime и не был изменён способ аутентификации. Дату последней установки (обновления) ключа обмена вы можете просмотреть по команде `iplir show key-info` (см. атрибут `Key effective date`).

---

2 Запишите на USB-носитель:

- Файл универсальной конфигурации (файл `*.vbe`).
- Дистрибутив ключей ViPNet Coordinator IG (файл `*.ds5`).

3 Начните инициализацию ViPNet Coordinator IG:

3.1 Выполните все шаги раздела «Начало инициализации» документа «Подготовка к работе».

3.2 Выполните шаги 1–4 раздела «Установка дистрибутива ключей» документа «Подготовка к работе».

4 Выберите загрузку конфигурации — в строке `Select the setup method` введите `2` и нажмите **Enter**.

5 Убедитесь, что USB-носитель с файлом универсальной конфигурации подключён к ViPNet Coordinator IG, и нажмите **Enter**.

- Если на USB-носителе обнаружен только один файл `*.vbe` (и нет файлов `*.ecf`), он будет выбран автоматически.
- Если обнаружено несколько файлов конфигурации, в строке `Found several appliance configuration files` введите номер файла из списка и нажмите **Enter**.

  Если найдено больше 20 файлов, список выводится постранично.

6 В строке `Enter configuration password` введите пароль к выбранной конфигурации и нажмите **Enter**.

7 Выберите импортируемые настройки:



Примечание. Если у вас одно из исполнений ViPNet Coordinator IG10, и вы хотите импортировать все настройки, рекомендуется сделать это в два этапа: сначала импортируйте одну часть настроек (например, шаги 7.1–7.3), затем после завершения инициализации импортируйте оставшуюся часть настроек с помощью команды `machine config import` (см. сценарий «Импорт настроек на ViPNet Coordinator IG с установленными справочниками и ключами» выше).

7.1 Чтобы импортировать настройки межсетевого экрана, в строке `Firewall [Yes/No]` введите `y` и нажмите **Enter**.

7.2 Чтобы импортировать настройки и маршруты шлюза Modbus, в строке `Modbus Gateway [Yes/No]` введите `y` и нажмите **Enter**.

7.3 Чтобы импортировать правила фильтрации промышленных протоколов, в строке `Industrial protocol filtration settings [Yes/No]` введите `y` и нажмите **Enter**.

7.4 Чтобы импортировать настройки интерфейса GPIO, в строке `General-purpose input/output settings (GPIO) [Yes/No]` введите `y` и нажмите **Enter**.

7.5 Чтобы импортировать настройки сетевых интерфейсов, в строке `Network-interface settings [Yes/No]` введите `y` и нажмите **Enter**.

7.6 Чтобы импортировать таблицы и политики статической маршрутизации, в строке `Static routing settings [Yes/No]` введите `y` и нажмите **Enter**.

8 Дождитесь сообщения `Host configuration successfully deployed.`

9 Отключите USB-носитель от ViPNet Coordinator IG.

10 В строке `Enter new admin password` задайте новый пароль для локальной учётной записи администратора `admin`.

В строке `Confirm new admin password` введите пароль ещё раз.

11 Если в дистрибутиве ключей указано, что используется аутентификация по сертификату, появится сообщение `Insert token and press Enter`.

11.1 Подключите USB-токен, на который вы хотите записать новый сертификат администратора с локальной учётной записью `admin`, или на котором уже есть действующий сертификат такого администратора, если вы хотите продолжить использовать его для аутентификации на ViPNet Coordinator IG. Нажмите **Enter**.

11.2 В строке `Do you want to initialize token? [Yes/No]` введите `Yes` — для инициализации USB-токена и записи нового сертификата; или `No` — чтобы использовать текущий сертификат и PIN-код на USB-токене.



Внимание! В ходе инициализации USB-токена все данные на нём будут удалены.

11.3 Если вы выбрали инициализацию USB-токена, в строке `Enter admin-token pincode` введите PIN-код администратора USB-токена (см. документацию на USB-токен).



Внимание! Если вы введёте некорректный PIN-код администратора USB-токена несколько раз подряд, он будет заблокирован (максимальное количество попыток ввода см. в документации на USB-токен). После этого вы больше не сможете записать сертификат на этот USB-токен.

Затем в строке `Enter new user-token pincode` задайте новый PIN-код пользователя USB-токена и подтвердите его. Этот PIN-код будет использоваться при локальной аутентификации администратора на ViPNet Coordinator IG.

11.4 Если вы отказались от инициализации USB-токена, в строке `Enter user-token pincode` введите текущий PIN-код пользователя USB-токена. Сертификат из USB-токена запишется в память ViPNet Coordinator IG и будет использоваться для аутентификации администратора.

12 В строке `For the proper application of the recovered settings, you must reboot IG appliance. Do you want to reboot now? [Yes/No]` введите `Yes` и нажмите **Enter**. ViPNet Coordinator IG перезагрузится.

13 Если при инициализации вы использовали старый дистрибутив ключей, обеспечьте обновление справочников и ключей из ViPNet Prime.

14

Обновление и восстановление программного обеспечения

Обновление ПО с версий 4.5.x до версии 5.2.0 286

Обновление ПО с версий 5.1.x до версии 5.2.0 296

Восстановление ПО ViPNet Coordinator IG 301

Обновление ПО с версий 4.5.x до версии 5.2.0

Внимание!

- Во время обновления ПО ViPNet Coordinator IG не выполняет свои функции.
- Обеспечьте гарантированное питание ViPNet Coordinator IG на время обновления ПО. Иначе ViPNet Coordinator IG может выйти из строя.
- Реализация алгоритмов шифрования ГОСТ 34.12–2018 «Магма» и «Кузнечик» в ViPNet Coordinator IG 5.2.0 несовместима с ViPNet Coordinator HW версий ниже 5.3.1. Чтобы избежать потери связанности между координаторами после обновления ПО, спланируйте одновременное обновление ViPNet Coordinator IG до версии 5.2.0 и ViPNet Coordinator HW до версии 5.3.1 или выше.

Условия обновления

- Текущая версия ПО — не ниже 4.5.x.

  Для более ранних версий обновите ПО последовательно: 4.3.3 > 4.5.1 > 5.2.0.
- Обновление доступно для исполнений:
  - ViPNet Coordinator IG10 I1;
  - ViPNet Coordinator IG10 I2;
  - ViPNet Coordinator IG100 I1;
  - ViPNet Coordinator IG100 I4;
  - ViPNet Coordinator IG100 I5.
- В качестве управляющего ПО используется ViPNet Prime.

Особенности обновления

- В ViPNet Coordinator IG 4.5.x и 5.2.0 используются разные алгоритмы шифрования, поэтому после обновления ПО необходимо выполнить инициализацию ViPNet Coordinator IG с помощью нового дистрибутива ключей (`ds5`). При этом:
  - устанавливаются новые справочники и ключи;
  - задаётся новый пароль администратора;
  - способ аутентификации пользователей выбирается автоматически из дистрибутива ключей.

Внимание! Инициализация выполняется локально, даже если обновление ПО было запущено удалённо из ViPNet Prime.

- Перед обновлением ПО на ViPNet Coordinator IG автоматически выполняется проверка ЭП файла обновления. Для этого необходимо наличие на ViPNet Coordinator IG актуального списка аннулированных сертификатов (далее — CRL). Срок действия CRL — 1 год. Если на момент обновления ПО срок действия CRL уже истечёт, обновление не выполнится. Чтобы избежать этого, получите от представителей ИнфоТеКС актуальный CRL и загрузите его на ViPNet Coordinator IG до обновления ПО с помощью команды: `service cert import`.
- В версии 5.2.0 по сравнению с 4.5.x некоторые функции ViPNet Coordinator IG лицензируются отдельно. Если в ViPNet Prime нет лицензий на такие функции или они выключены, работа таких функций в ViPNet Coordinator IG будет ограничена как при истечении срока действия соответствующих лицензий (см. документ «Подготовка к работе», раздел «Лицензирование»).
- Исполнения ViPNet Coordinator IG10 I1 и ViPNet Coordinator IG10 I2 с ПО версии 5.2.0 не могут управляться с помощью веб-интерфейса. Используйте командный интерпретатор.
- Будут сброшены настройки VPN:
  - видимость узлов сети ViPNet и туннелируемых узлов;
  - режим подключения к внешней сети;
  - состояние и порт сервера TCP-туннелей;
  - диапазон туннелируемых адресов;
  - диапазон присваиваемых виртуальных адресов;
  - L2OverIP (сетевые интерфейсы, номера портов, IP-адреса своего и удалённого координатора, время жизни MAC-адреса).
- Настраиваемые сетевые фильтры `Allow ViPNet base services` и `Allow ViPNet MFTP` конвертируются в служебные фильтры `Allow ViPNet base services in`, `Allow ViPNet base services out`, `Allow ViPNet MFTP in`, `Allow ViPNet MFTP out`.
- Начиная с версии ПО 5.2.0, не поддерживается автоматическое определение видимости узлов и сетей. После обновления ПО настройки видимости будут преобразованы: значения `auto` в параметрах конфигурационного файла `iplir.conf`, отвечающих за настройку видимости, будут заменены на `virtual` или `real`.
- Системный журнал в ПО версий 4.5.x архивируется. На время обновления включается локальное ведение журнала. Если ведение журнала было выключено, оно включается.
- Транспортный сервер MFTP переключается в транзитный режим работы (пересылка транспортных конвертов).
- Вы можете запустить обновление ПО локально или удалённо из ViPNet Prime.



Совет. После обновления ПО до версии 5.2.0 вы можете записать в память ViPNet Coordinator IG серийный номер, указанный на его этикетке. Это позволит просматривать серийный номер вашего ViPNet Coordinator IG без физического доступа к устройству.

Обновление системного загрузчика

Для обновления ПО необходимо, чтобы на вашем ViPNet Coordinator IG был установлен системный загрузчик, совместимый с ПО версии 5.2.0. Этот загрузчик уже содержится в файле обновления ПО до версии 5.2.0. Если при обновлении будет обнаружена несовместимая версия загрузчика на ViPNet Coordinator IG, сначала будет обновлён загрузчик, а затем ПО.

Подготовка к обновлению 4.5.x > 5.2.0

1 Ознакомьтесь с условиями и особенностями обновления ПО с версий 4.5.x до версии 5.2.0.

2 Подготовьте USB-носитель с файловой системой FAT32, ext2, ext3 или ext4.

3 Для локального обновления:

3.1 Получите у администратора защищённой сети:

- Файл обновления `*.lzh`.
- Дистрибутив ключей `*.ds5`.

3.2 Запишите файл обновления и дистрибутив ключей на USB-носитель.

Примечание. На один USB-носитель вы можете записать файлы обновления для разных исполнений ViPNet Coordinator IG, разместив их в разных каталогах. При обновлении будет доступен только файл для вашего исполнения.

---

4 Для удалённого обновления:

4.1 Получите у администратора защищённой сети дистрибутив ключей `*.ds5`.

4.2 Запишите дистрибутив ключей на USB-носитель.

5 На случай восстановления ПО и возврата к версии 4.5.x, экспортируйте:

- справочники, ключи и настройки;

Примечание. При работе ViPNet Coordinator IG в режиме кластера мы рекомендуем экспортировать справочники, ключи и настройки с каждого узла кластера. Это поможет быстрее восстановить настройки.

- журнал IP-пакетов;
- журнал пакетов промышленных протоколов;
- системный журнал.

Порядок экспорта см. в документе «Настройка с помощью командного интерпретатора» для версии 4.5.x.

Локальное обновление 4.5.x > 5.2.0

После обновления ПО ViPNet Coordinator IG будет находиться в режиме инициализации. Для восстановления его работоспособности необходимо выполнить инициализацию.

Обновление

1 Подключитесь к ViPNet Coordinator IG с помощью консоли.

2 Войдите как пользователь и включите режим администратора:

```
hostname> enable
```

3 Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания:

```
hostname# machine set mode service
```

4 Убедитесь, что запущена служба `failoverd` и ViPNet Coordinator IG не работает под нагрузкой:

```
hostname# failover show info
```

5 Для исполнений ViPNet Coordinator IG10 остановите работу прикладных служб:

```
service http-proxy stop
inet snmp stop
inet ntp stop
inet dns stop
inet dhcp server stop
inet dhcp relay stop
service piomonitor stop
service mbgw stop
```

6 Запустите обновление:

```
hostname# admin upgrade software usb
```

7 Подключите USB-носитель с файлом обновления и дистрибутивом ключей. Нажмите **Enter**:

```
Insert USB flash drive into empty USB slot and press <Enter>
```

8 Введите номер файла обновления из списка и нажмите **Enter**:

```
Select file to use for software upgrade:
1 — /mnt/tmp/sdb1/ig100_vipnet_base_arm_driv_5.2.0-120.lzh
Enter file number [1-1] or [q] to cancel: 1
Starting local upgrade...
```

Перед обновлением будет автоматически проверена ЭП файла обновления. Если подпись окажется недействительной, обновление не будет выполнено.

9 Если для обновления ПО требуется обновить системный загрузчик, появится сообщение:

```
Current u-boot version is unsupported new software version.
Need upgrade u-boot.
```

```
It is necessary to provide continuous power during the update. Do you want to upgrade
u-boot to <номер версии>? [Yes/No]
```

Введите `y` и нажмите **Enter**.

Если в сообщении сказано, что системный загрузчик поддерживается новой версией ПО, но файл обновления содержит более новый загрузчик, мы рекомендуем согласиться с его обновлением на новую версию.

10 Подтвердите, что вы экспортировали справочники, ключи и настройки перед обновлением ПО — введите `y` и нажмите **Enter**:

```
WARNING!
You are going to upgrade software to the version 5.
Downgrade to previous versions is not supported.
The saved software configurations will be deleted.
We strongly recommend to create VBE-backup before proceeding.
In order to create VBE-backup, you need to use the following command:
admin export keys binary-encrypted usb | tftp
Are you sure you want to proceed upgrade? [Yes/No] y
```

Далее выполните инициализацию ViPNet Coordinator IG (см. ниже).

Инициализация

1 В строке приглашения введите:

- имя пользователя — `user`;
- пароль — `user`.

2 Примите условия лицензионного соглашения — введите `y`.

3 В строке `Would you like to start installing keys/restoring configutarion` введите `y`.

4 Для установки дистрибутива ключей с USB-носителя в строке `Would you like to install appliance initialization file from TFTP, USB storage device` введите `u`.

5 Если на носителе только один файл `*.ds5`, он будет выбран для установки автоматически. Если файлов несколько, выберите нужный из списка `Found several appliance initialization files`.

6 При появлении сообщения о смене идентификатора узла `Node ID in the appliance initialization file does not match current Node ID. With the change of Node ID all VPN settings will be deleted. Do you really want to change Node ID` — введите `Yes`.

В ViPNet Prime версии 1.9.11 или выше есть возможность сохранить идентификатор узла ViPNet Coordinator IG, но в этом случае указанное выше сообщение всё-равно появится и настройки VPN будут сброшены (см. особенности обновления в разделе Обновление ПО с версий 4.5.x до версии 5.2.0).

7 В строке `Enter password` введите пароль к дистрибутиву ключей, который вы получили от администратора защищённой сети.

При вводе пароля на экране не отображаются вводимые символы, а курсор остаётся неподвижным.

8 В строке `Enter new admin password` задайте пароль для локальной учётной записи администратора `admin` на ViPNet Coordinator IG.

В строке `Confirm new admin password` введите пароль ещё раз.

9 Если в дистрибутиве ключей указано, что используется аутентификация по сертификату, появится сообщение `Insert token and press Enter`.

9.1 Подключите USB-токен, на который будет записан сертификат администратора для аутентификации под локальной учётной записью `admin`, и нажмите **Enter**.



Внимание! На следующем шаге все данные на USB-токене будут удалены.

9.2 Инициализируйте USB-токен — в строке `Do you want to initialize token? [Yes/No]` введите `y`.

9.3 В строке `Enter admin-token PIN` введите PIN-код администратора USB-токена (см. документацию на USB-токен).



Внимание! Если вы введёте некорректный PIN-код администратора USB-токена несколько раз подряд, он будет заблокирован (максимальное количество попыток ввода см. в документации на USB-токен). После этого вы больше не сможете записать сертификат на этот USB-токен.

9.4 В строке `Enter new user-token PIN` задайте PIN-код пользователя USB-токена и подтвердите его. Этот PIN-код будет использоваться при аутентификации администратора на ViPNet Coordinator IG.

10 Запустите драйверы и службы:

В строке `Do you want to start VPN services before leaving the installation wizard` введите `y`.

11 Дождитесь сообщений:

```
ViPNet Coordinator IG successfully deployed!
Press Enter to proceed to authentication form.
```

После чего нажмите **Enter** для запуска командного интерпретатора.

12 Отключите USB-носитель от ViPNet Coordinator IG.

13 Войдите под локальной учётной записью `admin` с помощью пароля или USB-токена — в зависимости от способа аутентификации, заданного в дистрибутиве ключей.

14 Проверьте версию ПО:

```
hostname# version
```

15 Перезагрузите ViPNet Coordinator IG для завершения настройки системных служб:

```
hostname# machine reboot
```

Если до обновления вы управляли ViPNet Coordinator IG с помощью веб-интерфейса, очистите кеш браузера.

Удалённое обновление 4.5.x > 5.2.0

Удалённое обновление запускается из ViPNet Prime (см. документ «ViPNet Prime. Руководство администратора»). После завершения обновления, необходимо выполнить инициализацию ViPNet Coordinator IG локально.



Внимание! Если на ViPNet Coordinator IG недостаточно места на диске, то обновление не выполнится, а в ViPNet Prime отправится транспортная квитанция «искажение».

Перед обновлением

1. Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», то перед рассылкой обновлений из ViPNet Prime переключите ViPNet Coordinator IG в режим регламентного обслуживания:

   ```
   hostname# machine set mode service
   ```

   Переключить режим работы можно также удалённо из ViPNet Prime Policy Management.

2. Убедитесь, что ViPNet Coordinator IG не работает под нагрузкой. Иначе обновление может быть не принято.

   Уровень нагрузки на процессор вы можете посмотреть по команде:

   ```
   hostname# failover show info
   ```

3. Для исполнений ViPNet Coordinator IG10 остановите работу прикладных служб:

   ```
   service http-proxy stop
   inet snmp stop
   inet ntp stop
   inet dns stop
   inet dhcp server stop
   inet dhcp relay stop
   service piomonitor stop
   service mbgw stop
   ```

Теперь вы можете сообщить администратору защищённой сети, что ViPNet Coordinator IG готов к обновлению. Процедура обновления ПО может длиться до 15 минут.

После обновления

Чтобы завершить обновление ПО:

1. Подключитесь к ViPNet Coordinator IG с помощью консоли.

2 Выполните инициализацию ViPNet Coordinator IG (см. подраздел «Инициализация» в сценарии Локальное обновление 4.5.x > 5.2.0).

Обновление на кластере 4.5.x > 5.2.0

Вы можете запустить обновление ПО ViPNet Coordinator IG локально или удалённо из ViPNet Prime.

Локальное обновление

1 Отключите пассивный узел (далее — узел 1) от сети и от активного узла (далее — узел 2).

2 Обновите ПО на узле 1 и выполните его инициализацию.

3 Убедитесь в стабильной работе узла:

3.1 Проверьте текущее состояние служб:

```
hostname# failover show info
```

Все службы должны быть запущены, система защиты от сбоев должна работать в режиме кластера.

3.2 В течение некоторого времени (около 15 минут) понаблюдайте за работой узла и убедитесь, что он не перезагружается.

4 Отключите узел 2 от сети.

5 Подключите узел 1 к сети.

6 Переключите узел 1 в активный режим:

```
hostname# failover stop
hostname# failover start active
```

7 Обновите ПО на узле 2 и выполните его инициализацию. При инициализации обратите внимание:

- На шаге 8 при задании пароля администратора введите тот же пароль, который вы задали при инициализации первого узла кластера.
- Если используется аутентификация по сертификату, на шаге 9.1 подключите новый USB-токен локального администратора для записи сертификата. На каждом узле кластера издаётся свой сертификат и записывается на отдельный USB-токен. Сертификаты пользователей не синхронизируются между узлами кластера.

8 Убедитесь в стабильной работе узла 2 (см. шаг 3).

9 На узле 2 остановите работу службы `failoverd`:

```
hostname# failover stop
```

10 Подключите узел 2 к сети.

11 Соедините интерфейсы синхронизации обоих узлов кластера.

12 На узле 2 запустите службу `failoverd` в пассивном режиме:

```
hostname# failover start passive
```

13 Убедитесь, что синхронизация работает:

13.1 Убедитесь, что резервирование группы файлов конфигурации включено:

```
hostname# failover show config
```

В секции `[sendconfig]` параметр `config` должен иметь значение `yes`.

13.2 Измените какую-либо настройку в конфигурационном файле на активном узле.

13.3 Через некоторое время проверьте наличие этих же изменений на пассивном узле.

Удалённое обновление



Внимание! По завершении удалённого обновления ПО оба узла кластера будут находиться в режиме инициализации и не будут выполнять своих функций. Для восстановления работоспособности кластера необходимо локально подключиться к каждому из узлов и выполнить инициализацию.

Если требуется обновить ПО, не приостанавливая обработку информации, выполните обновление локально на каждом из узлов кластера, начиная с пассивного.

Перед обновлением выполните действия на активном узле кластера:

1 Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», то перед рассылкой обновлений на ViPNet Coordinator IG переключите его в режим регламентного обслуживания:

```
hostname# machine set mode service
```

Переключить режим работы можно также удалённо из ViPNet Prime Policy Management.

2 Убедитесь, что ViPNet Coordinator IG не работает под нагрузкой. Иначе обновление может быть не принято.

Уровень нагрузки на процессор вы можете посмотреть по команде:

```
hostname# failover show info
```

3 Для исполнений ViPNet Coordinator IG10 остановите работу прикладных служб:

```
service http-proxy stop
inet snmp stop
inet ntp stop
inet dns stop
inet dhcp server stop
inet dhcp relay stop
service piomonitor stop
service mbgw stop
```

Теперь вы можете сообщить администратору защищённой сети, что ViPNet Coordinator IG готов к обновлению. Процедура обновления ПО может длиться до 15 минут.

Внимание! Если на ViPNet Coordinator IG недостаточно места на диске, то обновление не выполнится, а в ViPNet Prime отправится транспортная квитанция «искажение».

Чтобы завершить обновление ПО, необходимо выполнить инициализацию обоих узлов кластера. Для этого по очереди для каждого узла кластера:

1. Подключитесь к ViPNet Coordinator IG с помощью консоли.
2. Выполните инициализацию ViPNet Coordinator IG (см. подраздел «Инициализация» в сценарии Локальное обновление 4.5.x > 5.2.0). Обратите внимание, что при инициализации второго узла кластера:
   - На шаге 8 при задании пароля администратора введите тот же пароль, который вы задали при инициализации первого узла кластера.
   - Если используется аутентификация по сертификату, на шаге 9.1 подключите новый USB-токен локального администратора для записи сертификата. На каждом узле кластера издаётся свой сертификат и записывается на отдельный USB-токен. Сертификаты пользователей не синхронизируются между узлами кластера.

Активным узлом кластера станет узел, на котором служба `failoverd` будет запущена первой.

Обновление ПО с версий 5.1.x до версии 5.2.0

Внимание!

- Во время обновления ПО ViPNet Coordinator IG не выполняет свои функции.
- Обеспечьте гарантированное питание ViPNet Coordinator IG на время обновления ПО. Иначе ViPNet Coordinator IG может выйти из строя.
- Реализация алгоритмов шифрования ГОСТ 34.12–2018 «Магма» и «Кузнечик» в ViPNet Coordinator IG 5.2.0 несовместима с ViPNet Coordinator HW версий ниже 5.3.1. Чтобы избежать потери связанности между координаторами после обновления ПО, спланируйте одновременное обновление ViPNet Coordinator IG до версии 5.2.0 и ViPNet Coordinator HW до версии 5.3.1 или выше.

Особенности обновления

- Перед обновлением ПО на ViPNet Coordinator IG автоматически выполняется проверка ЭП файла обновления. Для этого необходимо наличие на ViPNet Coordinator IG актуального списка аннулированных сертификатов (далее — CRL). Срок действия CRL — 1 год. Если на момент обновления ПО срок действия CRL уже истечёт, обновление не выполнится. Чтобы избежать этого, получите от представителей ИнфоТеКС актуальный CRL и загрузите его на ViPNet Coordinator IG до обновления ПО с помощью команды: `service cert import`.
- Начиная с версии ПО 5.2.0, не поддерживается автоматическое определение видимости узлов и сетей. После обновления ПО настройки видимости будут преобразованы: значения `auto` в параметрах конфигурационного файла `iplir.conf`, отвечающих за настройку видимости, будут заменены на `virtual` или `real`.
- Вы можете обновить ПО ViPNet Coordinator IG локально или удалённо из ViPNet Prime.

Совет. После обновления ПО до версии 5.2.0 вы можете записать в память ViPNet Coordinator IG серийный номер, указанный на его этикетке. Это позволит просматривать серийный номер вашего ViPNet Coordinator IG без физического доступа к устройству.

Обновление системного загрузчика

Для обновления ПО необходимо, чтобы на вашем ViPNet Coordinator IG был установлен системный загрузчик, совместимый с ПО версии 5.2.0. Этот загрузчик уже содержится в файле обновления ПО до версии 5.2.0. Если при обновлении будет обнаружена несовместимая версия загрузчика на ViPNet Coordinator IG, сначала будет обновлён загрузчик, а затем ПО.

Подготовка к обновлению 5.1.x > 5.2.0

1 На случай возникновения ошибок при обновлении ПО, экспортируйте журналы на USB-носитель:

   - журнал IP-пакетов;
   - журнал пакетов промышленных протоколов;
   - системный журнал, журналы аудита и СКЗИ.

   Порядок экспорта см. в документе «Настройка с помощью командного интерпретатора» для версии 5.1.x.

2 Для локального обновления:

   2.1 Получите у администратора защищённой сети:

   - Файл обновления `*.zip`.
   - Файл электронной подписи `*.sig`.

   2.2 Запишите оба файла на USB-носитель с файловой системой FAT32, ext2, ext3 или ext4.



Примечание. На один USB-носитель вы можете записать файлы обновления для разных исполнений ViPNet Coordinator IG, разместив их в разных каталогах. При обновлении будет доступен только файл для вашего исполнения.

Локальное обновление 5.1.x > 5.2.0

1 Подключитесь к ViPNet Coordinator IG с помощью консоли.

2 Войдите как локальный администратор `admin`.

3 Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», переключите его в режим регламентного обслуживания:

```
hostname# machine mode set service
```

4 Убедитесь, что запущена служба `failoverd` и ViPNet Coordinator IG не работает под нагрузкой:

```
hostname# failover show info
```

5 Для исполнений ViPNet Coordinator IG10 остановите работу прикладных служб:

```
service http-proxy stop
inet snmp stop
inet ntp stop
inet dns stop
inet dhcp server stop
inet dhcp relay stop
service piomonitor stop
```

```
service mbgw stop
```

6 Запустите обновление:

```
hostname# admin upgrade software
```

7 Подключите USB-носитель с файлом обновления и нажмите **Enter**:

```
Insert USB flash drive into empty USB slot and press <Enter>
```

8 Введите номер файла обновления из списка и нажмите **Enter**:

```
Select file to use for software upgrade:
1 – /mnt/tmp/sdb1/ig100_vipnet_base_x86_64_driv_5.2.0-265.zip
Enter file number [1-1] or [q] to cancel: 1
Starting local upgrade...
```

Перед обновлением будет автоматически проверена ЭП файла обновления. Если подпись окажется недействительной, обновление не будет выполнено.

Процесс обновления ПО может длиться до 15 минут.

9 Если для обновления ПО требуется обновить системный загрузчик, появится сообщение:

```
Current u-boot version is unsupported new software version.
Need upgrade u-boot.
It is necessary to provide continuous power during the update. Do you want to upgrade
u-boot to <номер версии>? [Yes/No]
```

Введите `y` и нажмите **Enter**.

Если в сообщении сказано, что системный загрузчик поддерживается новой версией ПО, но файл обновления содержит более новый загрузчик, мы рекомендуем согласиться с его обновлением на новую версию.

10 После появления приглашения входа отключите USB-носитель от ViPNet Coordinator IG.

11 Войдите как локальный администратор `admin`.

12 Проверьте версию ПО:

```
hostname# version
```

13 Перезагрузите ViPNet Coordinator IG для завершения настройки системных служб:

```
hostname# machine reboot
```

Удалённое обновление 5.1.x > 5.2.0

Удалённое обновление запускается из ViPNet Prime (см. документ «ViPNet Prime. Руководство администратора»).



Внимание! Если на ViPNet Coordinator IG недостаточно места на диске, то обновление не выполнится, а в ViPNet Prime отправится транспортная квитанция «искажение».

Перед обновлением

1. Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», то перед рассылкой обновлений из ViPNet Prime переключите ViPNet Coordinator IG в режим регламентного обслуживания:

   ```
   hostname# machine mode set service
   ```

   Переключить режим работы можно также удалённо из ViPNet Prime Policy Management.

2. Убедитесь, что ViPNet Coordinator IG не работает под нагрузкой. Иначе обновление может быть не принято.

   Уровень нагрузки на процессор вы можете посмотреть по команде:

   ```
   hostname# failover show info
   ```

3. Для исполнений ViPNet Coordinator IG10 остановите работу прикладных служб:

   ```
   service http-proxy stop
   inet snmp stop
   inet ntp stop
   inet dns stop
   inet dhcp server stop
   inet dhcp relay stop
   service piomonitor stop
   service mbgw stop
   ```

Теперь вы можете сообщить администратору защищённой сети, что ViPNet Coordinator IG готов к обновлению. Процедура обновления ПО может длиться до 15 минут.

После обновления

1. Для завершения настройки системных служб перезагрузите ViPNet Coordinator IG:

   ```
   hostname> machine reboot
   ```

2. Если до обновления вы управляли ViPNet Coordinator IG с помощью веб-интерфейса, очистите кеш браузера.

Обновление на кластере 5.1.x > 5.2.0

Вы можете выполнить обновление ПО ViPNet Coordinator IG локально или удалённо из ViPNet Prime.

Локальное обновление

1. Отключите пассивный узел (далее — узел 1) от сети и от активного узла (далее — узел 2).
2. Обновите ПО на узле 1 (см. Локальное обновление 5.1.x > 5.2.0).
3. Убедитесь в стабильной работе узла:

3.1 Проверьте текущее состояние служб:

```
hostname# failover show info
```

Все службы должны быть запущены, система защиты от сбоев должна работать в режиме кластера.

3.2 В течение некоторого времени (около 15 минут) понаблюдайте за работой узла и убедитесь, что он не перезагружается.

4 Отключите узел 2 от сети.

5 Подключите узел 1 к сети.

6 Переключите узел 1 в активный режим:

```
hostname# failover stop
hostname# failover start active
```

7 Обновите ПО на узле 2 (см. Локальное обновление 5.1.x > 5.2.0).

8 Убедитесь в стабильной работе узла 2 (см. шаг 3).

9 На узле 2 остановите работу службы `failoverd`:

```
hostname# failover stop
```

10 Подключите узел 2 к сети.

11 Соедините интерфейсы синхронизации обоих узлов кластера.

12 На узле 2 запустите службу `failoverd` в пассивном режиме:

```
hostname# failover start passive
```

13 Убедитесь, что синхронизация работает:

13.1 Убедитесь, что резервирование группы файлов конфигурации включено:

```
hostname# failover show config
```

В секции `[sendconfig]` параметр `config` должен иметь значение `yes`.

13.2 Измените какую-либо настройку в конфигурационном файле на активном узле.

13.3 Через некоторое время проверьте наличие этих же изменений на пассивном узле.

Удалённое обновление

Чтобы выполнить удалённое обновление ПО на обоих узлах кластера, выполните сценарий Удалённое обновление 5.1.x > 5.2.0 для активного узла кластера. По завершении обновления активным узлом кластера станет узел, на котором служба `failoverd` будет запущена первой.

Восстановление ПО ViPNet Coordinator IG

Примечание. Восстановление ПО возможно во всех исполнениях ViPNet Coordinator IG10 и ViPNet Coordinator IG100. Для исполнений ViPNet Coordinator IG1000 используйте сброс к заводским настройкам.

Процедура восстановления ПО используется в случае перехода ViPNet Coordinator IG в режим ограниченного функционирования, в котором блокируется работа всех сетевых интерфейсов.

Примечание.

- Подробнее о режимах работы см. в документе «Подготовка к работе», раздел «Режимы работы».
- Состояние индикаторов на передней панели ViPNet Coordinator IG в режиме ограниченного функционирования см. в документе «Описание аппаратных платформ», в разделе «Световая индикация».

В процессе восстановления вам понадобятся:

- образ ПО ViPNet Coordinator IG (поставляется на оптическом диске вместе с ViPNet Coordinator IG);
- USB-носитель для записи образа ПО;
- дистрибутив ключей (файл `*.ds5`);
- файл индивидуальной конфигурации (файл `*.ecf`) — если необходимо восстановить настройки ViPNet Coordinator IG.

Порядок восстановления ПО

1. Запишите образ ПО ViPNet Coordinator IG на USB-носитель.
2. Удалите ПО ViPNet Coordinator IG.
3. Установите ПО ViPNet Coordinator IG.
4. Выполните инициализацию ViPNet Coordinator IG (см. документ «Подготовка к работе», раздел «Инициализация») или Восстановление из резервной копии индивидуальной конфигурации.

Запись образа ПО ViPNet Coordinator IG на USB-носитель

Для записи образа ПО ViPNet Coordinator IG в ОС Windows вы можете воспользоваться программой Win32 Disk Imager.

В GNU/Linux вы можете записать файл образа ПО ViPNet Coordinator IG с помощью команды `dd`. Для этого:

1. Подключите к компьютеру USB-носитель.
2. Определите в каталоге `/dev` подкаталог устройства, соответствующий USB-носителю.
3. Перейдите в каталог с образом ПО ViPNet Coordinator IG.
4. Выполните команду с правами суперпользователя или с правами записи на устройство, определённое на шаге 2:

   ```
   dd if=<имя образа> of=<путь к файлу устройства>
   ```

Примечание. При указании пути к файлу устройства используйте имя устройства, а не имя раздела, например `/dev/sdb` вместо `/dev/sdb1`. Определить имя устройства вы можете, например, с помощью команды `fdisk -l`.

Совет. Для более быстрой записи можно указать размер блока, равный 1 Мбайт:

```
dd if=<имя образа> of=<путь к файлу устройства> bs=1M
```

USB-носитель готов для установки ПО ViPNet Coordinator IG.

Удаление ПО

Внимание! В результате процедуры удаления ПО ViPNet Coordinator IG будут удалены все данные и системные файлы. ViPNet Coordinator IG станет неработоспособным. Данная процедура предназначена для случаев, когда работоспособность ViPNet Coordinator IG нельзя восстановить другими способами.

Вы можете удалить ПО ViPNet Coordinator IG одним из способов:

- С помощью командного интерпретатора.
- С помощью алгоритма нажатий на кнопку **Reset**.

  Данный способ позволяет удалить ПО, если нет возможности использовать командный интерпретатор (например, если утерян пароль или USB-токен администратора).

Примечание. Факт удаления ПО необходимо записать в специальные журналы или в раздел «Особые отметки» формуляра ViPNet Coordinator IG.

Удаление ПО с помощью командного интерпретатора

Внимание!

- Не отключайте питание от ViPNet Coordinator IG, пока процедура удаления ПО не будет завершена.
- Для удаления ПО потребуется физический доступ к аппаратной платформе ViPNet Coordinator IG, чтобы подтвердить удаление нажатием на кнопку **Reset**.

Перед удалением ПО экспортируйте файлы журналов на USB-носитель. Для этого подключите USB-носитель к ViPNet Coordinator IG и выполните команду:

```
hostname# machine logs export usb
```

Чтобы удалить ПО ViPNet Coordinator IG:

1 Выполните команду:

```
hostname# admin system erase
```

Примечание. Команда `admin system erase` недоступна по SSH.

2 Когда появится сообщение:

```
This command completely removes all VPN software and cannot be reverted,
it will be necessary to deploy new software after executing this command.
Do you really wish to execute this command ? [Yes/No]:
```

введите `Yes` и нажмите **Enter**.

3 Когда появится сообщение:

```
For removing all VPN software press RESET button within 30 seconds
```

нажмите и удерживайте кнопку **Reset** (1–2 секунды) на аппаратной платформе.

4 Если всё сделано правильно, появится сообщение `ViPNet system software erase started`. С этого момента начнётся удаление ПО.

5 Дождитесь завершения процедуры (до 20 минут). После чего ViPNet Coordinator IG перезагрузится, и на экране появится строка ввода:

```
Infotecs IG#
```

Теперь можно установить ПО с USB-носителя (см. Установка ПО с USB-носителя).

Удаление ПО с помощью кнопки Reset

Внимание! Не отключайте питание от ViPNet Coordinator IG, пока процедура удаления ПО не будет завершена.

Чтобы удалить ПО ViPNet Coordinator IG с помощью кнопки **Reset**, расположенной на передней панели ViPNet Coordinator IG:

Совет. Изучите все шаги процедуры удаления, прежде чем начинать её выполнение.

1. Нажмите кнопку **Reset** и удерживайте её, пока индикаторы мигают жёлтым. Когда индикаторы начнут мигать красным, отпустите кнопку (удерживание кнопки занимает 10–15 секунд).

   Если вы отпустили кнопку вовремя, индикаторы перестанут мигать и будут гореть красным. Иначе индикаторы будут мигать жёлтым и ViPNet Coordinator IG перезагрузится.

2. В течение следующих 5 секунд, пока индикаторы горят красным, нажмите и удерживайте кнопку **Reset** (1–2 секунды), пока индикаторы не начнут мигать красным.

   Если вы всё сделали правильно:

   - Индикаторы продолжат мигать красным, пока выполняется удаление ПО.
   - Если к ViPNet Coordinator IG подключена консоль, появится сообщение: `The connection to the device was disconnected because the configuration reset procedure was started. Do not power down until reset` и соединение будет завершено. Вы не сможете подключиться до завершения процедуры удаления ПО.

   Иначе удаление ПО будет отменено, а ViPNet Coordinator IG автоматически перезагрузится.

3. Дождитесь завершения процедуры (около 20 минут). После чего индикаторы начнут мигать жёлтым и ViPNet Coordinator IG перезагрузится. Когда останутся гореть только индикаторы **PWR** и **STAT**, можно устанавливать ПО с USB-носителя (см. Установка ПО с USB-носителя).

Установка ПО с USB-носителя

Внимание! Не отключайте питание от ViPNet Coordinator IG, пока процедура установки ПО не будет завершена.

Установка ПО ViPNet Coordinator IG возможна только после удаления ПО ViPNet Coordinator IG (см. Удаление ПО).

Чтобы установить ПО ViPNet Coordinator IG, вам понадобятся:

- USB-носитель с образом ПО (см. Запись образа ПО ViPNet Coordinator IG на USB-носитель);
- консоль.

Для установки ПО ViPNet Coordinator IG:

1. Отключите питание от ViPNet Coordinator IG.
2. Подключите USB-носитель с образом ПО к ViPNet Coordinator IG.



Внимание! В процессе установки ПО к ViPNet Coordinator IG не должны быть подключены никакие другие USB-носители, кроме носителя с образом ПО ViPNet Coordinator IG.

3. Включите питание ViPNet Coordinator IG. Программа установки ПО запустится автоматически.
4. Когда появится сообщение:

   `Installation of ViPNet software will start now. Are you sure? (Yes/No):`

   введите `Yes`.
5. Если после списка доступных дисков появится сообщение:

   `Is this correct? (Yes/No):`

   Введите `Yes`.
6. Когда появится сообщение:

   `INSTALLATION WILL ERASE ALL DATA ON HARD DISK(S). ARE YOU SURE? (Yes/No):`

   введите `Yes`.
7. Когда появится сообщение:

   `Please remove USB flash and press ENTER.`

   отключите USB-носитель и нажмите **Enter**. ViPNet Coordinator IG будет перезагружен автоматически.

Установка ПО ViPNet Coordinator IG завершена. Для подготовки ViPNet Coordinator IG к использованию выполните инициализацию или восстановление из резервной копии. Подробнее см.:

- Документ «Подготовка к работе», раздел «Инициализация» — если нет необходимости восстанавливать настройки или нет файла индивидуальной конфигурации (`ecf`).
- Раздел Восстановление из резервной копии индивидуальной конфигурации — для восстановления настроек из резервной копии (`ecf`).

15

Работа с журналами

Журнал IP-пакетов 307

Журнал пакетов промышленных протоколов 319

Журналы аудита и СКЗИ 330

Журнал DNS-запросов 332

Журнал MFTP 333

Системный журнал 335

Экспорт журналов на USB-носитель 338

Журнал IP-пакетов

ViPNet Coordinator IG может регистрировать IP-пакеты в журнале одним из способов:

- Регистрация по сетевым фильтрам. У каждого сетевого фильтра есть параметр `log`, который указывает, регистрировать обработанные им IP-пакеты или нет. По умолчанию этот параметр включён на всех сетевых фильтрах с действием `drop` и `reject`, поэтому регистрируются только заблокированные и отклонённые IP-пакеты. Вы можете включить или отключить регистрацию IP-пакетов на любом сетевом фильтре отдельно (см. Изменение сетевого фильтра). Этот способ используется по умолчанию после инициализации ViPNet Coordinator IG.
- Регистрация по сетевым интерфейсам:
  - каждый пропущенный и заблокированный локальный IP-пакет отображается в журнале один раз — на том интерфейсе, через который он прошёл, или на том интерфейсе, на котором он был заблокирован;
  - каждый пропущенный транзитный IP-пакет отображается в журнале дважды: первый раз — на интерфейсе, через который он пришёл, второй раз — на интерфейсе, через который он ушёл.

  Этот способ использовался в ViPNet Coordinator IG более ранних версий и будет по умолчанию использоваться после обновления ПО ViPNet Coordinator IG до версии 5.2.0. Параметр `log` у сетевых фильтров игнорируется.

Для каждого сетевого интерфейса может быть выбран только один из способов регистрации IP-пакетов.

Широковещательные (`registerbroadcast`) и служебные (`registerevents`) IP-пакеты регистрируются только по интерфейсам независимо от способа регистрации других IP-пакетов.

Настройка ведения журнала

Вы можете изменить способ регистрации IP-пакетов для каждого сетевого интерфейса отдельно.

Чтобы отключить регистрацию IP-пакетов по сетевым фильтрам на одном интерфейсе:

```
hostname# machine logs settings network-traffic <интерфейс> register passed {on | off}
```

- `on` — регистрировать все IP-пакеты на интерфейсе: пропущенные, заблокированные и отклонённые;
- `off` — регистрировать только заблокированные и отклонённые IP-пакеты на интерфейсе.

После выполнения команды параметр `log` в сетевых фильтрах не будет учитываться для IP-пакетов, проходящих через указанный интерфейс.

Чтобы включить регистрацию IP-пакетов по сетевым фильтрам на одном интерфейсе:

1 Остановите работу службы `iplircfg`:

```
hostname# iplir stop
```

2 Откройте файл конфигурации интерфейса:

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

3 В секции `[db]` удалите параметр `registerall`.

4 Запустите службу `iplircfg`:

```
hostname# iplir start
```

Другие параметры ведения журнала вы можете настроить в конфигурационном файле `iplir.conf-<интерфейс или группа интерфейсов>` или с помощью команд:

Таблица 9. Команды настройки параметров секции [db]

Параметр	Описание параметра	Команда
`maxsize`	Максимальный размер журнала IP-пакетов интерфейса	`machine logs settings network-traffic maxsize`
`timedif`	Период времени, в течение которого связанные IP-пакеты объединяются в одну запись журнала	`machine logs settings network-traffic timediff`
`omittcpclientport`	Регистрация только порта сервера для TCP-соединений: включена или выключена	`machine logs settings network-traffic omit-client-port`
`registerbroadcast`	Регистрация широковещательных IP-пакетов в журнале: включена или выключена	`machine logs settings network-traffic register`
`registerevents`	Регистрация служебных широковещательных IP-пакетов в журнале: включена или выключена	`machine logs settings network-traffic register`

Чтобы просмотреть значения параметров ведения журнала:

- для одного сетевого интерфейса — откройте конфигурационный файл интерфейса:

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

- для всех сетевых интерфейсов:

  ```
  hostname> machine logs settings show
  ```

Подробное описание команд и параметров конфигурационных файлов см. в документе «Справочник команд и конфигурационных файлов».

Просмотр журнала

Чтобы просмотреть записи журнала IP-пакетов:

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

Примечание. В кластере вы можете просмотреть журнал IP-пакетов только на активном узле.

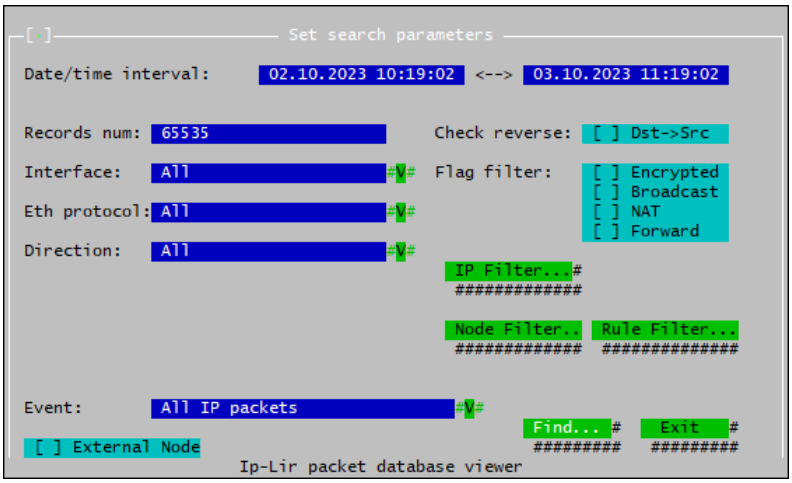


Рисунок 32. Задание параметров поиска записей в журнале IP-пакетов

Примечание. Внешний вид журнала может отличаться в зависимости от способа подключения к ViPNet Coordinator IG. Например, при локальном подключении с помощью программы PuTTY журнал отображается в чёрно-белом виде. Для отображения журнала в цветном виде, используйте:

- SSH-подключение;
- компьютер с Linux и стандартное приложение командной строки (терминал) или компьютер с Windows и приложение Git Bash.

Для подключения выполните команды:

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

где `<IP-адрес>` — IP-адрес сетевого интерфейса ViPNet Coordinator IG.

По умолчанию предполагается просмотр записей обо всех IP-пакетах, зарегистрированных в журнале за последние 24 часа. Чтобы просмотреть эти записи, нажмите **Find**.

Чтобы просмотреть записи об определённых IP-пакетах:

1. Укажите параметры:
   - **Date/time interval** — период времени, в течение которого были зарегистрированы пакеты в формате: `YYYY-MM-DD hh:mm:ss <--> YYYY-MM-DD hh:mm:ss`.
   - **Records num** — количество записей о зарегистрированных пакетах, которое будет отображено (по умолчанию — 65535). Поле **Records num** задаёт максимальное количество выводимых записей для каждого сетевого интерфейса. Если в параметрах поиска вы выбрали все сетевые интерфейсы (**All**), то общее количество выводимых записей будет равно сумме всех выводимых записей для каждого интерфейса.

- **Interface** — сетевой интерфейс, на котором были обработаны пакеты. По умолчанию — все доступные интерфейсы (**All**).
- **IP protocol** — IP-протокол, по которому были переданы пакеты:
  - **All** (по умолчанию) — любой протокол;
  - **ICMP** — только протокол ICMP;
  - **TCP** — только протокол TCP;
  - **UDP** — только протокол UDP;
  - **Except TCP, UDP, ICMP** — любой протокол, кроме TCP, UDP и ICMP.
- **Direction** — направление пакетов:
  - **All** (по умолчанию) — входящие и исходящие пакеты;
  - **Incoming** — входящие пакеты;
  - **Outgoing** — исходящие пакеты.
- **Event** — тип события, которому соответствует IP-пакет (см. События журнала IP-пакетов). По умолчанию — события всех типов (**All**).
- **Check reverse** — включение в журнал ответных пакетов от получателя отправителю (**Dst -> Src**). Устанавливать этот флажок имеет смысл только, если в качестве отправителя и/или получателя пакетов указаны конкретные IP-адреса (**IP Filter**) или узлы (**Node Filter**).
- **Flag filter** — вид пакетов:
  - **Encrypted** — зашифрованные;
  - **Broadcast** — широковещательные;
  - **NAT** — транслированные;
  - **Forward** — транзитные.

2 Чтобы задать IP-адреса или порты отправителя или получателя пакетов, нажмите **IP Filter**:

- Если в списке **IP protocol** вы выбрали все протоколы или все протоколы, кроме TCP, UDP и ICMP, укажите:
  - **Source IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) отправителей пакетов. По умолчанию — любой адрес (**All**).
  - **Destination IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) получателей пакетов. По умолчанию — любой адрес (**All**).
- Если в списке **IP protocol** вы выбрали протокол TCP или UDP, помимо IP-адресов отправителя и получателя, укажите:
  - **Source port** — порт (**Value**) или диапазон портов (**Range**) отправителей. По умолчанию — все порты (**All**).
  - **Destination port** — порт (**Value**) или диапазон портов (**Range**) получателей. По умолчанию — все порты (**All**).

- Если в списке **IP protocol** вы выбрали протокол ICMP, помимо IP-адресов отправителя и получателя, укажите:
  - **ICMP type** — тип (**Value**) или диапазон типов (**Range**) ICMP-пакетов.
  - **ICMP code** — код (**Value**) или диапазон кодов (**Range**) ICMP-пакетов.

3 Чтобы указать идентификатор сработавшего правила межсетевого экрана или номер конфигурации правил межсетевого экрана, нажмите **Rule Filter** и введите:

- идентификатор сетевого фильтра или правила трансляции адресов в поле **Rule ID**;
- номер конфигурации правил межсетевого экрана в поле **Rules Set ID**.

  Конфигурация правил межсетевого экрана — таблица всех сетевых фильтров и правил трансляции адресов в определённый момент времени. После установки дистрибутива ключей номер конфигурации правил равен единице. Этот номер увеличивается на единицу каждый раз:
  - при добавлении, изменении, удалении, включении и выключении правил межсетевого экрана;
  - запуске и завершении работы служб, которые добавляют служебные сетевые фильтры;
  - переключении в режим кластера или в одиночный режим работы системы защиты от сбоев.

  По умолчанию в поле **Rules Set ID** установлен номер текущей конфигурации правил межсетевого экрана.

Для отключения фильтрации по любому из параметров задайте значение **All**.

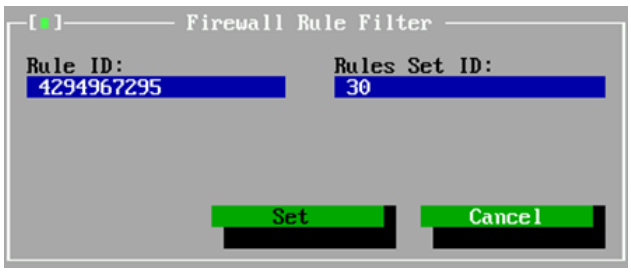


Рисунок 33. Фильтрация по идентификатору правила и номеру конфигурации

Внимание! При сохранении изменений в конфигурации правил межсетевого экрана (например, после добавления нового сетевого фильтра) номер текущей конфигурации увеличится, при этом поиск записей в журнале IP-пакетов будет выводить только записи, соответствующие новой конфигурации правил. Чтобы отображались записи, соответствующие всем конфигурациям правил, установите значение **ALL** или 0 в поле **Rules Set ID**.

---

4 Чтобы выбрать узел отправителя или получателя, нажмите **Node Filter**:

4.1 Для выбора узла отправителя нажмите **Select source Node**, для выбора узла получателя — **Select destination Node**.

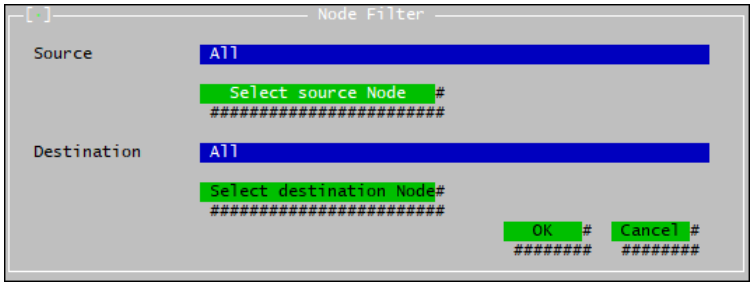


Рисунок 34. Выбор узла отправителя и получателя

В результате откроется таблица со списком узлов ViPNet, с которыми у ViPNet Coordinator IG есть связь: **ID** — идентификатор узла, **Name** — имя узла.

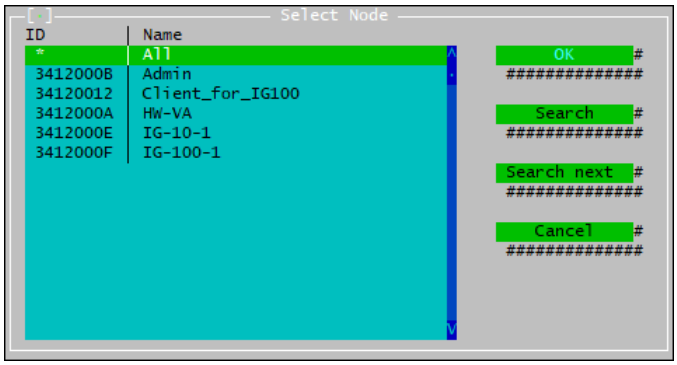


Рисунок 35. Выбор узла отправителя или получателя

4.2 Выберите нужный узел и нажмите **OK**.

Совет. Чтобы быстро найти нужный узел в списке, нажмите **Search**, введите часть идентификатора или имени узла и нажмите **OK**. Курсор будет переведён на строку первого узла, идентификатор или имя которого удовлетворяют условиям поиска. Для перехода к следующему такому узлу нажмите **Search next**.

---

5 Чтобы просмотреть журнал IP-пакетов удалённого узла:

Внимание! При просмотре журнала IP-пакетов удалённого узла действуют следующие особенности и ограничения:

- Удалённый узел должен быть доступен. При необходимости создайте разрешающие фильтры защищённой сети;
- Журнал координаторов версий 5.1.0 и выше имеет новый формат БД, поэтому его удалённый просмотр с помощью других продуктов ViPNet (за исключением ViPNet xFirewall версии 5.1 и выше) и ранних версий ViPNet Coordinator IG невозможен.

5.1 Установите флажок **External Node** и введите пароль администратора узла ViPNet.

5.2 Нажмите **Select** и выберите нужный узел ViPNet из списка.

6 Нажмите **Find**.

Список отфильтрованных записей журнала отображается в окне **View results**:

- **Date/time** — дата и время регистрации пакета;
- **Dev** — интерфейс, на котором был обработан пакет;
- **Flags** — направление и флаги пакетов:
  - **<** — исходящий пакет;
  - **>** — входящий пакет;
  - **C** — зашифрованный пакет;
  - **B** — широковещательный пакет;
  - **D** — заблокированный пакет;
  - **T** — транзитный пакет;
  - **R** — пакет, который будет обработан правилами NAT открытой сети;
  - **N** — пакет, который был обработан правилами NAT открытой сети;
- **Prot** — протокол, по которому был передан пакет;
- **Source IP** — IP-адрес отправителя пакета;
- **Port** — локальный порт для TCP- и UDP-пакетов или тип для ICMP-пакетов;
- **Destination IP** — IP-адрес получателя пакета;
- **Port** — порт удалённого компьютера для TCP- и UDP-пакетов или код для ICMP-пакетов.

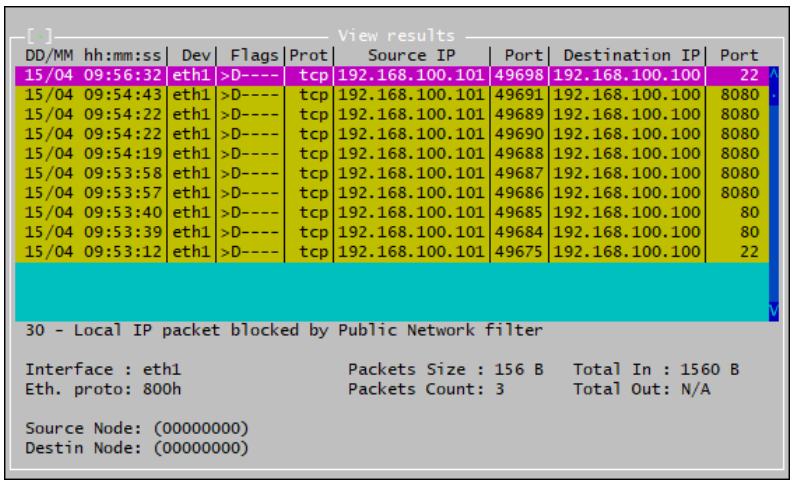


Рисунок 36. Просмотр записей из журнала IP-пакетов

1 Для просмотра краткой информации о пакете выберите соответствующую запись в списке. В окне под списком записей отобразятся:

- номер и тип события, которому соответствуют пакеты (см. События журнала IP-пакетов), агрегированные в выбранной записи;
- **Interface** — сетевой интерфейс, на котором были обработаны пакеты, агрегированные в выбранной записи;
- **Eth. proto** — шестнадцатеричный идентификатор протокола Ethernet;
- **Packets Size** — суммарный размер пакетов, агрегированных в выбранной записи;

Примечание. Для зашифрованных пакетов в параметре **Packets Size** отображается размер пакетов со всеми служебными заголовками.

- **Packets Count** — количество пакетов, агрегированных в выбранной записи;
- **Total In** — суммарный размер всех входящих пакетов, отфильтрованных по заданным критериям поиска;
- **Total Out** — суммарный размер всех исходящих пакетов, отфильтрованных по заданным критериям поиска;

Примечание. Единицы измерения суммарного размера пакетов: **B** — байты, **KB** — килобайты, **MB** — мегабайты.

Символ * в поле **Total In** или **Total Out** означает, что этот пакет не учтён в общем объёме входящего или исходящего трафика; N/A — отсутствие информации о размере пакетов.

- **Source Node** — номер сетевого узла ViPNet (отправителя пакетов);
- **Destin Node** — номер сетевого узла ViPNet (получателя пакетов).

2 Для просмотра подробной информации о пакете выберите запись и нажмите **Enter**. В окне **Record details** отобразятся:

- **Events** — номер и тип событий, объединённых в одну запись журнала (см. События журнала IP-пакетов);
- **Interval Begin, End** — начало и конец интервала времени, в течение которого несколько событий были объединены в одну запись журнала;
- **Source** — IP-адрес и порт отправителя пакетов;
- **Destination** — IP-адрес и порт получателя пакетов;
- **IP protocol** — тип транспортного протокола (TCP/UDP);
- **Count and size** — количество и суммарный размер пакетов, агрегированных в выбранной записи;
- **Interface** — имя сетевого интерфейса, на котором были зарегистрированы события;
- **Eth. protocol** — шестнадцатеричный идентификатор протокола Ethernet;
- **Direction** — направление пакета (входящий, исходящий);
- **NAT** — флаг транслированного пакета;
- **Drop** — флаг блокировки пакета;
- **Broadcast** — флаг широковещательного пакета;
- **Forward** — флаг транзитного пакета;
- **Encrypted** — флаг зашифрованного пакета;
- **Source node** — номер и имя сетевого узла ViPNet (отправителя пакетов);
- **Destin node** — номер и имя сетевого узла ViPNet (получателя пакетов);
- **Rule UID** — идентификатор сработавшего правила.

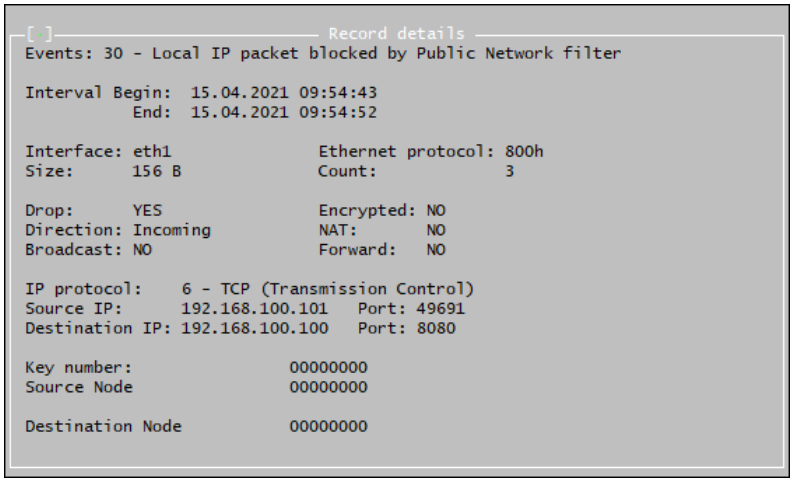


Рисунок 37. Просмотр подробной информации о пакете

3 Для экспорта записей в текстовый файл, например для последующего анализа, нажмите **F2** и укажите файл для экспорта.

Экспорт журнала IP-пакетов на USB-носитель

Внимание! Если вы используете удаленное подключение по SSH, то для корректного экспорта установите в настройках SSH-клиента тип терминала VT100+.

Чтобы экспортировать записи журнала IP-пакетов на USB-носитель:

1 Выполните команду:

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

2 Задайте параметры для выбора из журнала нужных записей и нажмите **Find**.

3 В окне **View results** нажмите клавишу **F2**.

4 Введите имя файла, в который вы хотите сохранить журнал, или выберите из списка существующий файл; затем нажмите **Enter**.

5 Завершите просмотр журнала: нажмите **Esc**, затем **Exit**.

6 Запустите экспорт журнала на USB-носитель:

```
hostname# machine logs export network-traffic usb <имя файла>
```

В качестве имени файла укажите имя, которое вы задали при сохранении журнала на шаге 4.

7 Подключите USB-носитель к ViPNet Coordinator IG и нажмите **Enter**.

8 Дождитесь завершения экспорта.

Файл архива журнала IP-пакетов `<имя файла>.tar.gz` будет сохранён на USB-носителе. Чтобы преобразовать журнал в удобный для чтения вид, распакуйте архив, откройте его с помощью Microsoft Excel и выполните импорт данных, указав в качестве разделителя символ «|»; журнал отобразится в виде таблицы:

- **Time begin** — дата и время начала регистрации пакета;
- **Time end** — дата и время окончания регистрации пакета;
- **Dev** — интерфейс, на котором был обработан пакет;
- **Eth** — шестнадцатеричный идентификатор протокола Ethernet;
- **Flags** — направление и флаги пакета;
- **Prot** — протокол, по которому был передан пакет;
- **Source IP** — IP-адрес отправителя пакета;
- **Port** — локальный порт TCP- и UDP-пакетов или тип для ICMP-пакетов;
- **Destination IP** — IP-адрес получателя пакета;
- **Port** — порт удалённого компьютера для TCP- и UDP-пакетов или код для ICMP-пакетов.
- **Size** — размер пакета (или суммарный размер пакетов, если количество пакетов больше единицы);
- **Cnt** — количество пакетов, относящихся к данному событию;
- **SourceNode** — узел отправителя;
- **DestinNode** — узел получателя;
- **Event** — код и название события, присвоенного пакету.

Экспорт журнала IP-пакетов по сети в формате CEF

Вы можете экспортировать события журнала IP-пакетов по сети в формате CEF, например в систему управления информационной безопасностью.

Чтобы настроить экспорт событий журнала:

1. Остановите службу `iplircfg`:

   ```
   hostname# iplir stop
   ```

2. Откройте файл конфигурации `iplir.conf`:

   ```
   hostname# iplir config
   ```

3. В секции `[misc]` задайте параметры экспорта журнала IP-пакетов:
   - `cef_enabled` — разрешение экспорта записей журнала по сети:
     - `yes` — запустить экспорт;
     - `no` — остановить экспорт.
   - `cef_ip` — IP-адрес сетевого узла, на который будут отправляться сообщения CEF.

Примечание. В качестве сетевого узла нельзя указывать локальный узел localhost, собственные IP-адреса и дополнительные IP-адреса (алиасы) интерфейсов.

- `cef_port` — порт UDP для передачи сообщений CEF (по умолчанию 514).

4 Сохраните изменения (**Ctrl+O**, затем **Enter**) и закройте редактор (**Ctrl+X**).

5 Откройте файл конфигурации интерфейса `iplir.conf-eth<номер>`, записи журнала IP-пакетов которого вы хотите экспортировать:

```
hostname# iplir config eth<номер>
```

6 В секции `[cef]` задайте параметры формирования сообщений CEF:

- `event` — определяет формирование сообщений CEF при регистрации IP-пакетов, проходящих через интерфейс:
  - `all` — для всех IP-пакетов.
  - `blocked` — для блокированных IP-пакетов (значение по умолчанию).
- `exclude` — определяет список событий, которые не будут входить в сообщения CEF. Полный список событий см. приложении События журнала IP-пакетов. Допускается перечисление номеров типов событий в любом порядке через запятую.

Примечание. При необходимости вы можете изменить значение параметра `timedif` секции `[db]` в файле конфигурации интерфейса `iplir.conf-eth<номер>`. Параметр `timedif` задаёт:

- интервал времени, в течение которого одинаковые события объединяются в одну запись журнала IP-пакетов;
- периодичность отправки записей журнала IP-пакетов в формате CEF по сети.

Подробнее см. в документе «Справочник команд и конфигурационных файлов», раздел «Файл iplir.conf-<интерфейс или группа интерфейсов>».

7 Сохраните изменения (**Ctrl+O**, затем **Enter**) и закройте редактор (**Ctrl+X**).

8 Запустите службу `iplircfg`:

```
hostname# iplir start
```

9 Если сетевой узел, на который будут отправляться сообщения CEF, расположен в открытой сети, создайте разрешающий сетевой фильтр:

```
hostname# firewall local add src @local dst <IP-адрес> service @Syslog pass
```

Примечание. Для сетевого узла, расположенного в защищённой сети, разрешающий сетевой фильтра для исходящего трафика протокола syslog создаётся автоматически.

Пример записи журнала IP-пакетов для экспорта по сети в формате CEF о событии блокировки открытого IP-пакета межсетевым экраном:

```
Sep 19 08:26:10 hw CEF:0|infotecs|hw|4.5|20|unencrypted IP packet
blocked|10|deviceExternalId=27e8000a start=1539756183000 end=1539756184000 src=10.0.0.1
```

```
dst=2.1.2.2 spt=1232 dpt=80 proto=tcp cnt=5 in=20 deviceInboundInterface=eth0 cn1=800h
cnLabel=Eth protocol hex cs1=NAT yes cs2=Drop yes cs3=Broadcast no cs4=Forward no
cs5=Encrypted no cs1Label=Flags deviceDirection=inbound
```

Описание структуры записи см. в приложении Структура записи журнала IP-пакетов для экспорта по сети в формате CEF.

Чтобы просмотреть настройки экспорта журнала IP-пакетов в формате CEF, выполните:

```
hostname# machine logs settings show
```

Также настройка части параметров экспорта теперь доступна и с помощью команд:

Таблица 10. Команды настройки параметров секции [cef]

Параметр	Описание параметра	Команда
event	Тип событий журнала IP-пакетов, экспортируемых в формате CEF: все события или события о заблокированных IP-пакетах	`machine logs settings cef event-type`
exclude	Список исключений событий журнала IP-пакетов, экспортируемых в формате CEF	`machine logs settings cef exclude` `machine logs settings cef include`

Подробное описание команд см. в документе «Справочник команд и конфигурационных файлов».

Журнал пакетов промышленных протоколов

Служба `IPF` ведет журнал, в который вносится информация обо всех пакетах, обработанных правилами фильтрации промышленных протоколов на прикладном уровне. Информация о каждом обработанном пакете вносится в журнал один раз, без разделения на сетевые интерфейсы.

Примечание. По умолчанию в журнале пакетов промышленных протоколов регистрируются только заблокированные пакеты. Чтобы включить регистрацию пропущенных пакетов:

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

Просмотр журнала пакетов промышленных протоколов

Чтобы просмотреть записи журнала пакетов промышленных протоколов:

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

В результате откроется окно **Set search parameters** для задания параметров поиска записей в журнале.

Примечание. В кластере журнал пакетов промышленных протоколов синхронизируется между узлами. При этом просмотреть журнал вы можете только на активном узле кластера.

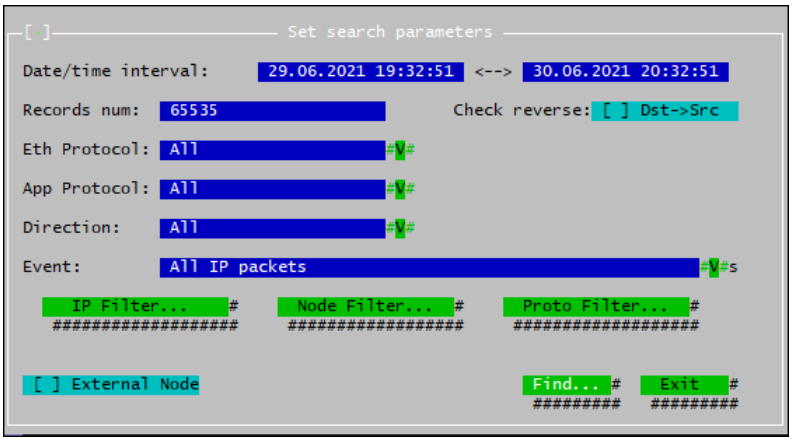


Рисунок 38. Задание параметров поиска записей в журнале пакетов промышленных протоколов

Примечание. Внешний вид журнала может отличаться в зависимости от способа подключения к ViPNet Coordinator IG. Например, при локальном подключении с помощью программы PuTTY журнал отображается в черно-белом виде. Для отображения журнала в цветном виде, используйте:

- SSH-подключение;
- компьютер с Linux и стандартное приложение командной строки (терминал) или компьютер с Windows и приложение Git Bash.

Для подключения выполните команды:

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

где `<IP-адрес>` — IP-адрес сетевого интерфейса ViPNet Coordinator IG.

По умолчанию предполагается просмотр записей обо всех пакетах, обработанных правилами фильтрации промышленных протоколов за последние сутки (плюс один час). Чтобы просмотреть такие записи, нажмите **Find**.

Чтобы выбрать записи журнала для просмотра:

1 Укажите параметры пакетов:

- **Date/time interval** — период времени, в течение которого были зарегистрированы пакеты в формате: `дд.мм.гггг чч:мм:сс <--> дд.мм.гггг чч:мм:сс`

  По умолчанию — текущие сутки.

- **Records num** — количество записей о зарегистрированных пакетах, которое будет отображено (по умолчанию — 65535).

- **Eth Protocol** — транспортный протокол, по которому были переданы пакеты. Возможные значения:

  - **All** (по умолчанию) — любой протокол;
  - **TCP** — только протокол TCP;
  - **UDP** — только протокол UDP;
  - **Except TCP, UDP** — любой протокол, кроме TCP и UDP.

- **App Protocol** — прикладной протокол, по которому были переданы пакеты. Возможные значения:

  - **All** (по умолчанию) — любой протокол;
  - **Modbus** — только протокол Modbus;
  - **IEC 104** — только протокол МЭК 60870-5-104.

- **Direction** — направление пакетов:

  - **All** (по умолчанию) — входящие и исходящие пакеты;
  - **Incoming** — входящие пакеты;
  - **Outgoing** — исходящие пакеты.

- **Event** — тип события, которому соответствует IP-пакет. Возможные значения:
  - **All IP packets** (по умолчанию) — события всех типов;
  - **Blocked IP packets** — заблокированные пакеты;
  - **140 — Modbus packet blocked by rules** — пакет заблокирован правилом фильтрации протокола Modbus;
  - **141 — Modbus anomaly packet blocked by filter** — пакет заблокирован правилом обработки аномалий Modbus;
  - **143 — IEC 104 packet blocked by rules** — пакет заблокирован правилом фильтрации протокола МЭК 60870-5-104;
  - **144 — IEC 104 anomaly packet blocked by filter** — пакет заблокирован правилом обработки аномалий МЭК 60870-5-104;
  - **Allowed IP packets** — пропущенные пакеты;
  - **66 — Modbus packet passed** — пакет пропущен правилом фильтрации протокола Modbus;
  - **68 — IEC 104 packet passed** — пакет пропущен правилом фильтрации протокола МЭК 60870-5-104.
- **Check reverse** — включение в журнал ответных пакетов от получателя отправителю (**Dst -> Src**). Устанавливать этот флажок имеет смысл только, если в качестве отправителя и/или получателя пакетов указаны конкретные IP-адреса (**IP Filter**) или узлы (**Node Filter**).

2 Чтобы задать IP-адреса или порты отправителя или получателя пакетов, нажмите **IP Filter** и в открывшемся окне укажите:

- **Source IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) отправителей пакетов. По умолчанию — любой адрес (**All**);
- **Destination IP address** — IP-адрес (**Value**) или диапазон IP-адресов (**Range**) получателей пакетов. По умолчанию — любой адрес (**All**);
- **Source port** — порт (**Value**) или диапазон портов (**Range**) отправителей. По умолчанию — все порты (**All**);
- **Destination port** — порт (**Value**) или диапазон портов (**Range**) получателей. По умолчанию — все порты (**All**);

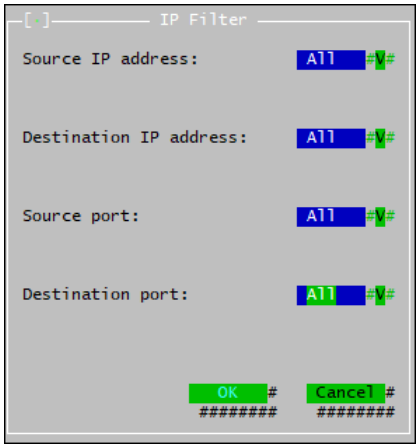


Рисунок 39. Задание IP-адреса и порта для отправителя и получателя IP-пакетов

Примечание. При задании в поле **Value** числового значения использование числа 0 не допускается.

3 Чтобы выбрать узел отправителя или получателя по идентификатору ViPNet, нажмите **Node Filter** и в открывшемся окне:

3.1 Для выбора узла отправителя нажмите **Select source Node**, для выбора узла получателя — **Select destination Node**.

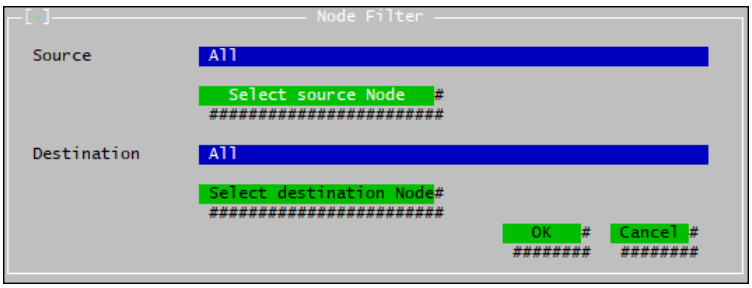


Рисунок 40. Выбор узла отправителя и получателя

Откроется таблица со списком узлов ViPNet, с которыми ViPNet Coordinator IG имеет связи. В левом столбце таблицы указан шестнадцатеричный идентификатор узла (**ID**), в правом — имя узла (**Name**).

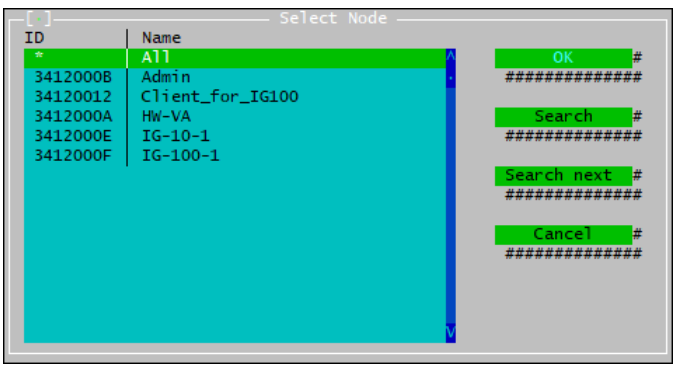


Рисунок 41. Выбор узла отправителя или получателя

3.2 Выберите нужный узел и нажмите **OK**.

Совет. Чтобы быстро найти нужный узел в списке, нажмите **Search**. В открывшемся окне введите часть идентификатора или имени узла и нажмите **OK**. В результате курсор будет переведён на строку первого узла, идентификатор или имя которого удовлетворяют условиям поиска. Для перехода к следующему такому узлу нажмите **Search next**.

---

4 Чтобы задать параметры прикладного протокола, нажмите **Proto Filter** и в открывшемся окне:

4.1 В поле **Protocol** выберите прикладной протокол. По умолчанию — любой протокол (**All**). При выборе протокола меняется список параметров, по которым можно выполнять поиск записей в журнале.

4.2 Если выбран протокол **Modbus**, задайте параметры поиска:

- **Address/ID** — идентификаторы (адреса) Modbus-устройств. По умолчанию — любой адрес (**All**).
- **Function/App** — коды функций команд Modbus. По умолчанию — все коды функций (**All**).
- **Read Registers** — номера регистров, запрашиваемых на чтение. По умолчанию — все номера регистров (**All**).
- **Write Registers** — номера регистров, запрашиваемые на запись. По умолчанию — все номера регистров (**All**).

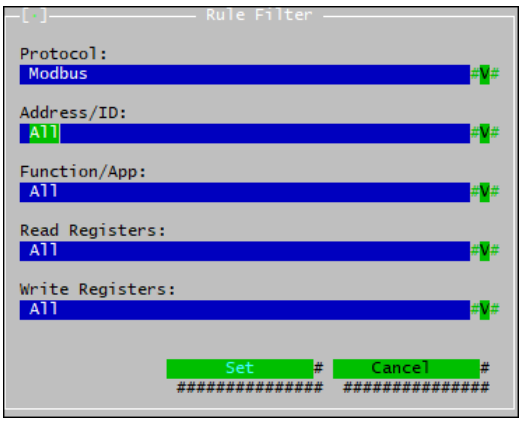


Рисунок 42. Задание параметров прикладного протокола

4.3 Если выбран протокол МЭК 60870-5-104 (**IEC 104**), задайте параметры поиска:

- **Address ASDU** — общие адреса ASDU. По умолчанию — любой адрес (**All**).
- **Address information object** — адреса (идентификаторы) объектов информации. По умолчанию — любой адрес (**All**).
- **Information object type** — идентификаторы типов объектов информации. По умолчанию — все идентификаторы (**All**).

4.4 Нажмите **Set**.

5 Чтобы просмотреть журнал пакетов промышленных протоколов удалённого узла:

Примечание. Для просмотра журнала пакетов промышленных протоколов удалённого узла необходимо, чтобы этот узел был доступен.

5.1 Выберите **External Node** и введите пароль администратора узла ViPNet.

5.2 С помощью **Select** откройте окно со списком узлов и выберите нужный узел.

6 Нажмите **Find**.

В результате откроется окно **View results**, содержащее таблицу со списком записей о пакетах, которые удовлетворяют выбранным параметрам. Записи упорядочены по времени регистрации. Таблица включает в себя следующие столбцы:

- **DD/MM hh:mm:ss** — дата и время регистрации пакета;
- **F** — результат фильтрации пакета:
  - **–** — пакет пропущен;
  - **D** — пакет заблокирован.
- **Prot** — транспортный протокол, по которому был передан пакет;
- **Source IP** — IP-адрес отправителя пакета;
- **Port** — порт отправителя пакета;
- **Destination IP** — IP-адрес получателя пакета;
- **Port** — порт получателя пакета.

Если пакет принадлежит протоколу Modbus, таблица содержит дополнительные поля:

- **ID** — адрес (идентификатор) Modbus-устройства;
- **FC** — код функции команды Modbus;

Если пакет принадлежит протоколу МЭК 60870-5-104, таблица содержит дополнительные поля:

- **T** — Тип объекта информации;
- **ASDU** — общий адрес ASDU;
- **COT** — код причины передачи.

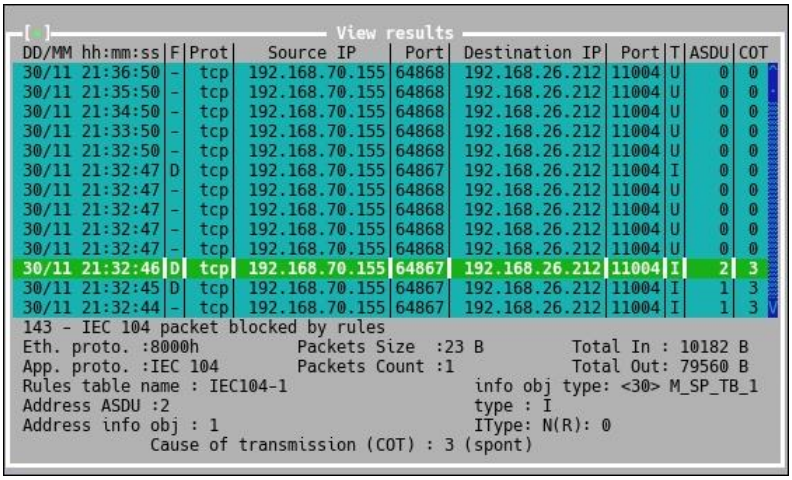


Рисунок 43. Просмотр записей из журнала пакетов промышленных протоколов

В окне **View results** вы можете:

- Экспортировать список записей в текстовый файл (например, для последующего анализа). Для этого нажмите клавишу **F2** и укажите имя файла для экспорта (см. Экспорт журнала пакетов промышленных протоколов).
- Просмотреть краткую информацию об IP-пакете, выбрав соответствующую запись в списке. В окне под списком отобразятся:
  - код и тип события, которому соответствуют пакеты, агрегированные в выбранной записи:
    - **140 — Modbus packet blocked by rules** — пакет заблокирован правилом фильтрации протокола Modbus;
    - **141 — Modbus anomaly packet blocked by filter** — пакет заблокирован правилом обработки аномалий Modbus;
    - **143 — IEC 104 packet blocked by rules** — пакет заблокирован правилом фильтрации протокола МЭК 60870-5-104;
    - **144 — IEC 104 anomaly packet blocked by filter** — пакет заблокирован правилом обработки аномалий МЭК 60870-5-104;
    - **66 — Modbus packet passed** — пакет пропущен правилом фильтрации протокола Modbus;
    - **68 — IEC 104 packet passed** — пакет пропущен правилом фильтрации протокола МЭК 60870-5-104.
  - **Eth. proto** — шестнадцатеричный идентификатор протокола Ethernet;
  - **App Protocol** — прикладной протокол, которому принадлежат пакеты, агрегированные в выбранной записи;
  - **Packets Size** — суммарный размер пакетов, агрегированных в выбранной записи;

Примечание. Для зашифрованных пакетов в параметре **Packets size** отображается размер пакетов со всеми служебными заголовками.

- **Packets Count** — количество пакетов, агрегированных в выбранной записи;
- **Total In** — суммарный размер всех входящих пакетов, отфильтрованных по заданным критериям поиска;
- **Total Out** — суммарный размер всех исходящих пакетов, отфильтрованных по заданным критериям поиска;



Примечание. Единицы изменения суммарного размера IP-пакетов: **B** — байты, **KB** — килобайты, **MB** — мегабайты.

Символ «*» в поле **Total In** или **Total Out** пакета означает, что этот пакет не учтён в общем объёме входящего или исходящего трафика. Символ «N/A» — означает отсутствие информации о размере пакетов.

Если пакет принадлежит протоколу Modbus, дополнительно отображается информация:

- **Rules table name** — имя набора правил фильтрации протокола Modbus;
- **Address/ID** — адрес (идентификатор) Modbus-устройства;
- **Function/App —** код функции команды Modbus;
- **Read Regs.** — номера регистров, запрашиваемые функцией команды Modbus на чтение;
- **Write Regs.** — номера регистров, запрашиваемые функцией команды Modbus на запись.

Если пакет принадлежит протоколу МЭК 60870-5-104, дополнительно отображается информация:

- **Rules table name** — имя набора правил фильтрации протокола МЭК 60870-5-104;
- **Address ASDU** — общие адреса ASDU;
- **Address info obj —** адреса (идентификаторы) объектов информации;
- **Info obj type** — идентификаторы типов объектов информации;
- **type** — формат поля управления:
  - **I** — формат передачи информации;
  - **S** — формат функций контроля с нумерацией (для передачи квитанций);
  - **U** — формат функций управления без нумерации (для передачи посылок установления связи и тестирования канала связи).
- **Utype | Stype | Itype** (в зависимости от значения поля **type**) — значение поля управления;
- **Cause of transmission (COT)** — код причины передачи:
  - **0** — не используется;
  - **1 (per/cyc)** — периодическая передача (periodic, cyclic);
  - **2 (back)** — фоновое сканирование (background scan);
  - **3 (spont)** — спорадическая передача при возникновении события (spontaneous);
  - **4 (init)** — сообщение об инициализации (initialized);

- **5 (req)** — запрос или запрашиваемые данные (request or requested);
- **6 (act)** — активация (activation);
- **7 (actcon)** — подтверждение активации (activation confirm);
- **8 (deact) —** деактивация (deactivation);
- **9 (deactcon)** — подтверждение деактивации (deactivation confirm);
- **10 (actterm)** — завершение активации (activation termination);
- **11 (retrem)** — обратная информация, вызванная удалённой командой (return information caused by a remote command);
- **12 (retloc)** — обратная информация, вызванная местной командой (return information caused by a local command);
- **13 (file)** — передача файлов (file transfer);
- **14–19** — резерв;
- **20 (inrogen)** — общий опрос (interrogated by station interrogation);
- **21 (inro1) – 36 (inro16)** — опрос группы 1–16;
- **37 (reqcogen)** — общий опрос счётчиков;
- **38 (reqco1) – 41 (reqco4)** — запрос счётчиков группы 1–4;
- **44 (unknown_type)** — неизвестный тип идентификатора;
- **45 (unknown_cause)** — неизвестная причина передачи;
- **46 (unknown_asdu_address)** — неизвестный общий адрес станции;
- **47 (unknown_object_address)** — неизвестный адрес объекта информации.

- Просмотреть подробную информацию о пакете, выбрав соответствующую запись в списке и нажав **Enter**. Откроется окно **Record details**, в котором дублируется информация из окна **View results** с добавлением дополнительной информации:
  - **Drop** — флаг блокировки пакета;
  - **Direction** — направление пакета (входящий, исходящий);
  - **Source Node identifier** — идентификатор узла ViPNet — отправителя пакетов;
  - **Destination Node identifier** — идентификатор узла ViPNet — получателя пакетов.

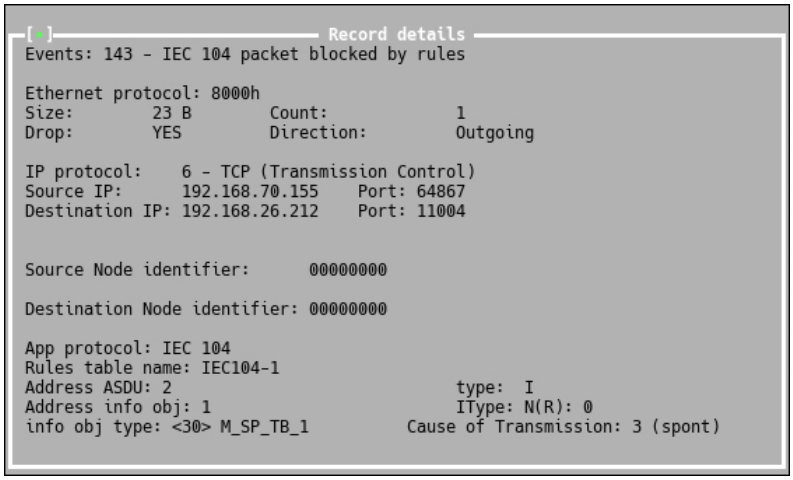


Рисунок 44. Просмотр подробной информации о пакете

Для завершения просмотра журнала или изменения параметров поиска нажмите клавишу **Esc**.

Экспорт журнала пакетов промышленных протоколов

Чтобы экспортировать список записей из журнала пакетов промышленных протоколов на USB-носитель:

Внимание! Если вы используете удалённое подключение по SSH, то для корректного экспорта установите в настройках используемого ПО SSH-клиента тип терминала VT100+.

---

1 Выполните команду:

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

2 Задайте параметры для выбора из журнала нужных записей и нажмите **Find**.

3 В окне **View results** нажмите клавишу **F2**.

4 Введите имя файла, в который вы хотите сохранить журнал, или выберите из списка существующий файл. Затем нажмите **Enter**.

5 Завершите просмотр журнала: нажмите клавишу **Esc**, затем кнопку **Exit**.

6 Выполните команду экспорта журнала на USB-носитель:

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

В качестве имени файла укажите имя, которое вы задали при сохранении журнала (на шаге 4).

7 Подключите USB-носитель к ViPNet Coordinator IG и нажмите **Enter**.

8 В списке подключенных к ViPNet Coordinator IG USB-носителей и имеющихся на них разделов найдите нужный, введите его номер, нажмите **Enter** и дождитесь завершения экспорта.

В результате журнал пакетов промышленных протоколов будет экспортирован в корневой каталог USB-носителя в виде архива `*.tar.gz`, содержащего файл в формате `*.csv`. Параметры журнала в файле разделены символом «`;`».

Чтобы преобразовать журнал в удобный для чтения вид, распакуйте архив, откройте его с помощью программы Microsoft Excel и выполните импорт данных, указав в качестве разделителя символ «;». В результате данные отобразятся в таблице, содержащей следующие столбцы:

- **DD/MM hh:mm:ss** — дата и время регистрации пакета;
- **F** — результат фильтрации пакета:
  - **–** — пакет пропущен;
  - **D** — пакет заблокирован.
- **Prot** — транспортный протокол, по которому был передан пакет;
- **Source IP** — IP-адрес отправителя пакета;
- **Port** — порт отправителя пакета;
- **Destination IP** — IP-адрес получателя пакета;
- **Port** — порт получателя пакета.

Для протокола Modbus добавляются следующие столбцы:

- **ID** — адрес (идентификатор) Modbus-устройства;
- **FC** — код функции команды Modbus.

Для протокола МЭК 60870-5-104 добавляются следующие столбцы:

- **T** — Тип объекта информации;
- **ASDU** — общий адрес ASDU;
- **COT** — код причины передачи.

Журналы аудита и СКЗИ

Ведение журнала аудита

В журнале аудита регистрируются события, связанные с выполнением запросов пользователей, в том числе от ViPNet Prime, и служебных запросов ViPNet Coordinator IG. Журнал ведётся локально и ротируется (после достижения максимального размера наиболее старые записи заменяются новыми). По умолчанию максимальный размер журнала — 50 Мбайт. Чтобы просмотреть значение максимального размера журнала и процент его заполнения, выполните:

```
hostname> machine logs setting show
```

При необходимости вы можете изменить максимальный размер журнала:

```
hostname# machine logs settings user-audit size <размер>
```

Минимальное значение — 10 Мбайт, максимальное — зависит от объёма свободной дисковой памяти.

Ведение журнала СКЗИ

В журнале СКЗИ регистрируются события, связанные с выполнением запросов криптографических операций. Журнал ведётся локально и не ротируется. По умолчанию максимальный размер журнала — 50 Мбайт. Чтобы просмотреть текущий максимальный размер журнала и процент его заполнения, выполните:

```
hostname> machine logs setting show
```

При необходимости вы можете изменить максимальный размер журнала:

```
hostname# machine logs settings crypto-audit size <размер>
```

Минимальное значение — 10 Мбайт, максимальное — зависит от объёма свободной дисковой памяти.

Очистить журнал СКЗИ вы можете двумя способами:

- С помощью веб-интерфейса (см. документ «Настройка с помощью веб-интерфейса», раздел «Настройка журналов»). Перед очисткой журнал скачивается на ваш компьютер.
- С помощью команды экспорта и очистки журналов:

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



Внимание! Команда `machine logs export-and-clear usb` очищает не только журнал СКЗИ, но и журналы аудита, MFTP, DNS-запросов, системный журнал.

Просмотр журнала аудита и журнала СКЗИ

Чтобы просмотреть журнал аудита или журнал СКЗИ, выполните:

```
hostname> machine logs show {user-audit | crypto-audit}
```

Подробнее о параметрах команд см. документ «Справочник команд и конфигурационных файлов», раздел «Команды группы machine».

Просмотр событий журнала аудита и журнала СКЗИ на удалённом сетевом узле

Чтобы просматривать события журнала аудита и журнала СКЗИ на удалённом сетевом узле, настройте удалённое протоколирование системного журнала (см. Системный журнал).

Формат событий журнала аудита и журнала СКЗИ в системном журнале:

```
<timestamp> <hostname> <hostname>[<pid>]: <type> [<hostname>] [<failover mode>] <event>
[<result>] [<initiator>] Details: <event details>
```

- `<timestamp>` — дата и время события.
- `<hostname>` — имя узла.
- `<pid>` — ID процесса.
- `<type>` — тип события:
  - `<crypto>` — событие журнала СКЗИ.
  - `<management>` — событие журнала аудита.
- `<failover mode>` — режим работы системы защиты от сбоев:
  - `Single Mode` — одиночный режим.
  - `Active Mode` — активный узел кластера.
  - `Passive Mode` — пассивный узел кластера.
- `<event>` — описание события.
- `<result>` — результат выполнения операции:
  - `success` — успешно.
  - `failed` — ошибка.
- `<initiator>` — инициатор события:
  - Имя учётной записи — `admin`, `user` или имя централизованной учётной записи.
  - `System` — служебный запрос.
  - `System.Prime` — запрос ViPNet Prime.
- `<event details>` — дополнительная информация о событии (может отсутствовать).

Например:

```
May 30 14:36:04 2022 va2000 itcs-aad[7375]: <crypto> [va51-3617] [local] [Single Mode]
<admin> logged in. [success] [System] Details: ticket:AAA__4ee13d_6272b0_ab9226_74df7c
```

```
May 30 14:36:04 2022 va2000 webgui-fcgi-server[10369]: <management> [va51-3617] [local]
[Single Mode] Show idle session time-out [success] [admin] Details:
```

Журнал DNS-запросов

Локальный DNS-сервер ViPNet Coordinator IG записывает информацию о поступивших DNS-запросах:

- дата и время запроса;
- IP-адрес и порт источника запроса;
- запрошенное доменное имя;
- тип запрошенной DNS-записи.

Журнал DNS-запросов ведётся локально и ротируется: когда файл журнала достигает максимального размера (по умолчанию — 10 Мбайт), он переименовывается, а предыдущий заполненный файл удаляется. Таким образом, на ViPNet Coordinator IG всегда находится один текущий файл журнала и один заполненный.

Настройка

По умолчанию журнал DNS-запросов включен. Ведение журнала начинается с момента включения DNS-сервера ViPNet Coordinator IG.

Вы можете:

- Выключить ведение журнала:

  ```
  hostname# inet dns querylog off
  ```

- Просмотреть настройки журнала:

  ```
  hostname> inet show dns
  ```

- Изменить максимальный размер журнала:

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

  Допустимые значения: 1–50 Мбайт.



Примечание. Если вы уменьшили максимальный размер журнала, а его текущий размер достиг или превышает новое значение, он автоматически будет ротирован.

- Очистить журнал:

  ```
  hostname# machine logs clear dns
  ```

Просмотр журнала

- Чтобы просмотреть содержимое журнала:

  ```
  hostname> inet dns querylog show
  ```

- Чтобы просмотреть записи журнала, содержащие определенный текст:

  ```
  hostname> inet dns querylog show filtered <строка>
  ```

Журнал MFTP

Транспортный сервер MFTP записывает информацию о полностью принятых, отправленных, удаленных и поврежденных транспортных конвертах в специальный журнал.

Для журнала предусмотрена автоматическая ротация. При превышении максимального размера (по умолчанию — 1 Мбайт) наиболее ранние записи перезаписываются новыми. Это позволяет экономить место на ViPNet Coordinator IG.

Для просмотра журнала в командном интерпретаторе транспортный сервер выгружает информацию об обработанных конвертах из журнала в текстовый файл (`mftpenv.log.<дата>`). По истечении периода времени (по умолчанию — 1 день) создается новый файл, в имени которого содержится текущая дата.

Просмотр журнала

Чтобы посмотреть записи журнала MFTP:

```
hostname> machine logs show mftp
```

При просмотре выводится следующая информация:

- имя конверта;
- размер конверта;
- имя узла-отправителя;
- имя узла-получателя;
- название события;
- имя прикладной задачи (роли) или тип узла-отправителя;
- описание конверта;
- дата и время события.

Настройка параметров журнала

1. Завершите работу службы `mftpd`:

   ```
   hostname# mftp stop
   ```

2. Откройте файл `mftp.conf` для редактирования:

   ```
   hostname# mftp config
   ```

3. В секции `[journal]` при необходимости измените значения:

   - `max_size` — максимальный размер журнала конвертов в мегабайтах (по умолчанию — `1`). В случае уменьшения размера журнала наиболее ранние записи удаляются из него.



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.

- `dump_interval` — период выгрузки информации из журнала в текстовый файл в днях (по умолчанию — `1`).

4 Сохраните изменения (**Ctrl+O**) и закройте редактор (**Ctrl+X**).

5 Запустите службу `mftpd`:

```
hostname# mftp start
```

Системный журнал

Ведение журнала

Службы `iplircfg`, `mftpd`, `failoverd` записывают информацию о событиях в системный журнал. Этот журнал позволяет контролировать работоспособность ViPNet Coordinator IG, своевременно выявлять и устранять причины сбоев в его работе.

По умолчанию журнал хранится на ViPNet Coordinator IG (локальное ведение журнала), но вы можете настроить ведение журнала на удалённом сетевом узле (удалённое ведение журнала). Запись информации в журнал выполняется по протоколу syslog.

При локальном ведении журнала выполняется автоматическая ротация файла журнала для экономии места на ViPNet Coordinator IG. Когда размер файла журнала достигает 1 Гбайт, заполненный файл переименовывается, а файл журнала, который был переименован раньше остальных, удаляется. В результате на ViPNet Coordinator IG всегда хранятся десять заполненных файлов и один текущий файл.

Настройка

- Чтобы настроить удалённое ведение журнала:

  ```
  hostname# machine set loghost {<IP-адрес> | <доменное имя>},
  ```

  указав IP-адрес или доменное имя сетевого узла, на котором будет вестись журнал.

  Особенности настройки удалённого ведения журнала:

  - Если вы выбрали открытый узел для удалённого ведения журнала, на ViPNet Coordinator IG задайте локальный фильтр открытой сети, разрешающий исходящий трафик по протоколу UDP на порт 514 этого открытого узла.
  - При переключении интерфейса ViPNet Coordinator IG, через который передаются события журнала на удалённый узел, в режим получения настроек от DHCP-сервера возможна временная потеря связи с удалённым узлом.

    Чтобы избежать потери информации в период отсутствия связи, перед настройкой интерфейса включите локальное ведение журнала:

    ```
    machine set loghost local
    ```

    После применения настроек снова включите удалённое ведение журнала.
  - Не рекомендуется использовать удалённое ведение журнала в кластере, так как на удалённый сетевой узел не будут передаваться журналы с пассивного узла (то есть часть информации о работе ViPNet Coordinator IG будет утеряна).

    Чтобы использовать удалённое ведение журнала в кластере, задайте параметры ведения журнала на обоих узлах кластера, так как они не передаются с активного узла на пассивный.

- Чтобы отключить ведение системного журнала:

```
hostname# machine set loghost null
```



Внимание! Отключать ведение журнала не рекомендуется.

- Чтобы изменить уровень важности событий, регистрируемых в журнале, в секции `[debug]` конфигурационных файлов `iplir.conf`, `failover.ini`, `mftp.conf`, настройте параметр `debuglevel`. Описание параметров секции `[debug]` в данных файлах см. в документе «Справочник команд и конфигурационных файлов».



Примечание. В большинстве случаев изменять уровень важности, выбранный по умолчанию, не рекомендуется. При повышении уровня необходимо учитывать, что размер файла журнала будет быстро расти, вследствие чего, будет чаще производиться его ротация при достижении максимального размера (см. Системный журнал).

- Чтобы сообщения о работе службы выводились в консоль командного интерпретатора:

  ```
  hostname# debug on <источник> <уровень важности>
  ```

  Описание параметров команды см. в документе «Справочник команд и конфигурационных файлов».

  При этом в секции `[debug]` конфигурационных файлов `iplir.conf`, `failover.ini`, `mftp.conf` должны быть заданы параметры `facility` и `level`.

  Например, вы можете настроить протоколирование так, чтобы следить за работой разных служб на разных терминалах:

  - В конфигурационном файле одной из служб в секции `[debug]` задайте параметры, например:

    ```
    [debug]
    debuglogfile = syslog:daemon.debug
    debuglevel = 3
    ```

    И на одном из терминалов выполните команду:

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

  - В конфигурационном файле другой службы в секции `[debug]` укажите другое значение источника, например:

    ```
    [debug]
    debuglogfile = syslog:local0.debug
    debuglevel = 3
    ```

    И на другом терминале выполните команду:

    ```
    hostname# debug on local0 debug
    ```

  В результате на первый терминал будут поступать сообщения только от первой службы, на второй терминал — только от второй службы. Чтобы на первом терминале можно было следить за работой обеих служб, на нём в дополнение к первой команде выполните команду:

  ```
  hostname# debug on local0 debug
  ```



Примечание. Выводимые в консоль командного интерпретатора сообщения о работе служб могут смешиваться с сообщениями самого интерпретатора и командами, набираемыми в консоли. Для просмотра набранной к данному моменту части команды и продолжения её ввода используйте комбинацию клавиш **Ctrl+L**.

- Чтобы выключить вывод сообщений в консоль командного интерпретатора, выполните команду `debug off`. С помощью этой команды вы можете выключить как вывод всех сообщений, так и вывод только тех сообщений, которые соответствуют конкретным значениям параметров `facility` и `level`.

Просмотр журнала

Чтобы просмотреть записи системного журнала:

```
hostname# machine logs show syslog
```

Подробнее о параметрах команды см. в документе «Справочник команд и конфигурационных файлов».

Экспорт журналов на USB-носитель

Примечание. Команда экспорта журналов недоступна по SSH.

В результате экспорта создаётся архив журналов `logs_<идентификатор узла>_<платформа><ревизия платформы>_<версия ПО>_<название узла>_<YYYY_MM_DD_HH_MM_SS>.tar.gz`, который содержит:

- системный журнал;
- журнал аудита;
- журнал СКЗИ;
- журнал DNS-запросов;
- журнал MFTP.

Примечание. Для экспорта журнала IP-пакетов и журнала пакетов промышленных протоколов см. Журнал IP-пакетов и Экспорт журнала пакетов промышленных протоколов.

Чтобы экспортировать журналы на USB-носитель:

1. Выполните:

   ```
   hostname> machine logs export usb
   ```

2. Подключите USB-носитель к ViPNet Coordinator IG и нажмите **Enter**.

Чтобы экспортировать журналы на USB-носитель с их последующим удалением на ViPNet Coordinator IG:

1. Выполните:

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

2. Подключите USB-носитель к ViPNet Coordinator IG и нажмите **Enter**.

Подробнее о командах см. документ «Справочник команд и конфигурационных файлов», раздел «Команды группы machine».

16

Мониторинг состояния и просмотр статистики

Мониторинг по SNMP 340

Просмотр статистики передачи данных 348

Просмотр состояния оборудования 350

Мониторинг по SNMP

С помощью SNMP-агента, входящего в состав ПО ViPNet Coordinator IG, вы можете удалённо получать информацию о работе ViPNet Coordinator IG, а также настроить автоматическое уведомление о наиболее важных событиях, например потере связи с пассивным узлом кластера.

Информация, доступная по протоколу SNMP, представлена в виде набора SNMP-параметров. Каждый параметр имеет уникальный идентификатор (OID). Список доступных SNMP-параметров ViPNet Coordinator IG вы можете просмотреть в приложении Базы управляющей информации (MIB) для протокола SNMP.

Примечание. Все SNMP-параметры доступны только для чтения.

Для получения информации о состоянии ViPNet Coordinator IG вы можете использовать любое ПО мониторинга по протоколу SNMP (SNMP-менеджер), например:

- ViPNet Prime (модуль Network Visibility System).
- Утилита snmpwalk (пакет net-snmp).
- Zabbix.

Сетевой узел с установленным SNMP-менеджером называется сервером мониторинга.

Примечание. В качестве сервера мониторинга мы рекомендуем использовать защищённый или туннелируемый узел. Если будет использоваться открытый узел, необходимо добавить сетевые фильтры, разрешающие SNMP-трафик:

```
hostname# firewall local add src <IP-адрес сервера мониторинга> dst @local udp dport 161 pass
hostname# firewall local add src @local dst <IP-адрес сервера мониторинга> udp dport 162 pass
```

Протокол SNMP поддерживает следующие способы получения информации:

- Передача параметров по запросу. При этом сервер мониторинга посылает SNMP-запрос на ViPNet Coordinator IG и получает в ответ значения необходимых параметров.
- Передача уведомлений. SNMP-агент ViPNet Coordinator IG автоматически отправляет SNMP-уведомления на сервер мониторинга при наступлении определённого события.

Примечание. Чтобы SNMP-запросы обрабатывались корректно, необходимо отправлять их на IP-адрес ViPNet Coordinator IG, который доступен с сервера мониторинга по кратчайшему маршруту.

Если вы включили передачу SNMP-уведомлений, то после включения или перезагрузки ViPNet Coordinator IG доставка первых уведомлений о старте служб `iplircfg`, `mftpd`, `webgui` и `failoverd` на сервер мониторинга не гарантирована. Причина — отсутствие связи с сервером мониторинга во время инициализации сетевой подсистемы.

Если вы импортируете на сервер мониторинга MIB-файлы, поддерживаемые ViPNet Coordinator IG, вы сможете:

- использовать в SNMP-запросах текстовые обозначения параметров вместо числовых (например, `infVipNetHostName` вместо `.1.3.6.1.4.1.10812.1.1.7`);
- получать текстовые обозначения некоторых числовых параметров в ответах на SNMP-запросы (например, при запросе состояния интерфейса, вместо значения `1` или `2`, вы получите значение `up` или `down`);
- получать уведомления от ViPNet Coordinator IG в виде текстовых обозначений параметров вместо числовых (например, `infvpnWebStart` вместо `.1.3.6.1.4.1.10812.1.0.10`).

Вы можете скачать MIB-файлы через веб-интерфейс ViPNet Coordinator IG (см. документ «Настройка с помощью веб-интерфейса»).

SNMP-агент ViPNet Coordinator IG поддерживает одновременную работу по протоколам SNMPv1, SNMPv2c и SNMPv3.

Для ограничения доступа к SNMP-параметрам используются следующие подходы:

- В SNMPv1 и SNMPv2c используется параметр community, который является идентификатором и паролем доступа к SNMP-параметрам. ViPNet Coordinator IG ответит на SNMP-запрос, если community в запросе совпадает с любым из community, заданных на ViPNet Coordinator IG.

  Для получения SNMP-уведомлений сервером мониторинга в настройках его SNMP-менеджера и в настройках ViPNet Coordinator IG необходимо задать community для уведомлений.

- В SNMPv3 используются учётные записи пользователей SNMP. ViPNet Coordinator IG ответит на SNMP-запрос, если пользователю разрешён доступ на чтение параметров и данные пользователя в запросе совпадают с данными любого из пользователей, заданных на ViPNet Coordinator IG:
  - имя пользователя;
  - пароль пользователя и алгоритм хэширования пароля;
  - ключ и алгоритм шифрования (если заданы).

  Для получения SNMP-уведомлений сервером мониторинга в настройках его SNMP-менеджера необходимо указать данные одного из пользователей SNMP, заданных на ViPNet Coordinator IG. При использовании уведомлений типа TRAP в настройках SNMP-менеджера дополнительно к учётным данным пользователя необходимо указать параметр `engineID` (OID .1.3.6.1.6.3.10.2.1.1.0).

Настройка SNMP-агента

1 Для протоколов SNMPv1 и SNMPv2c:

1.1 Добавьте community для чтения SNMP-параметров:

```
hostname# inet snmp community add
```

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

Максимальное количество community — 16.

1.2 Задайте адрес сервера мониторинга для отправки SNMP-уведомлений:

```
hostname# inet snmp trapsink add <адрес> [port <номер>] [{v1 | inform}]
```

- `<адрес>` — IP-адрес или доменное имя сервера мониторинга;
- `<номер>` — номер UDP-порта;
- `v1` — отправлять уведомления типа TRAP по протоколу SNMPv1;
- `inform` — отправлять уведомления типа INFORM по протоколу SNMPv2c.

Если порт и тип уведомлений не указан, устанавливаются следующие значения:

- Тип отправляемых уведомлений — TRAP.
- Протокол отправки уведомлений — SNMPv2c.
- Порт, на который отправляются уведомления — UDP 162.

При выполнении команды необходимо ввести community, которое задано на сервере мониторинга для приёма SNMP-уведомлений (trap community).

Вы можете использовать до 16 сетевых узлов в качестве серверов мониторинга.



Внимание! Если задан порт, отличный от UDP 162, необходимо добавить сетевой фильтр, разрешающий передачу SNMP-уведомлений на данный порт:

- для узла защищённой сети: `hostname# firewall vpn add src @local dst <идентификатор узла> udp dport <номер порта> pass`
- для туннелируемого узла: `hostname# firewall tunnel add src @local dst <IP-адрес> udp dport <номер порта> pass`
- для открытого узла: `hostname# firewall local add src @local dst <IP-адрес> udp dport <номер порта> pass`

1.3 Разрешите чтение SNMP-параметров ViPNet Coordinator IG:

```
hostname# inet snmp v2 ro on
```

1.4 Включите отправку SNMP-уведомлений:

```
hostname# inet snmp v2 traps on
```

2 Для протокола SNMPv3:

2.1 Добавьте нового пользователя для доступа к SNMP-параметрам ViPNet Coordinator IG:

```
hostname# inet snmp user add <имя пользователя> [{md5 | sha}]
```

При добавлении пользователя требуется задать пароль и алгоритм хэширования пароля MD5 (по умолчанию) или SHA.

Длина имени пользователя — от 1 до 32 символов. Разрешённые символы — прописные и строчные буквы латинского алфавита и цифры.

Длина пароля — от 8 до 32 символов. Разрешённые символы — 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.



Примечание. По умолчанию пользователю разрешено чтение SNMP-параметров. Вы можете запретить чтение SNMP-параметров:

```
hostname# inet snmp user set <имя пользователя> read off
```

2.2 Для шифрования SNMP-трафика между сервером мониторинга и ViPNet Coordinator IG (по алгоритму AES-128) создайте ключ шифрования для пользователя:

```
hostname# inet snmp user set <имя пользователя> key
```

Длина ключа шифрования — от 8 до 32 символов. Разрешённые символы — 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.



Примечание. Если задан ключ шифрования, его необходимо указывать в SNMP-запросах наряду с другими данными пользователя SNMP.

2.3 Разрешите отправку SNMP-уведомлений для пользователя:

```
hostname# inet snmp user set <имя пользователя> trapsess on
```

2.4 Задайте адрес сервера мониторинга для отправки SNMP-уведомлений:

```
hostname# inet snmp user set <имя пользователя> trapsess add <адрес> [port <номер>]
[inform]
```

- `<адрес>` — IP-адрес или доменное имя сервера мониторинга;
- `<номер>` — номер UDP-порта;
- `inform` — отправлять уведомления типа INFORM.

Если порт и тип уведомлений не указан, устанавливаются следующие значения:

- Тип отправляемых уведомлений — TRAP.
- Порт, на который отправляются уведомления — UDP 162.

Внимание! Если задан порт, отличный от UDP 162, добавьте сетевой фильтр, разрешающий передачу SNMP-уведомлений на данный порт:



- для узла защищённой сети: `hostname# firewall vpn add src @local dst <идентификатор узла> udp dport <номер порта> pass`
- для туннелируемого узла: `hostname# firewall tunnel add src @local dst <IP-адрес> udp dport <номер порта> pass`
- для открытого узла: `hostname# firewall local add src @local dst <IP-адрес> udp dport <номер порта> pass`

2.5 Разрешите чтение SNMP-параметров по протоколу SNMPv3:

```
hostname# inet snmp v3 ro on
```

2.6 Включите отправку SNMP-уведомлений по протоколу SNMPv3:

```
hostname# inet snmp v3 traps on
```

3 По умолчанию SNMP-агент принимает запросы на UDP-порт 161. При необходимости измените номер порта:

```
hostname# inet snmp port <порт>
```



Внимание! При изменении номера порта добавьте соответствующий сетевой фильтр.

4 Включите запуск SNMP-агента при загрузке ViPNet Coordinator IG:

```
hostname# inet snmp autostart on
```

5 По умолчанию SNMP-агент регистрирует в системном журнале события с уровнем важности `error`. При необходимости измените уровень важности:

```
hostname# inet snmp logging <уровень важности>
```

Список возможных значений параметра `<уровень важности>`:

- `off` — регистрация событий выключена;
- `critical` — регистрируются критические ошибки, после которых SNMP-агент не может продолжить работу;
- `error` — регистрируются ошибки, после которых SNMP-агент может продолжать работу;
- `info` — регистрируется полная информация о работе SNMP-агента;
- `debug` — регистрируется служебная информация, используемая при отладке.

6 При необходимости задайте информацию о вашем ViPNet Coordinator IG, которая будет доступна по SNMP при чтении SNMP-параметров:

- Чтобы задать параметр **Контактное лицо** (sysContact OID .1.3.6.1.2.1.1.4.0):

  ```
  hostname# inet snmp system contact
  ```

- Чтобы задать параметр **Имя устройства** (sysName OID .1.3.6.1.2.1.1.5.0):

  ```
  hostname# inet snmp system name
  ```

- Чтобы задать параметр **Местоположение** (sysLocation OID .1.3.6.1.2.1.1.6.0):

  ```
  hostname# inet snmp system location
  ```



Примечание. Параметры **Имя устройства** и **Местоположение** не синхронизируются между узлами кластера.

---

7 Включите SNMP-агент:

```
hostname# inet snmp start
```

8 Проверьте выполненную настройку SNMP-агента:

```
hostname# inet snmp show
```

Полный список команд по настройке SNMP-агента см. в документе «Справочник команд и конфигурационных файлов».

Мониторинг кластера

Вы можете следить за состоянием обоих узлов кластера по протоколу SNMP. Приём SNMP-запросов и отправку SNMP-уведомлений выполняет активный узел. Для мониторинга пассивного узла кластера активный узел перенаправляет полученные SNMP-запросы на пассивный через интерфейс синхронизации и возвращает ответы отправителю.

Поскольку узлы кластера могут переключаться, SNMP-запрос должен указывать, какой из узлов должен на него ответить. Для этого используются следующие параметры SNMP-агента:

- При использовании SNMPv1 и SNMPv2c для каждого ViPNet Coordinator IG кластера создаётся community для режима кластера. SNMP-запрос с таким community будет адресован конкретному ViPNet Coordinator IG независимо от его текущего режима работы в кластере (активный или пассивный). При переключении системы защиты от сбоев в одиночный режим, community для режима кластера автоматически удаляется.
- При использовании SNMPv3 каждому узлу кластера назначается свой контекст (строка, идентифицирующая ViPNet Coordinator IG в кластере). Контексты создаются автоматически на активном узле в формате `Node<порядковый номер>`, где `<порядковый номер>` — число от 1, которое выбирается по возрастанию в соответствии с IP-адресом интерфейса синхронизации.

Для мониторинга кластера по протоколу SNMP:

1 Настройте SNMP-агент на активном узле кластера (см. Настройка SNMP-агента).

Настройки будут переданы на пассивный узел при последующей синхронизации.



Примечание. Если на момент развёртывания кластера SNMP-агент уже настроен на одном из ViPNet Coordinator IG, запускайте `failover` в режиме кластера сначала на ViPNet Coordinator IG с настроенным SNMP-агентом. Тогда другой узел кластера получит актуальную конфигурацию SNMP-агента от активного узла. Исходная конфигурация агента на пассивном узле при этом удаляется.

---

2 Перезапустите SNMP-агент на активном узле кластера:

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

3 Для SNMPv1 и SNMPv2c выполните действия на активном узле кластера:

3.1 Задайте community для мониторинга каждого из узлов кластера. Для этого выполните команду для каждого узла:

```
hostname# inet snmp cluster node <IP-адрес> community
```

где `<IP-адрес>` — IP-адрес интерфейса синхронизации узла кластера.

В ответ на сообщение `Type community:` введите community, отличное от других community. Допустимая длина — от 6 до 18 символов: прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.

Примечание. Просмотреть созданные для режима кластера community вы можете:

```
hostname# inet snmp cluster show community
```

3.2 Разрешите чтение SNMP-параметров узлов кластера по протоколам SNMPv1 и SNMPv2c:

```
hostname# inet snmp cluster v2 on
```

Примечание. Если выводится ошибка: `SNMPv1 and SNMPv2c support is OFF. Please, turn it on first`, выполните действия:

- разрешите чтение SNMP-параметров на активном узле кластера: `hostname# inet snmp v2 ro on`
- повторно разрешите чтение SNMP-параметров: `hostname# inet snmp cluster v2 on`

---

4 Для SNMPv3 на активном узле кластера:

4.1 Просмотрите контексты, присвоенные узлам кластера, чтобы использовать их в SNMP-запросах:

```
hostname# inet snmp cluster show
```

4.2 Чтобы изменить контекст узла:

```
hostname# inet snmp cluster node <IP-адрес> context <контекст>
```

где `<IP-адрес>` – IP-адрес интерфейса синхронизации узла кластера.

Допустимая длина контекста — от 1 до 32 символов: прописные и строчные буквы латинского алфавита и цифры.

5 На пассивном узле запустите SNMP-агент:

```
hostname# inet snmp start
```

6 В зависимости от версии протокола SNMP используйте созданные community или контексты в SNMP-запросах для получения информации о состоянии конкретного узла кластера (см. руководство по настройке используемого SNMP-менеджера):

- При использовании протоколов SNMPv1 и SNMPv2c отправляйте SNMP-запрос с community соответствующего узла кластера.
- При использовании протокола SNMPv3 отправляйте SNMP-запрос с учётными данными пользователя, созданного с помощью команды `inet snmp user add`, и контекстом соответствующего узла. Если запрос не содержит контекст, ответ будет получен от активного узла кластера.

Просмотр статистики передачи данных

Статистика передачи данных ведётся раздельно по всем интерфейсам с момента включения ViPNet Coordinator IG. Статистика учитывает текущую скорость интерфейсов и объём трафика.

Чтобы просмотреть статистику передачи данных на всех физических и агрегированных интерфейсах:

```
hostname> inet show traffic

Please wait for 3 sec. Gathering traffic....

Interface             RX speed            TX speed           RX Total         TX Total
----------           ---------           ---------         ---------        ---------
eth0              10,24 Kbit/s        12,37 Kbit/s          456,12 KB        517,37 KB
eth1             999,99  bit/s       634,12  bit/s           12,31 KB          6,27 KB
bond0               1,00 Gbit/s      1000,00 Mbit/s            1,10 TB       1022,12 GB
eth2              512,00 Mbit/s       500,00 Mbit/s          563,20 GB        511,06 GB
eth3              512,00 Mbit/s       500,00 Mbit/s          563,20 GB        511,06 GB


Mon Feb 2 09:55:16 2025
```

После запуска команды статистика отображается в режиме реального времени с заданным интервалом обновления (по умолчанию — 3 секунды). Чтобы завершить просмотр статистики, нажмите **Ctrl**+**C**. После перезагрузки ViPNet Coordinator IG или удаления интерфейса данные статистики сбрасываются.

При работе ViPNet Coordinator IG в режиме кластера просмотр статистики доступен на обоих узлах.

Чтобы просмотреть статистику передачи данных виртуального интерфейса `eth2.10` с интервалом обновления 10 секунд:

```
hostname> inet show traffic interface eth2.10 interval 10

Please wait for 10 sec. Gathering traffic....

Interface             RX speed            TX speed           RX Total         TX Total
----------           ---------           ---------         ---------        ---------
eth2.10           500,00 Mbit/s       530,00 Mbit/s          565,25 GB        515,07 GB


Mon Feb 2 09:59:19 2025
```

Вы можете просмотреть статистику обработанных IP-пакетов с учётом приоритета:

```
hostname> machine show priority-stats
```

По команде выводятся значения:

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

Просмотр состояния оборудования

Примечание. Просмотр состояния оборудования доступен только в исполнениях ViPNet Coordinator IG10 и ViPNet Coordinator IG100.

- Чтобы просмотреть краткую информацию о перегреве процессора, модема и состоянии дисковой памяти:

  ```
  hostname> hardware-status show
  ```

- Чтобы просмотреть подробную информацию о состоянии основной и дополнительной дисковой памяти:

  ```
  hostname> hardware-status show memory
  ```

- Чтобы просмотреть информацию о состоянии модема и установленном мобильном соединении:

  ```
  hostname> service usbmodem show status
  ```

Примечание.

- Описание параметров, которые отображаются в результате выполнения команд, см в документе «Справочник команд и конфигурационных файлов».
- Время отображается в системе UTC.
- Информация о перегреве оборудования и работе модема фиксируется также в системном журнале. Перечень событий вы можете просмотреть в приложении События системного журнала и журнала аудита.

Восстановление памяти

Вы можете запустить проверку дополнительной памяти с автоматическим восстановлением повреждённых секторов. Для этого запустите регламентное тестирование ViPNet Coordinator IG с параметром `rbb`:

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

Сначала будет выполнена проверка и восстановление памяти, после чего запустится регламентное тестирование (см. Контроль целостности файлов ПО).

A

Сетевые фильтры по умолчанию

Для межсетевого экрана типа «А/Б» и типа «Д» при работе в штатном режиме и режиме регламентного обслуживания

Таблица 11. Фильтры защищённой сети (vpn)

Название	Источник	Назначение	Протокол	Действие
Фильтры, добавляемые в режиме кластера (нередактируемые)				
ViPNet Service in	@any	@local	udp: from 2060 to 2060	pass
ViPNet Service out	@local	@any	udp: from 2060 to 2060	pass
Служебные фильтры (нередактируемые)				
Block not original udp port	@local	@any	udp: from 0–2045 to 2046, from 2047–65535 to 2046	drop
Allow ViPNet base services out	@local	• @any — при наличии лицензии VPN; • @AllCoordinators — при отсутствии лицензии VPN	udp: to 2046, from 2048 to 2048, from 2050 to 2050 tcp: to 2046	pass

Название	Источник	Назначение	Протокол	Действие
Allow ViPNet base services in	@any — при наличии лицензии VPN; @AllCoordinators — при отсутствии лицензии VPN	@local	udp: to 2046, from 2048 to 2048, from 2050 to 2050 tcp: to 2046	pass
Allow ViPNet MFTP in	@any	@local	tcp: to 5000–5003	pass
Allow ViPNet MFTP out	@local	@any	tcp: to 5000–5003	pass
Allow ViPNet Control services out	@local	<идентификатор ViPNet Prime>	@any	pass
Allow ViPNet Control services in	<идентификатор ViPNet Prime>	@local	@any	pass
Настраиваемые фильтры				
ICMP redirect in	@any	@local	icmp: 5	drop
ICMP redirect out	@local	@any	icmp: 5	drop
Allow ICMP Ping in	@any	@local	icmp: 8	pass
Allow ICMP Ping out	@local	@any	icmp: 8	pass
Allow ViPNet DBViewer in	@any	@local	tcp: to 2047	pass
Allow ViPNet DBViewer out	@local	@any	tcp: to 2047	pass
Allow ViPNet IpfView in	@any	@local	tcp: to 20001	pass
Allow ViPNet IpfView out	@local	@any	tcp: to 20001	pass
Allow DNS client	@local	@any	udp: to 53, tcp: to 53	pass
Allow DNS server	@any	@local	udp: to 53, tcp: to 53	pass
Allow NTP client	@local	@any	udp: to 123	pass
Allow NTP server	@any	@local	udp: to 123	pass
Allow DHCP client req	@local	@any	udp: from 68 to 67	pass
Allow DHCP client resp	@any	@local	udp: from 67 to 68	pass
Allow DHCP server req	@local	@any	udp: from 67 to 68	pass
Allow DHCP server resp	@any	@local	udp: from 68 to 67	pass

Название	Источник	Назначение	Протокол	Действие
Allow DHCP-Relay service in	@any	@local	udp: from 67 to 67	pass
Allow DHCP-Relay service out	@local	@any	udp: from 67 to 67	pass
Allow SSH client	@local	@any	tcp: to 22	pass
Allow syslog outgoing	@local	@any	udp: to 514	pass
Allow cef outgoing	@local	@any	udp: to 5001	pass
Allow SNMP	@any	@local	udp: to 161	pass
Allow SNMP traps	@local	@any	udp: to 162	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 12. Фильтры туннелируемых узлов (`tunnel`)

Название	Источник	Назначение	Протокол	Действие
Настраиваемые фильтры				
To all tunnel nodes	@any	@tunneledip	@any	pass
From all tunnel nodes	@tunneledip	@any	@any	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 13. Локальные фильтры открытой сети (`local`)

Название	Источник	Назначение	Протокол	Действие
Фильтры, добавляемые в режиме кластера (нередактируемые)				
Failover test IP	@local	<список значений параметров `testip` из `failover.ini`>	icmp	pass
Failover Channel in	@remote	interface <имя интерфейса синхронизации>	@any	pass
Failover Channel out	interface <имя интерфейса синхронизации>	@remote	@any	pass
Служебные фильтры (нередактируемые)				

Название	Источник	Назначение	Протокол	Действие
ViPNet Service Common In	@any	@local	tcp/udp: to 2046, to 2047, to 10096, to 5100, to 10092	drop
ViPNet Service Common Out	@local	@any	tcp/udp: from 2046	drop
Настраиваемые фильтры				
ICMP redirect out	@local	@any	icmp: 5	drop
ICMP redirect in	@any	@local	icmp: 5	drop
Block ICMP timestamp response	@local	@any	icmp: 14	drop
Allow ICMP Ping	@local	@any	icmp: 8	pass
Allow DNS	@local	@any	udp: to 53, tcp: to 53	pass
Allow NTP	@local	@any	udp: to 123	pass
Allow DHCP server req	@local	@any	udp: from 67 to 68	pass
Allow DHCP server resp	@any	@local	udp: from 68 to 67	pass
Allow DHCP-Relay service out	@local	@any	udp: from 67 to 67	pass
Allow DHCP-Relay service in	@any	@local	udp: from 67 to 67	pass
Allow ICMP blackhole response	@local	@any	icmp: 3/4	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Таблица 14. Транзитные фильтры открытой сети (`forward`)

Название	Источник	Назначение	Протокол	Действие
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

Для межсетевого экрана типа «Д» при работе в специальном режиме

Таблица 15. Фильтры защищённой сети (`vpn`), фильтры туннелируемых узлов (tunnel), локальные фильтры открытой сети (`local`) и транзитные фильтры открытой сети (`forward`)

Название	**Источник**	**Назначение**	**Протокол**	**Действие**
Настраиваемые фильтры				
Allow all	@any	@any	@any	pass
Блокирующий фильтр (нередактируемый)				
Block All Traffic	@any	@any	@any	drop

B

Пользовательские группы протоколов по умолчанию

По умолчанию в ViPNet Coordinator IG настроены пользовательские группы протоколов, перечисленные в таблице ниже.

Таблица 16. Пользовательские группы протоколов, настроенные по умолчанию

Имя группы протоколов	Состав группы протоколов
ABB-ESCP	TCP: to 6316, UDP: to 6316
ANSI-C12	TCP: to 1153, UDP: to 1153
BACNET	TCP: to 47808, UDP: to 47808
CITRIX	TCP: to 1494
Cluster	UDP: from 2060 to 2060
ClusterMonitoring	UDP: from 2060 to 2065, UDP: from 2065 to 2060
DNP3	TCP: to 20000, UDP: to 20000
DNS	UDP: to 53
DHCP	UDP: from 67-68 to 67-68
EHS	TCP: to 4535, UDP: to 4535
EHS-SSL	TCP: to 4536, UDP: to 4536
EIBnet	TCP: to 3671, UDP: to 3671
EtherCAT	TCP: to 34980, UDP: to 34980
EtherNET-IPoverTLS	TCP: to 2221

Имя группы протоколов	Состав группы протоколов
EtherNET-IPoverDTLS	UDP: to 2221
EtherNET-IP_I_O	TCP: to 2222, TCP: to 44818, UDP: to 44818
FTP	TCP: to 21
GRE	IP: 47
H323	TCP: to 1720
HTTP	TCP: to 80, TCP: to 8080
HTTP-Proxy	TCP: to 3128
HTTPS	TCP: to 443
IEC-60870-5-104	TCP: to 2404, UDP: to 2404
IEC-60870-5-104-secure	TCP: to 19998
IEC61850	TCP: to 29999
IEEE-MMS	TCP: to 651, UDP: to 651
IEEE-MMS-SSL	TCP: to 695, UDP: to 695
IGMP	IP: 2
IKE	UDP: to 500
IMAP	TCP: to 143
IPSecESP	IP: 50
Kerberos	TCP: to 88, TCP: to 749, UDP: to 88, UDP: to 749
L2TP	UDP: to 1701
LDAP	TCP: to 389, UDP: to 389
LonWorks	TCP: to 2540, TCP: to 2541, UDP: to 2540, UDP: to 2541
LotusNotes	TCP: to 1352
MFTP	TCP: to 5000-5003
ModbusTcp	TCP: to 502, UDP: to 502
MS-SQL	TCP: to 1433-1434, UDP: to 1433-1434
MySQL	TCP: to 3306
NetBIOS-DGM	UDP: from 138 to 138
NetBIOS-NC	UDP: from 137 to 137
NetMeeting	TCP: to 1503
NTP	UDP: to 123
OSPF	IP: 89

Имя группы протоколов	Состав группы протоколов
OPC_UA	TCP: to 4840, UDP: to 4840
OPC_UA_TLS-SSL	TCP: to 4843, UDP: to 4843
PING	ICMP: 8
POP3	TCP: to 110
Postgres	TCP: to 5432
PPTP	TCP: to 1723
Profinet	TCP: to 34962, TCP: to 34963, TCP: to 34964, UDP: to 34962, UDP: to 34963, UDP: to 34964
PTPEven	TCP: to 319, UDP: to 319
PTPGeneral	TCP: to 320, UDP: to 320
Radius	TCP: to 1812, TCP: to 1813, UDP: to 1812, UDP: to 1813
RadiusDA	TCP: to 3799
Radsec	TCP: to 2083, UDP: to 2083
RDP	TCP: to 3389
RTSP	TCP: to 554
SCCP	TCP: to 2000
SIP	TCP: to 5060, UDP: to 5060
SMTP	TCP: to 25
SNMP	UDP: to 161
SNMP-Traps	UDP: to 162
SNTP-HEARTBEAT	TCP: to 580, UDP: to 580
SSH	TCP: to 22
StateWatcher	TCP: to 2047, TCP: to 5100, TCP: to 10092
Syslog	UDP: to 514
Telnet	TCP: to 23
TFTP	UDP: to 69
UPnP	TCP: to 1900, TCP: to 2869, UDP: to 1900, UDP: to 2869
ViPNetBase	UDP: to 2046, UDP: from 2048 to 2048, UDP: from 2050 to 2050
WindowsMobileDevices	TCP: to 990, TCP: to 999, TCP: to 5678, TCP: to 5721, TCP: to 26675
WindowsMobileDevices2	UDP: to 5679
VNC	TCP: to 5900

Имя группы протоколов	Состав группы протоколов
ZigBee	TCP: to 17754, UDP: to 17754
ZigBeeIP	TCP: to 17755, TCP: to 17756, UDP: to 17755, UDP: to 17756
Z-Wave	TCP: to 4123, UDP: to 4123
Z-Wave-SSL-TLS	TCP: to 41230
Z-Wave-DTLS	UDP: to 41230
Z-Wave-Secure	TCP: to 44123

C

События журнала IP-пакетов

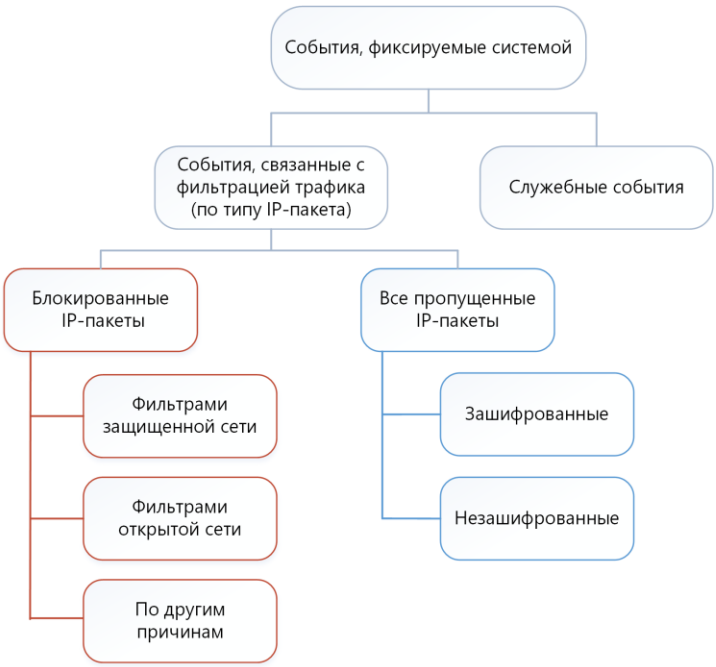


Рисунок 45. Классификация событий в журнале IP-пакетов

Таблица 17. События блокирования IP-пакетов фильтрами защищённой сети

Номер	Описание события
1	Не найден ключ для передачи пакета сетевому узлу с идентификатором, указанным в пакете
2	Неверное значение имитозащитной вставки пакета. Защищённые данные или открытая информация в пакете были изменены при передаче
3	Входящий зашифрованный или предназначенный для шифрования исходящий открытый пакет заблокирован фильтром защищённой сети

Номер	Описание события
4	Слишком большой таймаут пакета, то есть время его отправки отличается от времени его получения на величину, большую указанной в соответствующей настройке
5	Входящий пакет отправлен сетевым узлом с версией драйвера ViPNet, не совместимой с версией драйвера ViPNet на сетевом узле получателя
7	Метод шифрования, код которого указан во входящем пакете, не поддерживается
8	IP-пакет повреждён
9	Неизвестный идентификатор сетевого узла
11	IP-пакет заблокирован фильтром защищённой сети с ICMP или TCP RST ответом
13	Превышено максимальное время пребывания пакета в сети
14	Неверный адрес получателя пакета
15	Превышено допустимое количество одновременно обрабатываемых фрагментированных пакетов
16	Исчерпана лицензия на количество туннелируемых узлов
17	Неверный IP-адрес получателя
18	Неизвестный IP-адрес получателя
19	Подмена узла отправителя
26	Узел с данного координатора недоступен
27	Входящий зашифрованный или предназначенный для шифрования исходящий открытый пакет заблокирован фильтром защиты канала управления с генерацией REJECT сообщения ICMP
70	Транзитный IP-пакет заблокирован
71	Формат Iplir-пакета отличен от согласованного

Таблица 18. События блокирования IP-пакетов локальными фильтрами открытой сети

Номер	Описание события
20	Заблокирован открытый пакет
21	Идентификатор отправителя пакета неизвестен
22	От защищённого узла получен открытый пакет
23	От защищённого узла получен открытый широковещательный пакет
24	На порт, используемый одной из служб ViPNet, получен открытый пакет
30	Локальный пакет заблокирован фильтром открытой сети
31	Транзитный пакет заблокирован фильтром открытой сети

Номер	Описание события
32	Широковещательный пакет заблокирован фильтром открытой сети
33	Пакет заблокирован фильтром антиспуфинга
34	Локальный IP-пакет заблокирован фильтром открытой сети с ICMP или TCP RST ответом
35	Транзитный IP-пакет заблокирован фильтром открытой сети с ICMP или TCP RST ответом
36	IP-пакет заблокирован фильтром для туннелируемых узлов с ICMP или TCP RST ответом
37	Пакет заблокирован фильтром туннелируемых ресурсов
39	Пакет заблокирован фильтром по умолчанию при загрузке компьютера

Таблица 19. События блокирования IP-пакетов по другим причинам

Номер	Описание события
80	Размер заголовка IP-пакета меньше допустимого
81	Недопустимая версия протокола IP (поддерживается только IPv4)
82	Длина заголовка IP-пакета меньше допустимой
83	Длина IP-пакета меньше указанной в IP-заголовке
84	Значение контрольной суммы в заголовке IP-пакета отличается от её значения в IP-пакете
85	Размер TCP-заголовка меньше допустимого
86	Размер UDP-заголовка меньше допустимого
87	Обработаны не все фрагменты IP-пакета
88	Широковещательный адрес отправителя в IP-пакете
89	Перекрытие фрагментов IP-пакета. Наиболее устаревший из перекрываемых фрагментов IP-пакета отброшен
90	IP-пакет не был обработан, так как для его обработки недостаточно вычислительных ресурсов
91	IP-пакет получен во время инициализации драйвера ViPNet
92	Размер IP-пакета превышает 48 Кбайт
93	По истечении допустимого времени получены не все фрагменты IP-пакета
94	Недостаточно памяти
95	Получены два IP-пакета от узлов с разными IP-адресами и одинаковыми идентификаторами
97	Заблокирован пакет с установленным флагом DF, передача которого без фрагментации невозможна
98	Недостаточно ресурсов для обработки IP-пакета

Номер	Описание события
99	Заблокирован фрагментированный IP-пакет
100	IP-пакет заблокирован в ходе инспекции состояния соединения
101	Транзитный IP-пакет не может быть маршрутизирован
103	Количество установленных соединений превышает допустимое значение, заданное в соответствующих настройках
104	Соединение заблокировано, так как параметры исходящих пакетов (socketpair) для этого соединения совпадают с такими параметрами для ранее установленного соединения
105	Не удалось выделить динамический порт для правила трансляции адресов (в пуле нет свободных портов)
111	Не найден ключ обмена
112	Неверное значение имитозащитной вставки в незашифрованном пакете версии 4.2
113	Неизвестный идентификатор сетевого узла отправителя
115	Не удалось найти маршрут для IP-пакета в таблице маршрутизации
116	Не найден сетевой адаптер
117	Не удалось определить MAC-адрес получателя пакета по его IP-адресу
118	Ошибка при шифровании исходящего IP-пакета для защищённого узла
119	Получен зашифрованный IP-пакет неизвестного формата, который не может быть расшифрован
120	Ошибка при отправке IP-пакета защищённому узлу из-за проблем с доступом к этому узлу
121	Ошибка в работе кластера
122	Получен IP-пакет неизвестного протокола канального уровня
129	Получен широковещательный пакет с IP-адресом назначения, не принадлежащим подсети интерфейса
130	Отсутствуют свободные динамические порты, необходимые для создания соединения
131	Ошибка обработки прикладных протоколов: не удалось построить маршрут
132	Ошибка обработки прикладных протоколов: отсутствуют свободные динамические порты UDP
133	Ошибка обработки прикладных протоколов: порты источника и назначения IP-пакета принадлежат разным прикладным сервисам
134	Ошибка обработки прикладных протоколов: ошибка в таблице соответствия между прикладными сервисами и сетевыми протоколами, портами
135	Ошибка обработки модуля ALG
136	Недостаточно памяти для выполнения трансляции адреса (NAT)

Номер	Описание события
137	Шифрование исходящего IP-пакета с использованием данного алгоритма запрещено (тесты алгоритма не прошли)
138	Заблокирован IP-пакет на публичный DNS-сервер
139	Отсутствуют лицензии для туннелирования на узле назначения
147	Заблокирован IP-пакет с неизвестным протоколом

Таблица 20. События пропуска зашифрованных IP-пакетов

Номер	Описание события
40	Пропущен зашифрованный IP-пакет
41	Пропущен зашифрованный широковещательный IP-пакет
44	Маршрутизация зашифрованного транзитного IP-пакета с подменой адреса получателя
45	Пакет пропущен на туннелирующем координаторе, так как он поступил от туннелируемого узла или предназначен для такого узла

Таблица 21. События пропуска незашифрованных IP-пакетов

Номер	Описание события
60	Пропущен незашифрованный IP-пакет
61	Пропущен незашифрованный широковещательный IP-пакет
62	Пропущен незашифрованный транзитный IP-пакет
63	IP-пакет пропущен фильтром для туннелируемых ресурсов
64	IP-пакет пропущен при запуске ПО
65	Пропущен зашифрованный IP-пакет неизвестной ViPNet сети

Таблица 22. Служебные события

Номер	Описание события
42	Изменился IP-адрес сетевого узла
46	Изменились параметры доступа к сетевому узлу
47	Истёк интервал отправки IP-пакетов, передаваемых сетевым узлом своему серверу соединений. Событие может возникать только для тех узлов, которые работают через межсетевой экран с динамической трансляцией адресов
48	Узел доступен по широковещательному адресу
49	Изменился IP-адрес собственного сетевого узла

Номер	Описание события
50	IP-адрес перерегистрирован с другого узла на данный узел. Произведена перерегистрация адреса на данный узел. Если есть проблемы со связью, рекомендуется хотя бы для одного из конфликтных узлов, для которого это возможно, или для туннелируемых адресов узла с конфликтным адресом включить опцию «Использовать виртуальный адрес»
51	IP-адрес уже зарегистрирован на другом узле. Перерегистрация адреса на данный узел не произведена. Если есть проблемы со связью, рекомендуется хотя бы для одного из конфликтных узлов или для туннелируемых адресов узла с конфликтным адресом, для которого это возможно, включить опцию «Использовать виртуальный адрес»
110	Новый IP-адрес сетевого узла зарегистрирован на DNS-сервере
114	Пропущен зашифрованный IP-пакет для незарегистрированного узла ViPNet

D

Структура записи журнала IP-пакетов в формате CEF

Запись журнала IP-пакетов для экспорта по сети в формате CEF состоит из полей заголовка CEF и полей записи журнала.

Структура записи:

```
timestamp hostname CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

где:

- `timestamp` — отметка времени;
- `hostname` — имя сетевого узла;
- `Version` — номер версии CEF-нотации (значение равно нулю);
- `Device Vendor` — производитель устройства (`InfoTeCS`);
- `Device Product` — идентификатор устройства;
- `Device Version` — версия устройства;
- `Signature ID` — номер события (см. События журнала IP-пакетов) в журнале IP-пакетов;
- `Name` — описание события в журнале IP-пакетов;
- `Severity` — важность события:
  - 5 — если IP-пакет пропущен;
  - 10 — если IP-пакет блокирован;
- `Extension` — набор пар ключ-значение из словаря CEF, разделённых пробелом.

Таблица 23. Описание ключей словаря CEF поля Extension

Ключ словаря CEF	Описание ключа	Название поля в журнале
deviceExternalId	Идентификатор сенсора	
start	Начало интервала времени UTC, в течение которого несколько событий были объединены в одну запись журнала IP-пакетов	Interval Begin
end	Конец интервала времени UTC, в течение которого несколько событий были объединены в одну запись журнала IP-пакетов	Interval End
src	IP-адрес отправителя пакетов	Source IP
spt	Порт отправителя пакетов	Source port
dst	IP-адрес получателя пакетов	Destination IP
dpt	Порт получателя пакетов	Destination port
proto	Тип транспортного протокола (TCP или UDP)	IP protocol
cnt	Число пакетов, соответствующих выбранному типу события	Count
in	Размер входящих пакетов, соответствующих выбранному типу события	size in
out	Размер исходящих пакетов, соответствующих выбранному типу события	size out
deviceInboundInterface deviceOutboundInterface	Имя сетевого интерфейса, на котором были зарегистрированы события	Interface
cn1	Шестнадцатеричный идентификатор протокола Ethernet	Eth. protocol
cn1Label=Eth protocol hex		
deviceDirection	Направление пакета (входящий, исходящий)	Direction
• cs1=NAT {yes|no} • cs2=Drop {yes|no} • cs3=Broadcast {yes|no} • cs4=Forward {yes|no} • cs5=Encrypted {yes|no}	• NAT — флаг транслированного пакета; • Drop — флаг блокировки пакета; • Broadcast — флаг широковещательного пакета; • Forward — флаг транзитного пакета; • Encrypted — флаг зашифрованного пакета	

Ключ словаря CEF	Описание ключа	Название поля в журнале
cs1Label=Flags		
shost	Номер и имя сетевого узла ViPNet (отправителя)	Source node
dhost	Номер и имя сетевого узла ViPNet (получателя)	Destination node

E

События системного журнала и журнала аудита

Таблица 24. События, связанные с работой пользователя ViPNet Coordinator IG

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Перезагрузка по команде	`rvpn_shell[8548]: [02-01 09:46:09.213821]<8548>(00007f68d2725c40)[L3] | Command:'machine reboot'`	`Restart device SUCCESS`
Успешный запуск командного интерпретатора с помощью консоли	`login[23583]: pam_aauth(login:auth): granted access to user admin by LOGIN(uid=0)` `login[23583]: pam_aauth(login:session): session opened for user admin by LOGIN(uid=0)`	`User logon SUCCESS`

Выход из командного интерпретатора, работающего в режиме просмотра	`rvpn_shell[19591]: <EXIT> logout success`
	`...`
	`login[19247]: pam_aauth(login:session): session closed for user user`
		`Logoff SUCCESS`

Принудительное завершение сессии командного интерпретатора	`rvpn_shell[14381]: Session is forcefully terminated`	—

Событие	Пример записи в системном журнале	Пример записи в журнале аудита

Успешный удалённый запуск командного интерпретатора по протоколу SSH	`sshd[14734]: pam_aauth(sshd:auth): granted access to user user by (uid=0)`
	`sshd[14731]: Accepted keyboard-interactive/pam for user from 192.168.16.39 port 58168 ssh2`
	`sshd[14731]: pam_aauth(sshd:session): session opened for user user by (uid=0)`
	`...`
	`rvpn_shell[14742]: <LOGIN> Command: login - User logged in`
		`User logon SUCCESS`

Не удалось запустить командный интерпретатор при удалённом подключении по протоколу SSH	`aauth-tool[20299]: error: failed to login user user through AA: 8448` `sshd[20297]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.16.39 user=user`	`User logon FAILED`
Завершение удалённого подключения по протоколу SSH	`sshd[20626]: Received disconnect from 192.168.16.39 port 60808:11: disconnected by user` `sshd[20626]: Disconnected from 192.168.16.39 port 60808`	`Logoff SUCCESS`
Переход из режима настройки в режим просмотра	`rvpn_shell[10662]: <EXIT> Command 'exit'` `rvpn_shell[10662]: <EXIT> skip logout (admin mode)`	—
Изменение даты или времени	`rvpn_shell[13785]: <management> [ig100-2c670024] [local] [Single Mode] Set device date and time [success] [admin] Details: Command:'machine set date 2023-09-25 09:55:05 '`	`Set device date and time SUCCESS`
Переключение в режим регламентного обслуживания	`rvpn_shell[15197]: Mode switched successfully!` `rvpn_shell[15197]: service mode`	—
Успешное изменение файла `iplir.conf`	`rvpn_shell: <I_CFG> Command: iplir config - iplir.conf has been edited successfully.`	`SetIplirConfig SUCCESS`

Не удалось изменить файл `iplir.conf`	`rvpn_shell[26362]: error: Configuration checking failed`
	`rvpn_shell[26362]: Roll back the changes and restore the previous version of the file`
	или
	`rvpn_shell[26362]: error: Changing the settings is invalid when the process iplir is running. Please stop the process (iplir stop)`
		`SetIplirConfig FAILED`

Успешная смена пароля администратора	`rvpn_shell[26362]: The new password has been successfully set.`	`Set local administrator password SUCCESS`

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Не удалось сменить пароль администратора	`rvpn_shell[29610]: error: Entered passwords do not match.` `rvpn_shell[29610]: <management> [ig100-2c670024] [local] [Single Mode] Set local administrator password [failed] [admin] Details: Command:'admin passwd '`	`Set local administrator password FAILED`
Удаление справочников и ключей	`rvpn_shell[31061]: <management> [ig100-2c670024] [local] [Single Mode] Delete host links and keys [success] [admin] Details: Command:'admin remove keys '` `rvpn_shell[31061]: [02-01 13:54:06.144942]< 31061>(00007fd698e8dc40)[L3] | Command:'admin remove keys ' finished with rc=0 AAA__b141b9_7ae3c6_7a9cf8_60fafd rc=0 done`	`Delete host links and keys SUCCESS`
Успешная установка справочников и ключей	`keysetup[2242]: User password was correct and ds5-file VEM_ig10_vipnet_base_x86_64_5.1.0-4977.ds5 installed successfully`	—
Локальное обновление ПО	`rvpn_shell[8141]: /sbin/driv_upgrade.sh: process 8528 has been created`	`Update software locally using a USB drive SUCCESS`
Задание IP-адреса для сетевого интерфейса	`rvpn_shell[14053]: <management> [ig100-2c670024] [local] [Single Mode] Set network interface address [success] [admin] Details: Command:'inet ifconfig eth1 address 172.16.100.200 netmask 255.255.255.0 '`	`Set network interface address SUCCESS`
Сброс настроек сетевого интерфейса	`rvpn_shell[14053]: <management> [ig100-2c670024] [local] [Single Mode] Reset network interface [success] [admin] Details: Command:'inet ifconfig eth1 reset '` `rvpn_shell[14053]: [02-01 14:19:26.401259]< 14053>(00007ff757d34c40)[L3] | Command:'inet ifconfig eth1 reset ' finished with rc=0 AAA__fe5ce7_c48cd8_b47d02_77fe14 rc=0 done`	`Reset network interface SUCCESS`
Включение сетевого интерфейса	`vmunix: [13614.681497] vmxnet3 0000:0b:00.0 eth1: NIC Link is Up 10 Mbps`	`Set network interface state SUCCESS`
Выключение сетевого интерфейса	`rvpn_shell[14053]: <management> [ig100-2c670024] [local] [Single Mode] Set network interface state [success] [admin] Details: Command:'inet ifconfig eth1 down '`	`Set network interface state SUCCESS`

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Добавление статического маршрута	itcs-controld[5303]: [02-01 14:51:13.350100]<5303>(00007f192ee01700)[L3] | System::Routing<SR_ADD_ROUTE> Run command 'Command: inet route add' successful rvpn_shell[5154]: [02-01 14:51:13.354015]<5154>(00007ff178884c40)[L3] | Command:'inet route add distance=5,gateway=172.16.100.1,host=172.16.100.0,netmask=255.255.255.0,table_name=,table_number=254,weight=5' finished with rc=0 AAA__839737_b01001_4c11d5_b8e4a9 rc=0 done	Add static route SUCCESS
Удаление статического маршрута	itcs-controld[5303]: [02-01 14:56:52.463374]<5303>(00007f192f602700)[L3] | System::Routing<RT_DEL> Command: inet route delete 172.16.100.0. The following route was deleted: Table 254 (MAIN), Destination Netmask Next hop Distance Weight, ----------- ------- -------- -------- ------, 172.16.100.0 255.255.255.0 172.16.100.1 5 5 , itcs-controld[5303]: [02-01 14:56:52.463416]<5303>(00007f192f602700)[L3] | System::Routing<SR_DELETE_ROUTE_COMMON> 'Command: inet route delete' successful	Delete route SUCCESS
Создание виртуального интерфейса VLAN	rvpn_shell[5154]: New VLAN interface eth1.5 was created. ... rvpn_shell[5154]: <management> [va2000-3e130499] [local] [Single Mode] Add VLAN interface [success] [admin] Details: Command:'inet ifconfig eth1 VLAN add 5 '	Add VLAN interface SUCCESS
Удаление виртуального интерфейса VLAN	<management> [ig100-2c670024] [local] [Single Mode] Delete VLAN interface [success] [admin] Details: Command:'inet ifconfig eth1 vlan delete 5 '	Delete VLAN interface SUCCESS
Сохранение копии конфигурации VPN	rvpn_shell[5154]: <management> [ig100-2c670024] [local] [Single Mode] Current ViPNet configuration backing up [success] [admin] Details: Command:'vpn config save test_config '	Current ViPNet configuration backing up SUCCESS
Загрузка копии конфигурации VPN	rvpn_shell[5154]: <management> [ig100-2c670024] [local] [Single Mode] Load VPN configuration backup [success] [admin] Details: Command:'vpn config load test_config '	Load VPN configuration backup SUCCESS
Экспорт журнала регистрации IP-пакетов на USB-носитель	rvpn_shell[13459]: [02-06 15:57:56.005795]<13459>(00007fec1de51c40)[L3] | Command:'machine logs export network-traffic usb netlog' export_packetdb.sh[14737]: File successfully copied. Unmounting USB drive..	Export IP packet log to a USB drive SUCCESS

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Экспорт системного журнала	`export_log.sh[16540]: Copying logs_ig_3e130499_ig10-3e130499_2023_02_01_15_35_34.tar.gz to USB drive. Press —C to abort` `export_log.sh[16540]: File successfully copied. Unmounting USB drive...`	`Export event log SUCCESS`
Экспорт индивидуальной конфигурации на сервер ViPNet Prime	`export_appliance_configuration_file_to_usb.sh [20293]: File successfully copied. Unmounting USB drive..` `rvpn_shell[18277]: <management> [ig100-2c670024] [local] [Single Mode] Schedule configuration backup [success] [admin] Details: Command:'machine backup export '`	`Export configuration backup SUCCESS`

Экспорт индивидуальной конфигурации на USB-носитель	`export_appliance_configuration_file_to_usb.sh [4650]: File successfully copied. Unmounting USB drive..`
	`...`
	`export_appliance_configuration_file_to_usb.sh [4650]: ig100-2c670024-20230922T034846Z.ecf copied successfully.`
		`Export configuration backup SUCCESS`

Импорт индивидуальной конфигурации	`import_appliance_configuration_file.sh[12361]: Installing configuration /tmp/vipnet/ig100-2c670024-20230922T034846Z.ecf in /tmp/vipnet...`
	`...`
	`import_appliance_configuration_file_from_usb.sh[12361]: Settings successfully imported. You may remove the USB drive.`
		`Configuration import initiated SUCCESS`

Импорт универсальной конфигурации	`import_appliance_configuration_file.sh[9135]: Installing configuration /tmp/vipnet/ig100-2c670024-20230922T033003Z.vbe in /tmp/vipnet...`
	`...`
	`import_appliance_configuration_file.sh[8954]: Settings successfully imported. You may remove the USB drive.`
		`Configuration import initiated SUCCESS`

Экспорт универсальной конфигурации на USB-носитель	`export_appliance_configuration_file_to_usb.sh [8619]: File successfully copied. Unmounting USB drive..`
	`...`
	`export_appliance_configuration_file_to_usb.sh [8619]: ig100-2c670024-20230922T033003Z.vbe copied successfully.`
		`Export configuration backup SUCCESS`

Событие	Пример записи в системном журнале	Пример записи в журнале аудита

Изменение сетевых фильтров и правил трансляции адресов	Отображение изменения:
	`pncmd: [02-01 16:46:40.780465]< 24801>(00007f50d34c87c0)[L3] syslog | A rule was deleted:`
	`vpncmd: [02-01 16:46:40.780527]< 24801>(00007f50d34c87c0)[L3] syslog | Type:User ID:4000001 local src @any dst @local service @HTTP pass Enabled`
	`iplircfg[19943]: [02-01 16:46:40.797926]< 19943>(00007fdfc67fc700)[L3] syslog | User rules dataname has been changed.`
		`Add firewall filter SUCCESS`

Изменение правил фильтрации протокола Modbus	`rvpn_shell[4322]: <management> [ig100-2c670024] [local] [Single Mode] Ipf read/write request [success] [admin] Details: Command:'{"request":{"action":"update","objec t":"modbus","data":[{"name":"Rules_01","id":" 3361850049","clientid":"3580193441","enabled" :"true","fw_rule":[{"id":"0","name":"ipf_modb us_Rules_01_0","fw_table":"local","proto":"tc p","client_ip":{"sequence":[{"value":"192.168 .30.51"}]},"server_ip":{"sequence":[{"value": "10.10.10.12"}]},"server_port":{"sequence":[{ "value":"502"},{"value":"503"}]}}],"rule":[{" name":"Rule01","action":"pass","enabled":"tru e","id":{"sequence":[{"value":"2"},{"value":" 6"}]},"fc":{"sequence":[{"value":"3","upper": "4"}]},"r":{"sequence":[{"value":"30","upper" :"50"}]}}]}]}} '`	`Ipf read/write request SUCCESS`
Перевыпуск ключей локального SSH-сервера	`rvpn_shell[20540]: <management> [ig100-2c670024] [local] [Single Mode] Delete SSH local keys [success] [admin] Details: Command:'admin ssh remove key local '`	`Delete SSH local keys SUCCESS`
Издание сертификата администратора	`itcs-aad[1079]: [10-13 09:59:23.085637]<1079>(000000006f0fb3d0)[L0] | AUDIT ActionIsFinished: user:"admin" action System:AA:CreateLocalAdminCertificate ticket AAA_6deba6_lcl6ca_acbeb6_lc29fd`	—
Включение фильтрации протокола МЭК 60870-5-104 на прикладном уровне	`rvpn_shell[23329]: <management> [ig100-2c670024] [local] [Single Mode] Ipf read/write request [success] [admin] Details: Command:'{"request":{"action":"toggle","objec t":"iec104","data":[{"enabled":"true"}]}} '`	`Ipf read/write request SUCCESS`
Выключение фильтрации протокола Modbus на прикладном уровне	`rvpn_shell[16716]: <management> [ig100-2c670024] [local] [Single Mode] Ipf read/write request [success] [admin] Details: Command:'{"request":{"action":"toggle","objec t":"modbus","data":[{"enabled":"false"}]}} '`	`Ipf read/write request SUCCESS`
Включение вывода сообщений о событиях	`rvpn_shell[23693]: [02-01 16:52:13.269594]< 23693>(00007f07bbdaec40)[L3] | Command:'debug on'`	`Turn debug notification on/off SUCCESS`

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Выключение вывода сообщений о событиях	`rvpn_shell[23693]: [02-01 16:54:29.797997]<23693>(00007f07bbdaec40)[L3] | Command:'debug off'`	`Turn debug notification on/off SUCCESS`

Таблица 25. События, связанные с запуском или остановкой служб ViPNet Coordinator IG

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Запуск службы `failoverd`, отвечающей за систему защиты от сбоев	`rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Start/Stop failover daemon [success] [admin] Details: Command:'failover start '`	`Start failover daemon SUCCESS`
Завершение работы службы `failoverd`, отвечающей за систему защиты от сбоев	`rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Start/Stop failover daemon [success] [admin] Details: Command:'failover stop '`	`Stop failover daemon SUCCESS`
Запуск управляющей службы `iplircfg`	`hwvipmod[16584]: Loading ViPNet modules ...` `rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Start/Stop iplir daemon [success] [admin] Details: Command:'iplir start '`	`Start iplir daemon SUCCESS`
Завершение работы управляющей службы `iplircfg`	`rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Start/Stop iplir daemon [success] [admin] Details: Command:'iplir stop '`	`Stop iplir daemon SUCCESS`
Перезапуск веб-сервера ViPNet Coordinator IG	`rvpn_shell[10750]: <management> [ig100-2c670024] [local] [Single Mode] Restart web server [success] [admin] Details: Command:'webui restart '`	`Restart web server SUCCESS`
Запуск службы шлюза Modbus	`rvpn_shell[18999]: <management> [ig100-2c670024] [local] [Single Mode] Turn ModbusGateway on/off [success] [admin] Details: Command:'mbgw start '`	`Update ModbusGateway config SUCCESS`
Завершение работы службы шлюза Modbus	`rvpn_shell[18999]: <management> [ig100-2c670024] [local] [Single Mode] Turn ModbusGateway on/off [success] [admin] Details: Command:'mbgw stop '`	`Update ModbusGateway config SUCCESS`
Запуск службы `piomonotor`	`rvpn_shell[18320]: <management> [ig100-2c670024] [local] [Single Mode] Turn PIO_MONITOR on/off [success] [admin] Details: Command:'piomonitor on '`	`Turn PIO_MONITOR on`
Завершение работы службы `piomonotor`	`rvpn_shell[17495]: <management> [ig100-2c670024] [local] [Single Mode] Turn PIO_MONITOR on/off [success] [admin] Details: Command:'piomonitor off '`	`Turn PIO_MONITOR off`

Таблица 26. События, связанные с обменом служебной информацией с управляющим ПО

Событие	Пример записи в системном журнале	Пример записи в журнале аудита
Применение обновления информации об управляющем ПО	`itcs-external-controld[4378]: <management> [ig100-2c670024] [local] [Single Mode] control action [success] [System] Action id: Applying Manager Information Updates Details: Starting ApplyPolicy`	`Applying Manager Information Updates SUCCESS/FAIL`
Применение изменений фильтров межсетевого экрана из управляющего ПО	`itcs-external-controld[4378]: <management> [ig100-2c670024] [local] [Single Mode] control action [success] [System] Action id: Apply firewall filters received from the management software Details: Starting ApplyPolicy`	`Apply firewall filters received from the management software SUCCESS/FAIL`

Применение обновления лицензии от управляющего ПО	`itcs-external-controld[4742]: <management> [ig100-2c670024] [local] [Single Mode] control action [success] [System] Action id: Applying a license upgrade from a control application Details: Starting ApplyPolicy`
	`...`
	`itcs-external-controld[4742]: <management> [ig100-2c670024] [local] [Single Mode] control action [success] [System] Action id: Applying a license upgrade from a control application Details: Finish`
		`Applying a license upgrade from a control application SUCCESS/FAIL`

Подключение к транспортному серверу UT5	`Connection established, subcribed to publisher endpoint`	—
Отсутствие подключения к транспортному серверу UT5	`Connection error: <Connection timed out! Wait and repeat connection...>`	—

Таблица 27. События, связанные с работой системы защиты от сбоев

Событие	Пример записи в системном журнале

Переключение узла кластера в активный режим	`failoverd[6976]: [02-02 10:13:38.300387]< 6976>(00007f054f9847c0)[L2] Exit | active server not responding, switching to active mode`
	`failoverd[6976]: [02-02 10:13:38.300423]< 6976>(00007f054f9847c0)[L1] syslog | switching to active mode`
	`vmunix: [ 320.636326] [DUP] switch cluster mode: passive (1) => active (2)`

Переключение узла кластера в пассивный режим из-за отсутствия физического соединения на сетевом интерфейсе	`vmunix: [ 4927.663675] vmxnet3 0000:0b:00.0 eth1: NIC Link is Down`
	`failover-node[31518]: Configuring state of daemons for passive mode`
	`vmunix: [ 4940.296325] [DUP] switch cluster mode: active (2) => passive (1)`

Событие	Пример записи в системном журнале
Перезагрузка узла кластера из-за конфликта режимов	`failoverd[18143]: [02-02 13:04:44.026129]< 18143>(00007f4db882e7c0)[L1] syslog | Rebooted due conflict mode at Thu Feb 2 13:04:44 2023`

Перезагрузка узла кластера из-за обнаружения службой `failoverd` ошибки другой контролируемой службы	`failoverd[6973]: [02-02 12:19:35.032019]< 6973>(00007f9a752617c0)[L1] CheckApp | Reached maximum count of application restarts [iplircfg] pid 2008`
	`failoverd[6973]: [02-02 12:19:35.032029]< 6973>(00007f9a752617c0)[L3] OnInvokeEventCmd | Rebooting the appliance in order to recover`
	`failoverd[6973]: [02-02 12:19:35.470798]< 6973>(00007f9a752617c0)[L1] syslog | one or more subsystems failed, rebooting`
	`failoverd[6973]: [02-02 12:19:35.470823]< 6973>(00007f9a752617c0)[L1] syslog | Rebooted due to watcher detected error at Thu Feb 2 12:19:35 2023`
	`syslogd (GNU inetutils 1.9.4): restart`

Таблица 28. События, связанные с обменом служебной информацией между узлами ViPNet

Событие	Пример записи в системном журнале
Получение сообщения о доступности узла ViPNet (сообщения рассылаются при включении узла, а затем периодически)	`iplircfg[7226]: [02-02 15:11:38.237440]< 7226>(00007fcb66e40980)[L2] | got message: type 1 from ID 0x3E130001 (msg name 'YY0N29WO.KI5')`
Получение сообщения о доступности узла ViPNet (сообщения рассылаются при первом обращении к серверу IP-адресов)	`iplircfg[5095]: [01-23 10:14:59.709058]< 5095>(00007ff998c2f980)[L2] | got message: type 3 from ID 0x3E130001 (msg name 'GJ5ZUZSZ.JJ0')`
Первое обращение к серверу соединений, если сервер не является сервером IP-адресов	`iplircfg[1684]: [02-07 21:28:10.979295]< 1684>(00007f5563f66980)[L2] | got message: type 23 from ID 0x3E1305DA (msg name 'AAZD}YP7.493')`
Отключение узла ViPNet от сервера IP-адресов	`iplircfg[29142]: [02-02 13:36:53.678221]< 29142>(00007f40cc3a3980)[L2] | got message: type 2 from ID 0x3E130001 (msg name 'DKNYU56I.BV1')`
Проверка соединения с узлом ViPNet (запрос)	`iplircfg[29142]: [02-02 13:33:36.169191]< 29142>(00007f40cc3a3980)[L2] | got message: type 5 from ID 0x3E1304A5 (msg name '6RB8POLJ.DGC')`
Подтверждение получения сообщения (кроме уведомлений об изменении адреса доступа удалённого узла ViPNet)	`iplircfg[29142]: [02-02 13:33:36.320283]< 29142>(00007f40cc3a3980)[L2] | got message: type 7 from ID 0x3E1304A5 (msg name 'UOPO9T1T.DRR')`

Событие	Пример записи в системном журнале
Уведомление об изменении адреса доступа удалённого узла ViPNet	`iplircfg[29142]: [02-02 13:46:06.699250]< 29142>(00007f40cc3a3980)[L2] | got message: type 50 from ID 0x3E130002 (msg name 'NTP964KK.0FJ')`
Подтверждение получения уведомления об изменении адреса доступа удалённого узла ViPNet	`iplircfg[7226]: [02-02 15:03:56.491499]< 7226>(00007fcb66e40980)[L2] | got message: type 70 from ID 0x3E130001 (msg name '31J92W9V.6YN')`
Изменение параметров адреса доступа удалённого узла ViPNet	`iplircfg[25757]: [02-02 15:23:54.171023]< 25757>(00007fbcf1f9f980)[L2] | load natsettings for 0x3E130193: firewallip=192.168.166.105 port=55888 timeout=25 virtualip=0.0.0.1 proxyid=0x3E130001 DRV_ALWAYS_USE_SERVER=no DRV_GREEN_NODE=yes DRV_STOP_FIREWALL_IP=no DRV_ELAPSE=no DRV_BROADCAST_HOST=no DRV_INCAPS_FORCE_REAL_ADDR=yes`

Таблица 29. События, связанные с состоянием оборудования и беспроводных соединений

Событие	Пример записей в журнале
Достижение критического порога температур процессора	`vmunix: [60487.978244] CPU critical temps 105`
Достижение критического порога температур модема	`usbmodemd[6709]: RequestTemp: temp 71000 is max`
Достижения критического порога напряжения на модеме	`usbmodemd[6709]: RequestVoltage: voltage 32000 out of range`
Опрос уровня сигнала Wi-Fi	`root: [WifiClient] Station cc:2d:e0:90:d8:c7; signal: -49 dBm; connected time: 246 seconds`
Запуск модема	`usbmodemd[5544]: USBModemDevice: found support modem VID/PID: 05c6:9003, VendorModel: Quectel UC20` `usbmodemd[5544]: NetworkSettingInit: MCC/MNC 250/99`
Неисправность SIM-карты или её отсутствие	`usbmodemd[6709]: SimInit: sim card not insert`
Состояние SIM-карты невозможно определить	`usbmodemd[6709]: SimInit: unknown status`
SIM-карта готова к работе, ввод PIN-кода не требуется	`usbmodemd[5544]: SimInit: pin status READY`
Требуется PIN-код для SIM-карты	`usbmodemd[5544]: SimInit: pin status SIM PIN`
PIN-код для SIM-карты введён успешно	`usbmodemd[5544]: SimInit: enter pin OK`
Инициализация SIM-карты	`usbmodemd[5544]: SimInit: sim card initialization`

Событие	Пример записей в журнале
Обнаружены мобильные сети	`usbmodemd[6709]: FillNetworksList: networks Beeline,MTS,MegaFon,TELE2`
Опрос состояния текущего мобильного соединения	`usbmodemd[5045]: RequestNetworkName: network MegaFon (3G)`
Опрос уровня сигнала мобильного соединения	`usbmodemd[5045]: RequestSignalLevel: signal level 19`
Опрос счётчика исходящего трафика за текущую сессию мобильного соединения (в байтах)	`usbmodemd[5045]: PPPTrafficInfo: update traffic info, tx=854 rx=485`
Опрос состояния службы установки соединения по модему	`usbmodemd[5544]: PPPManager: check pppd, pid=5553`
Опрос количества подключений к мобильной сети с момента запуска службы установки соединения по модему	`usbmodemd[5544]: PPPManager: connect count 1`

Таблица 30. События, связанные с доступностью каналов связи в режиме работы MultiWAN

Событие	Пример записей в журнале
Шлюз недоступен	`dgdd[19471]: next hop: GW-1 switched from up to down`
Шлюз доступен	`dgdd[19471]: next hop: GW-1 switched from down to up`
Переключение политики маршрутизации	`dgdd[19471]: dgd rule: performing action: preference 10, type 1, command 'policy route-GW-1'`

Таблица 31. События, связанные с работой устройств, подключенных по технологии PoE

Событие	Пример записей в журнале
Число неудачных попыток опроса устройства достигло значения, при котором устройство считается недоступным	`igpoed[5610]: Error | channel eth1 restart; error: 2 icmp checks failed`
Превышение ограничения потребляемого тока	`igpoed[4401]: Error | channel eth1 in error: port overcurrent timeout`
Превышение ограничения потребляемого тока при подаче питания	`igpoed[4401]: Error | channel eth1 in error: port startup overcurrent timeout`
Превышение заданного	`igpoed[4401]: Error | channel eth1 in error: port current limit`

Событие	Пример записей в журнале
пользователем ограничения потребляемой мощности	`timeout`
Блокировка устройства при пониженном напряжении	`igpoed[4401]: Error | channel eth1 in error: port analog supply under voltage lockout`
Выход из режима блокировки при пониженном напряжении	`igpoed[4401]: Error | channel eth1 in error: port digital supply under voltage lockout`
Перегрев контроллера	`igpoed[2153]: Error | channel eth1 in error: port overtemperature`
Ошибка связи с микросхемой PoE	`igpoed[2153]: Error | channel eth1 in error: communication error`
Неисправность полевого транзистора	`igpoed[2153]: Error | channel eth1 in error: port mosfet has failed`

Таблица 32. События, связанные с ошибками датчика случайных чисел (ДСЧ) и шифратора

Событие	Пример записей в журнале

Проверка при запуске и регламентная проверка ДСЧ в криптодрайвере	`uprngd: uprngd 0x7f2963fff700 lcuprng.c :434 core_normative_control Normative control was successfully completed.`
	`itcshubd[17962]: <crypto> [ig100-2c670024] [local] [Single Mode] CryptoEvent0 [failed] [] Details: SoftToken 0x7f55da5ad700 Reglament inspection passed`
	`itcshubd[17962]: SoftToken 0x7f55da5ad700 Reglament inspection passed`

Событие	Пример записей в журнале
Проверка при запуске и регламентная проверка шифраторов в криптодрайвере	itcshubd[2652]: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem GOST status=0 (0x854CAC47) itcshubd[2652]: <crypto> [hw100] [local] [Single Mode] Cryptodriver status check completed successfully [success] [9b12a8a2-d776-43a4-b10b-d99949555cdb] Details: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem GOST status=0 (0x854CAC47) itcshubd[2652]: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem FIPS status=8000000 (0x854CAC47) itcshubd[2652]: <crypto> [hw100] [local] [Single Mode] Cryptodriver status check completed successfully [success] [9b12a8a2-d776-43a4-b10b-d99949555cdb] Details: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem FIPS status=8000000 (0x854CAC47) itcshubd[2652]: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem CUSTOM status=8000000 (0x854CAC47) itcshubd[2652]: <crypto> [hw100] [local] [Single Mode] Cryptodriver status check completed successfully [success] [9b12a8a2-d776-43a4-b10b-d99949555cdb] Details: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146 | AUDIT INFO: CryptSystem CUSTOM status=8000000 (0x854CAC47)

Примечание. Записи об успешной работе ДСЧ или шифратора не протоколируются.

Таблица 33. События антивирусной проверки и контент-фильтрации

Событие	Пример записей в журнале
Сработало запрещающее правило контроля содержимого трафика по HTTP-методу	(squid): 1 172.16.50.5 TCP_DENIED/403 19183 GET http://kremlin.ru/ - NONE/- text/html
Сработало запрещающее правило контроля содержимого трафика по MIME-типу	(squid): 58 172.16.100.5 TCP_DENIED_REPLY/403 19248 GET http://static.kremlin.ru/media/events/files/ru/QdJ0ybmN7Kocwc8eyTGosdyuylM6qXpj.pdf - DIRECT/95.173.136.78 text/html
Средство антивирусной защиты заблокировало скачивание заражённого файла	(squid): ICAP: 13 172.16.100.5 icap://192.168.32.11:1344/virus_scan RESPMOD http://www.virusanalyst.com/eicar.zip

F

Базы управляющей информации (MIB) для протокола SNMP

MIB-II System

MIB-II System (.1.3.6.1.2.1.1) включает в себя объекты, предназначенные для получения информации о системных параметрах сетевого узла (например, имя узла, ОС, количество и параметры сетевых интерфейсов, статистика по SNMP-сообщениям). Подробнее см. в RFC 1213.

Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator IG могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP рекомендуется вместо индексов использовать названия (логические имена) сетевых интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 34. SNMP-параметры. MIB-II System

OID	Описание
.1.3.6.1.2.1.1.1.0	Информация о сетевом узле (имя узла, информация об ОС).
.1.3.6.1.2.1.1.2.0	OID SNMP-агента.
.1.3.6.1.2.1.1.3.0	Время работы SNMP-агента с последнего запуска (sysUpTime).

OID	Описание
.1.3.6.1.2.1.1.4.0	Контактная информация администратора. Задается командой `inet snmp system contact`. Если информация не задана, параметр отсутствует.
.1.3.6.1.2.1.1.5.0	Имя, назначенное сетевому узлу. Задается командой `inet snmp system name`. Если имя не задано, параметр равен `hostname`.
.1.3.6.1.2.1.1.6.0	Место расположения сетевого узла. Задается командой `inet snmp system location`. Если не задано, параметр отсутствует.
.1.3.6.1.2.1.1.8.0	Значение sysUpTime с момента последнего изменения состояния или значения столбца .1.3.6.1.2.1.1.9.1.2.A из таблицы .1.3.6.1.2.1.1.9.1.

Таблица поддерживаемых MIB (.1.3.6.1.2.1.1.9.1):

A — индекс таблицы

.1.3.6.1.2.1.1.9.1.1.A	Индекс таблицы.
.1.3.6.1.2.1.1.9.1.2.A	OID для MIB, с которыми работает SNMP-агент.
.1.3.6.1.2.1.1.9.1.3.A	Текстовое описание MIB.
.1.3.6.1.2.1.1.9.1.4.A	Время с момента подключения MIB.

ARP-таблица (.1.3.6.1.2.1.3.1.1):

B — индекс интерфейса, присвоенный сетевым узлом

E — IP-адрес сетевого узла

.1.3.6.1.2.1.3.1.1.1.B.1.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.3.1.1.2.B.1.E	MAC-адрес.
.1.3.6.1.2.1.3.1.1.3.B.1.E	IP-адрес, соответствующий MAC-адресу.

Таблица описания маршрутов (.1.3.6.1.2.1.4.21.1):

E — IP-адрес сетевого узла или сети

.1.3.6.1.2.1.4.21.1.1.E	IP-адрес назначения маршрутов (маршрут по умолчанию 0.0.0.0).
.1.3.6.1.2.1.4.21.1.2.E	Индекс интерфейса (1.3.6.1.2.1.2.2.1.1), через который будет производится маршрутизация.
.1.3.6.1.2.1.4.21.1.3.E	Основная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.4.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.5.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.6.E	Дополнительная метрика протокола маршрутизации (если не используется, передается значение 1).
.1.3.6.1.2.1.4.21.1.7.E	IP-адрес следующего маршрутизатора по маршруту (Next Hop).

OID	Описание
.1.3.6.1.2.1.4.21.1.8.E	Тип маршрута: • 1 (other) — другое, не может быть причислено к другим категориям, • 2 (invalid) — некорректный, • 3 (direct) — маршрут к подключенной сети, • 4 (indirect) — маршрут к удаленной сети.
.1.3.6.1.2.1.4.21.1.9.E	Механизм маршрутизации, через который был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP.
.1.3.6.1.2.1.4.21.1.10.E	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.21.1.11.E	Маска маршрута.
.1.3.6.1.2.1.4.21.1.12.E	Дополнительная метрика протокола маршрутизации.
.1.3.6.1.2.1.4.21.1.13.E	Информация о протоколе маршрутизации, с помощью которого был получен маршрут. Если эта информация не представлена, параметр равен 0.0.
.1.3.6.1.2.1.11.1.0	Количество полученных сообщений SNMP.
.1.3.6.1.2.1.11.2.0	Количество отправленных сообщений SNMP.
.1.3.6.1.2.1.11.3.0	Количество полученных сообщений SNMP неподдерживаемой версии.
.1.3.6.1.2.1.11.4.0	Количество полученных сообщений SNMP, адресованных неизвестному сообществу.
.1.3.6.1.2.1.11.5.0	Количество полученных сообщений SNMP, содержащих операцию, не разрешенную на сетевом узле для сообщества.
.1.3.6.1.2.1.11.6.0	Количество ошибок ASN.1 или BER при разборе SNMP-сообщений.

OID	Описание
.1.3.6.1.2.1.11.8.0	Количество входящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.9.0	Количество входящих SNMP PDU, для которых значение поля error-status – «noSuchName».
1.3.6.1.2.1.11.10.0	Количество входящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.11.0	Количество входящих SNMP PDU, для которых значение поля error-status – «readOnly».
.1.3.6.1.2.1.11.12.0	Количество входящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.13.0	Количество успешно полученных MIB объектов с использованием Get-Request и Get-Next.
.1.3.6.1.2.1.11.14.0	Количество успешно записанных MIB объектов с использованием Set-Request.
.1.3.6.1.2.1.11.15.0	Количество успешно обработанных SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.16.0	Количество успешно обработанных SNMP Get-Next PDUs.
.1.3.6.1.2.1.11.17.0	Количество успешно обработанных SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.18.0	Количество успешно обработанных SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.19.0	Количество успешно обработанных SNMP Trap PDUs.
.1.3.6.1.2.1.11.20.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «tooBig».
.1.3.6.1.2.1.11.21.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «noSuchName».
.1.3.6.1.2.1.11.22.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «badValue».
.1.3.6.1.2.1.11.24.0	Количество исходящих SNMP PDU, для которых значение поля error-status – «genErr».
.1.3.6.1.2.1.11.25.0	Количество успешно сгенерированных исходящих SNMP Get-Request PDUs.
.1.3.6.1.2.1.11.26.0	Количество успешно сгенерированных исходящих SNMP Get-Next PDUs.
.1.3.6.1.2.1.11.27.0	Количество успешно сгенерированных исходящих SNMP Set-Request PDUs.
.1.3.6.1.2.1.11.28.0	Количество успешно сгенерированных исходящих SNMP Get-Response PDUs.
.1.3.6.1.2.1.11.29.0	Количество успешно сгенерированных исходящих SNMP Trap PDUs.

OID	Описание
.1.3.6.1.2.1.11.30.0	Возможность отправки authenticationFailure traps: • 1 - разрешено, • 2 – запрещено.

IF-MIB

IF-MIB (.1.3.6.1.2.1.2) включает в себя объекты, предназначенные для получения информации о параметрах сетевых интерфейсов сетевого узла (например, тип сетевого интерфейса, физический адрес, пропускная способность). Подробнее см. в RFC 2863.

Примечание. Количество и индексы сетевых интерфейсов ViPNet Coordinator IG могут различаться для разных групп OID в описывающих их таблицах. При настройке мониторинга по протоколу SNMP рекомендуется вместо индексов использовать названия (логические имена) сетевых интерфейсов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 35. SNMP-параметры. IF-MIB

OID	Описание
.1.3.6.1.2.1.2.1.0	Количество сетевых интерфейсов (физических, виртуальных, включая loopback).
Таблица объектов, описывающих сетевые интерфейсы (.1.3.6.1.2.1.2.2.1):	
A — индекс интерфейса	
.1.3.6.1.2.1.2.2.1.1.A	Индекс сетевого интерфейса (A).
.1.3.6.1.2.1.2.2.1.2.A	Описание интерфейса (производитель, название и версия оборудования или ПО).
.1.3.6.1.2.1.2.2.1.3.A	Тип сетевого интерфейса: • 6 — ethernet, • 24 — localhost. Остальные значения можно посмотреть здесь.
.1.3.6.1.2.1.2.2.1.4.A	MTU (в байтах).
.1.3.6.1.2.1.2.2.1.5.A	Максимальная пропускная способность (бит/сек).
.1.3.6.1.2.1.2.2.1.6.A	MAC-адрес.
.1.3.6.1.2.1.2.2.1.7.A	Назначенное состояние интерфейса: • 1 (up) — включен, • 2 (down) — выключен, • 3 (testing) — состояние тестирования, указывает, что никакие рабочие пакеты не могут быть переданы.

OID	Описание
.1.3.6.1.2.1.2.2.1.8.A	Текущее рабочее состояние интерфейса: • 1 (up) — включен, • 2 (down) — выключен, • 3 (testing) — состояние тестирования. Никакие рабочие пакеты не могут быть переданы, • 4 (unknown) — неизвестно, • 5 (dormant) — интерфейс ожидает внешних действий (таких как последовательная линия, ожидающая входящее соединение), • 6 (notPresent) — в интерфейсе отсутствуют компоненты (обычно аппаратные), • 7 (lowerLayerDown) — не работает из-за состояния интерфейса нижнего уровня.
.1.3.6.1.2.1.2.2.1.9.A	Время работы SNMP-агента с начала его запуска (sysUpTime) до момента перехода интерфейса в его текущее состояние.
.1.3.6.1.2.1.2.2.1.10.A	Количество полученных байт (октетов).
.1.3.6.1.2.1.2.2.1.11.A	Количество полученных одноадресных (unicast) пакетов.
.1.3.6.1.2.1.2.2.1.12.A	Количество полученных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.13.A	Количество отклоненных пакетов.
.1.3.6.1.2.1.2.2.1.14.A	Количество пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.15.A	Количество пакетов, которые были отклонены из-за неизвестного или не поддерживаемого протокола.
.1.3.6.1.2.1.2.2.1.16.A	Количество отправленных байт (октетов).
.1.3.6.1.2.1.2.2.1.17.A	Количество отправленных одноадресных (unicast) пакетов.
.1.3.6.1.2.1.2.2.1.18.A	Количество отправленных широковещательных (broadcast) и многоадресных (multicast) пакетов.
.1.3.6.1.2.1.2.2.1.19.A	Количество отклоненных отправленных пакетов.
.1.3.6.1.2.1.2.2.1.20.A	Количество отправленных пакетов, отклоненных из-за ошибок.
.1.3.6.1.2.1.2.2.1.21.A	Количество исходящих пакетов в очереди на отправку.
Таблица статистики дополнительных параметров сетевых интерфейсов (.1.3.6.1.2.1.31.1.1.1): **A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1**	
.1.3.6.1.2.1.31.1.1.1.1.A	Имя интерфейса.
.1.3.6.1.2.1.31.1.1.1.2.A	Количество входящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.3.A	Количество входящих широковещательных (broadcast) пакетов.
.1.3.6.1.2.1.31.1.1.1.4.A	Количество исходящих многоадресных (multicast) пакетов.
.1.3.6.1.2.1.31.1.1.1.5.A	Количество исходящих широковещательных (broadcast) пакетов.

OID	Описание
.1.3.6.1.2.1.31.1.1.1.6.A	Количество байт (октетов), принятых интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.7.A	Количество входящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.8.A	Количество входящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.9.A	Количество входящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.10.A	Количество байт (октетов), отправленных интерфейсом (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.11.A	Количество исходящих одноадресных (unicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.12.A	Количество исходящих многоадресных (multicast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.13.A	Количество исходящих широковещательных (broadcast) пакетов (64-разрядный счетчик).
.1.3.6.1.2.1.31.1.1.1.14.A	Необходимость отправки trap на события linkUp/linkDown: • 1 — отправлять trap, • 2 — не отправлять trap.
.1.3.6.1.2.1.31.1.1.1.15.A	Максимальная скорость интерфейса (Мегабит/сек).
.1.3.6.1.2.1.31.1.1.1.16.A	Режим работы интерфейса: • 1 (true) — принимает все пакеты, • 2 (false) — принимает только пакеты, адресованные сетевому узлу.
.1.3.6.1.2.1.31.1.1.1.17.A	Наличие физического коннектора у интерфейса: • 1 (true) — есть коннектор (для ethernet), • 2 (false) — нет коннектора (для localhost).
.1.3.6.1.2.1.31.1.1.1.18.A	Имя интерфейса, заданное администратором. Для координатора всегда равно 0.
.1.3.6.1.2.1.31.1.1.1.19.A	Время работы SNMP-агента с последнего запуска (sysUpTime) до появления разрыва в подсчете счетчиков на интерфейсе.

IP-MIB

IP-MIB (.1.3.6.1.2.1.4) включает в себя объекты, предназначенные для получения информации о работе сетевого узла по протоколу IP (например, параметры сетевых интерфейсов, статистика для IP-трафика, таблица IP-адресов). Подробнее см. в RFC 4293.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 36. SNMP-параметры. IP-MIB

OID	Описание
.1.3.6.1.2.1.4.1.0	Указывает, является ли сетевой узел маршрутизатором: • 1 — является (координатор всегда работает в данном режиме), • 2 — не является.
.1.3.6.1.2.1.4.2.0	TTL по умолчанию для IP-пакетов.
.1.3.6.1.2.1.4.3.0	Общее количество IP-пакетов, принятых сетевым узлом, включая пакеты с ошибками.
.1.3.6.1.2.1.4.4.0	Количество входящих IP-пакетов, отклонённых сетевым узлом по причине ошибок в заголовке пакета.
.1.3.6.1.2.1.4.5.0	Количество входящих IP-пакетов, отклонённых сетевым узлом по причине ошибок в адресе.
.1.3.6.1.2.1.4.6.0	Количество IP-пакетов, переданных на следующий шлюз.
.1.3.6.1.2.1.4.7.0	Количество IP-пакетов, отклонённых по причине неизвестного или неподдерживаемого протокола.
1.3.6.1.2.1.4.8.0	Количество отклонённых IP-пакетов по причине недостатка буфера.
.1.3.6.1.2.1.4.9.0	Количество успешно доставленных IP-пакетов.
.1.3.6.1.2.1.4.10.0	Количество IP-пакетов, отправленных сетевым узлом (не включая .1.3.6.1.2.1.4.6.0).
.1.3.6.1.2.1.4.11.0	Количество IP-пакетов, отклонённых по причине недостатка буфера.
.1.3.6.1.2.1.4.12.0	Количество IP-пакетов, отклонённых к дальнейшей передаче по причине отсутствия маршрута.
.1.3.6.1.2.1.4.13.0	Максимальное количество секунд ожидания сборки фрагментов.
.1.3.6.1.2.1.4.14.0	Количество принятых IP-фрагментов.
.1.3.6.1.2.1.4.15.0	Количество успешных сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.16.0	Количество ошибок сборок IP-пакетов из фрагментов.
.1.3.6.1.2.1.4.17.0	Количество успешно фрагментированных исходящих IP-пакетов.
.1.3.6.1.2.1.4.18.0	Количество ошибок при фрагментации исходящих IP-пакетов.
.1.3.6.1.2.1.4.19.0	Количество фрагментов IP-пакетов, сгенерированных данным сетевым узлом.
Таблица IP-адресов сетевого узла для протокола IPv4 (.1.3.6.1.2.1.4.20.1.):	
E — IP-адрес	
.1.3.6.1.2.1.4.20.1.1.E	IP-адрес.

OID	Описание
.1.3.6.1.2.1.4.20.1.2.E	Указатель на интерфейс, которому присвоен этот IP-адрес (A - из таблицы .1.3.6.1.2.1.2.2.1).
.1.3.6.1.2.1.4.20.1.3.E	Маска сети.
.1.3.6.1.2.1.4.20.1.4.E	Значение наименее значимого бита в широковещательном (broadcast) IP-адресе.
1.3.6.1.2.1.4.20.1.5.E	Максимальный размер входящего фрагментированного IP-пакета, который сетевой узел может собрать на этом интерфейсе.

Таблица разрешения IP-адресов в физические адреса (ARP-таблица) (.1.3.6.1.2.1.4.22.1.):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB

E — IP-адрес

.1.3.6.1.2.1.4.22.1.1.A.E	Индекс интерфейса, для которого видна связка IP-MAC.
.1.3.6.1.2.1.4.22.1.2.A.E	MAC-адрес.
.1.3.6.1.2.1.4.22.1.3.A.E	IP-адрес.
.1.3.6.1.2.1.4.22.1.4.A.E	Тип маппинга: • 1 — другое, • 2 — некорректный, • 3 — динамический, • 4 — статический.
.1.3.6.1.2.1.4.23.0	Количество отклонённых маршрутов.
.1.3.6.1.2.1.4.31.1.1.	Таблица, содержащая статистику (счётчики) IP-трафика различных версий на сетевом узле для всех интерфейсов.

Таблица префиксов IP-адресов (.1.3.6.1.2.1.4.32.1.):

A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB

B — тип адреса:

- **значение 0 — неизвестно,**
- **значение 1 — ipv4,**
- **значение 2 — ipv6,**
- **значение 3 — ipv4z,**
- **значение 4 — ipv6z,**
- **значение 16 — dns.**

C — префикс (адрес сети)

D — длина префикса

OID	Описание
.1.3.6.1.2.1.4.32.1.5.A.B.C.D	Источник префикса: • 1 — другое, • 2 — вручную, • 3 — общеизвестный префикс, • 4 — dhcp, • 3 — routeradv (значение получено от роутера).
.1.3.6.1.2.1.4.32.1.6.A.B.C.D	Указывает, может ли префикс использоваться как маршрут: • 1 — может, • 2 — не может.
.1.3.6.1.2.1.4.32.1.7.A.B.C.D	Указывает, может ли префикс использоваться для автоматической конфигурации адреса: • 1 — может, • 2 — не может.
.1.3.6.1.2.1.4.32.1.8.A.B.C.D	Время (в секундах), в течение которого префикс будет оставаться предпочтительным. Значение 4294967295 означает бесконечность.
.1.3.6.1.2.1.4.32.1.9.A.B.C.D	Время (в секундах), в течение которого префикс будет существовать. Значение 4294967295 означает бесконечность.
.1.3.6.1.2.1.4.33.0	Служебный объект, необходимый для синхронизации изменений параметров IP-MIB при взаимодействии с несколькими SNMP менеджерами. Используется только в случае записи данных в OID.

Таблица адресной информации по интерфейсам (.1.3.6.1.2.1.4.34.1):

B — тип адреса:

- **значение 0 — неизвестно,**
- **значение 1 — ipv4,**
- **значение 2 — ipv6,**
- **значение 3 — ipv4z,**
- **значение 4 — ipv6z,**
- **значение 16 — dns.**

E — IP-адрес

.1.3.6.1.2.1.4.34.1.3.B.E	Индекс сетевого интерфейса.
.1.3.6.1.2.1.4.34.1.4.B.E	Тип адреса: • 1 (unicast) — одноадресный, • 2 (anycast) — к ближайшему узлу, • 3 (broadcast) — широковещательный.
.1.3.6.1.2.1.4.34.1.5.B.E	Ссылка на строку таблицы префиксов.

OID	Описание
.1.3.6.1.2.1.4.34.1.6.B.E	Происхождение адреса: • 1 (other) — другое, • 2 (manual) — назначен вручную, • 4 (dhcp) — назначен по dhcp, • 5 (linklayer) — назначен механизмом автоконфигурации протокола IPv6 (SLAAC), • 6 (random) — назначен случайным образом.
.1.3.6.1.2.1.4.34.1.7.B.E	Статус адреса: • 1 (preferred) — предпочтительный, • 2 (deprecated) — устарел, • 3 (invalid) — недействителен, • 4 (inaccessible) — недоступен, • 5 (unknown)— неизвестен, • 6 (tentative) — предварительный, • 7 (duplicate) — дублированный, • 8 (optimistic) — оптимистичный.
.1.3.6.1.2.1.4.34.1.8.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента создания записи.
.1.3.6.1.2.1.4.34.1.9.B.E	Время работы SNMP-агента после запуска (sysUpTime) до момента изменения записи.
.1.3.6.1.2.1.4.34.1.10.B.E	Статус строки: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод её в статус active, • 5 (createAndWait) — создание строки и перевод её в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.2.1.4.34.1.11.B.E	Механизм хранения строки: • 1 (other) — другое, • 2 (volatile) — изменяемая, • 3 (nonvolatile) — энергонезависимая, • 4 (permanent) — постоянная, • 5 (readOnly) — только для чтения.

OID	Описание
Таблица трансляции MAC IP (.1.3.6.1.2.1.4.35.1):	
A — индекс интерфейса из таблицы .1.3.6.1.2.1.2.2.1.1 MIB-II	
B — тип адреса: • **0 — неизвестно,** • **1 — ipv4,** • **2 — ipv6,** • **3 — ipv4z,** • **4 — ipv6z,** • **16 — dns.**	
E — IP-адрес	
.1.3.6.1.2.1.4.35.1.4.A.B.E	Транслируемый MAC-адрес.
.1.3.6.1.2.1.4.35.1.5.A.B.E	Время работы SNMP-агента с момента последнего запуска (sysUpTime) до момента изменения MAC-адреса.
.1.3.6.1.2.1.4.35.1.6.A.B.E	Тип маппинга: • 1 (other) — другое, • 2 (invalid) — недопустимое значение, • 3 (dynamic) — динамическое, • 4 (static) — статическое, • 5 (local) — предоставляется для собственного адреса интерфейса объекта.
.1.3.6.1.2.1.4.35.1.7.A.B.E	Статус маппинга: • 1(reachable) — подтверждён, • 2 (stale) — не подтверждён, • 3 (delay) — ожидание, • 4 (probeprobe) — активное, • 5 (invalid) — недействителен, • 6 (unknown) — не определён, • 7 (incomplete) — выполняется разрешение адреса.
.1.3.6.1.2.1.4.35.1.8.A.B.E	Статус строки: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод её в статус active, • 5 (createAndWait) — создание строки и перевод её в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.2.1.5.1.0	Общее число ICMP-запросов, полученных сетевым узлом.
.1.3.6.1.2.1.5.2.0	Число ICMP-запросов с ошибкой, полученных сетевым узлом.

OID	Описание
.1.3.6.1.2.1.5.3.0	Количество сообщений о недоступности заданного сетевого узла, полученных данным сетевым узлом.
.1.3.6.1.2.1.5.4.0	Количество сообщений об истечении времени ожидания ответа, полученных сетевым узлом.
.1.3.6.1.2.1.5.5.0	Количество полученных сообщений ICMP Parameter Problem.
.1.3.6.1.2.1.5.6.0	Количество полученных сообщений ICMP Source Quench.
.1.3.6.1.2.1.5.7.0	Количество полученных сообщений ICMP Redirect messages.
.1.3.6.1.2.1.5.8.0	Количество полученных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.9.0	Количество полученных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.10.0	Количество полученных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.11.0	Количество полученных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.12.0	Количество полученных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.13.0	Количество полученных сообщений ICMP Address Mask Reply.
.1.3.6.1.2.1.5.14.0	Количество ICMP сообщений, отправленных сетевым узлом.
.1.3.6.1.2.1.5.15.0	Количество ICMP сообщений, которые сетевой узел не смог отправить из-за проблем с ICMP.
.1.3.6.1.2.1.5.16.0	Количество отправленных сообщений ICMP Destination Unreachable.
.1.3.6.1.2.1.5.17.0	Количество отправленных сообщений ICMP Time Exceeded.
.1.3.6.1.2.1.5.18.0	Количество отправленных сообщений ICMP Parameter Problem.
1.3.6.1.2.1.5.19.0	Количество отправленных сообщений ICMP Source Quench.
1.3.6.1.2.1.5.20.0	Количество отправленных сообщений ICMP Redirect.
1.3.6.1.2.1.5.21.0	Количество отправленных сообщений ICMP Echo (request).
.1.3.6.1.2.1.5.22.0	Количество отправленных сообщений ICMP Echo Reply.
.1.3.6.1.2.1.5.23.0	Количество отправленных сообщений ICMP Timestamp (request).
.1.3.6.1.2.1.5.24.0	Количество отправленных сообщений ICMP Timestamp Reply.
.1.3.6.1.2.1.5.25.0	Количество отправленных сообщений ICMP Address Mask Request.
.1.3.6.1.2.1.5.26.0	Количество отправленных сообщений ICMP Address Mask Reply.

IP-FORWARD-MIB

IP-FORWARD-MIB (.1.3.6.1.2.1.4.24) включает в себя объекты, предназначенные для получения информации о параметрах маршрутизации сетевого узла. Подробнее см. в RFC 4292.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 37. SNMP-параметры. IP-FORWARD-MIB

OID	Описание
Таблица маршрутизации сетевого узла (.1.3.6.1.2.1.4.24.4.1):	
.1.3.6.1.2.1.4.24.4.1.1.A.B.C.D	Адрес назначения маршрута (A).
.1.3.6.1.2.1.4.24.4.1.2.A.B.C.D	Маска адреса назначения маршрута (B).
.1.3.6.1.2.1.4.24.4.1.3.A.B.C.D	Параметр, обозначающий значение поля IP TOS Field (C).
.1.3.6.1.2.1.4.24.4.1.4.A.B.C.D	Адрес следующего маршрутизатора в маршруте (D).
.1.3.6.1.2.1.4.24.4.1.5.A.B.C.D	Индекс интерфейса, для которого задан маршрут из таблицы .1.3.6.1.2.1.2.2.1 IF-MIB.
.1.3.6.1.2.1.4.24.4.1.6.A.B.C.D	Тип маршрута: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (reject) — недостижимый, • 3 (local) — маршрут, в котором адрес следующего маршрутизатора является адресом назначения, • 4 (remote) — маршрут, в котором адрес следующего маршрутизатора не является адресом назначения.
.1.3.6.1.2.1.4.24.4.1.7.A.B.C.D	Механизм маршрутизации, с помощью которого был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP, • 15 (idpr) — протокол IDRP, • 16 (ciscoEigrp) — протокол cisco EIGRP.
.1.3.6.1.2.1.4.24.4.1.8.A.B.C.D	Время жизни маршрута с последнего обновления (в секундах).

OID	Описание
.1.3.6.1.2.1.4.24.4.1.9.A.B.C.D	Информация о протоколе маршрутизации, с помощью которого был получен маршрут. Если эта информация не представлена, параметр равен 0.0.
.1.3.6.1.2.1.4.24.4.1.10.A.B.C.D	Номер AS, к которой относится следующий маршрутизатор в маршруте. Если неизвестен или если для маршрутизации не используется, параметр равен 0.
.1.3.6.1.2.1.4.24.4.1.11.A.B.C.D	Основная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.12.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.13.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.14.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.15.A.B.C.D	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.4.1.16.A.B.C.D	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление
1.3.6.1.2.1.4.24.6.0	Количество текущих корректных маршрутов из таблицы .1.3.6.1.2.1.4.24.7.1
Таблица маршрутизации сетевого узла с указанием версии протокола IP (.1.3.6.1.2.1.4.24.7.1):	
.1.3.6.1.2.1.4.24.7.1.7	Индекс интерфейса, для которого задан маршрут из таблицы .1.3.6.1.2.1.2.2 IF-MIB.
.1.3.6.1.2.1.4.24.7.1.8	Тип маршрута: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (reject) — недостижимый, • 3 (local) — маршрут, в котором адрес следующего маршрутизатора является адресом назначения, • 4 (remote) — маршрут, в котором адрес следующего маршрутизатора не является адресом назначения, • 5 (blackhole) — маршрут, по которому пакеты теряются без сообщений об ошибках.

OID	Описание
.1.3.6.1.2.1.4.24.7.1.9	Механизм маршрутизации, с помощью которого был получен маршрут: • 1 (other) — другое, не может быть отнесен к остальным группам, • 2 (local) — статический маршрут, заданный в конфигурации, • 3 (netmgmt) — протокол SNMP, • 4 (icmp) — протокол ICMP (Redirect), • 5 (egp) — протокол EGP, • 6 (ggp) — протокол GGP, • 7 (hello) — протокол Hello, • 8 (rip) — протокол RIP, • 9 (is-is) — протокол IS-IS, • 10 (es-is) — протокол ES-IS, • 11 (ciscoIgrp) — протокол cisco IGRP, • 12 (bbnSpfIgp) — протокол BBNSPFIGP, • 13 (ospf) — протокол OSPF, • 14 (bgp) — протокол BGP, • 15 (idpr) — протокол IDRP, • 16 (ciscoEigrp) — протокол cisco EIGRP.
.1.3.6.1.2.1.4.24.7.1.10	Время жизни маршрута с последнего обновления (в секундах).
.1.3.6.1.2.1.4.24.7.1.11	Номер AS, к которой относится следующий маршрутизатор в маршруте. Если неизвестен или если для маршрутизации не используется, параметр равен 0.
.1.3.6.1.2.1.4.24.7.1.12	Основная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.13	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.14	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.15	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.
.1.3.6.1.2.1.4.24.7.1.16	Дополнительная метрика маршрута. Если метрика не используется, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.4.24.7.1.17	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

Ethernet-Like MIB

Ethernet-Like MIB (1.3.6.1.2.1.10) включает в себя объекты, предназначенные для получения статистической информации о работе интерфейсов сетевого узла. Подробнее см. в RFC 3635.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 38. SNMP-параметры. Ethernet-Like MIB

OID	Описание
Таблица статистики Ethernet-интерфейсов (.1.3.6.1.2.1.10.7.2.1): **A — индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB**	
.1.3.6.1.2.1.10.7.2.1.1.A	Индекс интерфейса из таблицы 1.3.6.1.2.1.2.2.1.1 IF-MIB.
.1.3.6.1.2.1.10.7.2.1.2.A	Количество ошибок на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.3.A	Количество FCS ошибок на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.4.A	Количество фреймов, вовлечённых в SingleCollision на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.5.A	Количество фреймов, вовлечённых в MultiplyCollision на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.6.A	Количество ошибок SQE TEST ERROR на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.7.A	Количество фреймов, для которых первая попытка отправки была отложена на интерфейсе.
.1.3.6.1.2.1.10.7.2.1.8.A	Количество обнаружения коллизий на интерфейсе, при котором коллизия обнаружена позднее одного slotTime.
.1.3.6.1.2.1.10.7.2.1.9.A	Количество фреймов, которые не удалось передать в связи с коллизиями.
.1.3.6.1.2.1.10.7.2.1.10.A	Количество фреймов, которые не удалось передать в связи с проблемами MAC уровня.
.1.3.6.1.2.1.10.7.2.1.11.A	Количество ошибок передачи в связи с потерей carrier sense condition на интерфейсе.

OID	Описание
.1.3.6.1.2.1.10.7.2.1.13.A	Количество фреймов, принятых на интерфейсе, размер которых превышал максимально допустимый.
.1.3.6.1.2.1.10.7.2.1.16.A	Количество фреймов, которые не удалось принять на интерфейсе в связи с ошибками MAC уровня.
.1.3.6.1.2.1.10.7.2.1.17.A	Идентификатор чипа, который реализует Ethernet-интерфейс.
.1.3.6.1.2.1.10.7.2.1.18.A	Количество ошибок.
.1.3.6.1.2.1.10.7.2.1.19.A	Текущий режим дуплекса на интерфейсе: • 1 — unknown, • 2 — halfDuplex, • 3 — fullDuplex. Для неподключённых интерфейсов параметр равен 1.
1.3.6.1.2.1.10.7.2.1.20.A	Возможность контроля скорости передачи на интерфейсе: • 1 — разрешено, • 2 — запрещено.
.1.3.6.1.2.1.10.7.2.1.21AA	Статус контроля скорости передачи на интерфейсе: • 1 — выключен, • 2 — включен, • 3 — неизвестно.

TCP-MIB

TCP-MIB (.1.3.6.1.2.1.6) включает в себя объекты, предназначенные для получения информации о работе сетевого узла по протоколу TCP (например, количество отправленных сегментов, активных соединений). Подробнее см. в RFC 4022.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 39. SNMP-параметры. TCP-MIB

OID	Описание
.1.3.6.1.2.1.6.1.0	Алгоритм определения таймаута для повторной передачи неопознанных октетов.
.1.3.6.1.2.1.6.2.0	Минимальное допустимое значение таймаута для повторной передачи (в миллисекундах).
.1.3.6.1.2.1.6.3.0	Максимальное допустимое значение таймаута для повторной передачи (в миллисекундах).
.1.3.6.1.2.1.6.4.0	Максимальное количество TCP-соединений. При динамическом определении, параметр равен -1.

OID	Описание
.1.3.6.1.2.1.6.5.0	Количество прямых переходов TCP-соединений из состояния CLOSED в состояние SYN-SENT.
.1.3.6.1.2.1.6.6.0	Количество прямых переходов TCP-соединений из состояния LISTEN в состояние SYN-RCVD.
.1.3.6.1.2.1.6.7.0	Количество прямых переходов TCP-соединений в состояние CLOSED из состояния SYN-SENT или SYN-RCVD, а также прямых переходов в состояние LISTEN из состояния SYN-RCVD.
.1.3.6.1.2.1.6.8.0	Количество переходов TCP-соединений в состояние CLOSED из состояния ESTABLISHED или CLOSE-WAIT.
.1.3.6.1.2.1.6.9.0	Количество TCP-соединений, находящихся в состоянии ESTABLISHED или CLOSE-WAIT.
.1.3.6.1.2.1.6.10.0	Количество полученных сегментов, в том числе с ошибками. Включает только количество полученных сегментов на соединениях, установленных в настоящий момент.
.1.3.6.1.2.1.6.11.0	Количество отправленных сегментов.
.1.3.6.1.2.1.6.12.0	Общее количество повторно отправленных сегментов.

Таблица TCP-соединений для протокола IPv4 (.1.3.6.1.2.1.6.13.1):

A - локальный IP-адрес

B - локальный порт

C - удаленный IP-адрес

D - удаленный порт

OID	Описание
.1.3.6.1.2.1.6.13.1.1.A.B.C.D	Состояние TCP-соединения: • 1 (closed) — закрыто, • 2 (listen) — ожидание запроса на соединение со стороны чужих портов и программ TCP, • 3 (synSent) — ожидание парного запроса на установление соединения, • 4 (synReceived) — ожидание подтверждения после того, как запрос соединения уже принят и отправлен, • 5 (established) — установлено, • 6 (finWait1) — ожидание запроса от программы TCP или подтверждения ранее отправленного запроса на закрытие соединения, • 7 (finWait2) — ожидание запроса на закрытие соединения со стороны программы TCP, • 8 (closeWait) — ожидание запроса на закрытие соединения со стороны своего клиента, • 9 (lastAck) — ожидание запроса на закрытие соединения, ранее отправленного программе TCP, • 10 (closing) — ожидание подтверждения со стороны программы TCP запроса о закрытии соединения, • 11 (timeWait) — ожидание, когда программа TCP получила подтверждение своего запроса на закрытие соединения, • 12 (deleteTCB) — удаление буфера управления передачей (TCB) для подключения TCP.
.1.3.6.1.2.1.6.14.0	Количество сегментов с ошибками.
.1.3.6.1.2.1.6.15.0	Количество отправленных сегментов с флагом RST.

Таблица TCP-соединений для протоколов IPv4 и IPv6 (.1.3.6.1.2.1.6.19.1):

V1 — версия протокола IP для локального адреса,

A — локальный IP-адрес,

B — локальный порт,

V2 — версия протокола IP для удаленного адреса,

C — удаленный IP-адрес,

D — удаленный порт

.1.3.6.1.2.1.6.19.1.7.V1.4.A.B.V2.C.D	Состояние TCP-соединения: • 1 (closed) — закрыто, • 2 (listen) — ожидание запроса на соединение со стороны чужих портов и программ TCP, • 3 (synSent) — ожидание парного запроса на установление соединения, • 4 (synReceived) — ожидание подтверждения после

OID	Описание
	того, как запрос соединения уже принят и отправлен, • 5 (established) — установлено, • 6 (finWait1) — ожидание запроса от программы TCP или подтверждения ранее отправленного запроса на закрытие соединения, • 7 (finWait2) — ожидание запроса на закрытие соединения со стороны программы TCP, • 8 (closeWait) — ожидание запроса на закрытие соединения со стороны своего клиента, • 9 (lastAck) — ожидание запроса на закрытие соединения, ранее отправленного программе TCP, • 10 (closing) — ожидание подтверждения со стороны программы TCP запроса о закрытии соединения, • 11 (timeWait) — ожидание, когда программа TCP получила подтверждение своего запроса на закрытие соединения, • 12 (deleteTCB) — удаление буфера управления передачей (TCB) для подключения.
.1.3.6.1.2.1.6.19.1.8.V1.4.A.B.V2.C.D	Системный идентификатор процесса, связанного с этим соединением. Если такого процесса нет, параметр равен 0.
Таблица открытых TCP-портов (.1.3.6.1.2.1.6.20.1): **V1 — версия протокола IP для локального адреса,** **A — локальный IP-адрес,** **B — локальный порт**	
.1.3.6.1.2.1.6.20.1.4.V1.4.A.B	Системный идентификатор процесса, использующего порт. Если такого процесса нет, параметр равен 0.

UDP-MIB

UDP-MIB (.1.3.6.1.2.1.7) включает в себя объекты, предназначенные для получения информации о различных характеристиках работы сетевого узла по протоколу UDP (например, общее количество полученных и отправленных датаграмм). Подробнее см. в RFC 4113.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 40. SNMP-параметры. UDP-MIB

OID	Описание
.1.3.6.1.2.1.7.1.0	Количество входящих UDP-датаграмм.
.1.3.6.1.2.1.7.2.0	Количество входящих UDP-датаграмм, для которых нет открытого порта.

OID	Описание
.1.3.6.1.2.1.7.3.0	Количество входящих UDP-датаграмм, для которых нет открытого порта.
.1.3.6.1.2.1.7.4.0	Количество исходящих UDP-датаграмм.
Таблица открытых UDP-портов для протокола IPv4 (.1.3.6.1.2.1.7.5.1): **A — IP-адрес локального порта,** **B — номер локального порта.**	
.1.3.6.1.2.1.7.5.1.1.A.B	IP-адрес локального порта.
.1.3.6.1.2.1.7.5.1.2.A.B	Номер порта.
Таблица открытых UDP-соединений (.1.3.6.1.2.1.7.7.1): **V1 — версия IP-протокола для локального адреса,** **A — IP-адрес локального порта,** **B — номер локального порта,** **V2 — версия IP-протокола для удаленного адреса,** **C — IP-адрес удаленного порта,** **D — номер удаленного порта.**	
.1.3.6.1.2.1.7.7.1.8.V1.4.A.B.V2.C.D	Системный идентификатор процесса, использующего порт. Если такого процесса нет, параметр равен 0.

HOST-RESOURCES-MIB

HOST-RESOURCES-MIB (.1.3.6.1.2.1.25) включает в себя объекты, предназначенные для получения информации о системных параметрах и оборудовании сетевого узла. Подробнее см. RFC 2790.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 41. SNMP-параметры. HOST-RESOURCES-MIB

OID	Описание
.1.3.6.1.2.1.25.1.1.0	Время работы системы с последнего запуска.

OID	Описание
.1.3.6.1.2.1.25.1.2.0	Системное время на сетевом узле (значение передается в виде строки байт): • 1-2 байт — год, • 3 байт — месяц, • 4 байт — день, • 5 байт — часы, • 6 байт — минуты, • 7 байт — секунды, • 8 байт — десятые секунды, • 9 байт — «направление» от UTC (соответствующие коды символов ascii), • 10 байт — часы от UTC, • 11 байт — минуты от UTC. Если часовой пояс неизвестен, то последние 3 байта отсутствуют.
1.3.6.1.2.1.25.1.3.0	Индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1, с которого загружается сетевой узел.
.1.3.6.1.2.1.25.1.4.0	Параметры при загрузке сетевого узла (в том числе название аппаратной платформы — для координатора).
.1.3.6.1.2.1.25.1.5.0	Количество сессий пользователя.
.1.3.6.1.2.1.25.1.6.0	Количество процессов загруженных или исполняемых на сетевом узле.
.1.3.6.1.2.1.25.1.7.0	Максимальное поддерживаемое сетевым узлом количество процессов. Если количество не ограничено, параметр равен 0.
1.3.6.1.2.1.25.2.2.0	Объем RAM (в килобайтах).
Таблица локальных логических хранилищ сетевого узла (.1.3.6.1.2.1.25.2.3.1):	
A — индекс хранилища	
.1.3.6.1.2.1.25.2.3.1.1.A	Идентификатор, присвоенный сетевым узлом (A).
.1.3.6.1.2.1.25.2.3.1.2.A	OID, присвоенный данному типу хранилища: 1.3.6.1.2.1.25.2.1 + • 1 — устройство не может быть причислено к какой-либо другой категории, • 2 — RAM, • 3 — виртуальная память, временное хранилище, SWAP, • 4 — не извлекаемые НЖМД, • 5 — извлекаемые НЖМД.
.1.3.6.1.2.1.25.2.3.1.3.A	Описание хранилища.

OID	Описание
.1.3.6.1.2.1.25.2.3.1.4.A	Размер в байтах объектов (размеры секторов/блоков/буферов/пакетов), размещенных в данном хранилище.
.1.3.6.1.2.1.25.2.3.1.5.A	Общее количество секторов/блоков/буферов/пакетов в хранилище.
.1.3.6.1.2.1.25.2.3.1.6.A	Количество использованных секторов/блоков/буферов/пакетов в хранилище.
.1.3.6.1.2.1.25.2.3.1.7.A	Количество ошибок операций записи по причине недостатка места.

Таблица устройств сетевого узла (.1.3.6.1.2.1.25.3.2.1):

B — индекс устройства

.1.3.6.1.2.1.25.3.2.1.1.B	Идентификатор, присвоенный сетевым узлом (B).
.1.3.6.1.2.1.25.3.2.1.2.B	OID, присвоенный данному типу устройства: 1.3.6.1.2.1.25.3.1 + • 1 — применяется, если не может быть отнесено к другой группе, • 2 — применяется, если устройство не опознано, • 3 — CPU (ядра), • 4 — сетевой интерфейс, • 5 — принтер, • 6 — жесткий диск (HDD, SSD), • 10 — видеоустройство, • 11 — аудиоустройство, • 12 — сопроцессор, • 13 — клавиатура, • 14 — модем, • 15 — параллельный порт, • 16 — манипулятор типа мышь, • 17 — последовательный порт, • 18 — ленточное хранилище, • 19 — часы, • 20 — энергозависимая память, • 21 — энергонезависимая память.
.1.3.6.1.2.1.25.3.2.1.3.B	Описание устройства.
.1.3.6.1.2.1.25.3.2.1.4.B	ID продукта.

OID	Описание
.1.3.6.1.2.1.25.3.2.1.5.B	Текущий статус устройства: • 1 — статус неизвестен (unknown), • 2 — работает (running), • 3 — предупреждение (warning), • 4 — проверка (testing), • 5 — не работает (down).
.1.3.6.1.2.1.25.3.2.1.6.B	Счетчик количества ошибок на устройстве.

Таблица загрузки процессоров сетевого узла (.1.3.6.1.2.1.25.3.3.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.3.1.1.B	ID продукта.
.1.3.6.1.2.1.25.3.3.1.2.B	Средняя нагрузка на ядро за последнюю минуту.

Таблица дисков сетевого узла (.1.3.6.1.2.1.25.3.6.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

.1.3.6.1.2.1.25.3.6.1.1.B	Доступ к диску: • 1 — чтение и запись, • 2 — чтение.
.1.3.6.1.2.1.25.3.6.1.2.B	Тип устройства: • 1 — применяется, если не может быть отнесено к другой группе, • 2 — неизвестен, • 3 — жесткий диск, • 4 — дискета, • 5 — оптический диск ROM, • 6 — оптический диск WORM, • 10 — оптический диск RW, • 11 — RAM диск.
.1.3.6.1.2.1.25.3.6.1.3.B	Возможность извлечения диска: • 1 — Разрешено, • 2 — Запрещено.
.1.3.6.1.2.1.25.3.6.1.4.B	Размер диска (в килобайтах). Если диск извлекаемый и он извлечен, параметр равен 0.

Таблица разделов сетевого узла (.1.3.6.1.2.1.25.3.7.1):

B — индекс устройства из таблицы .1.3.6.1.2.1.25.3.2.1

D — индекс устройства из таблицы .1.3.6.1.2.1.25.3.7.1

.1.3.6.1.2.1.25.3.7.1.1.B.D	Индекс устройства (D).
.1.3.6.1.2.1.25.3.7.1.2.B.D	Описание раздела.
.1.3.6.1.2.1.25.3.7.1.3.B.D	ID раздела в операционной системе - октетная строка.

OID	Описание
.1.3.6.1.2.1.25.3.7.1.4.B.D	Размер раздела (в килобайтах).
.1.3.6.1.2.1.25.3.7.1.5.B.D	Файловая система, используемая в разделе. Если файловой системы нет, параметр равен 0.
Таблица ПО, запущенного на сетевом узле (.1.3.6.1.2.1.25.4.2.1):	
F — индекс ПО	
.1.3.6.1.2.1.25.4.2.1.1.F	Индекс запущенного ПО (F).
.1.3.6.1.2.1.25.4.2.1.2.F	Наименование запущенного ПО.
.1.3.6.1.2.1.25.4.2.1.3.F	ID ПО производителя.
.1.3.6.1.2.1.25.4.2.1.4.F	Папка, из которой запущено ПО.
.1.3.6.1.2.1.25.4.2.1.5.F	Параметры, с которыми запущено ПО.
.1.3.6.1.2.1.25.4.2.1.6.F	Тип программного обеспечения: • 1 – неизвестно, • 2 – ОС, • 3 – драйвер устройства, • 4 – приложение.
.1.3.6.1.2.1.25.4.2.1.7.F	Текущее состояния ПО: • 1 – запущено (running), • 2 – работоспособно (runnable), • 3 – неработоспособно (notRunnable), • 4 – работает некорректно (invalid).
Таблица с потреблением каждого ПО ЦПУ и ОЗУ (.1.3.6.1.2.1.25.5.1.1):	
F — индекс ПО из таблицы .1.3.6.1.2.1.25.4.2.1	
.1.3.6.1.2.1.25.5.1.1.1.F	Количество процессорного времени, выделенного ПО, в сантисекундах (0,01 с).
.1.3.6.1.2.1.25.5.1.1.2.F	Количество занимаемой оперативной памяти (в килобайтах).

UCD-SNMP-MIB

UCD-SNMP-MIB (.1.3.6.1.4.1.2021) включает в себя объекты, предназначенные для получения информации о характеристиках и состоянии оборудования сетевого узла (например, состояние оперативной памяти и жесткого диска). Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 42. SNMP-параметры. UCD-SNMP-MIB

OID	Описание
.1.3.6.1.4.1.2021.4.5.0	Объем физической памяти (RAM) на сетевом узле (в кибибайтах).
.1.3.6.1.4.1.2021.4.6.0	Объем доступной физической памяти (в кибибайтах).
.1.3.6.1.4.1.2021.4.13.0	Общий объем памяти (в кибибайтах), выделенный под разделяемую память (shared memory).
.1.3.6.1.4.1.2021.4.14.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве буфера обмена.
.1.3.6.1.4.1.2021.4.15.0	Общий объем памяти (в кибибайтах), который выделен для использования в качестве кешированной памяти.
.1.3.6.1.4.1.2021.4.27.0	Объем памяти (в кибибайтах), доступный для запуска новых приложений без вымещения данных в swap.

Таблица сведений о разделах (.1.3.6.1.4.1.2021.9.1)

B — индекс диска, присвоенный сетевым узлом

.1.3.6.1.4.1.2021.9.1.1.B	Индекс раздела (B).
.1.3.6.1.4.1.2021.9.1.2.B	Точка монтирования раздела.
.1.3.6.1.4.1.2021.9.1.3.B	Устройство (или tmpfs), на котором находится раздел.
.1.3.6.1.4.1.2021.9.1.6.B	Общий объём раздела (в килобайтах).
.1.3.6.1.4.1.2021.9.1.7.B	Свободное место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.8.B	Занятое место в разделе (в килобайтах).
.1.3.6.1.4.1.2021.9.1.9.B	Занятое место в разделе (в процентах).
.1.3.6.1.4.1.2021.9.1.11.B	Общий объем раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если раздел менее 2ТБ, параметр равен .1.3.6.1.4.1.2021.9.1.6.B.
.1.3.6.1.4.1.2021.9.1.13.B	Общий объем свободного места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если свободно менее 2ТБ, параметр равен .1.3.6.1.4.1.2021.9.1.7.B.
.1.3.6.1.4.1.2021.9.1.15.B	Общий объем занятого места раздела, представленный в формате 64 бит. Параметр равен 1-32 бит числа. Если занято менее 2ТБ, параметр равен .1.3.6.1.4.1.2021.9.1.8.B

Таблица информации о средней загрузке системы за 1, 5, 15 минут (1.3.6.1.4.1.2021.10.1)

C — индекс, присвоенный сетевым узлом (постоянный):

- **1 — значение для 1 минуты,**
- **2 — значение для 5 минут,**
- **3 — значение для 15 минут**

OID	Описание
.1.3.6.1.4.1.2021.10.1.1.C	Индекс значения средней загрузки: • 1 — 1 минута, • 2 — 5 минут, • 3 — 15 минут
.1.3.6.1.4.1.2021.10.1.2.C	Имя загрузки (по умолчанию: Load-1, Load-5, Load-15).
.1.3.6.1.4.1.2021.10.1.3.C	Средняя загрузка системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.4.C	Пороговое значение загрузки системы в процентах (в виде строки).
.1.3.6.1.4.1.2021.10.1.5.C	Загрузка системы в процентах (в виде целого числа).
.1.3.6.1.4.1.2021.10.1.6.C	Загрузка системы в процентах (в виде числа с плавающей точкой).
.1.3.6.1.4.1.2021.10.1.100.C	Флаг, сигнализирующий о превышении средней загрузки порогового значения.
.1.3.6.1.4.1.2021.10.1.101.C	Сообщение о превышении порогового значения.
.1.3.6.1.4.1.2021.11.5.0	Среднее количество информации (в блоках данных), записанных на диск за минуту.
.1.3.6.1.4.1.2021.11.6.0	Среднее количество информации (в блоках данных), прочитанное с диска за минуту.
.1.3.6.1.4.1.2021.11.7.0	Среднее количество системных прерываний за минуту.
.1.3.6.1.4.1.2021.11.8.0	Среднее количество переключений контекста за минуту.
.1.3.6.1.4.1.2021.11.9.0	Процент времени, занятого пользовательскими процессами (за минуту).
.1.3.6.1.4.1.2021.11.10.0	Процент времени, когда процессор занят системными процессами (за минуту).
.1.3.6.1.4.1.2021.11.11.0	Процент времени, когда процессор не занят процессами (за минуту).
.1.3.6.1.4.1.2021.11.50.0	Количество тиков процессорного времени, затраченного на исполнения user-level code.
.1.3.6.1.4.1.2021.11.51.0	Количество тиков процессорного времени, затраченного на исполнение reduced-priority code.
.1.3.6.1.4.1.2021.11.52.0	Количество тиков процессорного времени, затраченного на исполнение system-level code.
.1.3.6.1.4.1.2021.11.53.0	Количество тиков процессорного времени, проведенного в состоянии idle.
.1.3.6.1.4.1.2021.11.54.0	Количество тиков процессорного времени, затраченного на исполнение ожидания ввода-вывода.
.1.3.6.1.4.1.2021.11.57.0	Количество блоков, отправленное блочному устройству (диску).
.1.3.6.1.4.1.2021.11.58.0	Количество блоков, полученное блочным устройством (диском).

OID	Описание
.1.3.6.1.4.1.2021.11.59.0	Количество обработанных аппаратных прерываний.
.1.3.6.1.4.1.2021.11.60.0	Количество выполненных переключений контекста.
.1.3.6.1.4.1.2021.11.61.0	Количество тиков процессорного времени, затраченного на исполнение программных прерываний.
.1.3.6.1.4.1.2021.11.67.0	Количество ядер процессоров.
.1.3.6.1.4.1.2021.100.2.0	Ключевое слово CVS.
.1.3.6.1.4.1.2021.100.3.0	Строка времени из ключевого слова RCS.
.1.3.6.1.4.1.2021.100.4.0	Строка времени из ctime.
.1.3.6.1.4.1.2021.100.5.0	Идентификатор из ключевого слова RCS.
.1.3.6.1.4.1.2021.101.100.0	Признак ошибки SNMP-агента.

UCD-DISKIO-MIB

UCD-DISKIO-MIB (.1.3.6.1.4.1.2021.13.15) включает в себя объекты, предназначенные для получения информации о состоянии памяти и дискового пространства сетевого узла. Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 43. SNMP-параметры. UCD-DISKIO-MIB

OID	Описание
Таблица значений текущих параметров оперативной памяти, виртуальной памяти, дискового пространства и их загрузки (.1.3.6.1.4.1.2021.13.15.1.1.)	
A — индекс таблицы	
.1.3.6.1.4.1.2021.13.15.1.1.1.A	Индекс таблицы (A).
.1.3.6.1.4.1.2021.13.15.1.1.2.A	Описание устройства, полученное от ОС. Для координатора принимает значения: ram0-ram15 loop0-loop7 sda, sda1, sda2, sdb1, sdb2, sdb3
.1.3.6.1.4.1.2021.13.15.1.1.3.A	Количество байт, считанных с устройства с момента запуска.
.1.3.6.1.4.1.2021.13.15.1.1.4.A	Количество байт, записанных на устройство с момента запуска.
.1.3.6.1.4.1.2021.13.15.1.1.5.A	Количество операций доступа к устройству на чтение.
.1.3.6.1.4.1.2021.13.15.1.1.6.A	Количество операций доступа к устройству на запись.

OID	Описание
.1.3.6.1.4.1.2021.13.15.1.1.9.A	Средняя загрузка устройства за 1 минуту (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.10.A	Средняя загрузка устройства за 5 минут (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.11.A	Средняя загрузка устройства за 15 минут (в процентах).
.1.3.6.1.4.1.2021.13.15.1.1.12.A	Количество операций доступа к устройству на чтение. 64-разрядный параметр.
.1.3.6.1.4.1.2021.13.15.1.1.13.A	Количество байт, записанных на устройство с момента запуска. 64-разрядный параметр.

NET-SNMP-MIB

NET-SNMP-MIB (1.3.6.1.4.1.8072) включает в себя объекты, предназначенные для получения служебной информации о работе SNMP-агента.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 44. SNMP-параметры. NET-SNMP-MIB

OID	Описание
Таблица, содержащая все OID, зарегистрированные MIB-модулями в SNMP-агенте (.1.3.6.1.4.1.8072.1.2.1.1):	
A – имя MIB-модуля	
B – OID MIB-модуля	
C – приоритет MIB-модуля	
.1.3.6.1.4.1.8072.1.2.1.1.4.A.B.C	Имя модуля, который зарегистрировал OID.
.1.3.6.1.4.1.8072.1.2.1.1.5.A.B.C	Биты, означающие режим работы OID.
.1.3.6.1.4.1.8072.1.2.1.1.6.A.B.C	Таймаут для модуля.
.1.3.6.1.4.1.8072.1.5.1.0	Время, на которое кешируется значение OID по умолчанию (в секундах), если оно не задано в параметре .1.3.6.1.4.1.8072.1.5.3.1.2.F.
.1.3.6.1.4.1.8072.1.5.2.0	Статус кеширования: • 1 — включено, • 2 — выключено.
Таблица кешированных OID (.1.3.6.1.4.1.8072.1.5.3.1):	
F – OID, значение которого кешировано	
.1.3.6.1.4.1.8072.1.5.3.1.2.F	Время, на которое кешируется значение OID (в секундах).

OID	Описание
.1.3.6.1.4.1.8072.1.5.3.1.3.F	Статус записи: • 1 (enabled) — включена, • 2 (disabled) — выключена, • 3 (empty) — пустая, • 4 (cached) — кешированная, • 5 (expired) — истекла.
1.3.6.1.4.1.8072.1.7.1.1.0	Статус режима debug SNMP-агента: • 1 — включен, • 2 — выключен.
.1.3.6.1.4.1.8072.1.7.1.2.0	Переключатель вывода для debug: • 1 — вывод всех значений, • 2 — фильтрация вывода. Для работы переключателя параметр .1.3.6.1.4.1.8072.1.7.1.1.0 должен быть равен 1.
.1.3.6.1.4.1.8072.1.7.1.3.0	Переключатель вывода сырого дампа пакетов: • 1 — включен, • 2 — выключен.

Таблица форм вывода сообщений SNMP-агента (.1.3.6.1.4.1.8072.1.7.2.1.1):

H – уровень важности событий:

0 – emergency

1 – alert

2 – critical

3 – error

4 – warning

5 – notice

6 – info

7 – debug

I – идентификатор журнала

.1.3.6.1.4.1.8072.1.7.2.1.1.3.H.I	Форма вывода сообщений для данной строки: • 1 — stdout, • 2 — stderr, • 3 — file, • 4 — syslog, • 5 — callback.

OID	Описание
.1.3.6.1.4.1.8072.1.7.2.1.1.4.H.I	Максимальное значение, для которого применима данная строка: • 0 — emergency, • 1 — alert, • 2 — critical, • 3 — error, • 4 — warning, • 5 — notice, • 7 — debug.
.1.3.6.1.4.1.8072.1.7.2.1.1.5.H.I	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
VACM таблица доступа сетевого узла (.1.3.6.1.4.1.8072.1.9.1.1.): **J – имя группы:** **K – префикс контекста доступа** **L – модель безопасности доступа** **M – уровень безопасности доступа** **N – тип аутентификации**	
.1.3.6.1.4.1.8072.1.9.1.1.2.J.K.L.M.N	Механизм выбора совпадений в VACM: • 1 — exact (полное совпадение), • 2 — prefix (совпадает префикс).
.1.3.6.1.4.1.8072.1.9.1.1.3.J.K.L.M.N	Значение секции ViewName.
.1.3.6.1.4.1.8072.1.9.1.1.4.J.K.L.M.N	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.

OID	Описание
.1.3.6.1.4.1.8072.1.9.1.1.5.J.K.L.M.N	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-MPD-MIB

SNMP-MPD-MIB (.1.3.6.1.6.3.11) включает в себя статистическую информацию об SNMP-пакетах.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 45. SNMP-параметры. SNMP-MPD-MIB

OID	Описание
.1.3.6.1.6.3.11.2.1.1.0	Количество полученных SNMP-пакетов, заблокированных по причине неподдерживаемой или неизвестной модели безопасности.
.1.3.6.1.6.3.11.2.1.2.0	Количество полученных SNMP-пакетов, заблокированных по причине ошибок в SNMP-сообщении.
.1.3.6.1.6.3.11.2.1.3.0	Количество полученных SNMP-пакетов, заблокированных по причине несоответствия pduType.

SNMP-TARGET-MIB

SNMP-TARGET-MIB (.1.3.6.1.6.3.12) включает в себя статистическую информацию об SNMP-пакетах.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 46. SNMP-параметры. SNMP-TARGET-MIB

OID	Описание
.1.3.6.1.6.3.12.1.1.0	Параметр для совместной работы нескольких SNMP-менеджеров, для одновременной работы с таблицами данного MIB.

OID	Описание
.1.3.6.1.6.3.12.1.4.0	Количество полученных SNMP-пакетов, заблокированных по причине недоступного контекста.
.1.3.6.1.6.3.12.1.5.0	Количество полученных SNMP-пакетов, заблокированных по причине неизвестного контекста.

SNMP-USER-BASED-SM-MIB

SNMP-USER-BASED-SM-MIB (.1.3.6.1.6.3.15) включает в себя объекты, предназначенные для получения информации о параметрах и событиях безопасности SNMP-агента.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 47. SNMP-параметры. SNMP-USER-BASED-SM-MIB

OID	Описание
.1.3.6.1.6.3.15.1.1.1.0	Количество заблокированных SNMP-пакетов по причине запроса неизвестного или недоступного уровня безопасности.
.1.3.6.1.6.3.15.1.1.2.0	Количество заблокированных SNMP-пакетов по причине появления вне определённого (доверенного) SNMP-агентом окна.
.1.3.6.1.6.3.15.1.1.3.0	Количество заблокированных SNMP-пакетов по причине использования неизвестного SNMP-агенту имени пользователя.
.1.3.6.1.6.3.15.1.1.4.0	Количество заблокированных SNMP-пакетов по причине обращения к неизвестному SNMP-агенту snmpEngineID.
.1.3.6.1.6.3.15.1.1.5.0	Количество заблокированных SNMP-пакетов по причине отсутствия ожидаемого значения digest value.
.1.3.6.1.6.3.15.1.1.6.0	Количество заблокированных SNMP-пакетов по причине невозможности их расшифровки.
.1.3.6.1.6.3.15.1.2.1.0	Параметр для совместной работы нескольких SNMP-менеджеров с таблицей .1.3.6.1.6.3.15.1.2.2.1.
Таблица параметров безопасности пользователя (.1.3.6.1.6.3.15.1.2.2.1):	
A – EngineID пользователя	
B – имя пользователя	
.1.3.6.1.6.3.15.1.2.2.1.3.A.B	Имя пользователя в формате модели безопасности.
.1.3.6.1.6.3.15.1.2.2.1.4.A.B	Ссылка на другую строку таблицы, в которой создана копия пользователя из текущей строки.
.1.3.6.1.6.3.15.1.2.2.1.5.A.B	Тип протокола аутентификации пользователя.
.1.3.6.1.6.3.15.1.2.2.1.8.A.B	Тип протокола конфиденциальности пользователя.
.1.3.6.1.6.3.15.1.2.2.1.11.A.B	Параметр для определения факта смены ключей пользователя.

SNMP-VIEW-BASED-ACM-MIB

SNMP-VIEW-BASED-ACM-MIB (.1.3.6.1.6.3.16) включает в себя объекты, предназначенные для получения информации о правах доступа к SNMP-параметрам.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 48. SNMP-параметры. SNMP-VIEW-BASED-ACM-MIB

OID	Описание
Таблица доступных контекстов сетевого узла (.1.3.6.1.6.3.16.1.1):	
A – строка контекста	
.1.3.6.1.6.3.16.1.1.1.A	Строка контекста.
Таблица групп доступа (.1.3.6.1.6.3.16.1.2.1):	
B – модель безопасности	
C – имя безопасности	
.1.3.6.1.6.3.16.1.2.1.3.B.C	Имя группы
.1.3.6.1.6.3.16.1.2.1.4.B.C	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.6.3.16.1.2.1.5.B.C	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
Таблица прав доступа к группам (.1.3.6.1.6.3.16.1.4.1):	
D – имя группы	
E – контекст доступа	
F – модель безопасности	
G – уровень безопасности	
.1.3.6.1.6.3.16.1.4.1.4.D.E.F.G	Формат совпадения: • 1 (exact) — полное совпадение, • 2 (prefix) — совпадает префикс.
.1.3.6.1.6.3.16.1.4.1.5.D.E.F.G	Имя view на просмотр.

OID	Описание
.1.3.6.1.6.3.16.1.4.1.6.D.E.F.G	Имя view на запись.
.1.3.6.1.6.3.16.1.4.1.7.D.E.F.G	Имя view для уведомлений.
.1.3.6.1.6.3.16.1.4.1.8.D.E.F.G	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.
.1.3.6.1.6.3.16.1.4.1.9.D.E.F.G	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.
.1.3.6.1.6.3.16.1.5.1.0	Параметр для совместной работы нескольких SNMP-менеджеров с таблицами данного MIB.

Таблица с параметрами view для семей поддеревьев (.1.3.6.1.6.3.16.1.5.2.1.):

H – имя view

I – поддерево

.1.3.6.1.6.3.16.1.5.2.1.3.H.I	Маска, заданная для view.
.1.3.6.1.6.3.16.1.5.2.1.4.H.I	Тип view: • 1 — included, • 2 — excluded.
.1.3.6.1.6.3.16.1.5.2.1.5.H.I	Тип хранилища: • 1 (other) — другое, • 2 (volatile) — изменяемый, • 3 (nonvolatile) — неизменяемый, • 4 (permanent) — постоянный, • 5 (readOnly) — только для чтения.

OID	Описание
.1.3.6.1.6.3.16.1.5.2.1.6.H.I	Статус строки таблицы: • 1 (active) — строка доступна для использования, • 2 (notInService) — строка недоступна для использования, • 3 (notReady) — отсутствует информация для использования, • 4 (createAndGo) — создание строки и перевод ее в статус active, • 5 (createAndWait) — создание строки и перевод ее в статус notInService, • 6 (destroy) — удаление.

SNMP-FRAMEWORK-MIB

SNMP-FRAMEWORK-MIB (.1.3.6.1.6.3.10) включает в себя объекты, предназначенные для получения служебной информации о работе SNMP-агента. Подробнее см. на веб-ресурсе.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 49. SNMP-параметры. SNMP-FRAMEWORK-MIB

OID	Описание
.1.3.6.1.6.3.10.2.1.1.0	Идентификатор SNMP-engine.
.1.3.6.1.6.3.10.2.1.2.0	Количество инициализаций SNMP-engine после создания идентификатора.
.1.3.6.1.6.3.10.2.1.3.0	Время, прошедшее с последнего изменения количества инициализаций SNMP-engine (в секундах).
.1.3.6.1.6.3.10.2.1.4.0	Максимальная длина входящего и исходящего SNMP-сообщения (в байтах).

VIPNET-MIB

VIPNET-MIB (.1.3.6.1.4.1.10812) включает в себя объекты, предназначенные для получения информации о параметрах сетевых узлов ViPNet. Для получения этой информации используется ветвь: `.iso.org.dod.internet.private.enterprises.infotecs.vipnet` (.1.3.6.1.4.1.10812.1).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 50. SNMP-параметры. VIPNET-MIB

OID	Описание
.1.3.6.1.4.1.10812.1.1.1.0	Шестнадцатеричный идентификатор сети ViPNet.
.1.3.6.1.4.1.10812.1.1.2.0	Шестнадцатеричный идентификатор сетевого узла ViPNet.

OID	Описание
.1.3.6.1.4.1.10812.1.1.3.0	Имя пользователя узла ViPNet.
.1.3.6.1.4.1.10812.1.1.4.0	Время работы ViPNet Coordinator IG (сбрасывается каждый раз при перезапуске службы iplircfg).
.1.3.6.1.4.1.10812.1.1.5.0	Шестнадцатеричный идентификатор, включающий в себя идентификаторы узла ViPNet и сети ViPNet.
.1.3.6.1.4.1.10812.1.1.7.0	Имя узла ViPNet.
.1.3.6.1.4.1.10812.1.2.1	Количество сетевых интерфейсов.
Таблица объектов, описывающих сетевые интерфейсы (.1.3.6.1.4.1.10812.1.2.2):	
.1.3.6.1.4.1.10812.1.2.2.1.1.X	Номер сетевого интерфейса X , где X — индекс интерфейса.
.1.3.6.1.4.1.10812.1.2.2.1.2.X	Имя сетевого интерфейса X.
.1.3.6.1.4.1.10812.1.2.2.1.3.X	Устаревший параметр, всегда равен 0.
.1.3.6.1.4.1.10812.1.2.2.1.4.X	Количество пропущенных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.5.X	Количество блокированных входящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.6.X	Количество пропущенных исходящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.7.X	Количество блокированных исходящих незашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.8.X	Количество пропущенных входящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.9.X	Количество блокированных входящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.10.X	Количество пропущенных исходящих зашифрованных пакетов.
.1.3.6.1.4.1.10812.1.2.2.1.11.X	Количество блокированных исходящих зашифрованных пакетов.
Таблица объектов, описывающих состояние служб iplircfg, failoverd, mftpd, webgui-fcgi-server, remote_management (.1.3.6.1.4.1.10812.1.7.1):	
.1.3.6.1.4.1.10812.1.7.1.1.2.Y	Индекс службы с индексом Y: • 1 — failoverd, • 2 — iplircfg, • 3 — mftpd, • 4 — webgui-fcgi-server, • 5 — external-controld.
.1.3.6.1.4.1.10812.1.7.1.1.3.Y	Состояние службы с индексом Y: • 0 (unknown) — состояние неизвестно, • 1 (shutdown) — работа службы завершена, • 2 (running) — служба работает.
.1.3.6.1.4.1.10812.1.7.1.1.4.Y	Время работы службы с индексом Y.

OID	Описание
.1.3.6.1.4.1.10812.1.8.1.0	Режим работы службы failoverd: • 0 (single) — одиночный, • 1 (cluster passive) — режим кластера, узел работает в пассивном режиме, • 2 (cluster active) — режим кластера, узел работает в активном режиме, • 3 (cluster switch) — режим кластера, узел меняет режим работы в текущий момент.
.1.3.6.1.4.1.10812.1.8.2.0	Время последнего переключения службы failover в текущий режим работы.
.1.3.6.1.4.1.10812.1.8.3.0	IP-адрес интерфейса синхронизации другого узла кластера.
.1.3.6.1.4.1.10812.1.8.4.0	Количество сетевых соединений, находящихся в кеше узла кластера.
.1.3.6.1.4.1.10812.1.8.5.0	Системное имя интерфейса синхронизации.
Таблица доступности соединений в канале между узлами кластера (.1.3.6.1.4.1.10812.1.8.6):	
X – индекс таблицы	
.1.3.6.1.4.1.10812.1.8.6.1.1.X	Индекс таблицы.
.1.3.6.1.4.1.10812.1.8.6.1.2.X	IP-адрес интерфейса синхронизации.
.1.3.6.1.4.1.10812.1.8.6.1.3.X	Статус доступности узла: • 1 — доступен, • 2 — недоступен.
Таблица сведений о ViPNet Coordinator IG (.1.3.6.1.4.1.10812.1.10.1):	
.1.3.6.1.4.1.10812.1.10.1.1.1.X	Индекс строки.
.1.3.6.1.4.1.10812.1.10.1.1.2.X	Serial number — имя параметра.
.1.3.6.1.4.1.10812.1.10.1.1.3.X	Значение параметра Serial number.

SNMP-агент ViPNet Coordinator IG может отправлять уведомления:

Таблица 51. SNMP-уведомления. VIPNET-MIB

OID	Описание
.1.3.6.1.4.1.10812.1.0.1	Запуск службы iplircfg.
.1.3.6.1.4.1.10812.1.0.2	Остановка службы iplircfg.
.1.3.6.1.4.1.10812.1.0.3	Запуск службы mftpd.
.1.3.6.1.4.1.10812.1.0.4	Остановка службы mftpd.
.1.3.6.1.4.1.10812.1.0.7	Запуск службы failoverd.
.1.3.6.1.4.1.10812.1.0.8	Остановка службы failoverd.

OID	Описание
.1.3.6.1.4.1.10812.1.0.9	Переключение службы failoverd из пассивного режима в активный.
.1.3.6.1.4.1.10812.1.0.10	Запуск службы webgui.
.1.3.6.1.4.1.10812.1.0.11	Остановка службы webgui.
.1.3.6.1.4.1.10812.1.0.12	Потеря связи с пассивным узлом кластера.
.1.3.6.1.4.1.10812.1.0.13	Восстановление связи с пассивным узлом кластера.
.1.3.6.1.4.1.10812.1.0.14	Запуск службы external-controld.
.1.3.6.1.4.1.10812.1.0.15	Остановка службы external-controld.

VIPNETMULTIWAN-MIB

VIPNETMULTIWAN-MIB (.1.3.6.1.4.1.10812.14) включает в себя объекты, предназначенные для получения информации об используемых ViPNet Coordinator IG каналах связи и доступности шлюзов.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 52. SNMP-параметры. VIPNETMULTIWAN-MIB

OID	Описание
Таблица доступности шлюзов (.1.3.6.1.4.1.10812.14.1): **X – индекс таблицы**	
.1.3.6.1.4.1.10812.14.1.1.1.X	Индекс таблицы (порядковый номер шлюза).
.1.3.6.1.4.1.10812.14.1.1.2.X	Имя шлюза.
.1.3.6.1.4.1.10812.14.1.1.3.X	Состояние проверки шлюза: • 1 – проверяется, • 2 – не проверяется, • 3 – состояние не определено.
.1.3.6.1.4.1.10812.14.1.1.4.X	Способ проверки доступности шлюза: • 1 – ICMP, • 2 – TCP 80, • 3 – TCP 443, • 4 – способ не определен (N/A).
.1.3.6.1.4.1.10812.14.1.1.5.X	IP-адрес шлюза.
.1.3.6.1.4.1.10812.14.1.1.6.X	IP-адрес для проверки доступности шлюза.

OID	Описание
.1.3.6.1.4.1.10812.14.1.1.7.X	Количество успешных проверок доступности шлюза.
.1.3.6.1.4.1.10812.14.1.1.8.X	Количество неудачных проверок доступности шлюза.
.1.3.6.1.4.1.10812.14.1.1.9.X	Имя и состояние сетевого интерфейса шлюза: • 1 – включен (up), • 2 – выключен (down), • 3 – состояние не определено (N/A). Параметр содержит пустую строку, если на сетевом интерфейсе шлюза задан статический IP-адрес.
.1.3.6.1.4.1.10812.14.1.1.10.X	Состояние сетевого интерфейса шлюза: • 1 – включен (up), • 2 – выключен (down), • 3 – состояние не определено (N/A).
.1.3.6.1.4.1.10812.14.1.1.11.X	Дата и время последнего изменения состояния шлюза.
.1.3.6.1.4.1.10812.14.2.1	Имя политики маршрутизации.

SNMP-агент ViPNet Coordinator IG может отправлять уведомления:

Таблица 53. SNMP-уведомления. VIPNETMULTIWAN-MIB

OID	Описание
.1.3.6.1.4.1.10812.14.0.1	Изменение состояния шлюза.
.1.3.6.1.4.1.10812.14.0.2	Смена активной политики маршрутизации.

MonitoringAgent-MIB

MonitoringAgent-MIB (.1.3.6.1.4.1.10812.4) включает в себя объекты, предназначенные для получения информации о характеристиках SNMP-агента (например, версия, уникальный идентификатор).

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 54. SNMP-параметры. MonitoringAgent-MIB

OID	Описание
.1.3.6.1.4.1.10812.4.3.1.0	Версия агента мониторинга.
.1.3.6.1.4.1.10812.4.3.2.0	Идентификатор инсталляции агента мониторинга.
.1.3.6.1.4.1.10812.4.4	Таблица плагинов агента мониторинга.

OID	Описание
.1.3.6.1.4.1.10812.4.5	Таблица функциональных возможностей агента мониторинга.

System-MonitoringAgent-MIB

System-MonitoringAgent-MIB (.1.3.6.1.4.1.10812.4.20) включает в себя объекты, предназначенные для получения информации об устройстве, на котором запущен SNMP-агент.

ПО ViPNet использует следующие объекты, для которых возможно только чтение данных:

Таблица 55. SNMP-параметры. System-MonitoringAgent-MIB

OID	Описание
.1.3.6.1.4.1.10812.4.20.5.0	Идентификатор устройства в HEX-формате.
.1.3.6.1.4.1.10812.4.20.9.0	Уникальный идентификатор устройства в виде строки.

G

Список служб ПО ViPNet Coordinator IG

Службы ViPNet:

- aad — служба аутентификации и авторизации;
- bonding_helper — скрипт управления модулем агрегирования каналов;
- controld — служба обработки запросов;
- dgdd — служба проверки состояния удалённых шлюзов (DGD);
- drviplir — драйвер перехвата сетевого трафика;
- external-controld — служба взаимодействия с ViPNet Prime;
- failover, failoverd — служба слежения за основными службами ViPNet и организации кластера;
- http_proxy — скрипты управления прокси-сервером squid;
- ipfd — служба фильтрации промышленных протоколов;
- igpoed — служба управления питанием по технологии PoE;
- iplircfg — служба настройки драйвера перехвата сетевого трафика, ведения журнала IP-пакетов, обновления справочно-ключевой информации;
- iplirpasswd — утилита проверки паролей аудитора и администратора;
- itcscrpt — драйвер шифрования IP-пакетов;
- itcskrniface — драйвер перехвата сетевого трафика;
- itcswd — драйвер службы мониторинга системы;
- l2overip — драйвер прозрачного соединения сегментов сети на уровне L2;
- mftp, mftpd — службы транспортного сервера MFTP;

- mbgw — служба шлюза Modbus;
- ntp_service — скрипт управления службы NTP;
- piomonitord — служба управления интерфейсом GPIO;
- rvpn_shell — командный интерпретатор ViPNet;
- session_watcher — служба, отслеживающая сессии пользователей ViPNet;
- vipnetsnmp — служба SNMP;
- unmerge — утилита распаковки дистрибутива справочников и ключей;
- vupgrade — утилита обновления ПО ViPNet Coordinator IG;
- webgui (webgui_captive_portal, webgui-fcgi-server, webgui_php, webgui_frontend) — служба веб-интерфейса.

Службы Linux:

- acpid — служба обработки ACPI-событий;
- bonding — модуль агрегирования каналов;
- crond — служба запуска задач по расписанию;
- dhcpd — служба DHCP-сервера;
- dhcrelay — служба агента-ретранслятора DHCP-запросов;
- icap — служба icap-сервера, используемая для антивирусной проверки совместно с прокси-сервером;
- licd — служба лицензирования;
- login — служба аутентификации и открытия сессий;
- named — служба DNS;
- ntpd — служба NTP;
- ospfd — служба протокола OSPF динамической маршрутизации;
- pcscd — служба работы с токенами;
- snmpd — служба SNMP;
- sshd — служба SSH;
- squid — служба прокси-сервера squid;
- syslogd — служба системного журнала;
- udhcpc — служба DHCP-клиента;
- watchquagga — служба слежения за службой динамической маршрутизации;
- xinetd — служба запуска сетевых серверных процессов;
- zebra — служба динамической маршрутизации;
- zdhcpd — служба протокола DHCP динамической маршрутизации.

H

Поддерживаемые MIME-типы

- **Application — Внутренний формат прикладной программы**
  - application/atom+xml: Atom
  - application/EDI-X12: EDI X12 (RFC 1767)
  - application/EDIFACT: EDI EDIFACT (RFC 1767)
  - application/json: JavaScript Object Notation JSON (RFC 4627)
  - application/javascript: JavaScript (RFC 4329)
  - application/octet-stream: двоичный файл без указания формата (RFC 2046)
  - application/ogg: Ogg (RFC 5334)
  - application/pdf: Portable Document Format, PDF (RFC 3778)
  - application/postscript: PostScript (RFC 2046)
  - application/soap+xml: SOAP (RFC 3902)
  - application/font-woff: Web Open Font Format
  - application/xhtml+xml: XHTML (RFC 3236)
  - application/xml-dtd: DTD (RFC 3023)
  - application/xop+xml: XOP
  - application/zip: ZIP
  - application/gzip: Gzip
  - application/x-bittorrent: BitTorrent

- application/x-tex: TeX

- **audio — Аудио**
  - audio/basic: mulaw аудио, 8 кГц, 1 канал (RFC 2046)
  - audio/L24: 24-bit Linear PCM аудио, 8-48 кГц, 1-N каналов (RFC 3190)
  - audio/mp4: MP4
  - audio/aac: AAC
  - audio/mpeg: MP3 или др. MPEG (RFC 3003)
  - audio/ogg: Ogg Vorbis, Speex, Flac или др. аудио (RFC 5334)
  - audio/vorbis: Vorbis (RFC 5215)
  - audio/x-ms-wma: Windows Media Audio
  - audio/x-ms-wax: Windows Media Audio перенаправление
  - audio/vnd.rn-realaudio: RealAudio
  - audio/vnd.wave: WAV (RFC 2361)
  - audio/webm: WebM
- **image — Изображение**
  - image/gif: GIF (RFC 2045 и RFC 2046)
  - image/jpeg: JPEG (RFC 2045 и RFC 2046)
  - image/pjpeg: JPEG
  - image/png: Portable Network Graphics (RFC 2083)
  - image/svg+xml: SVG
  - image/tiff: TIFF (RFC 3302)
  - image/vnd.microsoft.icon: ICO
  - image/vnd.wap.wbmp: WBMP
- **message — Сообщение**
  - message/http: (RFC 2616)
  - message/imdn+xml: IMDN (RFC 5438)
  - message/partial: E-mail (RFC 2045 и RFC 2046)
  - message/rfc822: E-mail; EML файлы, MIME файлы, MHT файлы, MHTML файлы (RFC 2045 и RFC 2046)
- **model — Для 3D моделей**
  - model/example: (RFC 4735)
  - model/iges: IGS файлы, IGES файлы (RFC 2077)
  - model/mesh: MSH файлы, MESH файлы (RFC 2077), SILO файлы

- model/vrml: WRL файлы, VRML файлы (RFC 2077)
- model/x3d+binary: X3D ISO стандарт для 3D компьютерной графики, X3DB файлы
- model/x3d+vrml: X3D ISO стандарт для 3D компьютерной графики, X3DV VRML файлы
- model/x3d+xml: X3D ISO стандарт для 3D компьютерной графики, X3D XML файлы

- **multipart — Составные файлы**
  - multipart/form-data: MIME Webform (RFC 2388)
  - multipart/signed: (RFC 1847)
  - multipart/encrypted: (RFC 1847)
  - multipart/mixed: MIME E-mail (RFC 2045 и RFC 2046)
  - multipart/alternative: MIME E-mail (RFC 2045 и RFC 2046)
  - multipart/related: MIME E-mail (RFC 2387 и используемое MHTML (HTML mail))
- **text — Текст**
  - text/cmd: команды
  - text/css: Cascading Style Sheets (RFC 2318)
  - text/csv: CSV (RFC 4180)
  - text/html: HTML (RFC 2854)
  - text/javascript (Obsolete): JavaScript (RFC 4329)
  - text/plain: текстовые данные (RFC 2046 и RFC 3676)
  - text/php: Скрипт языка PHP
  - text/xml: Extensible Markup Language (RFC 3023)
- **video — Видео**
  - video/mpeg: MPEG-1 (RFC 2045 и RFC 2046)
  - video/mp4: MP4 (RFC 4337)
  - video/ogg: Ogg Theora или другое видео (RFC 5334)
  - video/quicktime: QuickTime
  - video/webm: WebM
  - video/x-ms-wmv: Windows Media Video
  - video/x-flv: FLV
  - video/3gpp: .3gpp .3gp
  - video/3gpp2: .3gpp2 .3g2
- **vnd — Вендорные файлы**
  - application/vnd.oasis.opendocument.text: OpenDocument
  - application/vnd.oasis.opendocument.spreadsheet: OpenDocument

- application/vnd.oasis.opendocument.presentation: OpenDocument
- application/vnd.oasis.opendocument.graphics: OpenDocument
- application/vnd.ms-excel: Microsoft Excel файлы
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet: Microsoft Excel 2007 файлы
- application/vnd.ms-powerpoint: Microsoft Powerpoint файлы
- application/vnd.openxmlformats-officedocument.presentationml.presentation: Microsoft Powerpoint 2007 файлы
- application/msword: Microsoft Word файлы
- application/vnd.openxmlformats-officedocument.wordprocessingml.document: Microsoft Word 2007 файлы
- application/vnd.mozilla.xul+xml: Mozilla XUL файлы
- application/vnd.google-earth.kml+xml: KML файлы (например, для Google Earth)

- **x — Нестандартные файлы**
  - application/x-www-form-urlencoded: Form Encoded Data
  - application/x-dvi: DVI
  - application/x-latex: LaTeX файлы
  - application/x-font-ttf: TrueType (не зарегистрированный MIME-тип, но наиболее часто используемый)
  - application/x-shockwave-flash: Adobe Flash
  - application/x-stuffit: StuffIt
  - application/x-rar-compressed: RAR
  - application/x-tar: Tarball
  - text/x-jquery-tmpl: jQuery
  - application/x-javascript
- **x-pkcs — PKCS**
  - application/x-pkcs12: p12 файлы
  - application/x-pkcs12: pfx файлы
  - application/x-pkcs7-certificates: p7b файлы
  - application/x-pkcs7-certificates: spc файлы
  - application/x-pkcs7-certreqresp: p7r файлы
  - application/x-pkcs7-mime: p7c файлы
  - application/x-pkcs7-mime: p7m файлы
  - application/x-pkcs7-signature: p7s файлы

Использование ViPNet Coordinator IG в качестве межсетевого экрана типа А/Б четвертого класса защиты

Ниже перечислены рекомендации для администратора, использующего ViPNet Coordinator IG в качестве межсетевого экрана типа «А» или «Б» четвёртого класса защиты:

- Запретите трафик от нежелательных приложений. Для этого создайте сетевые фильтры, запрещающие передачу данных через порты, которые используют эти приложения.

  Разрешите трафик от доверенных приложений. Для этого создайте сетевые фильтры, разрешающие передачу данных через порты, которые используют эти приложения.

- Для ассоциации пользователей сети и IP-адресов:
  - для каждого сетевого узла задайте статический IP-адрес;
  - занесите в специальный журнал ФИО физических лиц, имеющих учётные записи на сетевых узлах;
  - организуйте фиксацию времени работы пользователей на сетевых узлах, где зарегистрировано несколько учётных записей, в специальном журнале.

J

Использование ViPNet Coordinator IG в качестве межсетевого экрана типа Д четвертого класса защиты

Ниже перечислены рекомендации для администратора, использующего ViPNet Coordinator IG в качестве межсетевого экрана типа «Д» четвёртого класса защиты:

- Создайте правила фильтрации промышленных протоколов, разрешающие передачу команд, которые используются на вашем промышленном объекте между устройствами вашей сети. Создайте наборы правил в каждом из режимов работы ViPNet Coordinator IG, — штатном, регламентного обслуживания и специальном, — в соответствии с особенностями инфраструктуры промышленного объекта, где вы устанавливаете ViPNet Coordinator IG.
- С помощью интерфейса GPIO настройте устройство для переключения ViPNet Coordinator IG в специальный режим и обратно. Подробнее см. раздел «Подключение внешнего устройства для перехода в специальный режим» в документе «Сценарии работы».
- Организуйте технический контроль за местом установки ViPNet Coordinator IG с помощью установки в специальный внешний шкаф с датчиком контроля вскрытия. Подробнее см. раздел «Подключение датчика вскрытия внешнего шкафа» в документе «Сценарии работы».
- Настройте сигнализацию о событиях безопасности для администратора информационной безопасности вашего промышленного объекта. Подробнее см. раздел «Настройка сигнализации для администратора информационной безопасности» в документе «Сценарии работы».

К

Возможные неполадки

Утерян пароль администратора

Если утерян пароль от локальной учётной записи `admin` и вы не можете авторизоваться на ViPNet Coordinator IG:

1. Войдите под централизованной учётной записью администратора.
2. Измените пароль от локальной учётной записи `admin`:

   ```
   hostname# admin passwd
   ```

Если утерян пароль от локальной учётной записи `admin` и на ViPNet Coordinator IG не настроено подключение к ViPNet Prime:

- Выполните сброс к заводским настройкам — для серверных исполнений ViPNet Coordinator IG.
- Выполните восстановление ПО — для промышленных исполнений ViPNet Coordinator IG.

Ошибка обновления справочников, ключей и лицензий

- Отдельные команды, связанные с системными процессами, вызывают глобальную блокировку управляющих запросов, которая накладывает ограничения на работу ViPNet Coordinator IG. В частности, обновление справочников, ключей и лицензий, поступившее из ViPNet Prime во время глобальной блокировки, не будет применено. Дождитесь завершения глобальной блокировки и повторно отправьте обновление из ViPNet Prime.

- Применение обновления справочников, ключей и лицензий по времени может совпасть с переключением узлов кластера. В этом случае обновление не будет применено. Поэтому повторно отправьте из ViPNet Prime обновление справочников и ключей.

Ошибка обновления ПО, справочников, ключей и лицензий

Ошибка обновления ПО, справочников, ключей и лицензий на узлах, связанных с ViPNet Coordinator IG, может быть связана с отсутствием доступа последнего к транспортному серверу ViPNet Prime:

1 Определите IP-адрес доступа к ViPNet Prime. Для этого откройте конфигурационный файл `iplir.conf`:

```
hostname# iplir show config
```

IP-адрес доступа указан в секции `[id]` узла `Control Center` в параметре `accessip`:

```
...
[id]
id= 0x3e130002
name= Control Center                                    VPN-15891
ip= 7.0.0.2, 11.0.0.2
accessip= 11.0.0.2
port= 55777
...
```

2 Проверьте, что IP-адрес доступа к ViPNet Prime соответствует его доменному имени:

```
hostname# machine hosts show
127.0.0.1 va1000 localhost localhost.localdomain
11.0.0.2 prime.vk
```

3 Иначе добавьте в файл `hosts` запись о соответствии IP-адреса доступа к ViPNet Prime и доменного имени ViPNet Prime:

```
hostname# machine hosts add <IP-адрес доступа к ViPNet Prime> <доменное имя ViPNet Prime>
```

Ошибка создания резервной копии индивидуальной конфигурации на ViPNet Prime

Одной из причин ошибки, возникающей при создании резервной копии индивидуальной конфигурации на ViPNet Prime, может быть выпуск нового дистрибутива ключей ViPNet Coordinator IG:

- Если вы создавали резервную копию в командном интерпретаторе, на эту причину указывает строка `error: Make sure that you are using the latest appliance initialization file for this appliance` в выводе команды.
- Если вы создавали резервную копию в веб-интерфейсе, на эту причину указывает событие системного журнала, содержащее текст `Make sure that you are using the latest appliance initialization file for this appliance`.

Для устранения причины обновите в ViPNet Prime справочники и ключи ViPNet Coordinator IG.

Сбои в работе агрегированного канала

Сбои в работе агрегированного канала могут быть вызваны неполадками в работе подчинённых интерфейсов, например:

- Неисправностью сетевого оборудования.
- Несогласованностью скоростных режимов работы интерфейсов.
- Неисправностью физического тракта.

Чтобы выяснить причины неполадок в работе подчинённого интерфейса:

1 Проверьте работоспособность интерфейса:

1.1 Просмотрите информацию об интерфейсе:

```
hostname# inet show interface <интерфейс>
```

1.2 Проверьте вывод в строке `Link detected`:

Если в строке отображается `no`, интерфейс неработоспособный.

2 Проверьте режим работы смежного устройства, с которым осуществляется связь по агрегированному интерфейсу. Режимы работы должны совпадать на обоих устройствах.

После настройки системного времени недоступна аутентификация пользователей

После настройки системного времени в некоторых случаях становится недоступной аутентификация пользователей.

Чтобы устранить проблему, перезагрузите ViPNet Coordinator IG.

Не выполнился импорт правил фильтрации промышленных протоколов из файла универсальной конфигурации

Сбой при импорте правил фильтрации промышленных протоколов может произойти в исполнениях ViPNet Coordinator IG10, если на момент импорта было настроено большое количество служб и для импорта были выбраны все группы настроек. В этом случае повторите импорт настроек из файла универсальной конфигурации (*.vbe), но при выборе групп настроек для импорта укажите только правила фильтрации промышленных протоколов.

Блокирование медиа-сессии SIP-соединения при завершении сигнальной сессии по таймауту

В SIP-клиентах некоторых производителей сигнальная сессия SIP-соединения может завершаться через 300 сек. при отсутствии активности. В этом случае ViPNet Coordinator IG блокирует медиа-сессию установленного SIP-соединения. Чтобы избежать блокирования медиа-сессии, установите в настройках SIP-клиента отправку сообщений `Keep Alive` каждые 30 сек. У разных производителей SIP-клиентов этот параметр может называться `re-INVITE`, `OPTIONS`, `INFO` или `NOTIFY`.

Неполадки в работе сервисов IP-телефонии, видео- и аудиоконференций после переключения кластера

Если в вашей сети используются сервисы IP-телефонии, видео- и аудиоконференций, которые работают по протоколам H.323, SCCP, SIP и устанавливают TCP-соединения, то после переключения узлов кластера возможны неполадки в их работе. В этих случаях пользователям сервисов необходимо сделать вызов заново или перезапустить клиента, например SIP-телефон.

Циклическая перезагрузка

Если ViPNet Coordinator IG автоматически перезагружается сразу после загрузки и не даёт возможности авторизоваться, причиной могут быть:

- ошибки в системных файлах;
- неисправность аппаратной платформы;
- ошибки обновления ПО;
- некорректная настройка ViPNet Coordinator IG;
- некорректная настройка кластера.

После трёх перезагрузок подряд автоматически запускается система восстановления, которая может восстановить системные файлы, если это необходимо.

Если после четырёх автоматических перезагрузок подряд ViPNet Coordinator IG по-прежнему не загружается и не даёт возможности выполнять команды:

1. Подключитесь к ViPNet Coordinator IG с помощью консоли и дождитесь появления сообщений:

   ```
   Cyclic reboot detected
   If you want to start VPN later, press ENTER
   ```

2. Нажмите клавишу **Enter**.

   Появятся сообщения:

   ```
   User has confirmed starting VPN later
   VPN start after <600> seconds
   ```

3. Когда появится приглашение ввода имени пользователя, введите `admin` и пароль от локальной учётной записи администратора.

   Появится сообщение:

   ```
   Late start VPN was disabled
   ```

   и вы получите доступ к командному интерпретатору.

4. Выполните экспорт системного журнала и передайте его в службу технической поддержки ИнфоТеКС.

5. Если у вас есть предположения о причине возникновения циклической перезагрузки, вы можете самостоятельно изменить настройки ViPNet Coordinator IG.

Термины и сокращения

PDU (Protocol Data Unit)

Общая для всех физических уровней часть пакета протокола. Содержит данные пакета.

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, со своим сервером соединений, а затем и с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг интернета.

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

ViPNet Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задает связи между ними.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в нее устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями.

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 удалённых узлов в приложениях ViPNet.

Динамический сетевой интерфейс

Разновидность сетевого интерфейса, который добавляется в процессе работы при наступлении некоторого события (например, при подключении встроенного модема, предоставляющего данный интерфейс).

Динамические интерфейсы объединяются в группы по типу интерфейса. Поэтому иногда может встречаться термин «групповой динамический интерфейс».

Существуют следующие группы динамических интерфейсов:

- `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
- `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi через встроенный интерфейс `wlan0` (для исполнений ViPNet Coordinator IG со встроенным модулем Wi-Fi).

Дистрибутив ключей

Набор, содержащий:

- ключи обмена;
- ключ защиты обновлений;
- справочники с информацией об узлах защищенной сети;
- лицензия.

Формируется в ViPNet Prime на основе заданных связей между узлами. Необходим для инициализации и работы ViPNet Coordinator IG.

Для узлов защищенной сети поколения 5 используется дистрибутив ключей `ds5`, для узлов поколения 4 — `dst`.

Доверенная сеть

Сеть ViPNet, с узлами которой узлы собственной сети ViPNet осуществляют защищенное взаимодействие.

Защищенный IP-трафик

Поток IP-пакетов, зашифрованных с помощью программного обеспечения ViPNet.

Защищенный узел

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

Класс сетевого интерфейса

Признак, определяющий назначение сетевого интерфейса. В ViPNet Coordinator IG 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 IG, один из которых (активный) выполняет функции координатора сети ViPNet, а другой (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet Coordinator IG на активном ViPNet Coordinator IG, пассивный ViPNet Coordinator IG переключается в активный режим для выполнения функций. При этом сбойный ViPNet Coordinator IG перезагружается и становится пассивным.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключи защиты обновлений

Ключи защиты обновлений обеспечивают безопасное удаленное обновление ключей обмена из ключевого центра ViPNet Prime и их хранение в ViPNet Coordinator IG.

Ключи обмена

На ключах обмена защищается канал передачи данных между двумя связанными узлами сети ViPNet.

Командный интерпретатор

Командная оболочка, предназначенная для администрирования программного обеспечения ViPNet Coordinator IG с помощью ряда специальных команд.

Компрометация ключей

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

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.

Межсетевое взаимодействие

Информационное взаимодействие, организованное между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

Открытый трафик

Поток незашифрованных IP-пакетов.

Открытый узел

Узел без ПО ViPNet с функцией шифрования трафика на сетевом уровне, расположенный в сети «за координатором».

Политики безопасности

Набор параметров — сетевых фильтров и правил трансляции сетевых адресов, регулирующих безопасность сетевого узла.

Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента функцию сервера соединений выполняет координатор, назначенный сервером IP-адресов.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищённых узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки транспортного конверта MFTP.

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на защищенные узлы ViPNet транспортным сервером MFTP.

Транспортный сервер MFTP

Компонент координатора, обеспечивающий маршрутизацию транспортных конвертов MFTP между узлами 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.

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

Туннелирующий координатор

Координатор, который осуществляет туннелирование.

Шлюз Modbus

Программно-аппаратная функциональность, выполняющая преобразование трафика интерфейса Ethernet в интерфейсы RS-232 и RS-485 и обратно для обеспечения взаимодействия Ethernet- и Modbus-устройств.

Шлюзовой координатор

Координатор, через который происходит обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие. Шлюзовые координаторы назначаются в ViPNet Prime каждой сети при организации взаимодействия между двумя различными сетями ViPNet.