

Первый российский криптошлюз и межсетевой экран с РоЕ

Андрей Иванов
Иван Герасименко

 **infotecs**



VIPNet Coordinator IG

Индустриальный
шлюз безопасности

Предназначен для:

- защиты периметра информационной и промышленной сети
- организации демилитаризованной зоны
- сегментирования сети и разграничения доступа
- организации управления сетевыми потоками
- сокрытия реальных адресов и архитектуры сети
- организации защищенного канала связи для распределенных систем
- организации защищенного удаленного доступа, в том числе с мобильных устройств



Функционал

- Защищенная сеть ViPNet
- Wi-Fi-модуль
- GSM-модуль
- Межсетевой экран + DPI протоколов Modbus и IEC 104
- Шлюз Modbus
- Коммутатор и маршрутизатор
- Отказоустойчивость
- Мониторинг состояния



Криптографическая защита

с использованием алгоритмов ГОСТ



- каналов передачи данных:
 - между АСУ, в т.ч. их сегментами
 - при подключении к сетям связи общего пользования
- доступа удаленных и мобильных пользователей
- удаленного мониторинга
- подключения для сервисного обслуживания

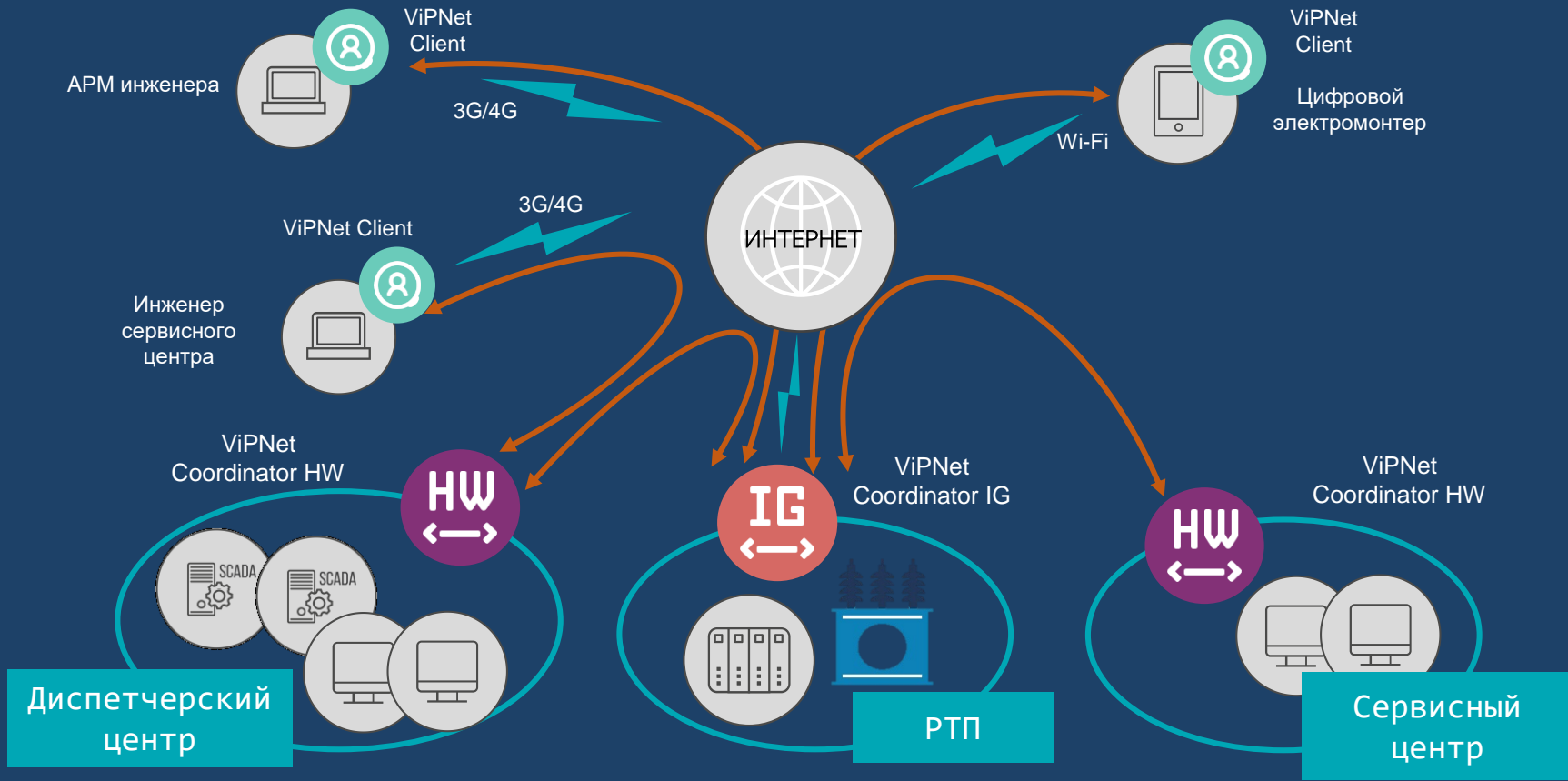
Соответствие требованиям ФСБ России
к СКЗИ класса КСЗ

Защищенная сеть ViPNet



- Защита каналов передачи данных между АСУ и/или сегментами
- Передача информации по каналам связи общего пользования
- Централизованная настройка сети и политик

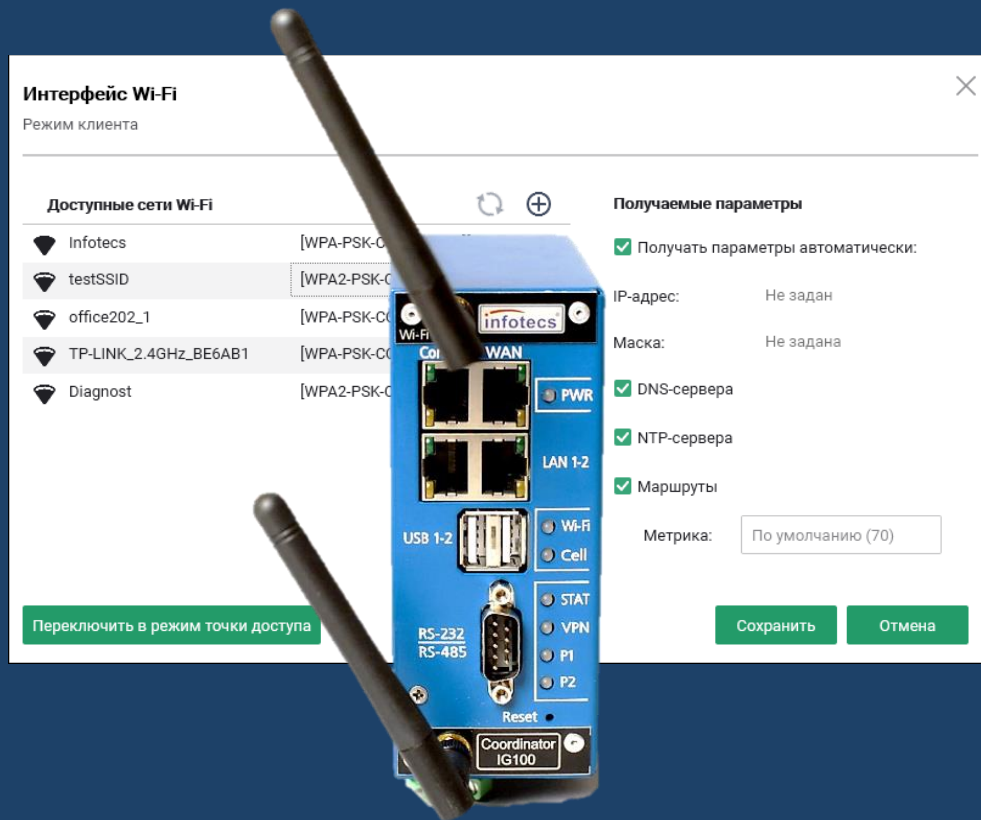
Защищенный удаленный доступ



Wi-Fi

- Клиент
- Точка доступа

Внимание! Wi-Fi модуль устанавливается только на производстве!



GSM-модуль

○ LTE-модуль

В комплект GSM-модуля входит внешняя GSM-антенна.

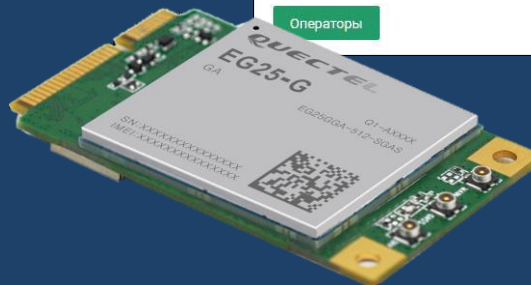
Внимание! GSM-модуль устанавливается только на производстве!

USB-модем подключен

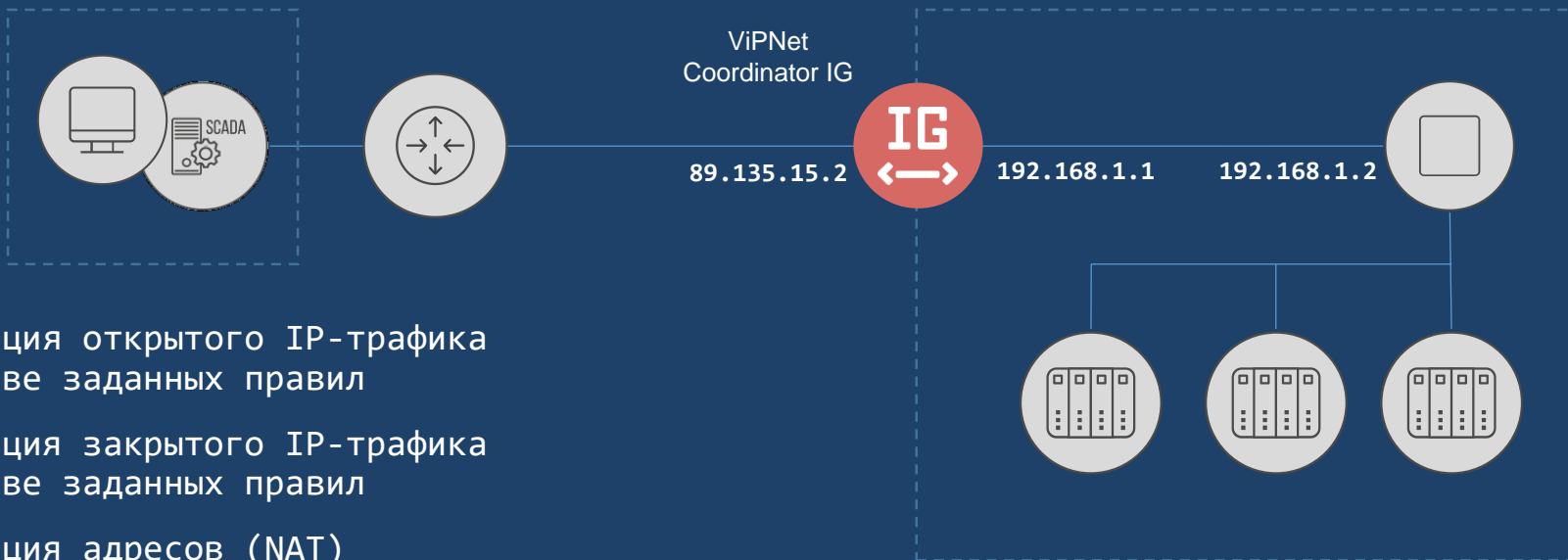
Параметры подключения	Информация об устройстве	Получаемые настройки
Метод настройки:	Модель: 3G/4G	<input checked="" type="checkbox"/> DNS-сервера
Оператор (MNC): N/A (0)	Производитель: Quectel UC20	<input checked="" type="checkbox"/> Маршруты
Страна (MCC): N/A (0)	Уровень сигнала: (0 dBm)	Метрика: По умолчанию (60)
DNS-адрес APN: N/A	SIM-карта: Установлена	
Имя пользователя: N/A	PIN-код: Не задан	
Пароль: N/A		
Набираемый номер: N/A		

[Сбросить параметры подключения](#)

[Операторы](#) [Сохранить](#) [Отмена](#)



Межсетевой экран



- Фильтрация открытого IP-трафика на основе заданных правил
- Фильтрация закрытого IP-трафика на основе заданных правил
- Трансляция адресов (NAT) для открытого IP-трафика
- Фильтрация на прикладном уровне трафика протоколов Modbus и МЭК 60870-5-104

МЭ тип Д: режимы работы



Фильтрация протокола Modbus TCP

- Номер порта
- Адреса устройств
- Коды функций
- Регистры чтения и записи
- Отдельный журнал регистрации пакетов

Настройка набора правил фильтрации Modbus

Набор правил включен

Название набора:

Правила транспортного уровня Правила прикладного уровня

[+](#) Добавить

Таблица	Адрес сервера	Адрес клиента	Протокол	Порт назначения
Local	89.175.26.1	192.168.11.5	tcp	502
VPN	@local	0x00010201	tcp	24358

№	Статус	Имя	Действие	ID	FC	R	W
:: 1	<input checked="" type="checkbox"/>	rule_1	✓ Пропуск...	1, 10-15	2, 3	100-200	Любой
:: 2	<input checked="" type="checkbox"/>	rule_2	✗ Блокиро...	Любой	20	Любой	Любой

Фильтрация протокола МЭК 60870-5-104 (4.5.1)

- Номер порта
- Общий адрес (ASDU)
- Адрес объекта информации (Information Object Address)
- Идентификатор типа (Type Identifier)

Набор правил фильтрации протокола МЭК104

Набор правил активен

* Название набора правил:

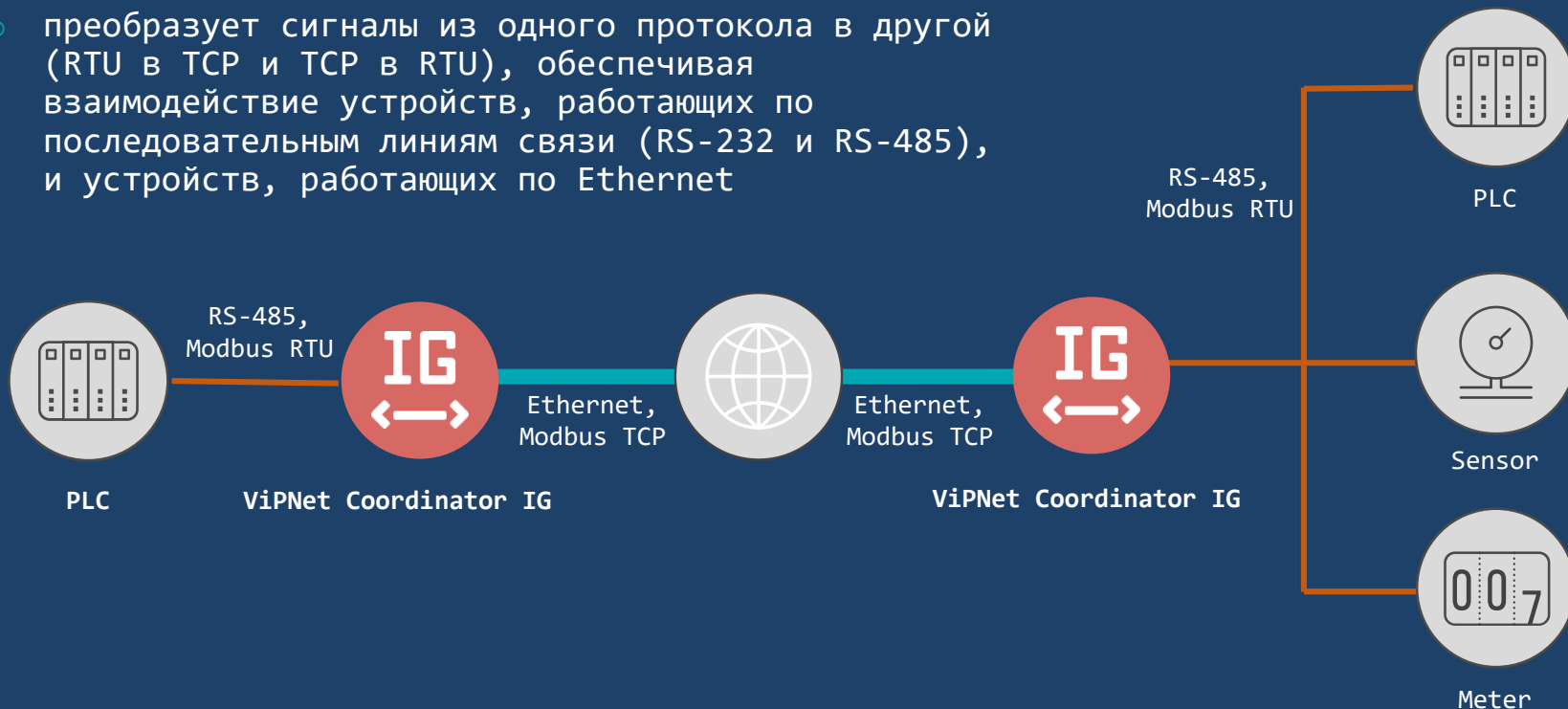
Правила транспортного уровня Правила прикладного уровня Формат протокола

[+](#) Добавить Правил: 57

№	Статус	Имя правила	Общий адрес	Адрес ОИ	Тип	Действие
⋮ 1	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 2	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 3	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 4	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 5	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить

Шлюз Modbus TCP-RTU и RTU-TCP

- преобразует сигналы из одного протокола в другой (RTU в TCP и TCP в RTU), обеспечивая взаимодействие устройств, работающих по последовательным линиям связи (RS-232 и RS-485), и устройств, работающих по Ethernet



Шлюз Modbus TCP-RTU и RTU-TCP

Служба Modbus остановлена

Настройки службы Маршруты RTU to TCP

Общие настройки

Интерфейс соединения: RS-232

RS-485

Режим работы: TCP to RTU

RTU to TCP

Адрес шлюза: Шлюз доступен по IP адресам, которые настроены на интерфейсах.

Порт шлюза:

Время по умолчанию на ожидание запроса: мс

Время по умолчанию на ожидание ответа: мс

Сохранить

Отмена

Настройки интерфейса RS-232

Скорость ТТУ устройства: бод

Контроль бита четности:

Настройки интерфейса RS-485

Скорость ТТУ устройства: бод

Контроль бита четности:

Задержка до отправки: мс

Задержка после отправки: мс

в другой

RS-485),

Ethernet,
Modbus TCP

VipNet Coordinator IG

RS-485,
Modbus RTU

PLC

Sensor

Meter

Сетевые сервисы

DNS
(client/server)

DHCP
(server/relay)

NTP
(client/server)

VLAN

QoS

EtherChannel

OSPF

Failover

Сетевые сервисы L2

- VLAN
- Агрегирование интерфейсов

Создание VLAN интерфейса

Разрешено взаимодействие интерфейса с сервисами

Статус и основные настройки

Родительский интерфейс:

Идентификатор:

Класс:

Получаемые параметры

Получать параметры автоматически:

IP-адрес:

Маска:

DNS-сервера

NTP-сервера

Маршруты

Метрика:

Создание bond интерфейса

Разрешено взаимодействие интерфейса со службами

Статус и основные настройки

Идентификатор:

* Класс:

Режим:

Сетевые интерфейсы:

Частота опроса: мс

Получаемые параметры

Получать параметры автоматически:

IP-адрес:

Маска:

DNS-сервера

NTP-сервера

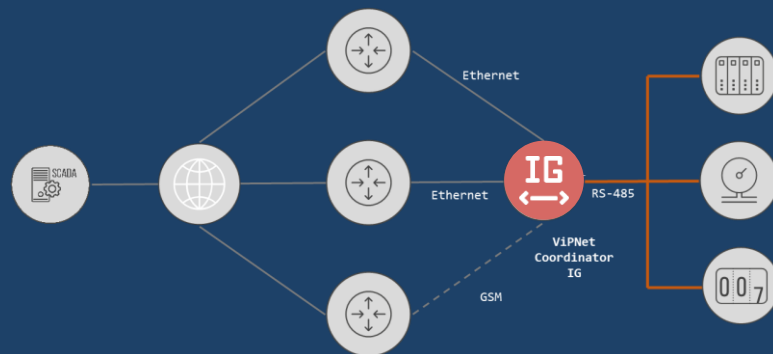
Маршруты

Метрика:

Сетевые сервисы L3

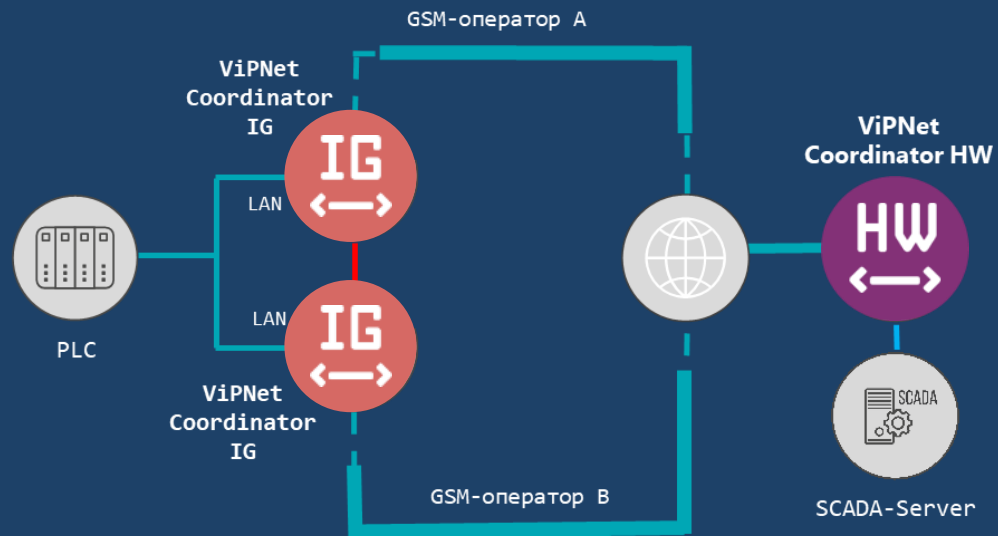
- Статическая и динамическая маршрутизация по протоколам DHCP/PPP и OSPF
- Резервирование каналов
- Балансировка трафика
- Обработка трафика в соответствии с приоритетом (поддержка протокола DiffServ)

Маршрутизация							
Сводная таблица	Статическая	Политики маршрутизации	DHCP	OSPF			
Статус и тип	Адрес назначения и маска	Диста...	Метри...	Вес	Шлюз	Сетевой интерфе...	Активность
✓ DHCP/PPP	0.0.0.0/0	70	70		192.168.179.2	eth0	
✓ Connected	10.0.40.0/24				directly	eth3	
✓ Connected	10.0.40.0/24				directly	eth1	
✓ Connected	10.0.40.0/24				directly	eth2	
✓ Connected	127.0.0.0/8				directly	lo	
✓ Connected	192.168.179.0/24				directly	eth0	



Отказоустойчивость

- Защита от программных сбоев
- Резервирование каналов связи
- Агрегирование каналов связи
- Кластер горячего резервирования:
 - с беспроводными интерфейсами
 - GSM-модем и модули Wi-Fi могут иметь разные настройки на нодах
 - с использованием шлюза Modbus
 - с использованием DHCP



Мониторинг состояния

- Удаленный мониторинг по протоколу SNMPv3
- Просмотр статистики IP-пакетов
- Просмотр журналов:
 - регистрации IP-пакетов
 - пакетов промышленных протоколов
 - транспортных конвертов (MFTP)
 - системного
- Экспорт журналов по протоколу syslog

Состояние системы

Сервисы
Время работы узла: 1 день 20:29

- Failover
- Iplir
- MFTP
- WebGUI

Место на дисках

Основной диск
163 МБ из 391 МБ (42%)

Загрузка процессора, %
За последние 2 минуты

Общая 6% Failover 1% Iplir 6% MFTP 0% W

Журнал пакетов АСУ ТП

Модбус МЭК104

Фильтр IP-пакетов Результат фильтрации за последний час, с 06.12.2021 12:21

✓	Конце интервала	Источник	Назначение	Транспорт.	Порт наа...	Размер	Адрес устр..	Код функции	Регистры ч...	Регистры з...	Событие
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	720	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	720	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:19:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:19:28, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:19:02, 06 Дек 20...	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен

GPIO

General-Purpose Input/Output –
интерфейс ввода/вывода общего назначения



Входной сигнал



- Датчик вскрытия шкафа



- Переключение в специальный режим работы (для типа Д)



- Сигнал с пользовательского устройства



Выходной сигнал

- Кластер с шлюзом Modbus TCP-RTU
- Индикатор событий:
 - работа в режиме обслуживания
 - работа в штатном режиме
 - работа в специальном режиме
 - вскрыт шкаф
 - сигнал на пользовательское устройство

Сценарии работы



ViPNet Coordinator IG 4

Сценарии работы

Версия продукта: 4.5.1

ViPNet Coordinator IG10
ViPNet Coordinator IG100

Содержание

Введение.....	5
О документе.....	6
Соглашения документа.....	6
Связанные документы.....	7
Обратная связь.....	8
Глава 1. ViPNet Coordinator IG как межсетевой экран сегмента промышленной сети.....	9
Защита сегмента промышленной сети.....	10
Защита сегмента с устройствами Modbus.....	10
Защита сегмента с устройствами МЭК 60870-5-104.....	12
Доступ из защищенного сегмента.....	14
Размещение общедоступного сервера в демилитаризованной зоне.....	16
Настройка политик безопасности для разных режимов работы.....	18
Глава 2. Построение защищенного канала связи.....	20
Защищенное взаимодействие сегментов промышленной сети.....	21
Удаленный доступ клиента к защищенному сегменту промышленной сети.....	24
Глава 3. Использование встроенного шлюза Modbus в ViPNet Coordinator IG.....	26
Взаимодействие устройств Modbus RTU с сервером сбора данных.....	27
Защищенное взаимодействие устройств Modbus RTU с удаленными сетевыми узлами.....	29
Защищенный удаленный доступ клиента к устройствам Modbus RTU.....	32
Защищенное удаленное взаимодействие устройств Modbus RTU.....	34
Глава 4. Использование технологии PoE.....	38
Защита канала связи между сервером и видеокамерами с PoE.....	39
Глава 5. Использование интерфейса GPIO.....	42
Подключение датчика вскрытия внешнего шкафа.....	43
Подключение внешнего устройства для перехода в специальный режим.....	45
Настройка сигнализации для администратора информационной безопасности.....	47
Глава 6. Использование функции MultiWAN для резервирования каналов связи.....	49
Резервирование каналов доступа в интернет.....	50
Создание резервного канала Ethernet или Wi-Fi.....	50
Создание резервного канала 3G/4G.....	52

Создание двух резервных каналов.....	55
Разделение каналов доступа в интернет для распределения (балансировки) нагрузки на сеть.....	59
Резервирование каналов доступа в интернет с балансировкой трафика.....	62
Мониторинг состояния каналов связи.....	64
Настройка мониторинга по SNMP.....	65
Настройка мониторинга по Syslog.....	66

Глава 7. Повышение отказоустойчивости ViPNet Coordinator IG.....	68
Организация кластера горячего резервирования.....	69
Типовая схема организации кластера.....	69
Кластер с беспроводными интерфейсами.....	73
Кластер с использованием шлюза Modbus и интерфейса GPIO.....	77
Кластер с использованием DHCP-сервера и DHCP-relay.....	79
Кластер с резервированием канала доступа в интернет.....	80
Организация агрегированного канала.....	85
Агрегированный канал между ViPNet Coordinator IG и коммутатором.....	85
Агрегированный канал между двумя ViPNet Coordinator IG.....	88
Глава 8. Использование сервисных функций ViPNet Coordinator IG.....	90
Организация обработки трафика из нескольких VLAN.....	91
Организация работы клиентов с локальным или удаленным DHCP-сервером.....	93
Организация работы клиентов с локальным DHCP-сервером.....	93
Организация работы клиентов с удаленным DHCP-сервером.....	95
Использование DHCP-сервера и DHCP-relay в разных сетях.....	97
Использование запасного DHCP-сервера.....	100
Использование сторонних DHCP-серверов.....	101
Одновременное использование DHCP-сервера и DHCP-relay.....	103
Организация работы клиентов удаленных офисов с DNS- и NTP-серверами, расположенными в центральном офисе.....	105
Защита соединения между удаленными сегментами сети на канальном уровне модели OSI.....	107
Настройка функции L2OverIP при отсутствии VLAN.....	107
Настройка функции L2OverIP в случае использования VLAN.....	109
Настройка функции L2OverIP для обеспечения работоспособности протоколов динамической маршрутизации.....	112
Настройка параметров L2OverIP.....	114
Настройка протокола OSPF.....	115

Сертификаты соответствия по требованиям ФСБ России



ViPNet Coordinator IG 4.3.3:

- Сертификат № СФ/124-4247 по требованиям к СКЗИ класса КСЗ
- Анализ изменений МЭ 4 класса защищенности

ViPNet Coordinator IG 4.5.1:

- Передан на анализ изменений

Сертификат соответствия по требованиям ФСТЭК России



ViPNet Coordinator IG 4.5.1:

Сертификат № 4379

- Требования к МЭ
- Профиль защиты МЭ типа Д 4 класса защиты (ИТ.МЭ.Д4.ПЗ)
- Профиль защиты МЭ типа А 4 класса защиты (ИТ.МЭ.А4.ПЗ)
- Профиль защиты МЭ типа Б 4 класса защиты (ИТ.МЭ.Б4.ПЗ)
- 4 уровень доверия по ТДБ (2020 г)

Реестры РПО, РЭП



- ПО ViPNet Coordinator IG включено в реестр российского ПО – рег.номер 5102 (19.01.2019)
- Единый реестр российской радиоэлектронной продукции (РЭП) – как ПАК ViPNet Coordinator IG, в процессе подтверждения

Линейка шлюзов безопасности ViPNet Coordinator IG



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG10 I2



ViPNet
Coordinator
IG100 I4



ViPNet
Coordinator
IG100 I5

Классические исполнения

Новые исполнения

Линейка шлюзов безопасности ViPNet Coordinator IG



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG10 I2



ViPNet
Coordinator
IG100 I4



ViPNet
Coordinator
IG100 I5

Классические исполнения

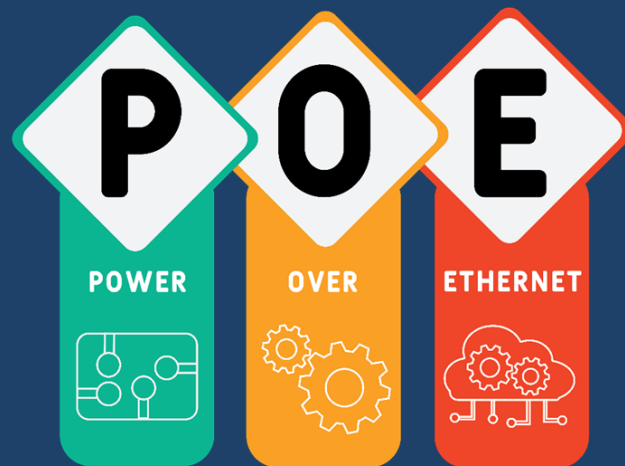
Новые исполнения

Что такое PoE?

PoE (Power over Ethernet) – технология использования витой пары стандарта Ethernet для передачи данных и для питания устройства.

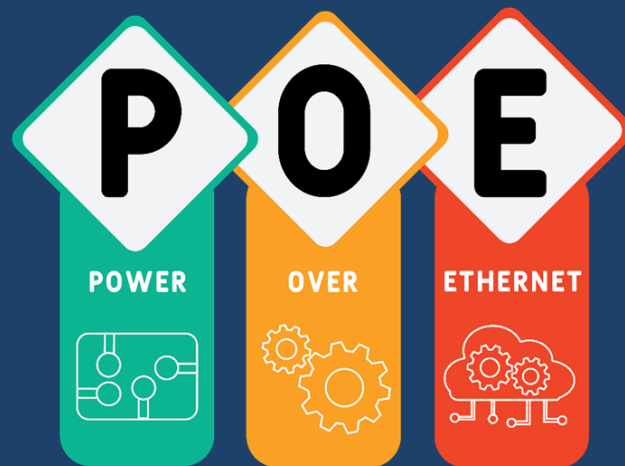
Питающие устройства - инжекторы;
Power Sourcing Equipment, PSE

Питаемые устройства
Powered Device, PD



Зачем?

- Подключение устройств в труднодоступных местах
- Управление питанием (включение/выключение/перезапуск)
- Упрощенное обслуживание (нет отдельных блоков питания)
- Электробезопасность



ViPNet Coordinator IG100 I5



- Питание: 24В DC, PoE
- Ethernet: 2 x LAN 10/100BASE-T
с возможностью питать PoE-устройства по
стандартам IEEE 802.3af и IEEE 802.3at
(PoE PSE)
- 1 x WAN 10/100BASE-T
с возможностью получать питание по
стандартам IEEE 802.3af и IEEE 802.3at
(PoE PD)
- Рабочая температура - -20°C^* ... $+50^{\circ}\text{C}$

* Для AP с беспроводными модулями

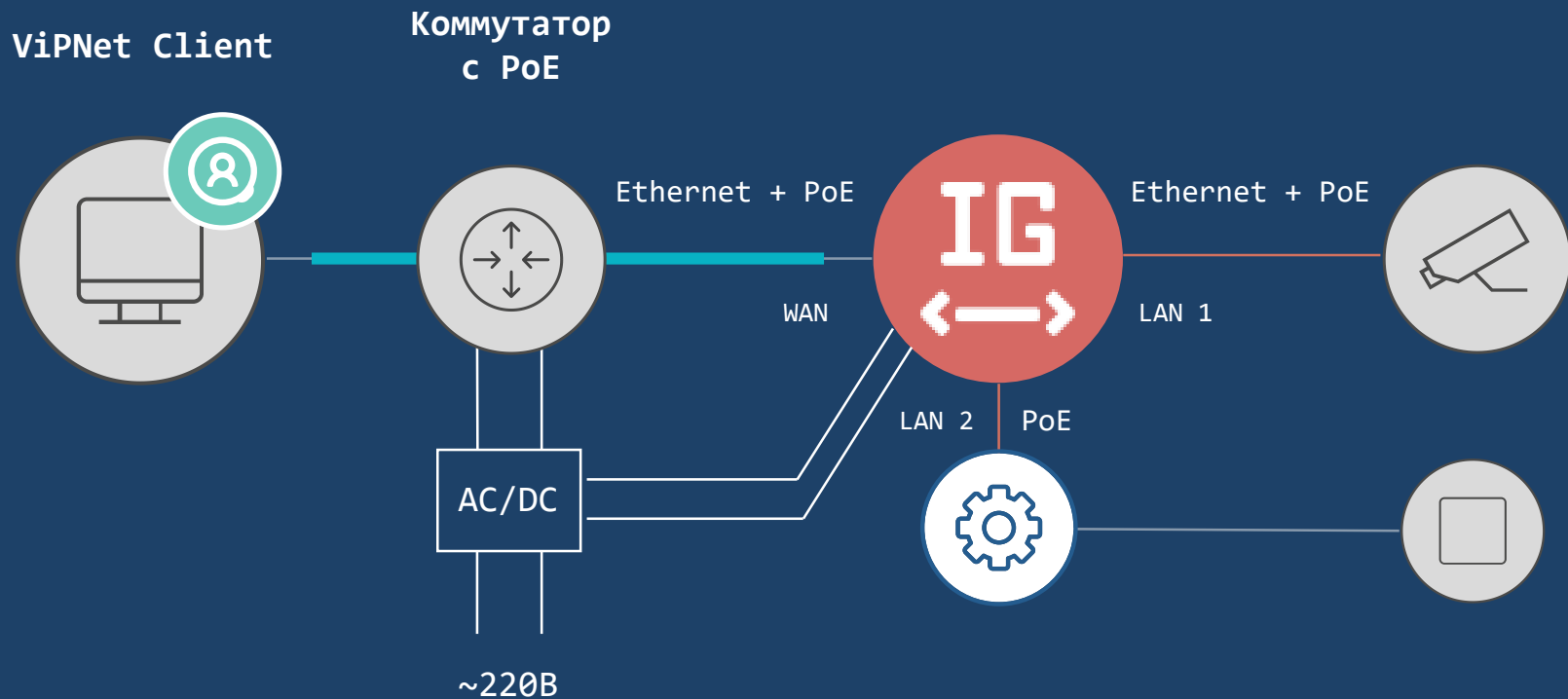
МАСТЕР-КЛАСС: сценарии

Индикаторы
PoE

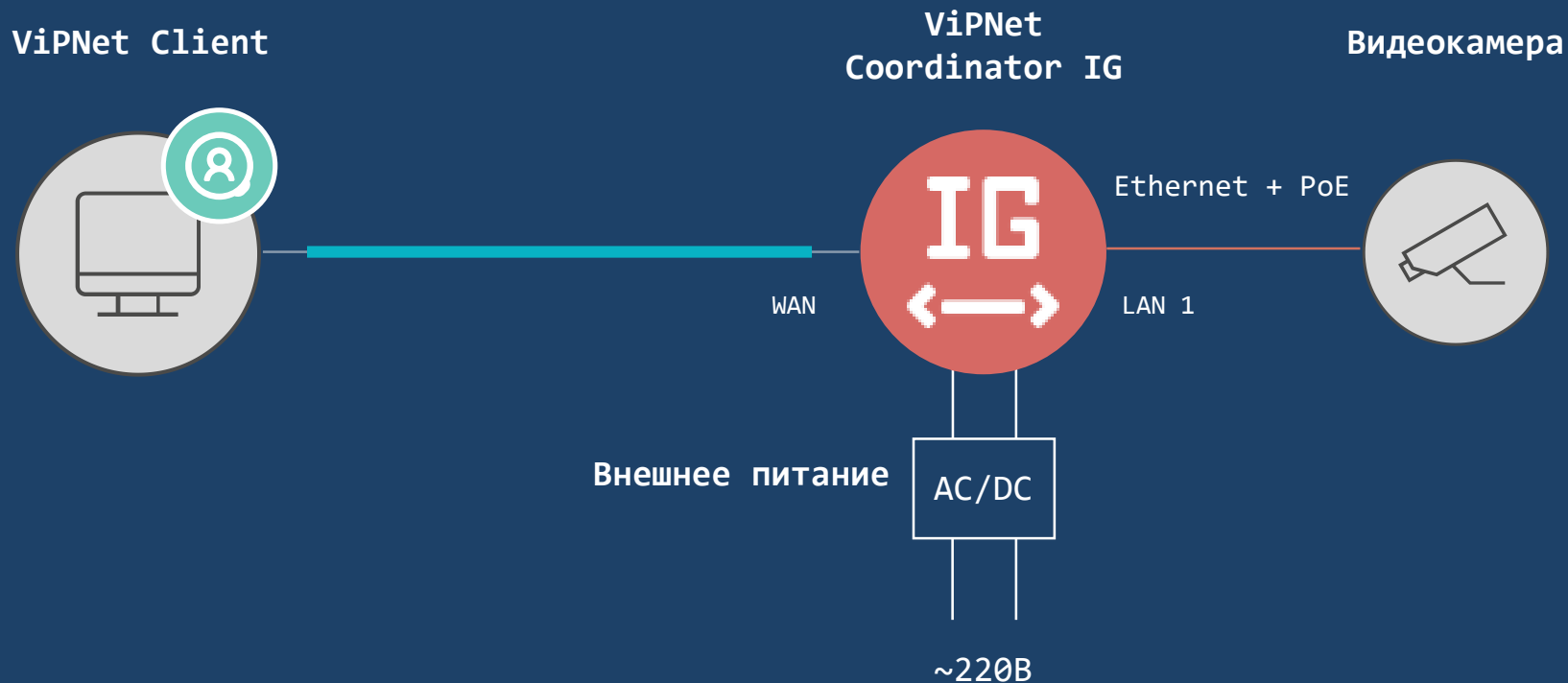
PD
PSE1
PSE2



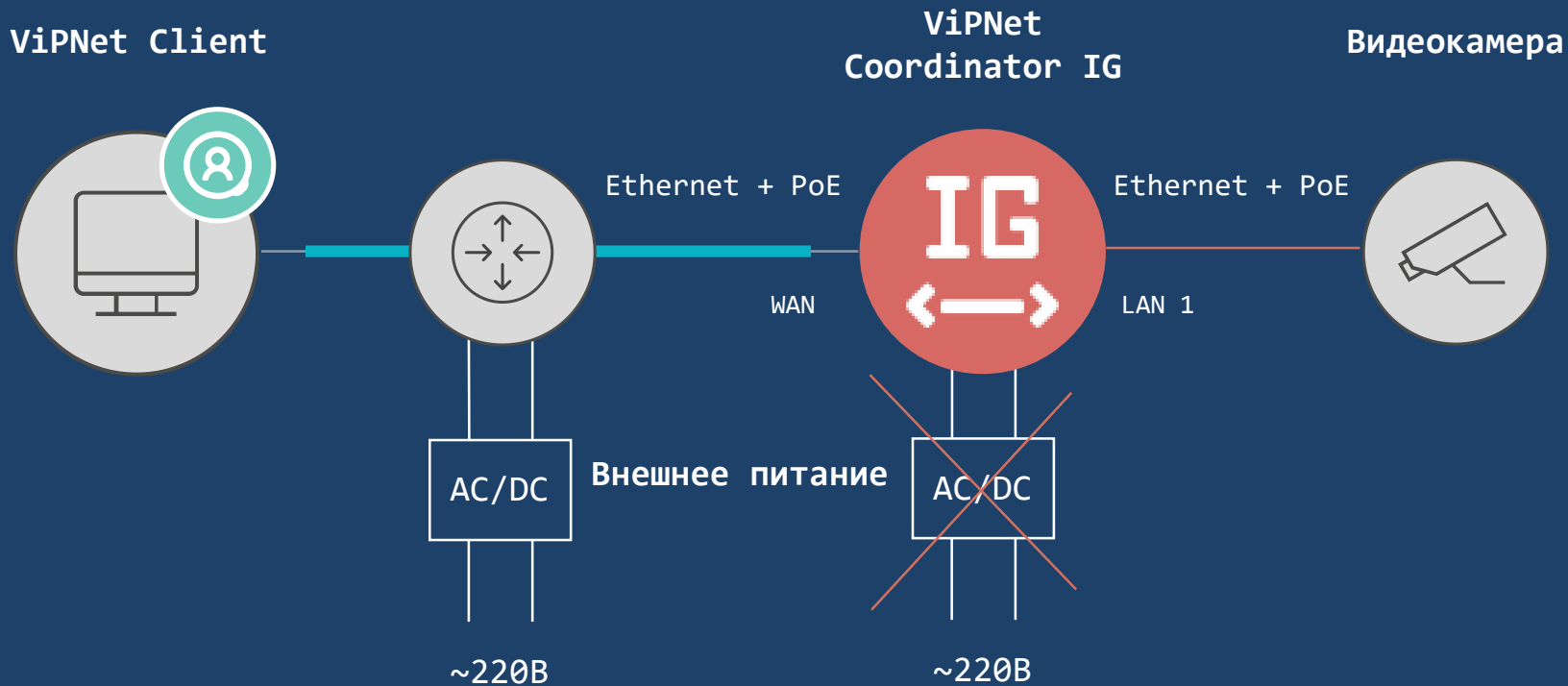
Схема стенда



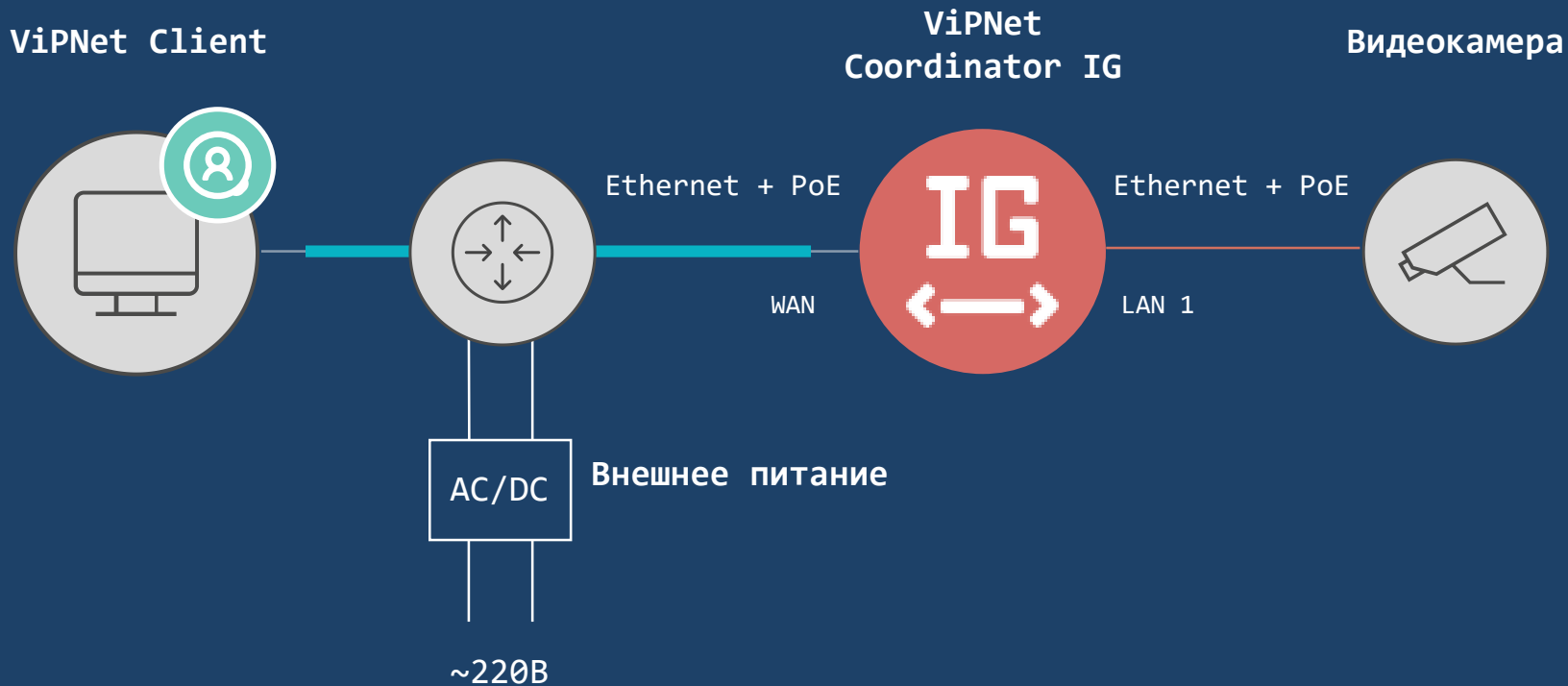
PoE-источник (PSE)



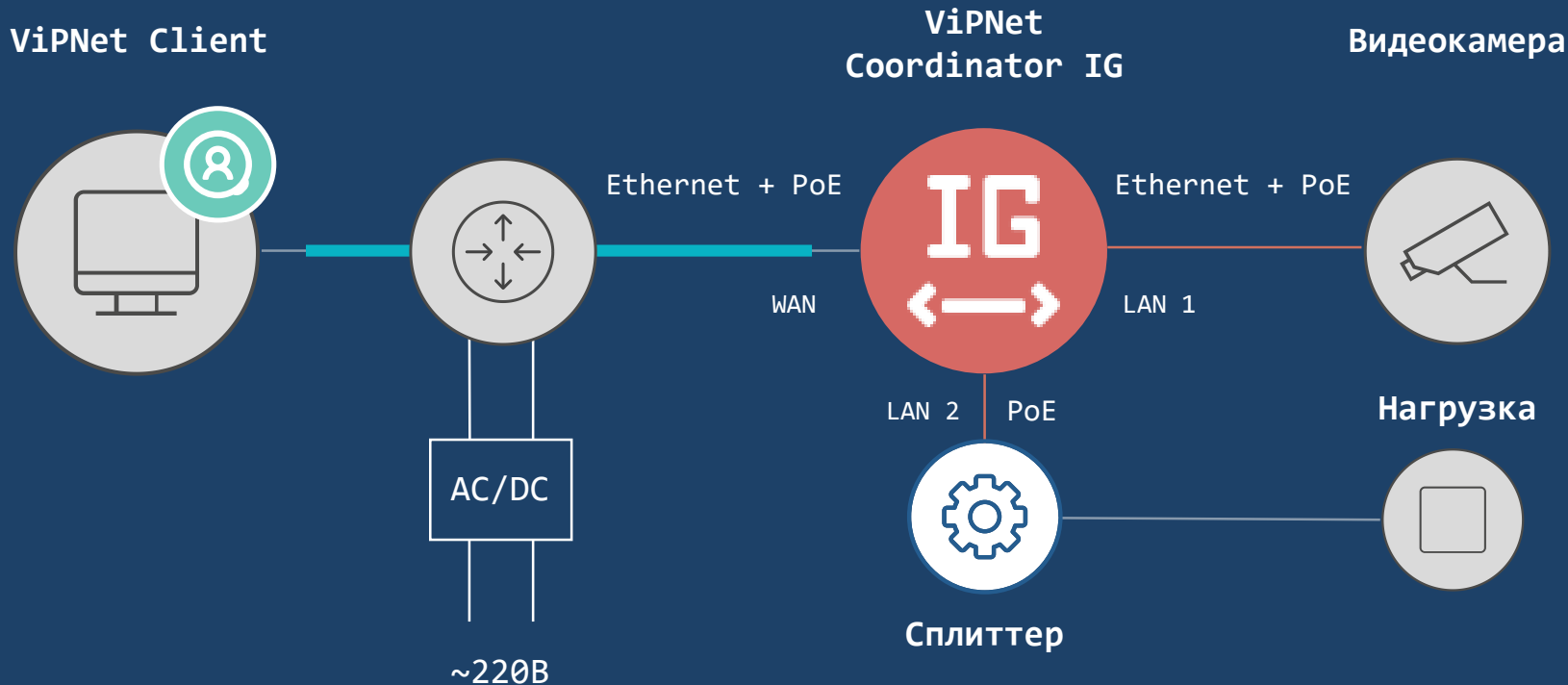
PoE-Delivery (PD + PSE)



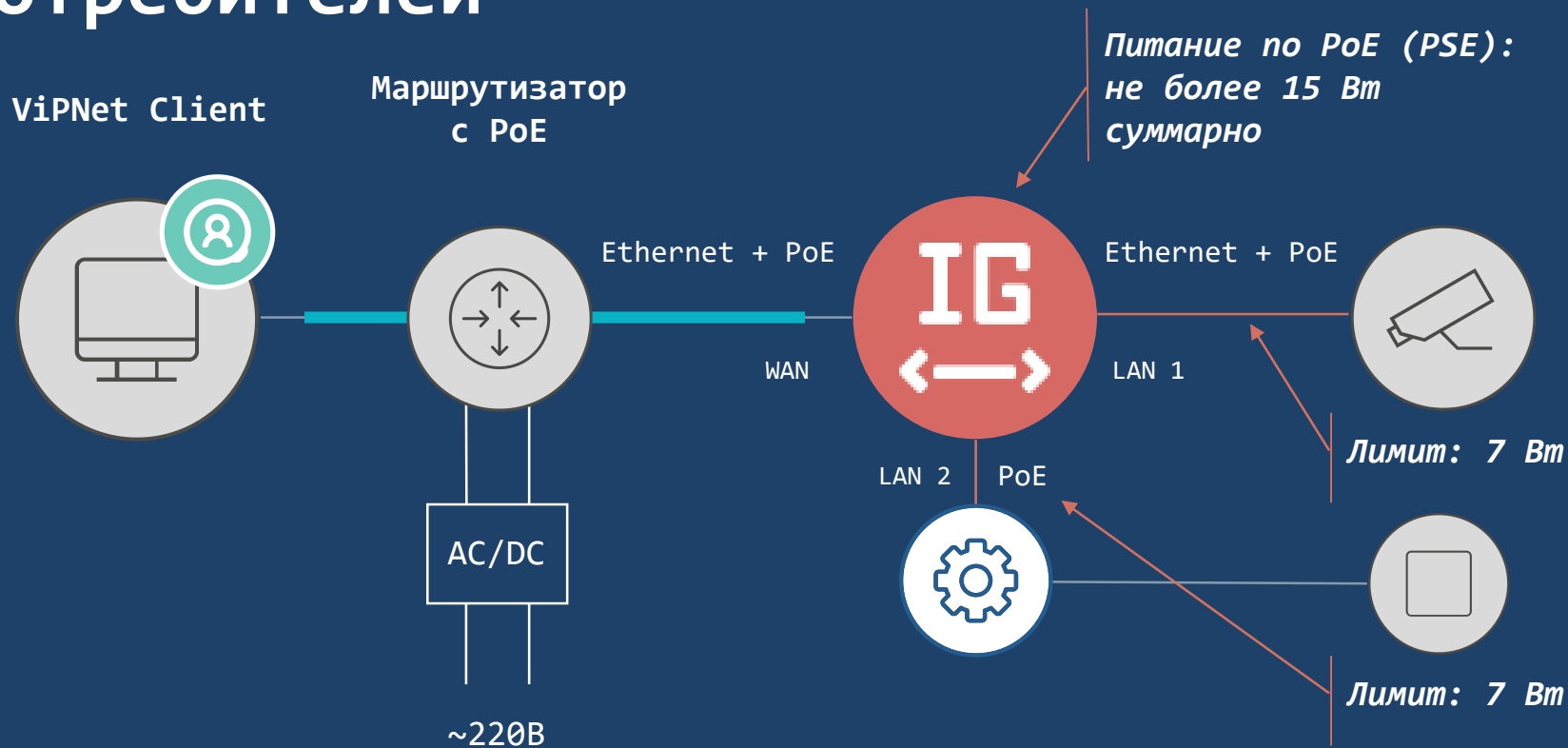
PoE-Delivery (PD + PSE)



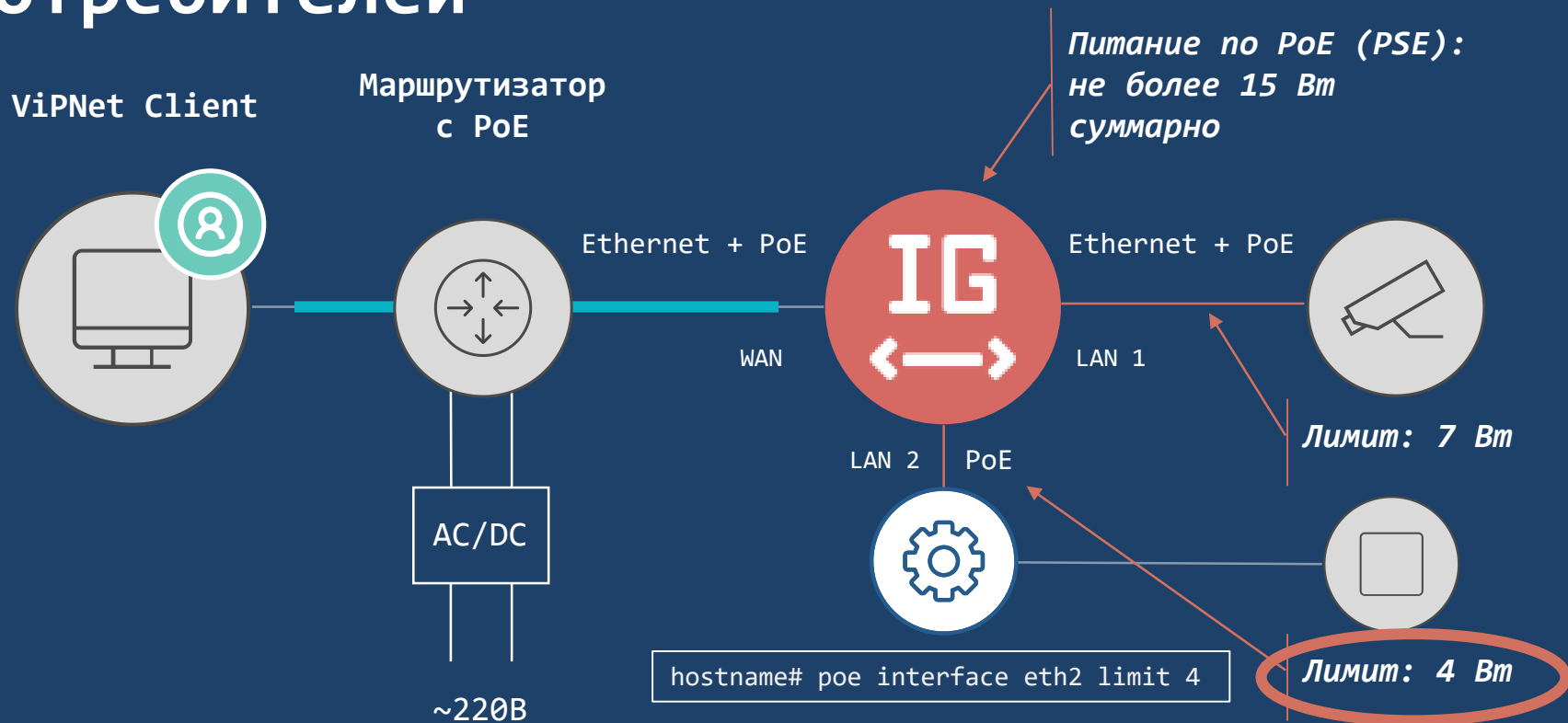
Питание потребителей по двум каналам



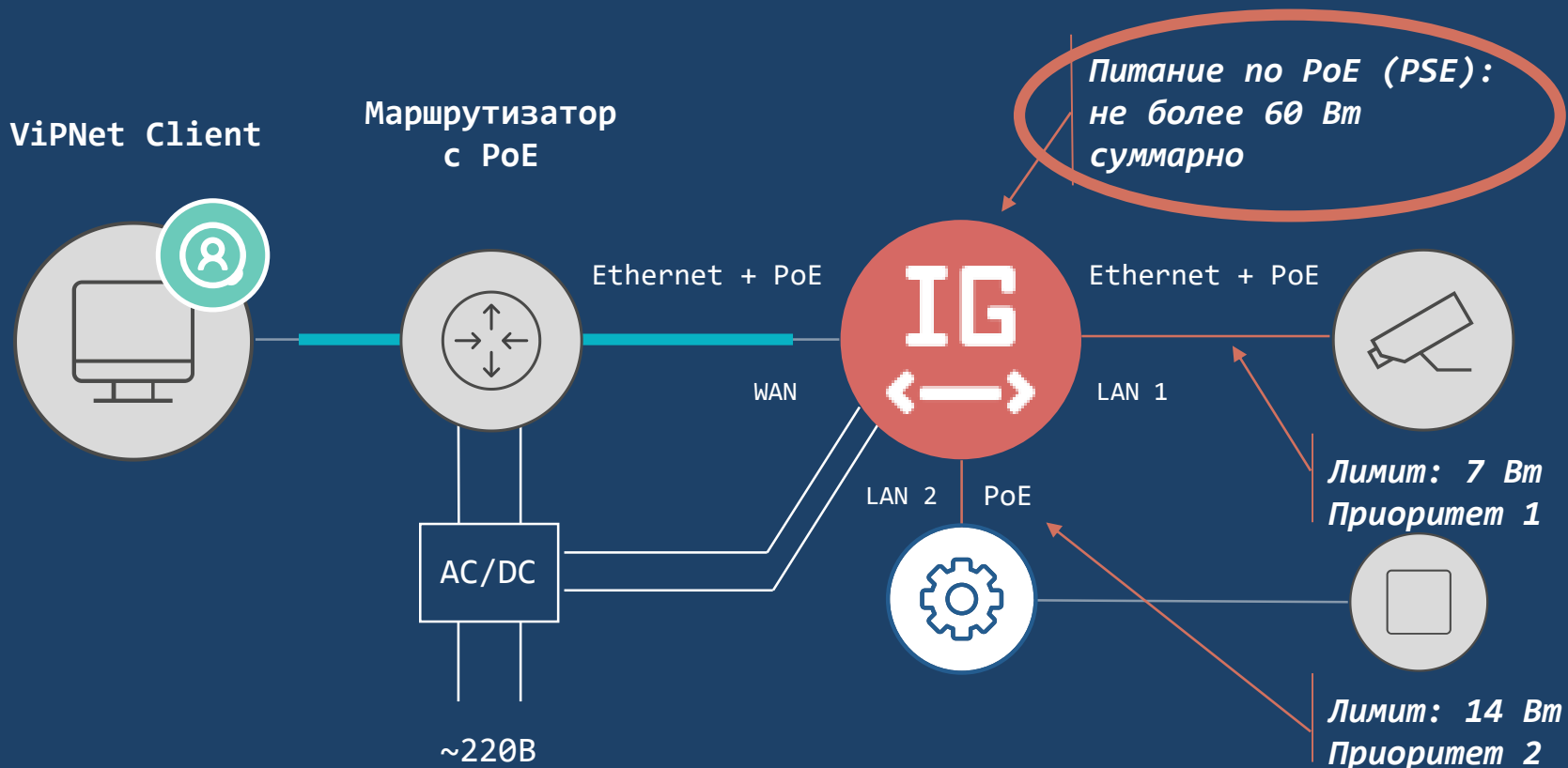
Ограничение мощности потребителей



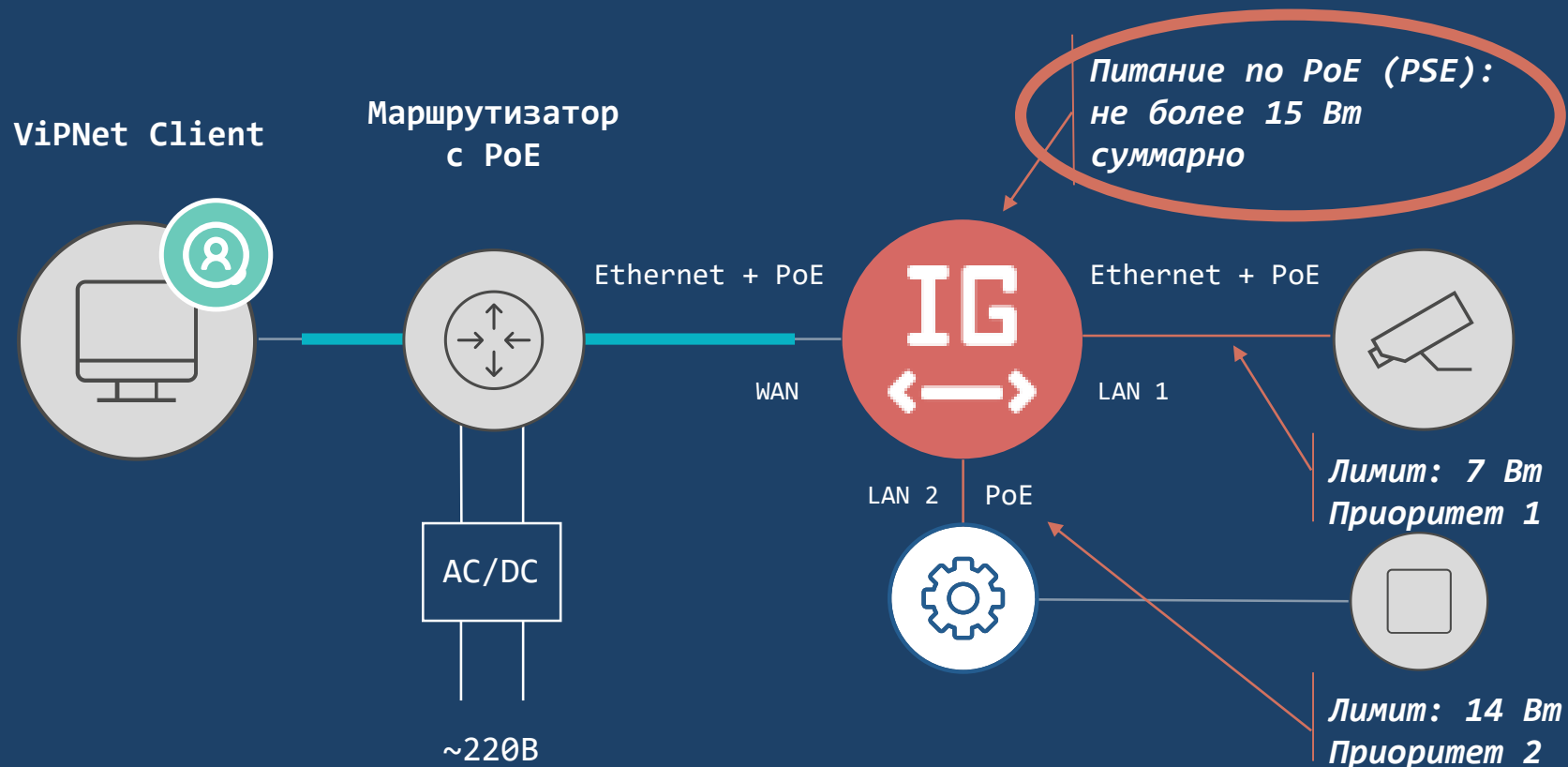
Ограничение мощности потребителей



Power Delivery

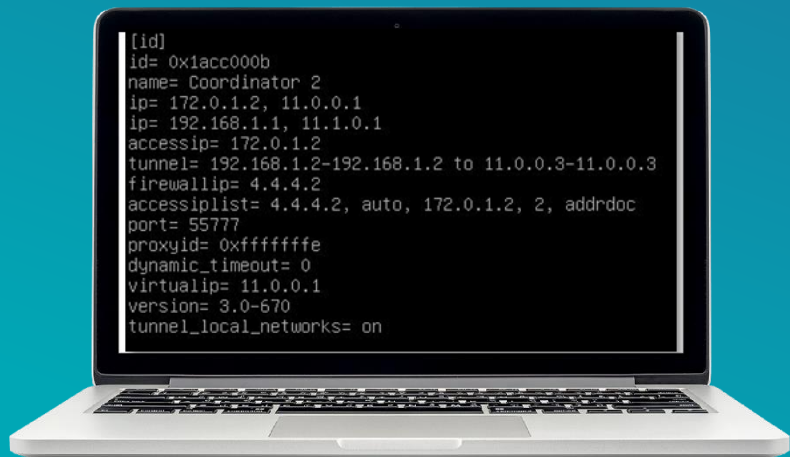


Приоритеты потребителей



МАСТЕР-КЛАСС: демонстрация

Индикаторы
PoE





Андрей Иванов Andrey.Ivanov2@infotecs.ru

Иван Герасименко Ivan.Gerasimenko@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363