

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ГК МФМК»
(ООО «ГК МФМК»)

УТВЕРЖДАЮ
Генеральный директор
ООО «ГК МФМК»
_____ Лудиков А.В.
« ____ » _____ 2026 г.

ОПЕРАЦИОННАЯ СИСТЕМА «TITANWRT_N1IMXKK»
Руководство пользователя

РАЗРАБОТАНО
ООО «ГК МФМК»

Дата введения: _____
Без ограничения срока действия.

г. Москва
2026

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Содержание

Сокращения и обозначения	1
1. Введение	5
1.1. Подключение к Web-интерфейсу	6
1.2. Автоматическое обновление информации	7
2. Состояние	8
2.1. Обзор	8
2.1.1. «Система»	8
2.1.2. «Оперативная память (RAM)»	8
2.1.3. «Состояние портов сетевых интерфейсов»	9
2.1.4. «Сеть»	10
2.1.5. «Активные DHCP-аренды»	10
2.2. Маршрутизация	11
2.3. Межсетевой экран	11
2.4. Процессы	12
2.5. Графики в реальном времени	13
2.5.1. «Нагрузка»	14
2.5.2. «Трафик»	14
2.5.3. «Соединения»	14
2.6. Журналы	15
2.6.1. Журнал ядра	16
2.6.2. Системный журнал	16
2.6.3. Запланированные задания (cron)	17
2.6.4. SNMP	18
3. Система	19
3.1. Общие настройки	19
3.1.1. «Устройство»	19
3.1.2. «Журналирование»	20
3.1.3. Вкладка «Язык и тема»	20
3.1.4. Вкладка «Дополнительные»	21
3.2. Время	21
3.2.1. «Системное время»	22
3.2.2. «Синхронизация времени»	22
3.3. Управление доступом	22
3.3.1. Пароль устройства	22
3.3.2. Настройка доступа по SSH	23
3.3.3. SSH-ключи	24
3.3.4. Доступ HTTP(S)	24
3.4. Сторожевой таймер	25

3.5. Автозапуск	25
3.5.1. Скрипты инициализации	26
3.5.2. Запуск пакетов и служб пользователя при включении устройства	26
3.6. Планировщик	27
3.7. Точки монтирования	27
3.7.1. Основные настройки	28
3.7.2. Смонтированные разделы	29
3.7.3. Точки монтирования	29
3.7.4. Разделы подкачки (swap)	30
3.8. Индикаторы	31
3.9. Резервное копирование	32
3.9.1. Действия	32
3.9.2. Конфигурация	32
3.10. Обновление прошивки	34
3.11. Терминал	34
3.11.1. Терминал	34
3.11.2. Настройки	37
3.12. Перезагрузка	38
4. Службы	39
4.1. DDNS	39
4.1.1. Информация	39
4.1.2. Глобальные настройки	39
4.1.3. Службы	40
Редактирование параметров DDNS-службы	41
Добавление новой службы	43
4.2. LLDP	43
4.2.1. Состояние	43
4.2.2. Настройки	45
Поддержка протоколов	47
4.3. STP/RSTP	48
4.3.1. Состояние	48
4.3.2. Настройки	48
4.4. Настройки SNMP	49
4.4.1. Глобальные	49
4.4.2. SNMPv1/SNMPv2c	50
4.4.3. SNMPv3	50
4.4.4. Трапы	51
4.4.5. Система	51
4.4.6. Журналирование	52
4.5. Настройки FTP-сервера	52
4.5.1. Настройки службы	53

4.5.2. Настройки подключения	53
4.5.3. Основные настройки	54
4.5.4. Локальные пользователи	55
4.5.5. Виртуальные пользователи	55
4.5.6. Анонимный доступ	56
4.5.7. Настройки журналирования	57
4.6. Шлюз Modbus TCP в Modbus RTU	57
4.7. HTTP/HTTPS	59
4.7.1. Основные настройки	59
4.7.2. Второстепенные настройки	60
4.7.3. Дополнительные настройки	61
4.7.4. Параметры самоподписанного сертификата	62
5. Сеть	64
5.1. Интерфейсы	64
5.1.1. Интерфейсы	64
Редактирование интерфейса Eth0	64
Редактирование интерфейса Eth1	68
Создание нового интерфейса	69
Удаление интерфейсов	69
5.1.2. Устройства	69
5.1.3. Основные настройки сети	71
5.2. Маршрутизация	71
5.2.1. Статические маршруты IPv4	72
5.2.2. Правила IPv4	73
5.3. DHCP и DNS	75
5.3.1. Общие настройки	76
5.3.2. Файлы resolv и hosts	77
5.3.3. Настройки PXE/TFTP	78
5.3.4. Дополнительные настройки	79
5.3.5. Постоянные аренды	81
5.3.6. Имена устройств	82
5.3.7. Списки IP	82
5.4. Диагностика	83
5.4.1. Пинг-запрос	83
5.4.2. Трассировка	84
5.4.3. DNS-запрос	84
5.4.4. Внешний IP-адрес	85
5.4.5. ARP сканирование	85
5.5. Межсетевой экран	85
5.5.1. Общие настройки	85
5.5.2. Перенаправление портов	88

5.5.3. Правила для трафика	90
5.5.4. Правила NAT	93
5.5.5. Пользовательские правила	93
6. VPN	95
6.1. OpenVPN	95
6.1.1. Экземпляры OpenVPN	95
6.1.2. Конфигурация на основе шаблонов	96
6.1.3. Загрузка конфигурационного файла OVPN	96
7. Статистика	98
7.1. Графики	98
7.1.1. Статистика	98
7.1.2. CPU	98
7.1.3. Интерфейсы	99
7.1.4. Загрузка системы	100
7.1.5. Оперативная память (RAM)	101
7.1.6. Thermal	101
7.2. Настройки статистики	102
7.2.1. Настройки collectd	102
7.2.2. Основные плагины	103
7.2.3. Сетевые плагины	106
7.2.4. Плагины вывода	107

Сокращения и обозначения

Сокращение	Расшифровка	Описание
3G	Third Generation	Стандарт мобильной связи третьего поколения.
APN	Access Point Name	Имя точки доступа оператора мобильной связи, используемое для подключения к сети передачи данных.
ARP	Address Resolution Protocol	Протокол определения MAC-адреса по известному IPv4-адресу.
ASCII	American Standard Code for Information Interchange	Стандарт кодирования символов латинского алфавита, цифр и специальных символов.
BPDU	Bridge Protocol Data Unit	Служебный пакет протоколов STP/RSTP, используемый для обмена информацией между сетевыми коммутаторами.
CA	Certification Authority	Удостоверяющий центр, выпускающий и подписывающий цифровые сертификаты.
CDMA	Code Division Multiple Access	Технология множественного доступа, применяемая в сетях мобильной связи.
CHAP	Challenge Handshake Authentication Protocol	Протокол аутентификации пользователей с использованием механизма запрос–ответ.
CPU	Central Processing Unit	Центральный процессор устройства.
CSV	Comma-Separated Values	Текстовый формат хранения табличных данных, в котором значения разделяются запятыми или другим разделителем.
DDNS	Dynamic DNS	Служба автоматического обновления DNS-записей при изменении IP-адреса.
DHCP	Dynamic Host Configuration Protocol	Протокол автоматической выдачи сетевых параметров устройствам.
DNS	Domain Name System	Система преобразования доменных имен в IP-адреса.
EV-DO	Evolution-Data Optimized	Технология высокоскоростной передачи данных в сетях CDMA.
F2FS	Flash-Friendly File System	Файловая система, оптимизированная для флеш-памяти.
FAT	File Allocation Table	Файловая система семейства FAT.
FAT32	File Allocation Table 32	Версия файловой системы FAT с использованием 32-разрядной таблицы размещения файлов.
FIFO	First In, First Out	Принцип обработки данных или задач в порядке их поступления.

Сокращение	Расшифровка	Описание
FQDN	Fully Qualified Domain Name	Полное доменное имя узла.
FTP	File Transfer Protocol	Протокол передачи файлов по сети.
GPRS	General Packet Radio Service	Технология пакетной передачи данных в сетях GSM.
HTTP	HyperText Transfer Protocol	Протокол передачи данных Web.
HTTPS	HyperText Transfer Protocol Secure	Защищенная версия протокола HTTP с использованием TLS.
ICMP	Internet Control Message Protocol	Протокол передачи служебных сообщений IP-сети.
ID	Identifier	Уникальный идентификатор объекта.
IGMP	Internet Group Management Protocol	Протокол управления членством в группах многоадресной рассылки IPv4.
IP	Internet Protocol	Протокол сетевого уровня, обеспечивающий адресацию и маршрутизацию пакетов.
IPv4	Internet Protocol version 4	Четвертая версия протокола IP.
IPv6	Internet Protocol version 6	Шестая версия протокола IP.
LAN	Local Area Network	Локальная вычислительная сеть.
LCP	Link Control Protocol	Протокол управления соединением PPP.
MAC	Media Access Control	Уникальный аппаратный адрес сетевого интерфейса.
MMC	MultiMedia Card	Тип карты флеш-памяти.
MSS	Maximum Segment Size	Максимальный размер полезной нагрузки TCP-сегмента.
MTU	Maximum Transmission Unit	Максимальный размер сетевого пакета без фрагментации.
NAT	Network Address Translation	Механизм преобразования сетевых IP-адресов.
NDP	Neighbor Discovery Protocol	Протокол обнаружения соседних узлов и определения их параметров в сетях IPv6.
NTFS	New Technology File System	Файловая система семейства Microsoft Windows.
NTP	Network Time Protocol	Протокол синхронизации системного времени по сети.
OPC	Open Platform Communications	Семейство стандартов обмена данными между промышленным оборудованием и программным обеспечением.

Сокращение	Расшифровка	Описание
OPC UA	OPC Unified Architecture	Платформонезависимый стандарт OPC для безопасного обмена промышленными данными.
PAP	Password Authentication Protocol	Протокол аутентификации пользователя по имени и паролю.
PID	Process Identifier	Уникальный идентификатор процесса в операционной системе.
PIN	Personal Identification Number	Персональный идентификационный номер, используемый для аутентификации пользователя или устройства.
PPP	Point-to-Point Protocol	Протокол передачи данных по соединению типа «точка-точка».
RA	Router Advertisement	Сообщение протокола IPv6, используемое маршрутизатором для автоматической настройки сетевых параметров узлов.
RNDIS	Remote Network Driver Interface Specification	Протокол Microsoft для передачи сетевых данных через интерфейс USB.
RSS	Resident Set Size	Объем физической оперативной памяти, используемой процессом.
RSTP	Rapid Spanning Tree Protocol	Протокол быстрого построения отказоустойчивой древовидной топологии Ethernet.
SFTP	SSH File Transfer Protocol	Протокол безопасной передачи файлов по соединению SSH.
SIM	Subscriber Identity Module	Модуль идентификации абонента мобильной сети.
SSH	Secure Shell	Протокол защищенного удаленного доступа к устройствам.
SSL	Secure Sockets Layer	Криптографический протокол защиты сетевых соединений. В современных системах обычно заменен протоколом TLS.
STP	Spanning Tree Protocol	Протокол предотвращения петель в коммутируемых сетях Ethernet.
TCN	Topology Change Notification	Служебное сообщение STP/RSTP, уведомляющее об изменении топологии сети.
TCP	Transmission Control Protocol	Транспортный протокол с установлением соединения и гарантированной доставкой данных.
TTL	Time To Live	Поле IP-пакета, определяющее максимальное количество переходов через маршрутизаторы.

Сокращение	Расшифровка	Описание
UDP	User Datagram Protocol	Транспортный протокол без установления соединения и подтверждения доставки данных.
ULA	Unique Local Address	Локальный IPv6-адрес, не маршрутизируемый через сеть Интернет.
UMTS	Universal Mobile Telecommunications System	Стандарт мобильной связи третьего поколения.
URL	Uniform Resource Locator	Унифицированный указатель ресурса в сети.
USB	Universal Serial Bus	Стандарт интерфейса для подключения периферийных устройств.
UTC	Coordinated Universal Time	Всемирное координированное время.
UTP	Unshielded Twisted Pair	Неэкранированная витая пара.
UUID	Universally Unique Identifier	Универсальный уникальный идентификатор.
VFAT	Virtual File Allocation Table	Расширение файловой системы FAT с поддержкой длинных имен файлов.
VPN	Virtual Private Network	Технология создания защищенного виртуального сетевого соединения.
VSZ	Virtual Size	Общий объем виртуальной памяти, выделенной процессу.
WAN	Wide Area Network	Глобальная вычислительная сеть.
ПЛК	Программируемый логический контроллер	Промышленное устройство, предназначенное для автоматизации технологических процессов.

Chapter 1. Введение

В данном документе описываются основные страницы Web-интерфейса программного технического комплекса «ТИТАН КОНТРОЛ 1000». Web-интерфейс является используемой по умолчанию системой управления для операционной системы OpenWrt.

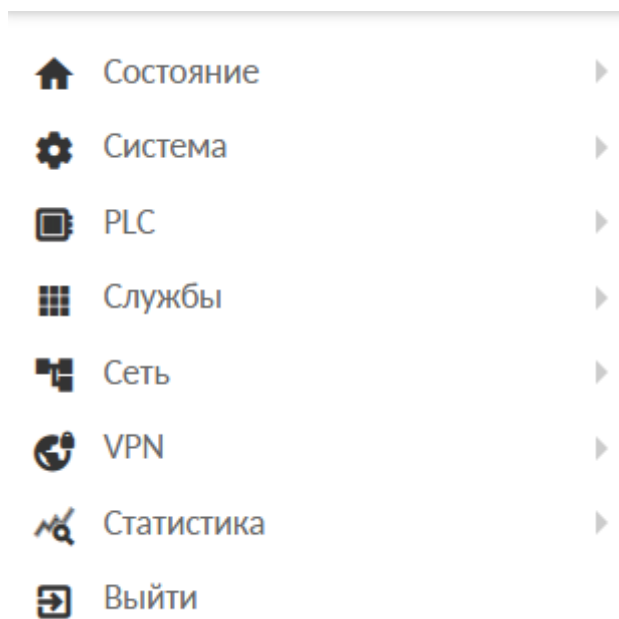


Рисунок 1 - 1. Основные страницы Web-интерфейса

В разделе [Состояние](#) описаны страницы, отображающие различную информацию о системе в целом и страницы конкретных служб или приложений.

В разделе [Система](#) описаны страницы для управления различными системными параметрами.

В разделе [ПЛК](#) описаны страницы для настройки и мониторинга функций контроллера.

В разделе [Службы](#) содержатся страницы настройки различных служб и приложений.

В разделе [Сеть](#) описаны страницы управления сетевыми параметрами системы (настройка сетевых интерфейсов, настройка статических маршрутов и т. п.) и базовыми сетевыми службами DNS и DHCP.

В разделе [VPN](#) описывается настройка VPN-подключений с использованием OpenVPN.

В разделе [Статистика](#) содержатся страницы просмотра графиков, а также страницы настройки сбора статистики.

1.1. Подключение к Web-интерфейсу

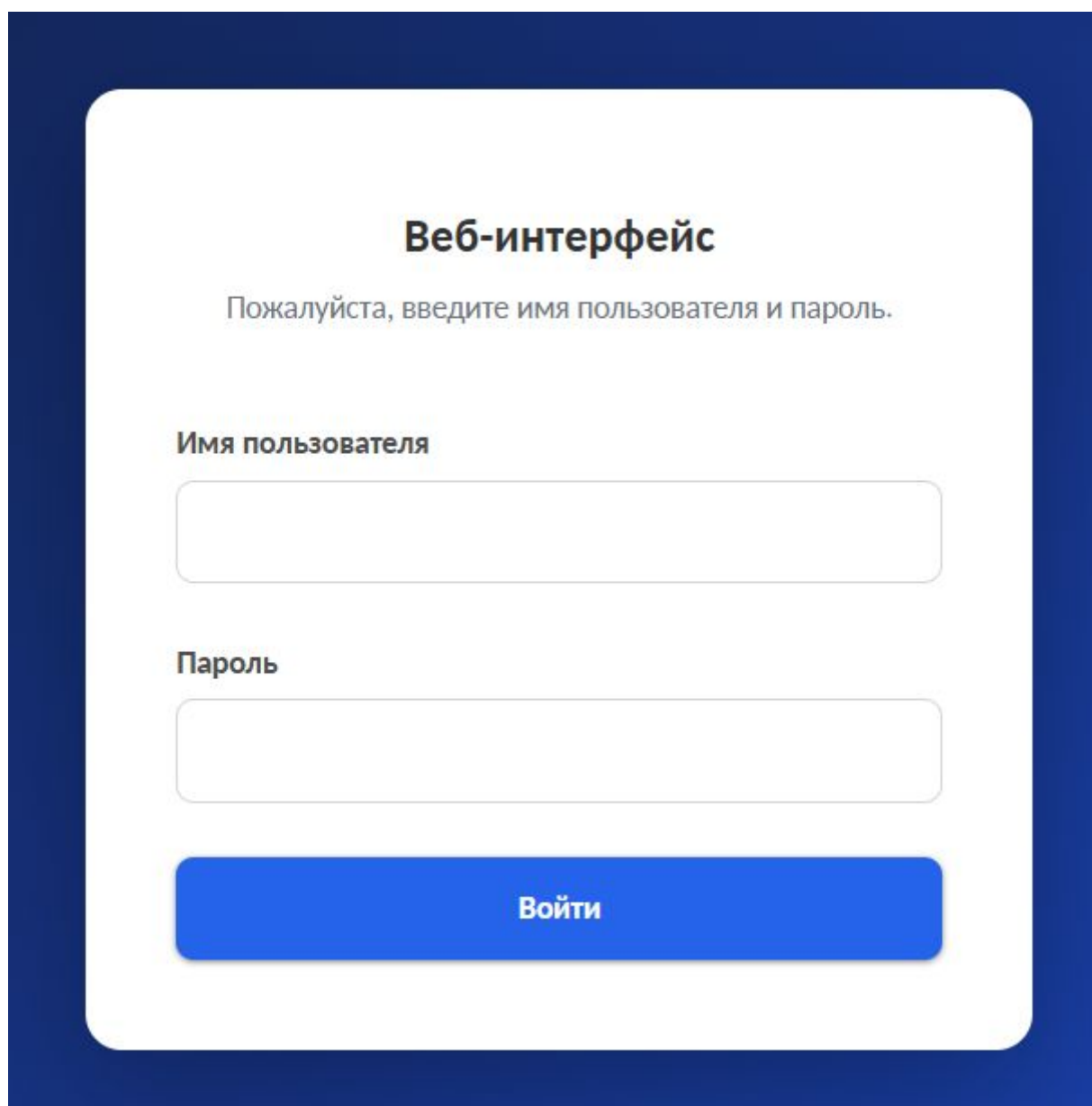
Доступ к Web-интерфейсу ПЛК «ТИТАН КОНТРОЛ» осуществляется по протоколу HTTP с использованием IP-адреса контроллера. Для подключения необходимо открыть любой современный веб-браузер и ввести в адресной строке IP-адрес сетевого интерфейса, через который установлено соединение с контроллером.

По умолчанию сетевые интерфейсы контроллера имеют следующие параметры:

ETH0 — статический IP-адрес **192.168.151.100**;

ETH1 — получение параметров сети автоматически по протоколу DHCP.

При обращении к Web-интерфейсу отображается страница аутентификации, содержащая поля для ввода имени пользователя и пароля.



Веб-интерфейс

Пожалуйста, введите имя пользователя и пароль.

Имя пользователя

Пароль

Войти

Рисунок 1 - 2. Основные страницы Web-интерфейса

Для входа в систему по умолчанию используются следующие учётные данные:

Параметр	Значение
Имя пользователя	root
Пароль	root

После успешной аутентификации пользователю предоставляется доступ к функциям Web-интерфейса в соответствии с назначенными правами доступа.



В целях обеспечения информационной безопасности рекомендуется изменить пароль пользователя «root» сразу после первого входа в систему.

Настройка пароля пользователя «root» с использованием Web-интерфейса рассмотрена в разделе 3.3.1 данного руководства.

1.2. Автоматическое обновление информации

На ряде страниц Web-интерфейса реализована функция автоматического обновления данных, позволяющая отображать актуальную информацию без ручного обновления страницы.

Если для текущей страницы доступно автоматическое обновление, в её заголовке справа отображается индикатор «Автообновление включено».

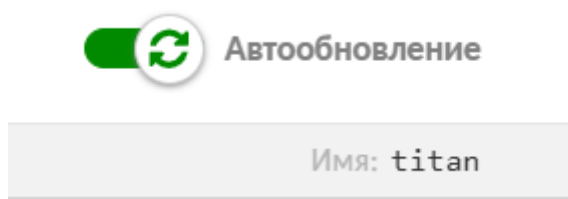


Рисунок 1 - 3. Автоматическое обновление включено

Для отключения автоматического обновления нажмите на индикатор «Автообновление включено». После отключения его состояние изменится на «Автообновление выключено». Повторное нажатие на индикатор вновь включает автоматическое обновление.

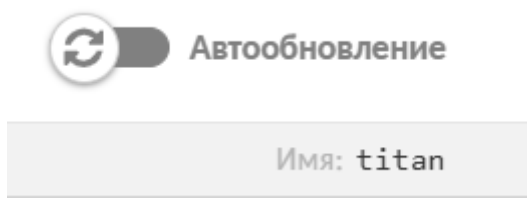


Рисунок 1 - 4. Автоматическое обновление выключено

По умолчанию интервал автоматического обновления составляет 5 секунд. При необходимости пользователь может изменить данный интервал в разделе «Система → Общие настройки → [Дополнительные](#)».

Chapter 2. Состояние

2.1. Обзор

На странице «Обзор» раздела «Состояние» отображается сводная информация о текущем состоянии устройства.

Страница разделена на пять подразделов:

- «Система» — сведения об аппаратной и программной конфигурации устройства;
- «Оперативная память (RAM)» — сведения об использовании оперативной памяти;
- «Состояние портов сетевых интерфейсов» — информация о сетевых подключениях;
- «Сеть» — сведения о текущих параметрах сетевых интерфейсов;
- «Активные DHCP-аренды» — список устройств, получивших IP-адреса от DHCP-сервера контроллера.

2.1.1. «Система»

В подразделе «Система» отображаются основные сведения о контроллере и его текущем состоянии.

Система	
Имя	Morozov
Модель	PLC TITAN SBC v1.0
Архитектура	ARMv8 Processor rev 0 (v8l)
Целевая платформа	titan-1000-sd
Версия прошивки	TanoWrt CROATOAN titan-1000-sd git-676c106a7db9 2026-07-07 16:03:33 UTC
Версия ядра	6.1.118-tano-rk-standard-gd2b4477a1d-tano0.2.2.21.1.0
Время	2026-07-13 14:29:16 +0300
Время работы	5д 19ч 19м 22с
Нагрузка (1, 5, 15м)	0.11, 0.08, 0.08

Рисунок 2 - 1. Обзор. Подраздел «Система»

2.1.2. «Оперативная память (RAM)»

В подразделе «Оперативная память (RAM)» отображается информация об использовании оперативной памяти контроллера.

Оперативная память (RAM)	
Свободно	1.78 ГиБ / 1.94 ГиБ (91%)
Занято	229.47 МиБ / 1.94 ГиБ (11%)
Буфер	8.73 МиБ / 1.94 ГиБ (0%)
Кеш	104.60 МиБ / 1.94 ГиБ (5%)

Рисунок 2 - 2. Обзор. Подраздел «Оперативная память (RAM)»

В подразделе отображаются следующие параметры:

- «Свободно» — доступный для использования объём памяти;
- «Занято» — используемый объём оперативной памяти;
- «Буфер» — объём памяти, используемый операционной системой для временного хранения данных при выполнении операций ввода-вывода;
- «Кеш» — объём памяти, используемый для хранения часто используемых данных и файлов. Кеш очищается автоматически.

2.1.3. «Состояние портов сетевых интерфейсов»

В подразделе «Состояние портов сетевых интерфейсов» отображается информация о состоянии всех сетевых портов контроллера.

Состояние портов сетевых интерфейсов

luci-app-ttn-netports 2.0.3

Имя и MAC-адрес	Состояние подключения	Интерфейс	В составе моста	Зоны межсетевого экрана	Получено (RX)	Передано (TX)
Port 1 72:2E:D4:47:12:91	 Не подключено	eth0 (LAN0)	-		-	-
Ethernet 72:2E:D4:47:12:90	 1000 Мбит/с, полный дуплекс	eth1 (LAN1)	-		1.03 Гиб (6328044 пакетов)	874.50 МиБ (4476721 пакетов)
can0	 Подключено	can0	-	-	7.84 МиБ (1257194 пакетов)	9.04 МиБ (2403018 пакетов)

Рисунок 2 - 3. Обзор. Подраздел «Состояние портов сетевых интерфейсов»

Каждая строка таблицы соответствует одному физическому сетевому порту.

Таблица содержит следующие столбцы:

- «Имя и MAC-адрес»;
- «Состояние подключения» (при наличии информации дополнительно отображаются скорость соединения и режим работы (дуплекс));
- «Интерфейс» — имя системного сетевого интерфейса. В скобках указывается имя связанного виртуального сетевого интерфейса (при наличии). При нажатии на имя виртуального интерфейса открывается [страница](#) его настройки;
- «В составе моста» — имя сетевого моста, в который включён данный интерфейс. В скобках указывается имя связанного виртуального сетевого интерфейса (при наличии). При нажатии на имя виртуального интерфейса открывается [страница](#) его настройки;
- «Зоны межсетевого экрана» — перечень зон межсетевого экрана, к которым относится данный интерфейс;
- «Получение (RX)» — объём принятых данных и количество полученных пакетов;
- «Отправка (TX)» — объём переданных данных и количество отправленных пакетов.

В столбце «Состояние подключения» отображается иконка, обозначающая тип подключения и его текущее состояние. Возможные варианты иконок приведены в ниже:

Table 1. Иконки типов и состояний подключений портов сетевых интерфейсов

Тип подключения	Отключено	Не подключено	Подключено
Проводное			
Wi-Fi			
LTE/3G/2G			
USB RNDIS			
VPN			
PPP			

2.1.4. «Сеть»

В подразделе «Сеть» собрана информация об основных сетевых интерфейсах контроллера.

Сеть

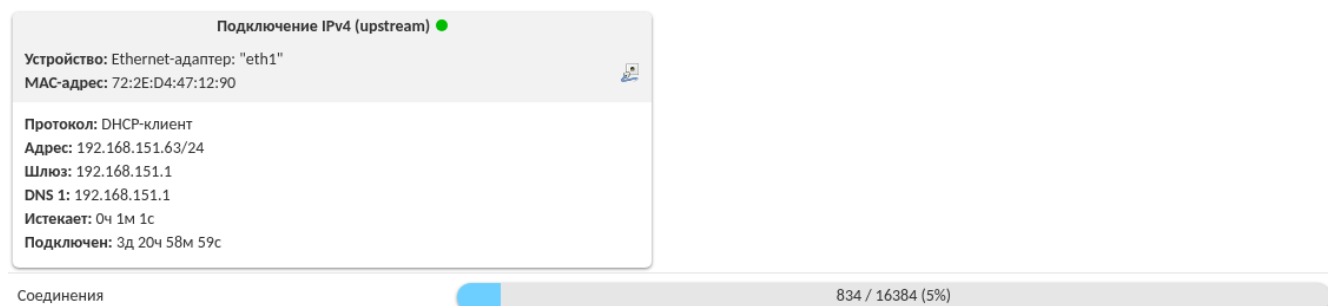


Рисунок 2 - 4. Подраздел «Сеть»

В нижней части подраздела отображается индикатор использования сетевых соединений. Индикатор показывает текущее количество активных сетевых соединений и максимально допустимое количество соединений, поддерживаемое системой.

2.1.5. «Активные DHCP-аренды»

В подразделе «Активные DHCP-аренды» отображается список IP-адресов, выданных DHCP-сервером контроллера подключённым устройствам. Каждая строка таблицы соответствует одной активной DHCP-аренде.

DHCP аренды

Имя	IPv4-адрес	MAC-адрес	До конца аренды	Бессрочная аренда
Нет активных арендованных адресов				

Рисунок 2 - 5. Подраздел «Активные DHCP-аренды»

2.2. Маршрутизация

На странице «Маршрутизация» раздела «Состояние» отображаются текущие IPv4 и IPv6 таблицы маршрутизации. Также на странице приведена текущая ARP-таблица (таблица соответствия MAC-адресов IP-адресам).

ТИТАН
контроль **ICCC**

Состояние » Маршрутизация

Имя: Morozov

Состояние

Обзор

Маршрутизация

Межсетевой экран

Процессы

Мониторинг

Журналы

Система

PLC

Службы

Сеть

VPN

Статистика

Выйти

Маршрутизация

На данном устройстве активны следующие правила.

IPv4 маршрутизация

IPv6 маршрутизация

IPv4 соседи (ARP)

IP-адрес	MAC-адрес	Интерфейс
192.168.151.1	B8:69:F4:7F:AE:D9	lan1

Активные IPv4-маршруты

Сеть	Назначение	Шлюз	Метрика	Таблица	Протокол
lan1	0.0.0.0/0	192.168.151.1	0	main	static
lan0	192.168.150.0/24	-	0	main	kernel
lan1	192.168.151.0/24	-	0	main	kernel

Активные IPv4-правила

Приоритет	Правило
0	from all lookup local
32766	from all lookup main
32767	from all lookup default

Рисунок 2 - 6. Общий вид страницы «Маршруты»



Настройка статических маршрутов IPv4 и IPv6 выполняется на странице [Маршрутизация](#) раздела «Сеть»

2.3. Межсетевой экран

На странице «Межсетевой экран» раздела «Состояние» отображаются активные правила межсетевого экрана для всех таблиц (Filter, NAT, Mangle) и их цепочек.

Состояние межсетевого экрана

[Скрыть пустые цепочки](#)[«Сырые» \(raw\) счётчики](#)[Сбросить счётчики](#)[Перезапустить межсетевой экран](#)

Таблица: Filter

Цепочка **INPUT** (Политика: **DROP**, 0 Пакеты, 0 В Трафик)

пакетов	Трафик	Назначение	Прот.	В	Вне	Отправитель	Получатель	Опции	Комментарий
851	61.81 KB	ACCEPT	0	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
43.41 K	3.78 MB	input_rule	0	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
38.03 K	3.02 MB	ACCEPT	0	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
1.45 K	83.68 KB	syn_flood	6	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
5.38 K	764.73 KB	zone_lan_input	0	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	reject	0	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Цепочка **FORWARD** (Политика: **DROP**, 0 Пакеты, 0 В Трафик)

пакетов	Трафик	Назначение	Прот.	В	Вне	Отправитель	Получатель	Опции	Комментарий
0	0 B	forwarding_rule	0	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	0	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-

Рисунок 2 - 7. Фрагмент страницы «Межсетевой экран»

Настройка межсетевого экрана, включая создание, изменение и удаление правил, выполняется на странице [Межсетевой экран](#) раздела «Сеть»



Для более глубокого понимания принципов работы межсетевого экрана и структуры отображаемых правил рекомендуется ознакомиться с документацией к подсистеме Netfilter и утилите iptables.

2.4. Процессы

Страница «Процессы» раздела «Состояние» отображает список работающих в системе процессов и их основные параметры.

Процессы

Страница содержит работающие процессы и их состояние.

PID	Владелец	Команда	Использование ЦП (%)	Использование памяти (%)			
1	root	/sbin/procd	0%	0%	Перезапустить	Завершить	Убить
2	root	[kthreadd]	0%	0%	Перезапустить	Завершить	Убить
12	root	[ksoftirqd/0]	0%	0%	Перезапустить	Завершить	Убить
14	root	[migration/0]	0%	0%	Перезапустить	Завершить	Убить
15	root	[cpuhp/0]	0%	0%	Перезапустить	Завершить	Убить
16	root	[cpuhp/1]	0%	0%	Перезапустить	Завершить	Убить
17	root	[migration/1]	0%	0%	Перезапустить	Завершить	Убить
18	root	[ksoftirqd/1]	0%	0%	Перезапустить	Завершить	Убить
21	root	[cpuhp/2]	0%	0%	Перезапустить	Завершить	Убить

Рисунок 2 - 8. Фрагмент страницы «Процессы»

Каждая строка таблицы соответствует одному физическому сетевому порту. В правой части каждой строки расположены кнопки управления процессом.

Таблица имеет следующие столбцы:

- «PID» — идентификатор процесса;
- «Владелец» — пользователь, от имени которого запущен процесс;
- «Команда» — имя исполняемого файла или команда, запустившая процесс;
- «Использование ЦП (%)»;
- «Использование памяти (%)».

2.5. Графики в реальном времени

На странице «Мониторинг» раздела «Состояние» отображаются графики изменения системных величин.

Страница разделена на три подраздела:

- «Нагрузка»;
- «Трафик»;
- «Соединения».

2.5.1. «Нагрузка»

В подразделе «Нагрузка» отображается график средней загрузки системы за 1, 5 и 15 минут. График построен с временным окном 2 минуты и интервалом обновления 3 секунды.

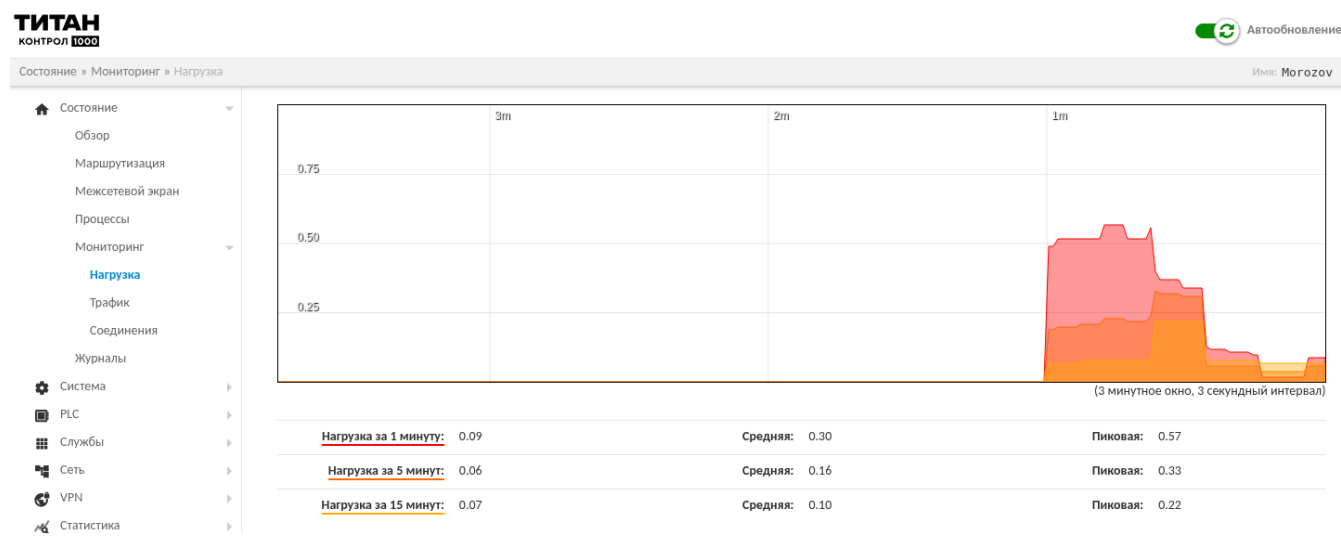


Рисунок 2 - 9. Мониторинг. График загрузки CPU

2.5.2. «Трафик»

В подразделе «Трафик» отображается график входящего и исходящего трафика для выбранного сетевого интерфейса (can0, eth0, eth1 и др.). График построен с временным окном 2 минуты и интервалом обновления 3 секунды.

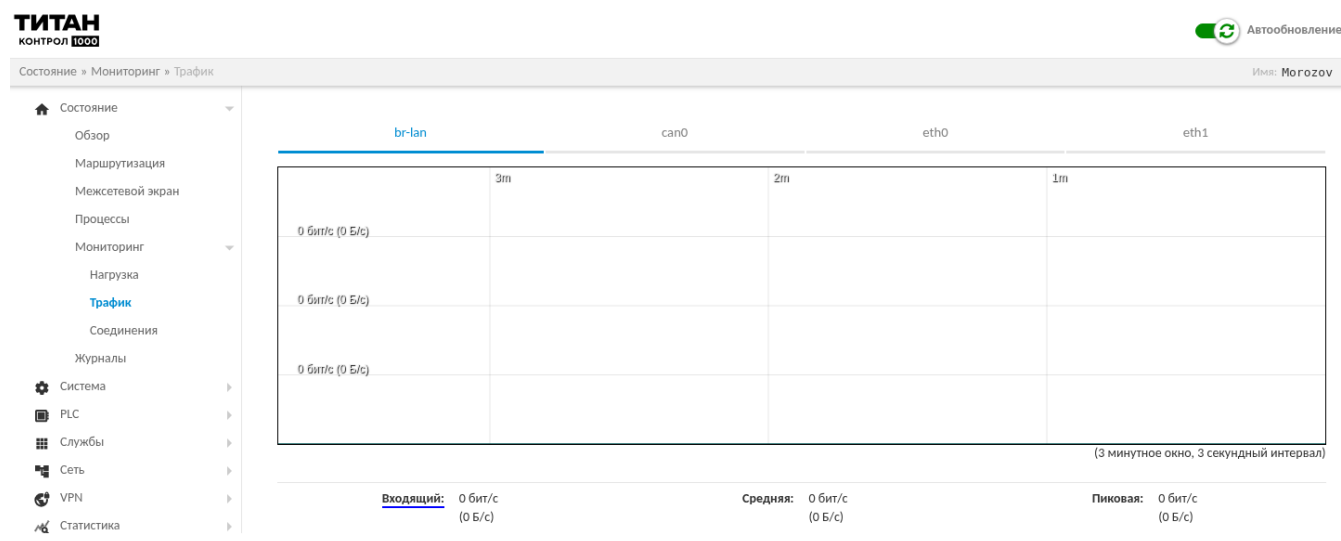


Рисунок 2 - 10. Мониторинг. График трафика

2.5.3. «Соединения»

В подразделе «Соединения» отображается график количества активных сетевых соединений с разбивкой по протоколам (UDP, TCP, Другие). График построен с временным окном 2 минуты и интервалом обновления 3 секунды.

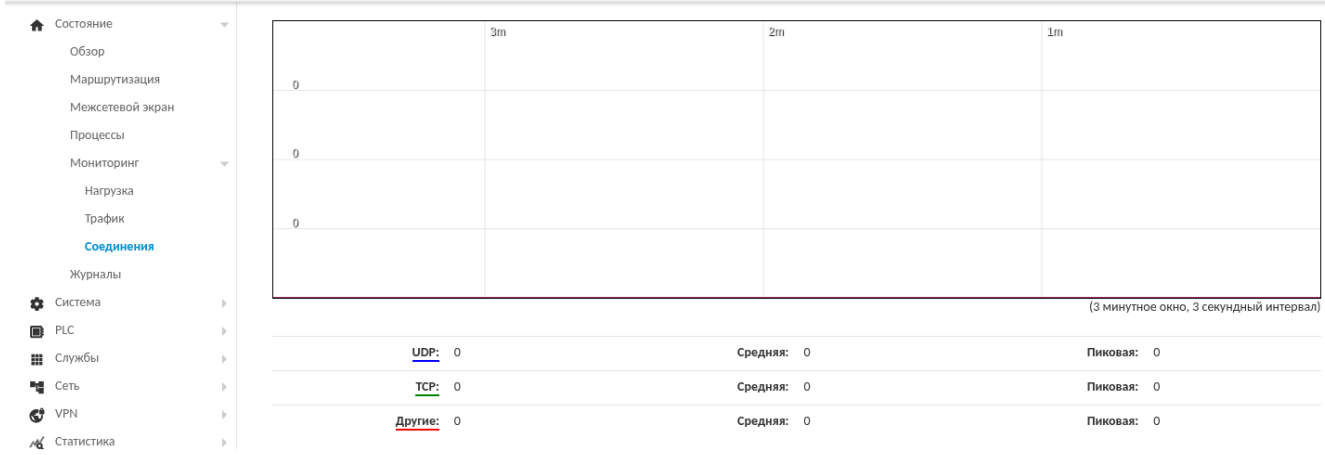


Рисунок 2 - 11. Мониторинг. График активных соединений

2.6. Журналы

Страница «Журналы» раздела «Состояние» предназначена для просмотра системных журналов различных служб

Страница разделена на четыре подраздела:

- «Журнал ядра»;
- «Системный журнал»;
- «Запланированные задачи»;
- «SNMP».

В верхней части страницы каждого журнала расположены элементы управления:

- переключатель «Отображать по убыванию времени (последнее сверху)» — задает порядок сортировки записей журнала;
- кнопка «Обновить» — повторно считывает записи из журнала и актуализирует их;
- кнопка «Скачать» — инициирует загрузку журнала в формате RAW (.txt), CSV, JSON;
- кнопки-переключатели «Отображать приоритеты» — включают или отключают отображение записей с выбранными уровнями приоритета;
- кнопки-переключатели «Отображать столбцы» — включают или отключают отображение столбцов таблицы журнала;
- поле «Фильтр записей» — предназначено для фильтрации отображаемых записей по заданному критерию;
- кнопка «Очистить» — очищает содержимое поля «Фильтр».

☒ Отображать по убыванию времени (последнее сверху)

ОбновитьСкачать (JSON)▼

Отображать приоритеты:

Info (411)Notice (19)Error (7)Debug (174)Warning (17)

Отображать столбцы:

№ВремяПриоритетСообщение

Фильтр записей: Очистить

Рисунок 2 - 12. Элементы управления журналом

2.6.1. Журнал ядра

На странице «Журнал ядра» раздела «Состояние» отображается вывод журнала ядра, в который записываются сообщения работы ядра Linux, начиная с момента загрузки. В журнале ядра не регистрируются какие-либо события от приложений и служб уровня пользователя.

Просмотр журналов

Журнал ядраСистемный журналЗапланированные задания (cron)SNMP

☒ Отображать по убыванию времени (последнее сверху)

ОбновитьСкачать (RAW)▼

Отображать приоритеты:

Info (428)Notice (25)Error (7)Debug (182)Warning (17)

Отображать столбцы:

№ВремяПриоритетСообщение

Фильтр записей: Очистить

Записи журнала (659)

№	Время	Приоритет	Сообщение
659	166824.157705	Info	rk_gmac-dwmac fe2a0000.ethernet eth1: Link is Up - 1Gbps/Full - flow control rx
658	165722.639393	Info	rk_gmac-dwmac fe2a0000.ethernet eth1: Link is Down
657	7663.229902	Info	rockchip-vop2 fe040000.vop: [drm:vop2_crtc_atomic_disable] Crtc atomic disable vp0
656	31.924345	Info	rk_gmac-dwmac fe2a0000.ethernet eth1: Link is Up - 1Gbps/Full - flow control rx
655	30.498937	Warning	process '/usr/bin/codesyscontrol' started with executable stack
654	30.333532	Info	UDC core: g_ether: couldn't find an available UDC
653	27.828798	Info	rk_gmac-dwmac fe2a0000.ethernet eth1: configuring for phy/rgmii-id link mode
652	27.825278	Info	rk_gmac-dwmac fe2a0000.ethernet eth1: registered PTP clock
651	27.823924	Info	rk_gmac-dwmac fe2a0000.ethernet eth1: IEEE 1588-2008 Advanced Timestamp supported
650	27.823203	Info	rk_gmac-dwmac fe2a0000.ethernet eth1: No Safety Features support found
649	27.822670	Info	dwmac4: Master AXI performs any burst length
648	27.821148	Info	rk_gmac-dwmac fe2a0000.ethernet eth1: PHY [stmmac-0:00] driver [RTL8211F Gigabit Ethernet] (irq=POLL)
647	27.730768	Info	rk_gmac-dwmac fe2a0000.ethernet eth1: Register MEM_TYPE_PAGE_POOL RxQ-0
646	27.696517	Info	rk_gmac-dwmac fe010000.ethernet eth0: configuring for phy/rgmii-id link mode
645	27.694982	Info	rk_gmac-dwmac fe010000.ethernet eth0: registered PTP clock
644	27.693750	Info	rk_gmac-dwmac fe010000.ethernet eth0: IEEE 1588-2008 Advanced Timestamp supported
643	27.693055	Info	rk_gmac-dwmac fe010000.ethernet eth0: No Safety Features support found
642	27.692560	Info	dwmac4: Master AXI performs any burst length
641	27.691088	Info	rk_gmac-dwmac fe010000.ethernet eth0: PHY [stmmac-1:00] driver [RTL8211F Gigabit Ethernet] (irq=POLL)

Рисунок 2 - 13. Журнал ядра

2.6.2. Системный журнал

На странице «Системный журнал» раздела «Состояние» отображается вывод системного журнала, в который записываются все события ядра Linux, приложений и служб, запущенных в системе.



Журнал ядра Системный журнал Запланированные задания (cron) SNMP

☒ Отображать по убыванию времени (последнее сверху) Обновить Скачать (RAW) ▼

Отображать приоритеты:
Info (793) Notice (24)

Отображать столбцы:
№ Временная метка Тег Приоритет Категория Сообщение

Фильтр записей: Очистить

Записи журнала (817)

№	Временная метка	Тег	Приоритет	Категория	Сообщение
817	13.07.2026 14:29:26	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
816	13.07.2026 14:29:15	uhttpd	Info	user	luci: accepted login on / for root from 192.168.200.25
815	13.07.2026 14:29:11	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
814	13.07.2026 14:28:56	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
813	13.07.2026 14:28:41	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
812	13.07.2026 14:28:26	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
811	13.07.2026 14:28:11	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
810	13.07.2026 14:27:56	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
809	13.07.2026 14:27:41	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
808	13.07.2026 14:27:26	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
807	13.07.2026 14:27:16	uhttpd	Info	user	luci: accepted login on / for root from 192.168.200.25
806	13.07.2026 14:27:11	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
805	13.07.2026 14:26:56	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
804	13.07.2026 14:26:41	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
803	13.07.2026 14:26:26	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
802	13.07.2026 14:26:23	sysfixtime	Info	daemon	saved localtime (Mon Jul 13 14:26:23 MSK 2026) to /dev/rtc0
801	13.07.2026 14:26:22	sysfixtime	Info	daemon	applied time zone 'Europe/Moscow'
800	13.07.2026 14:26:11	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory
799	13.07.2026 14:25:56	lldpd[3453]	Info	daemon	cannot connect to /var/run/agentx.sock: No such file or directory

Рисунок 2 - 14. Системный журнал

2.6.3. Запланированные задания (cron)

В подразделе «Запланированные задания (cron)» отображается журнал службы cron, которая выполняет периодически запускаемые задачи.



Журнал ядра Системный журнал **Запланированные задания (cron)** SNMP

☒ Отображать по убыванию времени (последнее сверху) Обновить Скачать (RAW) ▼

Отображать приоритеты:
Info (295)

Отображать столбцы:
№ Временная метка Тег Приоритет Категория Сообщение

Фильтр записей: Очистить

Записи журнала (295)

№	Временная метка	Тег	Приоритет	Категория	Сообщение
295	13.07.2026 14:01:00	CROND[19340]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.hourly)
294	13.07.2026 14:01:00	CROND[19341]	Info	cron	(root) CMD (cd / && run-parts /etc/cron.hourly)
293	13.07.2026 13:01:00	CROND[13800]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.hourly)
292	13.07.2026 13:01:00	CROND[13801]	Info	cron	(root) CMD (cd / && run-parts /etc/cron.hourly)
291	13.07.2026 12:01:00	CROND[5567]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.hourly)
290	13.07.2026 12:01:00	CROND[5568]	Info	cron	(root) CMD (cd / && run-parts /etc/cron.hourly)
289	13.07.2026 11:01:01	CROND[2078]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.hourly)
288	13.07.2026 11:01:00	CROND[2079]	Info	cron	(root) CMD (cd / && run-parts /etc/cron.hourly)
287	13.07.2026 10:01:00	CROND[747]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.hourly)
286	13.07.2026 10:01:00	CROND[748]	Info	cron	(root) CMD (cd / && run-parts /etc/cron.hourly)
285	13.07.2026 09:01:00	CROND[550]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.hourly)
284	13.07.2026 09:01:00	CROND[551]	Info	cron	(root) CMD (cd / && run-parts /etc/cron.hourly)
283	13.07.2026 08:01:00	CROND[326]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.hourly)
282	13.07.2026 08:01:00	CROND[327]	Info	cron	(root) CMD (cd / && run-parts /etc/cron.hourly)
281	13.07.2026 07:30:00	CROND[32707]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.daily)
280	13.07.2026 07:30:00	CROND[32708]	Info	cron	(root) CMD (cd / && run-parts /etc/cron.daily)
279	13.07.2026 07:01:00	CROND[32592]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.hourly)
278	13.07.2026 07:01:00	CROND[32593]	Info	cron	(root) CMD (cd / && run-parts /etc/cron.hourly)
277	13.07.2026 06:01:00	CROND[32403]	Info	cron	(root) CMDEND (cd / && run-parts /etc/cron.hourly)

Рисунок 2 - 15. Журнал запланированных заданий (cron)

2.6.4. SNMP

В подразделе «SNMP» отображается журнал работы службы SNMP (Simple Network Management Protocol), предназначенной для управления сетевыми устройствами.



Журнал ядра Системный журнал Запланированные задания (cron) **SNMP**

☒ Отображать по убыванию времени (последнее сверху) Обновить Скачать (RAW) ▼

Отображать столбцы:
№ Сообщение

Фильтр записей: Очистить

Записи журнала (5)

№	Сообщение
5	Server Exiting with code 1
4	Error opening specified endpoint "UDP6:161"
3	Turning on AgentX master support.
2	pcilib: pci_init failed
1	pcilib: Cannot find any working access method.

Рисунок 2 - 16. Журнал службы SNMP

Chapter 3. Система

3.1. Общие настройки

На странице «Общие настройки» раздела «Система» расположены основные параметры настройки контроллера.

Страница разделена на несколько вкладок:

- «Устройство»;
- «Журналирование»;
- «Язык»;
- «Дополнительные».

Общими элементами каждой вкладки являются кнопки «Применить», «Сохранить» и «Очистить».

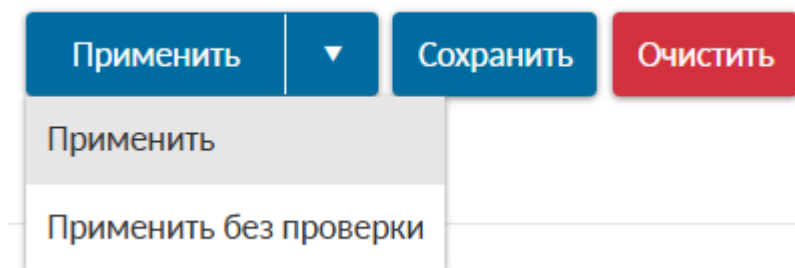


Рисунок 3 - 1. Кнопки

Кнопка «Сохранить» записывает изменения в память, но не применяет их сразу. Записанные настройки отображаются в правом верхнем углу интерфейса.

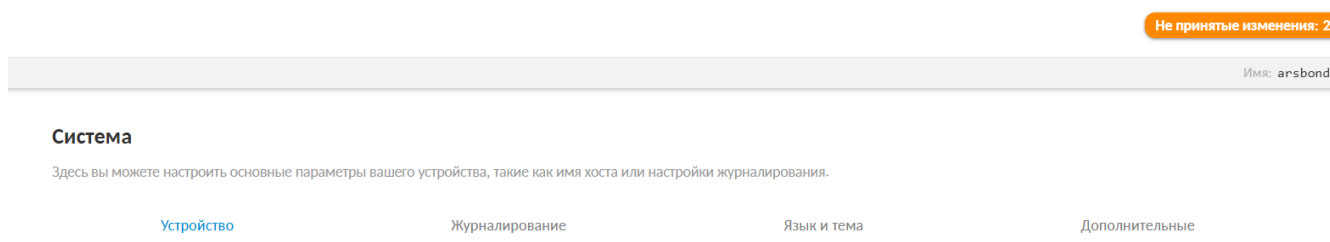


Рисунок 3 - 2. Сохраненные, но не принятые настройки

Кнопка «Применить» соответственно применяет внесенные настройки, при этом проверяется корректность изменений.

Кнопка «Применить без проверки» применяет внесенные настройки без их проверки.

3.1.1. «Устройство»

Вкладка «Устройство» позволяет задать имя и описание контроллера.

Устройство	Журналирование	Язык и тема	Дополнительные
Имя	Morozov		
Описание			
	Необязательное, краткое описание для этого устройства		
Примечания			
	Необязательные, произвольные заметки об этом устройстве		

Рисунок 3 - 3. Общие настройки. Вкладка «Устройство»

3.1.2. «Журналирование»

На вкладке «Журналирование» выполняется настройка системной службы журналирования.

Устройство	Журналирование	Язык и тема	Дополнительные
Размер системного журнала	64		
	КиБ		
Внешний сервер системного журнала	0.0.0.0		
	Оставьте пустым для отключения		
Порт внешнего сервера системного журнала	514		
Протокол внешнего сервера системного журнала	UDP		
Записывать системные события в файл	/var/log/messages		
Уровень журналирования консоли	Отладка		
	На консоли будут отображаться только сообщения ядра с уровнем равным или ниже выбранного. Самый низкий уровень — «Чрезвычайная ситуация», самый высокий — «Отладка».		

Рисунок 3 - 4. Общие настройки. Вкладка «Журналирование»

Доступны следующие параметры:

- «Размер системного журнала» — при превышении указанного значения наиболее старые записи автоматически удаляются.
- «Внешний сервер системного журнала» — IP-адрес сервера Syslog, куда передаются записи системного журнала.
- «Порт внешнего сервера системного журнала» — номер порта внешнего сервера Syslog.
- «Протокол внешнего сервера системного журнала» — протокол обмена с сервером Syslog (UDP или TCP).
- «Записывать системные события в файл» — путь к локальному файлу, куда будет сохраняться журнал.
- «Уровень журналирования консоли».

3.1.3. Вкладка «Язык и тема»

На вкладке «Язык и тема» задаются язык интерфейса и тема оформления.

В выпадающем списке «Язык» содержится элемент «автоматически», который устанавливает язык интерфейса в зависимости от языка, используемого в браузере клиента.

Устройство	Журналирование	Язык и тема	Дополнительные
Язык	Русский (Russian) ▼		
Тема оформления	Titan ▼		

Рисунок 3 - 5. Общие настройки. Вкладка «Язык и тема»

3.1.4. Вкладка «Дополнительные»

На вкладке «Дополнительные» настраивается интервал автообновления страниц.

Настройка «Интервал автообновления» определяет, как часто будет обновляться информации на страницах, поддерживающих данную возможность. Более подробная информация о функции автоматического обновления содержится в разделе [«Автоматическое обновление информации»](#).

Устройство	Журналирование	Язык и тема	Дополнительные
Интервал автообновления	5 ▼ Интервал автообновления данных страниц в секундах		

Рисунок 3 - 6. Общие настройки. Вкладка «Дополнительные»

3.2. Время

На странице «Время» раздела «Система» размещены настройки локального времени устройства, а также настройки синхронизации времени при помощи службы NTP.

ТИТАН
контроль 1000

Автообновление

Система » Время

Имя: Morozov

Состояние

Система

Общие настройки

Время

Администрирование

Сторожевой таймер

Автозапуск

Планировщик

Точки монтирования

Индикаторы

Резервное копирование

Обновление прошивки

Терминал

Перезагрузка

PLC

Службы

Сеть

VPN

Статистика

Выйти

Время
Здесь вы можете настроить основные параметры времени.

Системное время

Время

2026-07-13 14:29:34 +0300

Синхронизировать с браузером

Синхронизировать по NTP

Часовой пояс

Europe/Moscow ▼

Синхронизация времени

Включить NTP-клиент

☒

Включить NTP-сервер

☐

Использовать серверы, объявленные через DHCP

☒

Список NTP-серверов

1.ru.pool.ntp.org

0.europe.pool.ntp.org

2.europe.pool.ntp.org

Применить

Сохранить

Очистить

Рисунок 3 - 7. Страница «Время»

3.2.1. «Системное время»

В подразделе «Системное время» отображается текущее локальное время и дата. Кнопка «Синхронизировать с браузером» выполняет установку локальной даты и времени на устройстве в соответствии с текущей датой и временем, установленными на компьютере клиента (то есть в браузере). При следующем обновлении значения поля «Время» обновится на актуальное.

Кнопка «Синхронизировать по NTP» выполняет синхронизацию времени устройства с NTP-серверами.

В выпадающем списке «Часовой пояс» выполняется выбор часового пояса локального времени устройства.

3.2.2. «Синхронизация времени»

Опция «Включить NTP-клиент» активирует синхронизацию времени. Для синхронизации используются только NTP-сервера, перечисленные в поле «Список NTP-серверов».

В поле «Список NTP-серверов» указываются адреса NTP-серверов, используемых для синхронизации локального времени при активной опции «Включить NTP-клиент».

Опция «Включить NTP-сервер» разрешает устройству быть NTP-сервером в сети.

Опция «Использовать серверы, объявленные через DHCP» разрешает использование дополнительных NTP-серверов, полученных от DHCP-сервера.



NTP-клиент контроллера использует протокол NTP версии 4 (NTPv4). Для корректной синхронизации используемый NTP-сервер должен поддерживать данную версию протокола.

3.3. Управление доступом

Страница «Администрирование» раздела «Система» содержит настройки локального и удалённого доступа к устройству.

Страница разделена на четыре подраздела:

- [Пароль устройства](#);
- [Доступ по SSH](#);
- [SSH-ключи](#);
- [Доступ HTTP\(S\)](#).

3.3.1. Пароль устройства

В подразделе «Пароль устройства» можно изменить пароль по умолчанию «root». Данный пароль используется для доступа как к консоли, так и к Web-интерфейсу контроллера.

Пароль устройства

Изменить пароль администратора для доступа к устройству

Пароль		✖
Подтверждение пароля		✖

Сохранить

Рисунок 3 - 8. Администрирование. Пароль устройства

3.3.2. Настройка доступа по SSH

В подразделе «Доступ по SSH» размещены настройки сервера Dropbear, который предоставляет доступ к устройствам по протоколам SSH и SFTP.

Доступ по SSH

Dropbear — это [SSH](#)-сервер со встроенным [SCP](#).

Экземпляр Dropbear

Удалить

Интерфейс

не определено

Принимать подключения только на указанном интерфейсе или, если интерфейс не задан, на всех интерфейсах

Порт

22

С помощью пароля



Разрешить [SSH](#) аутентификацию с помощью пароля

Root входит по паролю



Разрешить пользователю root входить в систему с помощью пароля

Порты шлюза



Разрешить удалённое подключение к локальным перенаправленным портам SSH

Добавить экземпляр

Применить



Сохранить

Очистить

Рисунок 3 - 9. Администрирование. Доступ по SSH

Кнопки «Добавить экземпляр» и «Удалить» позволяют соответственно добавить или удалить экземпляры сервера Dropbear. По умолчанию в системе запущен только один экземпляр сервера Dropbear, работающий на TCP-порту 22 на всех сетевых интерфейсах.



По умолчанию входящие подключения из зоны WAN запрещены правилами межсетевого экрана. Поэтому, несмотря на то, что сервер Dropbear настроен на прием подключений на всех сетевых интерфейсах, подключение по SSH через интерфейсы зоны WAN невозможно.

Настройки экземпляра Dropbear:

- Интерфейс — по умолчанию доступны все.
- Порт — по умолчанию 22; при смене проверьте занятость порта.
- С помощью пароля — если отключить, то для входа в систему пользователю потребуется [SSH-ключ](#).
- Root входит по паролю — если отключить, то для входа в систему с доступом ROOT потребуется [SSH-ключ](#).
- Порты шлюза — разрешает или запрещает подключение удалённых клиентов к локальным перенаправленным портам.

3.3.3. SSH-ключи

В подразделе «SSH-ключи» реализована возможность добавления публичных OpenSSH ключей (.pub). Эти SSH ключи используются для выполнения авторизации.

SSH ключи

Публичные SSH ключи позволяют выполнять беспарольный SSH вход с большим уровнем безопасности по сравнению с использованием входа по паролю. Чтобы загрузить новый публичный SSH ключ, вставьте строку публичного OpenSSH ключа или перетащите .pub файл в поле ввода ключа.

Нет публичных ключей.

Перетащите файл SSH ключа или вставьте содержимое...

Добавить ключ

Рисунок 3 - 10. Администрирование. SSH-ключи

После успешного добавления ключ отображается в списке на странице.

Для удаления ранее добавленного ключа нажмите кнопку с изображением красного крестика, расположенную справа от соответствующей записи.

3.3.4. Доступ HTTP(S)

В подразделе «Доступ HTTP(S)» размещены настройки доступа к Web-интерфейсу устройства по протоколам HTTP и HTTPS.

Доступ HTTP(S)

uHTTPd предоставляет доступ по [HTTP](#) или [HTTPS](#).

Настройки

Перенаправлять на HTTPS ☐

Перенаправлять запросы с HTTP на HTTPS

Применить



Сохранить

Очистить

Рисунок 3 - 11. Администрирование. Доступ HTTP(S)

Включите «Перенаправлять на HTTPS» для шифрования трафика управления.

3.4. Сторожевой таймер

На странице «Сторожевой таймер» раздела «Система» выполняется настройка службы сторожевого таймера (watchdog).

Сторожевой таймер автоматически перезагружает устройство при зависании. Служба фоново сбрасывает аппаратный таймер с заданным периодом. Если сброс не происходит в течение таймаута, то система перезагружается.



Таймаут должен быть больше периода, рекомендуется в 3–6 раз, иначе устройство будет циклично перезагружаться.

ТИТАН
контроль 1000

Система » Сторожевой таймер Имя: M09020V

Состояние

Система

Общие настройки

Время

Администрирование

Сторожевой таймер

Автозапуск

Планировщик

Точки монтирования

Индикаторы

Резервное копирование

Обновление прошивки

Терминал

Перезагрузка

PLC

Службы

Сеть

VPN

Статистика

Выйти

Настройки сторожевого таймера

На этой странице можно выполнить настройку параметров сторожевого таймера (watchdog).

Устройство

/dev/watchdog

Удалить

Таймаут

31

Значение таймаута в секундах. Если сторожевой таймер не сбрасывается в течении указанного времени, система будет перезагружена.

Период

5

Интервал сброса сторожевого таймера в секундах.

Политика планировщика задач

SCHED_RR

Данный параметр определяет значение приоритета для политик SCHED_FIFO и SCHED_RR. Значение приоритета является числом в диапазоне от 1 (низкий приоритет) до 99 (высокий приоритет).

Приоритет задачи

60

Данный параметр определяет значение «nice» для политики SCHED_OTHER. Значение «nice» является числом в диапазоне от -20 (высокий приоритет) до +19 (низкий приоритет).

Значение «nice»

0

Данный параметр определяет значение «nice» для политики SCHED_OTHER. Значение «nice» является числом в диапазоне от -20 (высокий приоритет) до +19 (низкий приоритет).

Добавить

Применить

Сохранить

Очистить

Рисунок 3 - 12. Внешний вид страницы «Сторожевой таймер»

Политика и приоритеты определяют, в какой очерёдности и с какой срочностью служба watchdog будет выполняться в системе.



Подробная информация о политиках планирования задач Linux, а также параметрах приоритета и nice приведена в разделе **Scheduling policies** документа **sched — overview of CPU scheduling**.

3.5. Автозапуск

На странице «Автозапуск» раздела «Система» производится управление скриптами инициализации (службами и пакетами), которые запускаются автоматически при включении устройства. Также здесь можно добавить пользовательские команды для выполнения при загрузке.

Страница разделена на две вкладки:

- «Скрипты инициализации»;
- «Запуск пакетов и служб пользователя при включении устройства».

3.5.1. Скрипты инициализации

Во вкладке «Скрипты инициализации» отображается таблица всех установленных скриптов инициализации с их параметрами.

Скрипты инициализации

Запуск пакетов и служб пользователя, при включении устройства

Здесь вы можете включить или выключить установленные скрипты инициализации. Изменения вступят в силу после перезагрузки устройства.
Внимание: если вы выключите один из основных скриптов инициализации (например "network"), ваше устройство может оказаться недоступным!

Приоритет	Скрипт инициализации	Автозагрузка	Действия		
00	watchdog	☒ Включена	Запустить	Перезапустить	Остановить
00	sysfixtime	☒ Включена	Запустить	Перезапустить	Остановить
00	rngd	☒ Включена	Запустить	Перезапустить	Остановить
10	system	☒ Включена	Запустить	Перезапустить	Остановить
10	boot	☒ Включена	Запустить	Перезапустить	Остановить
11	cgroups	☐ Выключена	Запустить	Перезапустить	Остановить

Рисунок 3 - 13. Автозапуск. Вкладка «скрипты инициализации»

В таблице перечислены службы, их приоритет запуска (чем меньше число, тем раньше запуск) и статус автозагрузки.

Кнопки в столбце «Действия» позволяют запускать, перезапускать и останавливать службы вручную.

3.5.2. Запуск пакетов и служб пользователя при включении устройства

Во вкладке «Запуск пакетов и служб пользователя при включении устройства» отображается содержимое конфигурационного файла «/etc/rc.local».

Содержимое конфигурационного файла «/etc/rc.local». Вы можете добавить свои команды (перед `exit 0`), чтобы выполнить их во время загрузки устройства.

```
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.
exit 0
```

[Сохранить](#)

Рисунок 3 - 14. Автозапуск. Вкладка «Запуск пакетов и служб пользователя при включении устройства»

3.6. Планировщик

На странице «Планировщик» раздела «Система» производится настройка запланированных задач с использованием службы `cron`.

Планировщик

Это конфигурационный файл службы `crontab`, в котором могут быть определены запланированные задачи.

Рисунок 3 - 15. Страница «Планировщик»

3.7. Точки монтирования

На странице «Точки монтирования» раздела «Система» осуществляется управление монтированием разделов.

Монтирование разделов осуществляется утилитой `block` на основе конфигурационного файла `/etc/config/fstab`. Все настройки, представленные на странице «Точки монтирования» хранятся в конфигурационном файле `/etc/config/fstab`.

Страница разделена на четыре подраздела:

- [Основные настройки](#);
- [Смонтированные разделы](#);
- [Точки монтирования](#);
- [Разделы подкачки \(swap\)](#).

3.7.1. Основные настройки

В подразделе «Основные настройки» собраны глобальные опции монтирования.

Основные настройки

Создать конфигурационный файл	Создать конфигурационный файл Найти все разделы (включая разделы подкачки) и записать в конфигурационный файл информацию об обнаруженных разделах, т.е. выполнить команду «<code>block detect > /etc/config/fstab</code>»
Монтировать подключенные устройства	Монтировать подключенные устройства Пытаться включить сконфигурированные точки монтирования для подключенных устройств
Неизвестный swap	☐ Монтирование не сконфигурированного раздела подкачки
Неизвестный раздел	☐ Монтирование не сконфигурированного раздела
Hotplug раздела подкачки	☒ Автоматическое монтирование раздела подкачки при подключении к системе во время её работы без выключения питания и остановки системы (hotplug)
Hotplug раздела	☒ Автоматическое монтирование раздела, при подключении к системе во время её работы, без выключения питания и остановки системы (hotplug)
Проверка файловых систем перед монтированием	☐ Автоматическая проверка файловой системы раздела на ошибки, перед монтированием

Рисунок 3 - 16. Точки монтирования. Основные настройки



- При активации чекбокса «Неизвестный раздел» неизвестные разделы будут автоматически смонтированы в папку «`/mnt/<имя_устройства>`».
- При активации чекбокса «Hotplug раздела» автоматически монтируются только разделы из таблицы «Точки монтирования». Для остальных монтирование работает, только если активен чекбокс «Неизвестный раздел».
- При проверке файловых систем используются утилиты VFAT, F2FS, Btrfs, ext2, ext3, ext4.

3.7.2. Смонтированные разделы

В подразделе «Смонтированные разделы» страницы «Монтирование разделов» приведена текущая таблица монтирования.

В таблице перечислены все смонтированные разделы, их точки монтирования и объём доступного пространства. Имеется возможность ручного размонтирования пользовательских разделов при помощи кнопки «Отмонтировать».

Смонтированные разделы

Файловая система	Точка монтирования	Доступно	Занято	Отмонтировать
/dev/root	/rom	0 Б / 58.88 МиБ	100.00% (58.88 МиБ)	-
devtmpfs	/dev	512.00 КиБ / 512.00 КиБ	0.00% (0 Б)	-
tmpfs	/tmp	983.20 МиБ / 984.61 МиБ	0.14% (1.41 МиБ)	-
/dev/mmcblk1p6	/overlay	25.92 ГиБ / 27.33 ГиБ	0.01% (2.49 МиБ)	-
overlayfs:/overlay	/	25.92 ГиБ / 27.33 ГиБ	0.01% (2.49 МиБ)	-

Рисунок 3 - 17. Точки монтирования. Смонтированные разделы

3.7.3. Точки монтирования

В подразделе «Точки монтирования» осуществляется управление точками монтирования.

Точки монтирования

Точки монтирования определяют, куда в файловой системе будут смонтированы разделы запоминающего устройства

Включено	Устройство	Точка монтирования	Файловая система	Опции монтирования	Проверить	
☐	UUID: fd332988-1dae-4ac5-b269-76d1787c6949 (/dev/mmcblk1p4, 64.00 МиБ)	/mnt/mmcblk1p2	auto (ext4)	defaults	Нет	☰ Изменить Удалить
☐	UUID: d3c36863-61092e24-c2033a31-a001f090 (/dev/mmcblk1p5, 384.00 МиБ)	/rom	auto (squashfs)	defaults	Нет	☰ Изменить Удалить
☐	UUID: fd332988-1dae-4ac5-b269-76d1787c6949 (/dev/mmcblk1p4, 64.00 МиБ)	/mnt/mmcblk1p4	auto (ext4)	defaults	Нет	☰ Изменить Удалить
☐	UUID: d3c36863-61092e24-c2033a31-a001f090 (/dev/mmcblk1p5, 384.00 МиБ)	/mnt/mmcblk1p5	auto (squashfs)	defaults	Нет	☰ Изменить Удалить
☐	UUID: fdf7f34d-9652-44c3-b5d9-04219e29ff4f (/dev/mmcblk1p6, 28.23 ГиБ)	/overlay	auto (ext4)	defaults	Нет	☰ Изменить Удалить
						Добавить

Рисунок 3 - 18. Точки монтирования

Для редактирования точки монтирования нажмите кнопку «Изменить» в строке соответствующего раздела. Откроется страница с вкладками «Общие настройки» и «Дополнительные настройки».

Точки монтирования — Настройки раздела

Общие настройки

Дополнительные настройки

Включено

☐

UUID

-- проверка по uuid --

Если выбрано, монтировать устройство используя его UUID, а не фиксированный файл устройства

Метка

-- проверка по метке --

Если выбрано, монтировать устройство используя название его раздела, а не фиксированный файл устройства

Устройство

не определено

Устройство или раздел (например, /dev/sda1)

Точка монтирования

-- Сделайте выбор --

Папка, к которой монтируется раздел устройства

Рисунок 3 - 19. Изменение точки монтирования. Базовые настройки



Если в общих настройках указан «UUID» или «Метка», они используются вместо фиксированного пути /dev/....

Точки монтирования — Настройки раздела

Общие настройки

Дополнительные настройки

Файловая система

auto

Опции монтирования

defaults

Для подробной информации обратитесь к справке по команде mount (man mount)

Проверить

☐

Проверять файловую систему перед монтированием раздела

Заккрыть

Сохранить

Рисунок 3 - 20. Изменение точки монтирования. Дополнительные настройки



Для корректной работы с кириллицей в именах файлов в дополнительных настройках укажите: 'codepage=1251, iocharset=utf8'.

Для добавления новой точки монтирования необходимо нажать кнопку «Добавить», расположенную под таблицей точек монтирования.

При добавлении новой точки монтирования откроется такая же страница редактирования параметров, как и при редактировании уже существующей.

Для удаления точки монтирования необходимо нажать кнопку «Удалить», расположенную в строке соответствующего раздела таблицы.

3.7.4. Разделы подкачки (swap)

Подраздел «Разделы подкачки» используются для временного хранения данных при нехватке оперативной памяти.

Таблица содержит список существующих swap-разделов с флагом активности («Включено») и указанием устройства.

Разделы подкачки (swap)

Если физической памяти не достаточно, то неиспользуемые данные могут быть временно перемещены в раздел подкачки, что в свою очередь приведет к увеличению объёма свободной RAM. Однако, перемещение в файл — это достаточно долгий процесс, так как устройство, на котором располагается раздел подкачки, работает гораздо медленнее, чем RAM.

Включено	Устройство
Этот раздел не содержит данных	

Добавить

Рисунок 3 - 21. Точки монтирования. Разделы подкачки

Для добавления раздела нажмите кнопку «Добавить» в правой нижней части страницы. Откроется окно настроек.

Точки монтирования — Настройка раздела подкачки

Включено

☐

UUID

-- проверка по uuid --

Если выбрано, монтировать устройство используя его UUID, а не фиксированный файл устройства

Метка

-- проверка по метке --

Если выбрано, монтировать устройство используя название его раздела, а не фиксированный файл устройства

Устройство

не определено

Устройство или раздел (например, /dev/sda1)

Рисунок 3 - 22. Разделы подкачки. Настройка раздела подкачки

3.8. Индикаторы

На странице «Индикаторы» настраиваются правила управления светодиодами контроллера.

Таблица содержит список правил с названием, системным именем LED и условием срабатывания (триггер).

Настройка LED индикации

Настройка поведения светодиодной индикации устройства, если это возможно.

Название	Имя LED	Триггер
Этот раздел не содержит данных		

Добавить действие LED

Применить

▼

Сохранить

Очистить

Рисунок 3 - 23. Индикаторы

Для добавления правила нажмите «Добавить действие LED». Откроется окно настроек поведения LED.

Настройка LED индикации

Название	
Имя LED	mmc activity
Триггер	Всегда включен (kernel: default-on)

ЗакрытьСохранить

Рисунок 3 - 24. Индикаторы

3.9. Резервное копирование

Страница «Резервное копирование» предназначена для создания и восстановления архива конфигурации, а также сброса к заводским настройкам.

Страница разделена на две вкладки:

- Действия;
- Конфигурация;

3.9.1. Действия

Во вкладке «Действия» представлены элементы управления архивами резервного копирования.

Резервное копирование

Действия	Конфигурация
----------	--------------

Резервное копирование

Нажмите «Создать архив», чтобы создать и загрузить архив текущих конфигурационных файлов прошивки устройства, таким образом вы сохраните его настройки.

Загрузить резервную копию Создать архив

Восстановить

Чтобы восстановить конфигурационные файлы, вы можете загрузить ранее созданный архив резервной копии здесь. Для сброса настроек прошивки к исходному состоянию (сброс на заводские настройки) нажмите «Выполнить сброс».

Восстановить резервную копию Загрузить архив...

Пользовательские файлы (сертификаты, скрипты) могут остаться в системе. Чтобы этого не произошло, выполните сначала сброс к заводским настройкам.

Рисунок 3 - 25. Резервное копирование. Вкладка «Действия»

3.9.2. Конфигурация

Во вкладке «Конфигурация» доступно редактирование файла `/etc/sysupgrade.conf`. В нём указываются дополнительные пути к файлам и папкам (по одному на строку), которые нужно сохранять в резервной копии.

Конфигурация

В данном конфигурационном файле перечислены пути к файлам и/или папкам, содержимое которых необходимо сохранить в резервной копии. Изменённые конфигурационные файлы из папки /etc/config, а также некоторые другие, сохраняются в резервной копии автоматически.

Показать текущий список...

```
## This file contains files and directories that should
## be preserved during an upgrade.

# /etc/example.conf
# /etc/openvpn/
```

Сохранить

Рисунок 3 - 26. Резервное копирование. Вкладка «Конфигурация»

Кнопка «Показать текущий список...» отображает полный список файлов, которые будут сохранены в архиве (стандартные + добавленные в sysupgrade.conf).

Список файлов для резервного копирования

Ниже приводится определённый список файлов для резервного копирования. Он состоит из изменённых конфигурационных файлов, отмеченных орк, необходимых базовых файлов, а также шаблонов резервного копирования, определенных пользователем.

```
/etc/collectd.conf
/etc/config/dhcp
/etc/config/luci
/etc/config/luci_netports
/etc/config/luci_statistics
/etc/config/ucitrack
/etc/dropbear/dropbear_rsa_host_key
/etc/group
/etc/hosts
/etc/inittab
/etc/passwd
/etc/profile
/etc/rc.local
/etc/shadow
/etc/shellinabox/ssl/certificate.pem
/etc/shells
```

Закреть

Рисунок 3 - 27. Список файлов для резервного копирования

3.10. Обновление прошивки

На странице «Обновление прошивки» доступно обновление прошивки устройства.

Обновление прошивки

Здесь вы можете выполнить обновление прошивки на этого устройства.

Конфигурация и действия обновления прошивки

Очистка пользовательских данных ☐

Включение этой опции приведет к полной очистке пользовательских данных (включая конфигурацию устройства) при обновлении прошивки

Файл прошивки

Обзор...

Файл: не выбран
Размер: 0 Б (0 байт)

Обновление прошивки

Обновить...

Внимание

После начала процедуры обновления прошивки НЕ ВЫКЛЮЧАЙТЕ устройство, пока обновление прошивки не будет полностью завершено. Обратите внимание, что обновление прошивки может занять длительное время, вплоть до 5–15 минут (в зависимости от скорости подключения). Поэтому, пожалуйста, будьте терпеливы во время этой операции.

Рисунок 3 - 28. Обновление прошивки

Для автоматического сброса всех настроек к заводскому состоянию отметьте чекбокс «Очистка пользовательских данных».

Для обновления прошивки необходимо выбрать новый файл образа для загрузки на устройство при помощи кнопки «Обзор...». При наличии на внешнем устройстве корректного файла образа прошивки кнопка «Обновить...» становится активной. Нажатие этой кнопки начинает процедуру обновления прошивки устройства.

3.11. Терминал

На странице «Терминал» реализован доступ к командной строке устройства через браузер.

Страница разделена на два подраздела:

- [Терминал](#);
- [Настройки](#);

3.11.1. Терминал

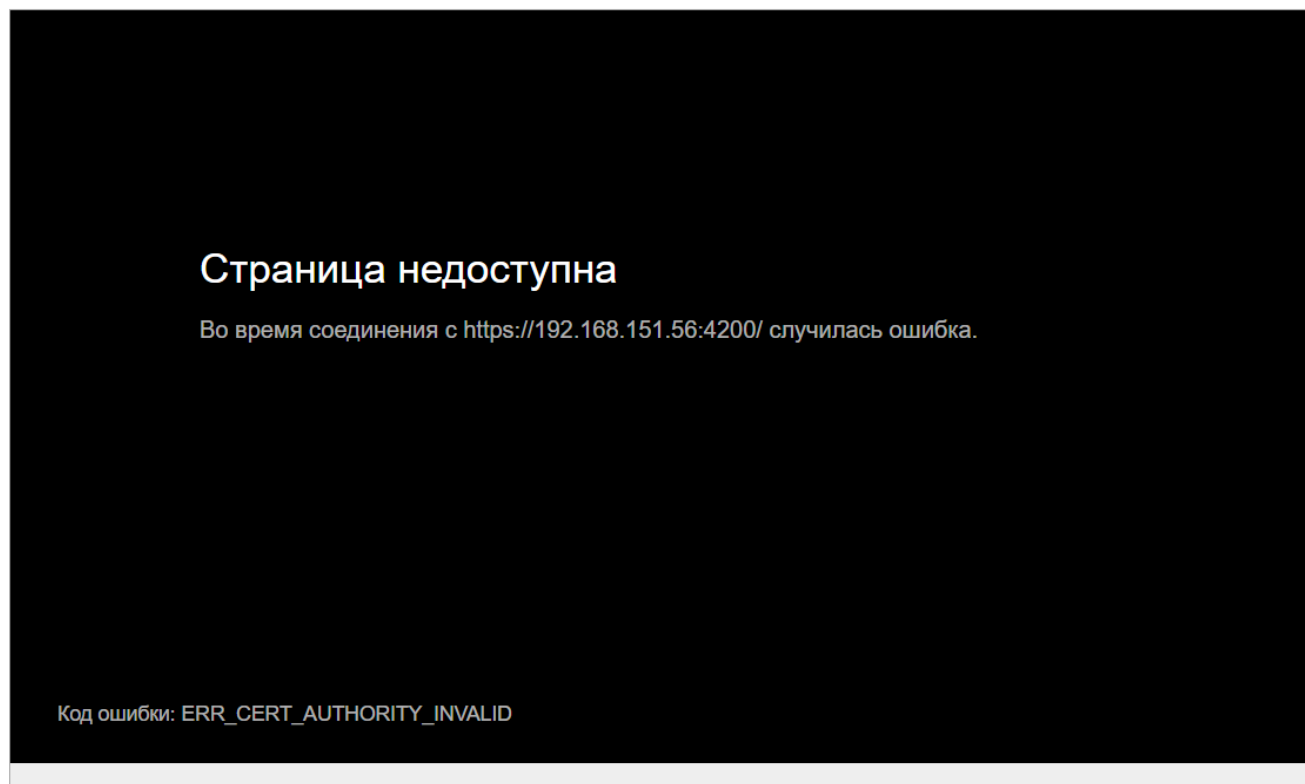
Подраздел «Терминал» отведен полностью под окно терминала.

Веб-терминал



Рисунок 3 - 29. Терминал

При открытии терминала может отображаться ошибка сертификата:



[Открыть терминал в отдельном окне](#)

Рисунок 3 - 30. Терминал. Ошибка сертификата

Чтобы исправить данную ошибку, сделайте следующее:

1. Нажмите «Открыть терминал в отдельном окне».
2. В открывшемся окне нажмите «Подробнее» → «Сделать исключение для этого сайта».

Невозможно установить безопасное соединение

Переходить на страницу опасно. Ваши личные данные на сайте 192.168.151.56 (пароли, переписка или платёжная информация) могут быть перехвачены.

Уйти со страницы

Подробнее ^

Сайт не смог подтвердить, что он действительно 192.168.151.56. Его сертификат не прошёл проверку.

Кто-то намеренно подменил сертификат, чтобы перехватить данные, или на вашем устройстве отсутствуют доверенные сертификаты.

[Зачем нужны сертификаты](#)

Сделать исключение для этого сайта

Рисунок 3 - 31. Терминал. Разрешение работы

После этого терминал станет доступен.

3.11.2. Настройки

Страница настроек терминала разделена на две вкладки: основные настройки и настройки SSL.

Настройки веб-терминала

Основные настройки

Настройки SSL

Порт

4200

Порт для входящих соединений (по умолчанию: 4200)

Отключить вывод звуковых сигналов

☒

Применить

▼

Сохранить

Очистить

Рисунок 3 - 32. Терминал. Основные настройки

Отключение вывода звуковых сигналов запрещает, например, сигнал при выводе ASCII BEL).

Включить SSL

☒

Сертификат HTTPS (формат PEM)

 /etc/shellinabox/ssl/certificate.pem (2.81 KB)

Файл должен включать в себя части с закрытым ключом и сертификатом.

Перегенерировать SSL-сертификат

Перегенерировать SSL-сертификат

Служба терминала удалит существующий сертификат и автоматически сгенерирует новый самоподписанный сертификат

Рисунок 3 - 33. Терминал. Настройки SSL

Рекомендуется всегда включать SSL, иначе логин и пароль передаются в открытом виде.

3.12. Перезагрузка

Страница «Перезагрузка» предназначена для выполнения программной перезагрузки устройства. Данная функция аналогична выполнению в консоли команды `gboot`.

Перезагрузка

Программная перезагрузка вашего устройства, т.е. выполнение команды `reboot`

Выполнить перезагрузку

Рисунок 3 - 34. Перезагрузка

Chapter 4. Службы

4.1. DDNS

На странице «Динамический DNS» производится настройка автоматического обновления DNS-записей для доменных имён при изменении IP-адреса устройства.

Страница разделена на три подраздела:

- [Информация](#);
- [Глобальные настройки](#);
- [Службы](#).

4.1.1. Информация

В подразделе «Информация» отображается состояние и версия DDNS-клиента, элементы управления для его запуска и обновления.

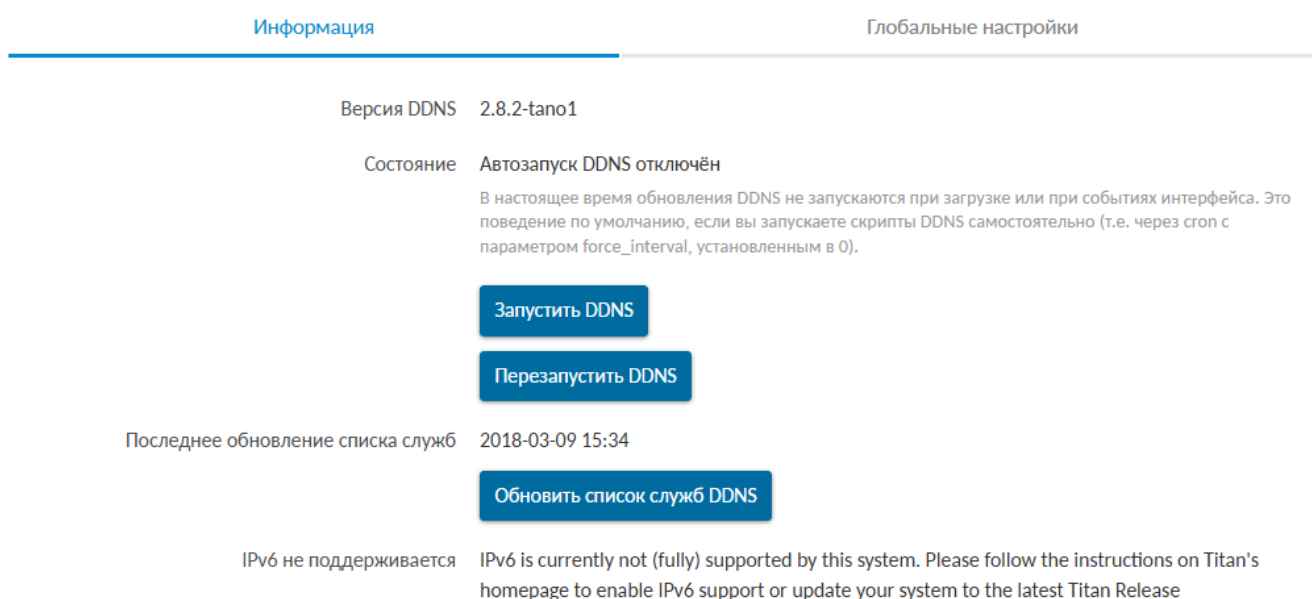


Рисунок 4 - 1. DDNS. Информация

Обновление списка служб выполняется из внешнего источника, актуальность данных зависит от доступности сети на момент запроса.

4.1.2. Глобальные настройки

В подразделе «Глобальные настройки» расположены параметры DDNS-клиента, влияющие на поведение всех служб.

Разрешить не публичные IP-адреса ☐

Непубличные и заблокированные по умолчанию IP-адреса:

- IPv4: 0/8, 10/8, 100.64/10, 127/8, 169.254/16, 172.16/12, 192.168/16
- IPv6: ::/32, f000::/4

Формат даты %F %R

[С поддерживаемыми кодами вы можете ознакомиться здесь](#). Текущие настройки: 2017-08-04 13:22

Папка состояния /var/run/ddns

Каталог содержащий PID файлы и другую информацию о состоянии каждой запущенной службы.

Папка системного журнала /var/log/ddns

Каталог содержащий файлы журналов для каждой запущенной службы.

Просмотр журнала 250

Число последних строк, для хранения в системном журнале

Использовать cURL ☐

Если установлены пакеты wget и cURL, то по умолчанию будет использоваться wget

Путь к CA-сертификатам IGNORE

Путь к CA-сертификатам, которые будут использоваться для загрузки данных сервисов. Установите IGNORE, чтобы пропустить проверку сертификата.

URL файла поддержки служб

URL used to download services file. By default is the master Titan core layer repo.

Рисунок 4 - 2. DDNS. Глобальные настройки

По умолчанию DDNS-клиент не передаёт провайдеру приватные IP-адреса (192.168.x.x и др.). Включение опции «Разрешить не публичные IP-адреса» снимает это ограничение.

4.1.3. Службы

В подразделе «Службы» отображается таблица всех настроенных DDNS-служб и информация об их состоянии.

Состояние	Название	Поиск имени хоста Зарегистрированный IP-адрес	Включено	Последнее обновление Следующее обновление			
Не работает	myddns_ipv4	yourhost.example.com Нет данных	☐	Никогда Остановлена	Остановить	Перезапустить	⋮
					Изменить	Удалить	
Не работает	myddns_ipv6	yourhost.example.com Нет данных	☐	Никогда Остановлена	Остановить	Перезапустить	⋮
					Изменить	Удалить	
Добавить новую службу...							

Рисунок 4 - 3. DDNS. Службы

Редактирование параметров DDNS-службы

Страница редактирования параметров DDNS-службы открывается при нажатии кнопки «Изменить» в строке соответствующей службы.

Настройки разделяются на четыре группы: основные настройки, дополнительные настройки, настройка таймера, просмотр системного журнала.

В группе «Основные настройки» задаются параметры подключения к провайдеру DDNS: домен, учётные данные, версия IP-протокола, а также источник определения текущего IP-адреса.

Основные настройки

Дополнительные настройки

Настройка таймера

Просмотр системного журнала

Включено

☒

Если служба отключена, её нельзя будет запустить ни с веб-интерфейса LuCI, ни с консоли

Поиск имени хоста

Имя хоста/полное доменное имя для проверки, если происходит обновление IP-адреса или оно необходимо

Версия IP-адреса

IPv4-адрес

Задайте версию протокола IP-адреса 'IPv4/IPv6' отправляется провайдеру DDNS

Провайдер службы DDNS

dyndns.org

Домен

Заменяет [DOMAIN] в Update-URL (URL-encoded)

Имя пользователя

Заменяет [USERNAME] в Update-URL (URL-encoded)

Пароль

Заменяет [PASSWORD] в Update-URL (URL-encoded)

Необязательный кодированный параметр

Необязательно: заменяет [PARAMENC] в Update-URL (URL-encoded)

Необязательный параметр

Необязательно: заменяет [PARAMOPT] в Update-URL (не URL-encoded)

Использовать HTTPS

☐

Включить безопасное соединение с провайдером DDNS

Рисунок 4 - 4. Службы. Основные настройки

В группе «Дополнительные настройки» уточняется поведение службы: интервалы проверки

IP-адреса и отправки обновлений провайдеру, количество повторов при ошибках и интервал между ними, а также уровень детализации журналирования.

Основные настройки	Дополнительные настройки	Настройка таймера	Просмотр системного журнала
IP-адрес источника	Сеть Определяет источник для чтения системного IP-адреса, который будет отправляться провайдеру DDNS		
Сеть	не определено Определяет сеть для считывания системного IP-адреса		
Событие сети	wan Сеть, в которой будут запущены скрипты ddns-updater		
Назначенная версия IP протокола	☐ Необязательно: использовать только чистые версии протоколов IPv4/IPv6.		
DNS сервер	mydns.lan Необязательно: использовать DNS сервер не используемый по умолчанию, для обнаружения "Зарегистрированного IP-адреса". В виде: IP-адрес или полное доменное имя		
Использовать протокол TCP для DNS	☐ Необязательно: использовать протокол TCP вместо UDP по умолчанию для DNS-запросов.		
Прокси сервер	Необязательно: прокси-сервер для обнаружения и обновления. Формат: [user:password@]proxyhost:port. IPv6-адрес должен быть указан в квадратных скобках: [2001:db8::1]:8080		
Запись в журнал	Сообщение Задайте уровень журналирования. Критические ошибки всегда будут записаны в системный журнал.		
Запись в файл	☒ Записывать подробные сообщения в системный журнал. Файл будет автоматически обрезан . Файл: "/var/log/ddns/myddns_ipv4.log"		

Рисунок 4 - 5. Службы. Дополнительные настройки

В группе «Настройки таймера» определяются временные параметры работы службы: как часто проверять изменения IP-адреса, как часто отправлять обновления провайдеру, сколько раз повторять попытки при сбоях и с каким интервалом.

Основные настройки	Дополнительные настройки	Настройка таймера	Просмотр системного журнала
Интервал проверки	30		
Элемент проверки	минут(ы) Размерность интервала проверки изменений IP-адреса		
Интервал обновления	72 Интервал для отправки обновлений провайдеру DDNS. Установка значения 0 заставит сценарий отработать только один раз		
Размерность интервала обновления	минут(ы) Размерность интервала отправки обновления DDNS провайдеру		
Счётчик попыток повтора при ошибке	0 При ошибке скрипт прекратит выполнение после заданного количества повторных попыток. При значении 0 (по умолчанию) количество повторных попыток бесконечно.		
Интервал попытки повтора при ошибке	60 При ошибке скрипт прекратит выполнение после заданного количества повторных попыток. При значении 0 (по умолчанию) количество повторных попыток бесконечно.		
Размерность интервалов повтора	секунд(ы) В случае ошибки, скрипт повторит требуемые действия по истечении заданного времени		

Рисунок 4 - 6. Службы. Настройки таймера

В группе «Просмотр системного журнала» отображается содержимое лог-файла службы для мониторинга работы службы и выявления ошибок.

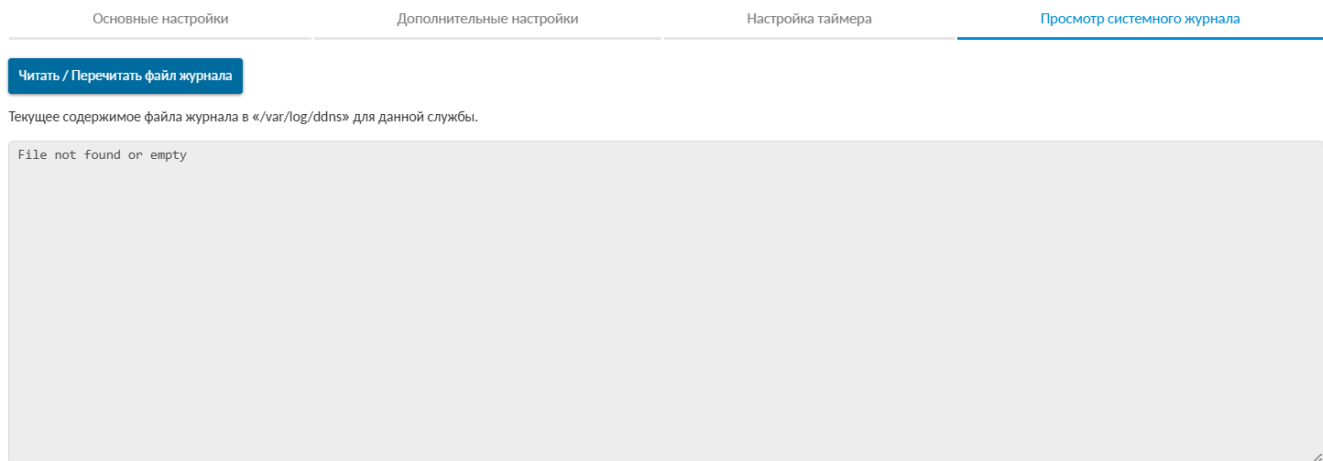


Рисунок 4 - 7. Службы. Просмотр системного журнала

Добавление новой службы

Для добавления новой DDNS-службы предназначена кнопка «Добавить новую службу...», расположенная в подразделе «Службы». При её нажатии открывается диалоговое окно.

Добавить новую службу...

Название	Новая DDNS служба...
Версия IP-адреса	IPv4-адрес Задайте версию протокола IP-адреса 'IPv4/IPv6' отправляется провайдеру DDNS
Провайдер службы DDNS	-- Сделайте выбор --
Отмена Создать службу	

Рисунок 4 - 8. Добавление новой службы

4.2. LLDP

На странице «LLDP» доступен просмотр информации о соседях и настройки службы LLDPd.

Страница разделена на два подраздела:

- [Состояние](#);
- [Настройки](#).

4.2.1. Состояние

Подраздел «Состояние LLDP» позволяет просмотреть информацию о локальном шасси, обнаруженных соседях и статистику интерфейсов.

Состояние LLDP

На данной странице вы можете посмотреть таблицу обнаруженных соседей LLDP, статистику локальных интерфейсов и информацию о локальном шасси.

Локальное шасси

Название:	titan	IP-адреса:	192.168.151.150
Описание:	PLC TITAN SBC v1.0	Возможности:	Bridge (включено)
ID:	a6:4f:2d:f5:08:41		Router (включено)
Тип ID:	MAC-адрес		Wlan (отключено)
			Station (отключено)

Рисунок 4 - 9. Состояние LLDP

Во вкладке «Обнаруженные соседи» ниже отображается таблица соседних устройств, обнаруженных по протоколам LLDP, CDP и другим.

Для каждого обнаруженного соседа приводятся следующие сведения:

- Локальный интерфейс — имя интерфейса устройства и время с момента последнего получения LLDP-пакета от соседа.
- Протокол, с помощью которого обнаружен сосед.
- Обнаруженное шасси — имя, описание, идентификатор и тип идентификатора соседнего устройства, его IP-адреса, а также поддерживаемые и включённые возможности.
- Обнаруженный порт — идентификатор порта соседа, его тип, текстовое описание порта и время жизни (TTL) полученной информации в секундах.

Состояние LLDP

На данной странице вы можете посмотреть таблицу обнаруженных соседей LLDP, статистику локальных интерфейсов и информацию о локальном шасси.

Локальное шасси

Название:	titan	IP-адреса:	192.168.151.150
Описание:	PLC TITAN SBC v1.0	Возможности:	Bridge (включено)
ID:	a6:4f:2d:f5:08:41		Router (включено)
Тип ID:	MAC-адрес		Wlan (отключено)
			Station (отключено)

Рисунок 4 - 10. LLDP. Обнаруженные соседи

Во вкладке «Статистика интерфейсов» отображается сводная информация по каждому интерфейсу: количество переданных и принятых LLDP-пакетов, ошибки, устаревшие записи и т.д.

Обнаруженные соседи					Статистика интерфейсов					
Локальный интерфейс	Протокол	Административное состояние	Tx	Rx	Tx (отброшено)	Rx (не распознано)	Устарело	Обнаружено	Удалено	
Название: eth0 Возраст: — ID a6:4f:2d:f5:08:41 порта: Тип ID MAC-адрес порта: Описание порта: eth0 TTL: 120	—	Rx и Tx	—	—	—	—	—	—	—	—
eth1 a2:4f:2d:f5:08:41	CDPv2	Rx и Tx	691	2072	—	1	—	3	—	—

Рисунок 4 - 11. LLDP. Статистика интерфейсов

4.2.2. Настройки

Подраздел «Настройки LLDPd» позволяет сконфигурировать параметры службы LLDPd.

«Основные настройки» включают службу, переопределяют системные идентификаторы, настраивают интервалы передачи, а также включают режим «только приём».

Основные настройки

Сетевые интерфейсы

Дополнительные настройки

Поддержка протоколов

Включить службу

☒

Описание системы

PLC TITAN SBC v1.0

Переопределить описание системы заданным значением.

Имя системы

titan

Переопределить имя системы заданным значением.

Описание платформы

System platform description

Переопределить описание платформы заданным значением. По умолчанию используется имя используемого ядра (Linux).

Адреса управления данной системы

Management addresses

Адреса управления данной системой. Если не указано, используется первый IPv4 и первый IPv6 адреса. Если указан конкретный IP-адрес, он будет использован как адрес управления без какой-либо проверки. Если вы хотите занести в черный список IPv6-адреса, вы можете использовать шаблон ! *: *. Подробнее о доступных шаблонах читайте [здесь](#).

Задержка отправки

30

Задержка между двумя передачами LLDP PDU. Значение по умолчанию составляет 30 секунд.

Значение «transmit hold»

4

Это значение используется для вычисления TTL переданных пакетов, которое является произведением этого значения и задержки передачи. Значение по умолчанию равно 4. Соответственно, значение TTL по умолчанию составляет 120 секунд.

Включить режим «только приём»

☐

С этой опцией LLDPd не будет отправлять какие-либо пакеты, LLDPd будет только прослушивать сеть для обнаружения соседей.

Рисунок 4 - 12. LLDP. Основные настройки

«Сетевые интерфейсы» выбирают интерфейсы для работы службы и указывают интерфейсы для вычисления ID шасси.

Основные настройки

Сетевые интерфейсы

Дополнительные настройки

Поддержка протоколов

Сетевые интерфейсы

 eth0

 eth1

▼

Укажите какие интерфейсы должны прослушивать и отправлять LLDPDU. Если интерфейсы не указаны, LLDPd будет использовать все доступные физические интерфейсы.

Сетевые интерфейсы, используемые для вычисления ID шасси (chassis ID)

не определено

▼

Укажите какие интерфейсы необходимо использовать для вычисления идентификатора шасси (chassis ID). Если интерфейсы не указаны, будут использованы все интерфейсы, LLDPd получит первый MAC-адрес из всех доступных интерфейсов для вычисления ID шасси.

Рисунок 4 - 13. LLDP. Сетевые интерфейсы

«Дополнительные настройки» настраивают SNMP AgentX, параметры LLDP-MED, поведение при обнаружении нескольких соседей, идентификацию порта и MAC-адрес назначения для LLDPDU.

Основные настройки

Сетевые интерфейсы

Дополнительные настройки

Поддержка протоколов

Путь к сокету SNMP agentX

/var/run/agentx.sock

Если указан путь к сокету, то LLDPd включит SNMP агент, используя протокол AgentX. Это позволяет получать информацию о локальной системе и удаленных системах через SNMP.

Класс устройства LLDP-MED

Network Connectivity Device (класс IV)

▼

Отключить отправку инвентарной информации LLDP-MED TLV

☐

LLDPd будет по-прежнему получать (и публиковать, используя SNMP, если он включен) информацию LLDP-MED TLV, но не будет отправлять. Используйте эту опцию, если вы не хотите передавать важную информацию, такую как серийные номера.

Поведение при обнаружении нескольких соседей

	Фильтр	Входящие			Исходящие		
		E	P	N	E	P	N
☐	1						
☐	2	✓	✓		✓	✓	
☐	3	✓	✓				
☐	4				✓	✓	
☐	20	✓			✓	✓	

☐ E — включить фильтр

☐ P — хранить только один протокол

☐ N — хранить только одного соседа

По умолчанию используется фильтр 15. Более подробную информацию о данной опции можно посмотреть в разделе «FILTERING NEIGHBORS» [здесь](#).

Использовать в качестве ID порта

MAC-адрес интерфейса

▼

Данная настройка позволяет принудительно использовать в качестве идентификатор порта имя интерфейса или MAC-адрес.

MAC-адрес назначения, используемый для отправки LLDPDU

01:80:c2:00:00:0e (nearest-bridge)

▼

MAC-адрес назначения, используемый для отправки LLDPDU. Данный параметр позволяет агенту контролировать распространение LLDPDU. По умолчанию используется MAC-адрес 01:80:c2:00:00:0e и ограничивает распространение LLDPDU до ближайшего моста.

Рисунок 4 - 14. LLDP. Дополнительные настройки

46

Поддержка протоколов

На вкладке «Поддержка протоколов» производится настройка поддержки различных протоколов обнаружения соседей.

В настройках LLDP включается поддержка протокола и форсируется отправка LLDP-пакетов.

Основные настройки Сетевые интерфейсы Дополнительные настройки **Поддержка протоколов**

LLDP CDP FDP EDP SONMP (NTDP, NDP, BNMP, BDP)

Включить LLDP ☒

Форсировать от отправку LLDP пакетов ☐

Принудительно отправлять пакеты LLDP, даже если соседей с поддержкой LLDP не обнаружено, но есть соседи, с поддержкой другого протокола. По умолчанию пакеты LLDP отправляются, когда обнаружен сосед с поддержкой LLDP или когда вообще нет обнаруженных соседей.

Рисунок 4 - 15. Настройки протокола LLDP

В настройках CDP включается поддержка протокола, выбирается его версия и форсируется отправка CDP-пакетов.

LLDP **CDP** FDP EDP SONMP (NTDP, NDP, BNMP, BDP)

Включить CDP ☒

Версия протокола CDP CDPv1 и CDPv2

Отправлять CDP пакеты даже если не обнаружено соседей с CDP протоколом ☐

Включить поддержку протокола CDP для работы с маршрутизаторами Cisco, которые не имеют поддержки LLDP

Рисунок 4 - 16. Настройки протокола CDP

В настройках FDP включается поддержка протокола и форсируется отправка FDP-пакетов.

LLDP CDP **FDP** EDP SONMP (NTDP, NDP, BNMP, BDP)

Включить FDP ☒

Отправлять FDP пакеты даже если не обнаружено соседей с FDP протоколом ☐

Включить поддержку протокола FDP для работы с маршрутизаторами Foundry, которые не имеют поддержки LLDP

Рисунок 4 - 17. Настройки протокола FDP

В настройках EDP включается поддержка протокола и форсируется отправка EDP-пакетов.

LLDP	CDP	FDP	EDP	SONMP (NTDP, NDP, BNMP, BDP)
Включить EDP ☒ Включить поддержку протокола EDP для работы с маршрутизаторами и коммутаторам Extreme, которые не имеют поддержки LLDP. Отправлять EDP пакеты даже если не обнаружено соседей с EDP протоколом ☐				

Рисунок 4 - 18. Настройки протокола EDP

В настройках SONMP включается поддержка протокола и форсируется отправка SONMP-пакетов.

LLDP	CDP	FDP	EDP	SONMP (NTDP, NDP, BNMP, BDP)
Включить SONMP ☒ Включить поддержку протокола SONMP для работы с маршрутизаторами и коммутаторами Nortel, которые не имеют поддержки LLDP. Отправлять SONMP пакеты даже если не обнаружено соседей с SONMP протоколом ☐				

Рисунок 4 - 19. Настройки протокола SONMMP

4.3. STP/RSTP

На странице «STP/RSTP» доступен просмотр информации о службах STP и RSTP.

Страница разделена на два подраздела:

- [Состояние](#);
- [Настройки](#).

4.3.1. Состояние

Подраздел «Состояние STP/RSTP» позволяет просмотреть текущее состояние мостов, управляемых протоколами STP/RSTP, и их портов.

Состояние STP/RSTP

На этой странице можно просмотреть текущее состояние мостов STP/RSTP и их портов

Нет данных для отображения. Необходимо **выбрать** для управления службой STP/RSTP как минимум один мост.

Рисунок 4 - 20. Состояние STP/RSTP

При отсутствии настроенных мостов или если ни один мост не выбран для управления службой STP/RSTP, на странице отображается информационное сообщение.

4.3.2. Настройки

Подраздел «Настройки STP/RSTP» позволяет сконфигурировать уровень детализации журналирования и выбрать мосты, управляемые службой.

Настройки STP/RSTP

На этой странице можно настроить параметры STP/RSTP

Общие параметры

Общие параметры

Уровень журналирования

Ошибки (1)

Мосты управляемые службой STP/RSTP

не определено

Нельзя выбрать мосты с отключенной поддержкой STP. Включить или отключить поддержку STP для мостов можно на странице [настройки сетевых интерфейсов](#)

Необходимо выбрать хотя бы один мост для управления службой STP/RSP

Применить



Сохранить

Очистить

Рисунок 4 - 21. Настройки STP/RSTP

4.4. Настройки SNMP

На странице «Настройки SNMP» производится конфигурация SNMP-агента.

Страница разделена на шесть вкладок:

- [Глобальные](#);
- [SNMPv1/SNMPv2c](#);
- [SNMPv3](#);
- [Трапы](#);
- [Система](#);
- [Журналирование](#).

4.4.1. Глобальные

На вкладке «Глобальные» задаются основные параметры SNMP-агента: автоматический запуск агента, версия IP-протокола, порт, версия SNMP и путь к сокету AgentX.

Глобальные	SNMPv1/SNMPv2c	SNMPv3	Трапы	Система	Журналирование
Включить службу SNMP ☒					
Запускать службу SNMP при запуске системы					
Версия IP-протокола		IPv4 и IPv6			
Порт		161			
Версия SNMP		SNMPv1 и SNMPv2c			
Используемая версия SNMP для мониторинга и управления устройством					
Путь к сокету AgentX		/var/run/agentx.sock			
Если не задано, AgentX будет отключен					

Рисунок 4 - 22. SNMP. Глобальные настройки

4.4.2. SNMPv1/SNMPv2c

На вкладке «SNMPv1/SNMPv2c» задаются строки сообщества для чтения и записи, а также ограничиваются источники запросов для каждого из них.

Глобальные	SNMPv1/SNMPv2c	SNMPv3	Трапы	Система	Журналирование
SNMP сообщество для чтения		public			
Источник SNMP сообщества для чтения		любой (default)			
Доверенный источник SNMP сообщества для чтения (имя хоста, IP-адрес/маска, IP-адрес/биты или эквиваленты для IPv6)					
SNMP сообщество для записи		private			
Источник SNMP сообщества для записи		localhost			
Доверенный источник SNMP сообщества для записи (имя хоста, IP-адрес/маска, IP-адрес/биты или эквиваленты для IPv6)					

Рисунок 4 - 23. SNMP. Настройки SNMPv1/SNMPv2c

4.4.3. SNMPv3

На вкладке «SNMPv3» задаются имя пользователя, разрешение на запись, типы аутентификации и шифрования с соответствующими паролями.

Глобальные	SNMPv1/SNMPv2c	SNMPv3	Трапы	Система	Журналирование
Имя пользователя SNMPv3		writeuser			
Имя пользователя SNMPv3					
Разрешить запись		☐			
Тип аутентификации SNMPv3		SHA			
Пароль аутентификации SNMPv3					
Тип шифрования SNMPv3		AES			
Пароль шифрования SNMPv3					

Рисунок 4 - 24. SNMP. Настройки SNMPv3

4.4.4. Трапы

В настройках SNMP-трапов включается отправка уведомлений, задается версия протокола, адрес и порт хоста назначения, а также строка сообщества для трапов.

Глобальные	SNMPv1/SNMPv2c	SNMPv3	Трапы	Система	Журналирование
Включить SNMP трапы		☐			
Включить функционал SNMP трапов					
Версия SNMP трапов		SNMPv2c			
Используемая версия SNMP для отправки трапов					
Хост/IP-адрес		localhost			
Адрес хоста назначения для отправки трапов (имя хоста или IP-адрес)					
Порт		162			
Порт для отправки трапов					
SNMP сообщество		public			
SNMP сообщество для трапов					

Рисунок 4 - 25. SNMP. Настройки SNMP-трапов

4.4.5. Система

В настройках системы SNMP задаются идентификационные сведения об устройстве: имя системы, контакт администратора и физическое расположение.

Глобальные	SNMPv1/SNMPv2c	SNMPv3	Трапы	Система	Журналирование
Название		System Name			
Имя системы					
Контакт		System Contact			
Контакт системы					
Расположение		System Location			
Расположение системы					

Рисунок 4 - 26. SNMP. Настройки системы

4.4.6. Журналирование

В настройках журналирования SNMP задаются параметры записи событий: включение записи в файл и в syslog, путь к файлу журнала и минимальный приоритет сообщений для файлового журнала.

Глобальные	SNMPv1/SNMPv2c	SNMPv3	Трапы	Система	Журналирование
Включить журналирование в файл ☒					
Путь к файлу журнала		/var/log/snmpd.log			
Приоритет сообщений журналирования в файл		LOG_INFO			
Будут регистрироваться сообщения выбранного приоритета и выше.					
Включить журналирование в syslog ☐					

Рисунок 4 - 27. SNMP. Настройки журналирования

4.5. Настройки FTP-сервера

На странице «Настройки FTP-сервера» раздела «Службы» производится конфигурация параметров доступа, пользователей и журналирования.

Страница разделена на семь вкладок:

- [Настройки службы;](#)
- [Настройки подключения;](#)
- [Основные настройки;](#)
- [Локальные пользователи;](#)
- [Виртуальные пользователи;](#)
- [Анонимный доступ;](#)
- [Настройки журналирования.](#)

4.5.1. Настройки службы

В настройках службы FTP задаются основные параметры запуска сервера: включение службы, поддержка IPv4 и IPv6 с указанием адресов, а также порты для управления и передачи данных.

Настройки службы	Настройки подключения	Основные настройки	Локальные пользователи	Виртуальные пользователи
Анонимный доступ		Настройки журналирования		
Включить FTP-сервер ☒				
Запускать FTP-сервер при запуске системы				
Включить IPv4 ☒				
IPv4 адрес		0.0.0.0		
Включить IPv6 ☐				
Порт для входящих соединений		21		
Порт для данных		20		

Рисунок 4 - 28. FTP. Настройки службы

4.5.2. Настройки подключения

В настройках подключения FTP задаются параметры сетевых соединений и режимов работы.

Настройки службы	Настройки подключения	Основные настройки	Локальные пользователи	Виртуальные пользователи
Анонимный доступ		Настройки журналирования		
Включить режим PORT ☒				
Включить режим PASV ☒				
Номер порта, начиная с которого размещаются порты для PASV режима		10050		
Номер порта, до которого размещаются порты для PASV режима		10100		
Режим ASCII		Для скачивания и загрузки		
Таймаут неактивной сессии		1800		
		В секундах		
Таймаут подключения		120		
		В секундах		
Таймаут подключения для данных		120		
		В секундах		
Максимальное количество клиентов		0		
		0 — без ограничений		
Максимальное количество клиентов для одного IP-адреса		0		
		0 — без ограничений		
Максимальная скорость передачи		0		
		Байт/с, 0 — без ограничений		
Максимальное количество ошибок авторизации		3		
		Не может быть 0, по умолчанию 3		

Рисунок 4 - 29. FTP. Настройки подключения

4.5.3. Основные настройки

В основных настройках FTP задаются права доступа, отображение скрытых файлов, значение `umask`, приветственное сообщение сервера, а также включение сообщений при входе в каталог и имя файла с таким сообщением.

Настройки службы	Настройки подключения	Основные настройки	Локальные пользователи	Виртуальные пользователи
Анонимный доступ		Настройки журналирования		
Разрешить запись ☒ Если отключено, все запросы на запись будут вызывать ошибку доступа				
Разрешить скачивание (download) ☒ Если отключено, все запросы на скачивание будут вызывать ошибку доступа				
Разрешить просмотр списка директорий ☒ Если отключено, все запросы на просмотр списка каталога будут вызывать ошибку доступа				
Разрешить рекурсивный просмотр каталогов ☐				
Показывать скрытые файлы (dot files) ☐ Если опция установлена, файлы начинающиеся с «.» будут показываться в листинге директории, даже если флаг «a» не используется клиентом. Эта опция исключает директории «.» и «..»				
Режим создания файлов (umask) 022 Права загружаемых файлов устанавливаются в значение 666 – umask, каталогов — 777 – umask				
Сообщение сервера (FTP баннер)				
Включить сообщения при входе в каталоги ☐ Сообщение отображается при входе в каталог				
Имя файла сообщения директории .message				

Рисунок 4 - 30. FTP. Основные настройки

4.5.4. Локальные пользователи

В настройках локальных пользователей FTP задаются разрешение доступа системным пользователям устройства и корневая папка для них.

Настройки службы	Настройки подключения	Основные настройки	Локальные пользователи	Виртуальные пользователи
Анонимный доступ		Настройки журналирования		
Включить локальных пользователей ☐				
Корневая папка Если не задано, будут использоваться домашние папки пользователей				

Рисунок 4 - 31. FTP. Локальные пользователи

4.5.5. Виртуальные пользователи

В настройках виртуальных пользователей FTP включается их поддержка и указывается системный пользователь, от имени которого они работают.

В таблице задаются имя виртуального пользователя, домашний каталог и права на запись, загрузку и прочие действия.

Настройки службы
Настройки подключения
Основные настройки
Локальные пользователи
Виртуальные пользователи

Анонимный доступ
Настройки журналирования

Включить виртуальных пользователей ☒

Имя пользователя

Имя локального пользователя, от имени которого обеспечивается доступ виртуальным пользователям

Имя пользователя	Домашний каталог	Разрешить запись и создание директорий	Разрешить загрузку (upload)	Разрешить прочие действия	
ftp	/home/ftp	Да	Да	Нет	Изменить Удалить

Добавить

Рисунок 4 - 32. FTP. Виртуальные пользователи

Для редактирования виртуального пользователя FTP нажмите на кнопку «Изменить». При редактировании задаются имя пользователя, пароль, домашний каталог, значение umask, ограничение скорости, а также права на запись, загрузку и прочие действия.

Виртуальные пользователи » ftp

Имя пользователя

Пароль

*

Домашний каталог

Режим создания файлов (umask)

Максимальная скорость передачи

Байт/с, 0 — без ограничений

Разрешить запись и создание директорий ☒

Разрешить загрузку (upload) ☒

Разрешить прочие действия ☐

Включая переименование, удаление, ...

Закрыть

Сохранить

Рисунок 4 - 33. Редактирование виртуального пользователя

Страница добавления виртуального пользователя вызывается по кнопке «Добавить» и содержит те же параметры, что и страница редактирования. Поля «Имя пользователя» и «Пароль» должны быть заполнены обязательно.

4.5.6. Анонимный доступ

На вкладке «Анонимный доступ» настраиваются параметры доступа для анонимных пользователей.

Включить анонимного пользователя ☐

Имя пользователя

ftp

Имя локального пользователя, от имени которого обеспечивается анонимный доступ

Корневая папка

/home/ftp

Режим создания файлов (umask)

022

Максимальная скорость передачи

0

Байт/с, 0 — без ограничений

Разрешить запись и создание директорий ☐Разрешить загрузку (upload) ☐Разрешить прочие действия ☐

Включая переименование, удаление, ...

Рисунок 4 - 34. FTP. Анонимный доступ

4.5.7. Настройки журналирования

В настройках журналирования FTP включается запись событий в файл и задаётся путь к файлу журнала.

Включить журналирование

в файл



Файл журнала

/var/log/vsftpd.log

Рисунок 4 - 35. FTP. Настройки журналирования

4.6. Шлюз Modbus TCP в Modbus RTU

Шлюз Modbus TCP в Modbus RTU позволяет устройствам, поддерживающим протокол Modbus TCP, взаимодействовать с устройствами Modbus RTU, подключёнными через последовательные интерфейсы. Шлюз выполняет преобразование протоколов: принимает Modbus TCP-запросы, транслирует их в Modbus RTU и возвращает ответы обратно.

На странице конфигурации портов шлюза Modbus включаются или отключаются порты, задаются параметры последовательного соединения и указывается TCP-порт для приёма соединений.

Шлюз Modbus TCP в Modbus RTU

Конфигурация портов

Включить	Устройство	Скорость	Чётность	Стоповые биты	TCP порт		Изменить	Удалить
☐	/dev/ttyUSB0	115200	Чёт	1	502		Изменить	Удалить
Добавить								
Применить Сохранить Очистить								

Рисунок 4 - 36. Шлюз Modbus TCP в Modbus RTU. Конфигурация портов

Страница редактирования шлюза открывается при нажатии кнопки «Изменить» в строке соответствующего порта.

В общих настройках шлюза Modbus включается или отключается шлюз и выбирается уровень журналирования.

Шлюз Modbus TCP в Modbus RTU

Общие настройки

Настройки RTU

Настройки TCP

Включить

Уровень журналирования

Предупреждения

Рисунок 4 - 37. Редактирование шлюза. Общие настройки

В настройках RTU шлюза Modbus задаются параметры последовательного интерфейса.

Шлюз Modbus TCP в Modbus RTU

Общие настройки

Настройки RTU

Настройки TCP

Устройство

/dev/ttyUSB0

Скорость

115200

Чётность

Чёт

Стоповые биты

1

Попытки запроса

3

Определяет максимальное количество повторных попыток запроса (0–15, 0 — без повторных попыток)

Пауза между запросами

100

Определяет паузу между запросами в миллисекундах (1–10000)

Время ожидания ответа

500

Определяет время ожидания ответа в миллисекундах (1–10000)

Рисунок 4 - 38. Редактирование шлюза. Настройки RTU

В настройках TCP шлюза Modbus задаются IP-адрес и порт для приёма соединений, максимальное количество одновременных подключений и таймаут

Общие настройки	Настройки RTU	Настройки TCP
TCP адрес	0.0.0.0	
TCP порт	502	
Максимальное количество TCP подключений	32	
	Определяет максимальное количество одновременных TCP-соединений (1–128)	
Таймаут	60	
	Определяет таймаут подключения в секундах (0–1000, 0 — без таймаута)	

Рисунок 4 - 39. Редактирование шлюза. Настройки TCP

Страница добавления нового шлюза содержит те же вкладки и параметры, что и страница редактирования. При добавлении нового шлюза необходимо заполнить параметры на всех трёх вкладках, после чего сохранить изменения.

4.7. HTTP/HTTPS

На странице «HTTP/HTTPS» находятся настройки веб-сервера, предназначенного для встраиваемых систем.

Страница разделена на четыре вкладки

- [Основные настройки](#);
- [Второстепенные настройки](#);
- [Дополнительные настройки](#);
- [Параметры самоподписанного сертификата](#).

4.7.1. Основные настройки

В основных настройках веб-сервера uHTTPd задаются адреса и порты для HTTP и HTTPS, перенаправление HTTP на HTTPS, игнорирование частных IP-адресов, выбор SSL-сертификата и частного ключа, а также кнопки для удаления сертификата и ключа.

Основные настройки	Второстепенные настройки	Дополнительные настройки
Входящие HTTP (адрес:порт)	0.0.0.0:80 ✕ [:,]:80 ✕ +	Привязка к конкретному интерфейсу:порту (путем указания адреса интерфейса)
Входящие HTTPS (адрес:порт)	0.0.0.0:443 ✕ [:,]:443 ✕ +	Привязка к конкретному интерфейсу:порту (путем указания адреса интерфейса)
Перенаправление всех HTTP запросов на HTTPS	☐	
Игнорировать приватные IP-адреса на публичном интерфейсе	☒	Запретить доступ с приватных IP-адресов на интерфейсе, если он имеет публичный IP-адрес (RFC1918)
Сертификат HTTPS (в DER или PEM формате)	Выбрать файл...	
Приватный ключ HTTPS (в DER или PEM формате)	Выбрать файл...	
Удалить старый сертификат и ключ	Удалить старый сертификат и ключ	uHTTPd создаст самоподписанный сертификат используя параметры, расположенные ниже
Удалить настройки для сертификата и ключа	Удалить настройки для сертификата и ключа	Полное удаление сертификата и ключа с отключением поддержки HTTPS
		Добавить

Рисунок 4 - 40. HTTP/HTTPS. Основные настройки

4.7.2. Второстепенные настройки

Во второстепенных настройках uHTTPd задаются индексные страницы, обработчики файлов CGI, запрет перехода по символическим ссылкам и создания списков папок, псевдонимы путей, хост и путь к файлу аутентификации, а также виртуальный URL для ошибки 404.

Страница в основном предназначена для настройки параметров обслуживания сервера, а не веб-интерфейса

Страница или страницы индекса

index.html



Например, укажите index.html и index.php, если используется PHP

Обработчик типа файла CGI



Обработчик для сопоставления расширений файлов ('суффикс=обработчик', например: '.php=/usr/bin/php-cgi')

Не следовать по символическим ссылкам вне
корневого каталога документов

☐

Не создавать списки папок.

☐

Псевдонимы (aliases)



(/старый/путь=/новый/путь) или (просто /старый/путь становится /cgi-prefix/старый/путь)

Хост для аутентификации

titan

Конфигурационный файл (например, с учётными
данными базовой HTTP-аутентификации)

HTTP-аутентификация не будет использоваться, если файла не существует

Ошибка 404

Виртуальный URL-адрес или CGI скрипт для отображения статуса '404 не найдено'. Должно начинаться с '/'

Добавить

Рисунок 4 - 41. HTTP/HTTPS. Второстепенные настройки

4.7.3. Дополнительные настройки

В дополнительных настройках uHTTPd задаются корневая папка, префиксы для CGI и Lua-скриптов, настройки JSON-RPC и CORS, авторизация ubus, а также таймауты выполнения скриптов и сетевой активности, параметры keepalive и ограничения по количеству соединений и запросов.

Страница содержит параметры, которые редко используются или влияют на обслуживание веб-интерфейса

Основная папка	/www
Основная папка для файлов, которые будут обслуживаться сервером	
Префикс пути для CGI скриптов	/cgi-bin
CGI будет отключен, если не задано	
Виртуальный префикс пути для скриптов Lua	/cgi-bin/luci=/usr/lib/lua/luci/cgi/uhttpd.lua
Полный путь к обработчику скриптов Lua	
Интерпретатор Lua будет отключен, если не задано	
Виртуальный префикс пути для ubus через интеграцию JSON-RPC	/ubus
Интеграция с ubus будет отключена, если не задано	
Переопределить путь для сокета ubus	
Включение поддержки CORS (совместное использование ресурсов между разными источниками) для JSON-RPC протокола	☐
Отключение авторизации JSON-RPC через API системы ubus	☐
Максимальное время ожидания завершения выполнения для Lua, CGI или ubus	60
Максимальное время ожидания сетевой активности	30
Повторное использование соединения	0
Значение TCP keepalive	0
Максимальное количество соединений	100
Максимальное количество запросов скрипта	20

Рисунок 4 - 42. HTTP/HTTPS. Дополнительные настройки

4.7.4. Параметры самоподписанного сертификата

Самоподписанный сертификат используется при включении HTTPS и отсутствии загруженного сертификата.

В параметрах самоподписанного сертификата uHTTPd задаются срок действия сертификата в днях, длина ключа RSA, полное доменное имя сервера, организация, штат или область, город и двухбуквенный код страны.

Параметры самоподписанного сертификата

Количество дней, в течение которых
сгенерированный сертификат действителен

730

Длина приватного ключа в битах

2048

Common name (/CN)

OpenWrt

Полное доменное имя сервера

Организация

Если пусто, то при генерации сертификата будет использовано случайное/уникальное значение

Название штата или области (/ST)

Somewhere

Область, где была проведена официальная регистрация компании

Расположение (/L)

Unknown

Название города, где была проведена официальная регистрация компании

Страна (/C)

zz

ISO-код страны

Рисунок 4 - 43. HTTP/HTTPS. Параметры самоподписанного сертификата

Chapter 5. Сеть

5.1. Интерфейсы

Для управления сетевыми интерфейсами системы предназначена страница «Интерфейсы» раздела «Сеть».

Страница «Интерфейсы» разделена на три вкладки:

- [Интерфейсы](#);
- [Устройства](#);
- [Основные настройки сети](#);

5.1.1. Интерфейсы

На странице расположен список интерфейсов, в которой перечислены имеющиеся сетевые интерфейсы в системе. Для каждого интерфейса приведён значок, который содержит следующую информацию:

- Название интерфейса;
- Тип интерфейса и состояние подключения;
- Название системного сетевого интерфейса, соответствующего данному интерфейсу.

Интерфейсы	Устройства	Основные настройки сети
Интерфейсы		
LAN0 eth0	Протокол: Статический адрес Время работы: 1д 16ч 52м 49с MAC: AE:7B:4E:EA:D9:6B Получено (RX): 1.17 МБ (6099 пакетов) Передано (TX): 6.32 МБ (19548 пакетов) IPv4: 192.168.150.100/24	Перезапустить Остановить Изменить Удалить
LAN1 eth1	Протокол: DHCP-клиент Время работы: 1д 16ч 52м 46с MAC: AA:7B:4E:EA:D9:6B Получено (RX): 61.61 МБ (656069 пакетов) Передано (TX): 12.44 МБ (59494 пакетов) IPv4: 192.168.151.81/24	Перезапустить Остановить Изменить Удалить
Добавить новый интерфейс...		

Рисунок 5 - 1. Интерфейсы

Слева от значка для каждого интерфейса выводится краткая информация и статистика в режиме реального времени.

В последнем столбце таблицы расположены кнопки управления интерфейсом. Для редактирования интерфейса необходимо нажать кнопку «Изменить» в нужной строке.

Редактирование интерфейса Eth0

По умолчанию для интерфейса Eth0 установлен протокол «Статический адрес».

В подразделе «Общие настройки» отображаются параметры состояния интерфейса, а также задаются статические адреса и публичный префикс IPv6 для клиентов.

Общие настройки Дополнительные настройки Настройки межсетевого экрана DHCP-сервер

Состояние

Устройство: eth0
Время работы: 1д 17ч 25м 13с
MAC: AE:7B:4E:EA:D9:6B
Получено (RX): 1.17 МБ (6099 пакетов)
Передано (TX): 6.34 МБ (19741 пакетов)
IPv4: 192.168.150.100/24

Протокол: Статический адрес

Устройство: eth0

Запустить при загрузке: ☒

IPv4-адрес: 192.168.150.100

Маска сети IPv4: 255.255.255.0

IPv4-адрес шлюза: 192.168.151.1 (lan1)

Широковещательный IPv4-адрес: 192.168.150.255

IPv6-адрес: Добавить IPv6 адрес...

IPv6-адрес шлюза:

IPv6 направление префикса:

Публичный префикс, направляемый на это устройство для распространения среди клиентов.

Рисунок 5 - 2. Eth0. Общие настройки

Выбор протокола производится при помощи выпадающего списка «Протокол».

Статический адрес

UMTS/GPRS/EV-DO

DHCP-клиент

DHCPv6 клиент

NCM

Неуправляемый

PPP

PPPoE

PPTP

QMI модем

Статический адрес

WireGuard VPN

Рисунок 5 - 3. Eth0. Выпадающий список протоколов

После выбора нового протокола, на странице основных настроек будет отображена кнопка «Изменить протокол».

Протокол: Статический адрес

Вы действительно хотите изменить протокол?

Изменить протокол

Рисунок 5 - 4. Eth0. Кнопка смены протокола

При нажатии кнопки «Изменить протокол» протокол сетевого интерфейса будет изменён на выбранный. При этом набор основных и дополнительных настроек будет заменён в соответствии с выбранным протоколом.

В дополнительных настройках сетевого интерфейса задаются параметры поведения интерфейса, настройки DHCP-клиента, а также переопределение таблиц маршрутизации для IPv4 и IPv6.

Общие настройки

Дополнительные настройки

Настройки межсетевого экрана

DHCP-сервер

Принудительное подключение (Force link)

☐

Устанавливать параметры (свойства) интерфейса независимо от реального состояния подключения. Если опция включена, события подключения/отключения кабеля для данного интерфейса не будут вызывать hotplug обработки.

Использовать широковещательный флаг

☐

Требуется для некоторых Интернет провайдеров, например использующих DOCSIS 3

ID клиента при DHCP-запросе

Класс производителя (Vendor class), который отправлять при DHCP-запросах

Использовать шлюз по умолчанию

☒

Если не выбрано, то маршрут по умолчанию не настраивается

Использовать объявляемые узлом DNS сервера

☒

Если не выбрано, то извещающие адреса DNS серверов игнорируются

Вес DNS

Записи DNS-сервера в локальном resolv.conf в первую очередь сортируются по весу, указанному здесь

Использовать метрику шлюза

Переопределить таблицу маршрутизации IPv4

не определено

Переопределить таблицу маршрутизации IPv6

не определено

Рисунок 5 - 5. Eth0. Дополнительные настройки

В дополнительных настройках сетевого интерфейса также задаются параметры IPv6: делегирование префиксов, длина префикса, фильтр, суффикс и привилегии.

Делегировать IPv6 префиксы

☒

Включить нисходящее делегирование префиксов IPv6, доступных на этом интерфейсе

IPv6 назначение длины

отключено

Задайте часть данной длины, каждому публичному IPv6-префиксу этого интерфейса

Фильтр IPv6 префикса

— Сделайте выбор —

Если установлено, нисходящие подсети выделяются только из заданных классов префиксов IPv6.

IPv6 суффикс

Необязательно. Допустимые значения: «eui64», «random», фиксированное значение (например, «::1» или «::1:2»). Когда IPv6 префикс такой как «a:b:c:d::», используйте суффикс подобный «::1» для этого IPv6 адреса или «a:b:c:d::1» для этого интерфейса.

IPv6 привилегии

При делегировании префиксов нескольким нисходящим потокам, интерфейсы с более высоким значением привилегий учитываются в первую очередь при распределении подсетей.

Рисунок 5 - 6. Eth0. Дополнительные настройки

Во вкладке «Настройки межсетевого экрана» производится выбор или создание новой зоны, прикрепленной к редактируемому сетевому интерфейсу.

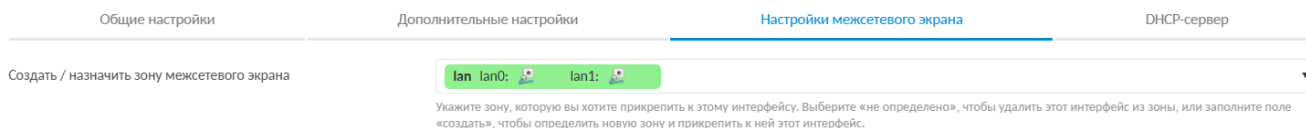


Рисунок 5 - 7. Eth0. Настройки межсетевого экрана

На вкладке размещён только один элемент управления — выпадающий список «Создать / назначить зону сетевого экрана». При помощи данного выпадающего списка можно выбрать существующую зону межсетевого экрана или создать новую, введя её имя в поле «создать». При выборе «не определённо», редактируемый сетевой интерфейс будет удалён из зоны, к которой он был прикреплён ранее.

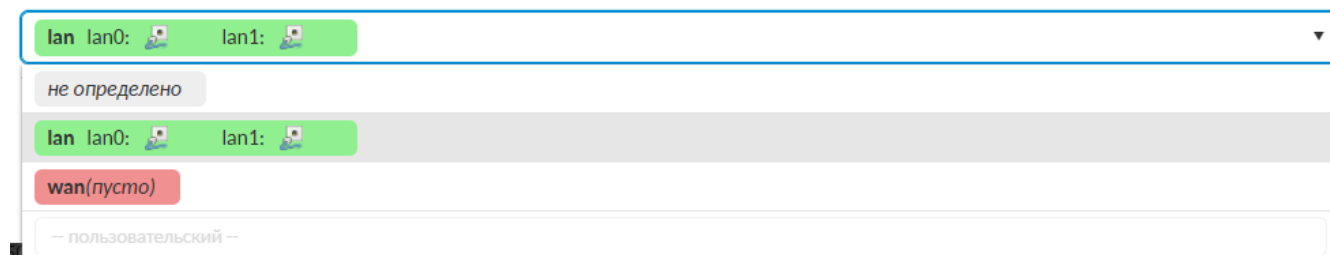


Рисунок 5 - 8. Eth0. Выпадающий список выбора зоны межсетевого экрана

Для настройки DHCP-сервера необходимо нажать на кнопку «Настроить сервер DHCP». После этого появятся еще три вкладки настроек: «Общие настройки», «Дополнительные настройки» и «Настройки IPv6».

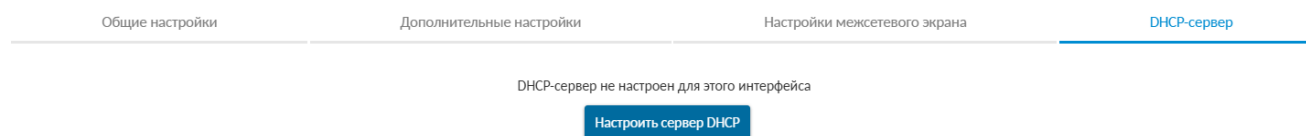


Рисунок 5 - 9. Eth0. DHCP-сервер

Во вкладке «Общие настройки» задаются параметры DHCP-сервера: отключение DHCP для интерфейса, минимальный и максимальный адреса аренды, а также срок аренды адреса.

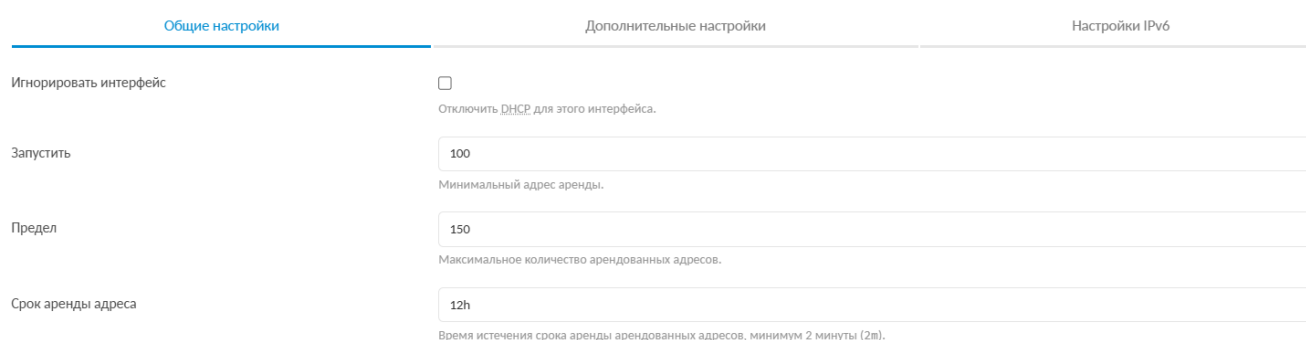


Рисунок 5 - 10. Общие настройки DHCP-сервера

В дополнительных настройках DHCP задаются динамическое выделение адресов, принудительный запуск DHCP, маска сети и дополнительные опции.

Общие настройки	Дополнительные настройки	Настройки IPv6
Динамический DHCP	☒	
Принудительно (Force)	☐	
IPv4-маска сети	255.255.255.0	
DHCP настройки		

Определить дополнительные опции DHCP, например, «6, 192.168.2.1, 192.168.2.2», чтобы известить клиентов о DNS-серверах.

Рисунок 5 - 11. Дополнительные настройки DHCP-сервера

В подразделе «Настройки IPv6» задаются режимы работы служб RA, DHCPv6 и NDP-Proxu на данном интерфейсе, а также устанавливается флаг «Назначенный мастер» для ретрансляции RA и DHCPv6 и проксирования NDP.

Общие настройки	Дополнительные настройки	Настройки IPv6
Назначенный мастер	☐	
Служба RA	отключено	
DHCPv6 сервис	отключено	
NDP-Proxu	отключено	

Рисунок 5 - 12. Настройки IPv6 DHCP-сервера

Редактирование интерфейса Eth1

По умолчанию для интерфейса Eth1 установлен протокол «DHCP-клиент», поэтому в окне настроек будет активна вкладка «DHCP-сервер».

Общие настройки	Дополнительные настройки	Настройки межсетевого экрана	DHCP-сервер
DHCP-сервер не настроен для этого интерфейса			
Настроить сервер DHCP			

Рисунок 5 - 13. Eth1. Вкладка «DHCP-сервер»

Для начала настройки необходимо нажать на кнопку «Настроить сервер DHCP». После этого появятся еще две вкладки настроек: «Общие настройки» и «Настройки IPv6».

В подразделе «Общие настройки» задаётся параметр, включающий или отключающий DHCP-сервер для данного интерфейса

Общие настройки	Настройки IPv6
Игнорировать интерфейс	☒

Рисунок 5 - 14. Eth1. Общие настройки DHCP-сервера

В подразделе «Настройки IPv6» задаются режимы работы служб RA, DHCPv6 и NDP-Proxu на данном интерфейсе, а также устанавливается флаг «Назначенный мастер» для

ретрансляции RA и DHCPv6, а также проксирования NDP.

Общие настройки | **Настройки IPv6**

Назначенный мастер ☐
Установить этот интерфейс в качестве мастера для ретрансляции RA и DHCPv6, а также проксирования NDP.

Служба RA: **отключено**
Конфигурирует режим работы службы RA на данном интерфейсе.

DHCPv6 сервис: **отключено**
Конфигурирует режим работы службы DHCPv6 на этом интерфейсе.

NDP-Прoxy: **отключено**
Конфигурирует режим работы службы NDP прокси на этом интерфейсе.

Рисунок 5 - 15. Eth1. Настройки IPv6 DHCP-сервера

Создание нового интерфейса

Для создания нового интерфейса предназначена кнопка «Добавить новый интерфейс», расположенная внизу таблицы интерфейсов.

При нажатии кнопки «Добавить новый интерфейс» будет открыта страница создания нового сетевого интерфейса, на которой следует указать символьное имя и протокол интерфейса.

Добавить новый интерфейс...

Название: Новое имя интерфейса...

Протокол: UMTS/GPRS/EV-DO

Отмена | Создать интерфейс

Рисунок 5 - 16. Создание нового интерфейса

После ввода основных параметров интерфейса, для его создания следует нажать кнопку «Создать интерфейс». Если основные параметры создаваемого интерфейса были введены без ошибок, произойдет переход на страницу редактирования нового интерфейса.

Удаление интерфейсов

Для удаления интерфейса предназначена кнопка «Удалить», расположенная в строке соответствующего интерфейса.

При нажатии кнопки «Удалить» интерфейс будет помечен для удаления.

LAN: br-lan

Интерфейс помечен для удаления

Перезапустить | Остановить | Изменить | Удалить

Рисунок 5 - 17. Удаление интерфейса

5.1.2. Устройства

Во вкладке «Устройства» можно определить пользовательский список хостов и соответствующее им параметры.

Интерфейсы

Устройства

Основные настройки сети

Устройства

Устройство	Тип	MAC-адрес	MTU		
br-lan	Мост	A6:4F:2D:F5:08:41	1500	Настроить...	Декофигурировать
can0	Сетевое устройство	-	16	Настроить...	Декофигурировать
eth0	Сетевое устройство	A6:4F:2D:F5:08:41	1500	Настроить...	Декофигурировать
eth1	Сетевое устройство	A2:4F:2D:F5:08:41	1500	Настроить...	Декофигурировать

Добавить конфигурацию устройства...

Применить

▼

Сохранить

Очистить

Рисунок 5 - 18. Интерфейсы. Страница «Устройства»

Добавление нового устройства осуществляется нажатием кнопки «Добавить конфигурацию устройства» с последующим указанием имени хоста и соответствующих параметров в таблице.

Добавление конфигурации устройства

Общие опции устройства

Дополнительные опции устройства

Тип устройства

Сетевое устройство

Существующее устройство

can0

MTU

16

MAC-адрес

Длина очереди Tx

10

Включить IPv6

☒

IPv6 MTU

16

DAD отправки

1

Количество отправляемых проб обнаружения дубликатов адресов (DAD)

Рисунок 5 - 19. Интерфейсы. Добавление нового устройства, общие опции

При необходимости можно настроить дополнительные опции добавляемого устройства.

Общие опции устройства

Дополнительные опции устройства

Включить неразборчивый (promiscuous) режим

Фильтр обратного пути

отключено

Принимать локальные данные

Принимать пакеты с локальными адресами источника

Отправлять ICMP перенаправления

Действительность кэша соседей

30000

Время в миллисекундах

Таймаут кэша просроченных соседей

60

Таймаут в секундах

Минимальный срок действия ARP

0

Минимальное требуемое время в секундах, прежде чем запись ARP может быть заменена. Предотвращает атаку ARP-кэша.

Включить поддержку мультикаста

Применяемая версия IGMP

Любая

Применяемая версия MLD

Любая

Рисунок 5 - 20. Интерфейсы. Добавление нового устройства, дополнительные опции

Удалить существующую запись имени хоста можно при помощи кнопки «Деконфигурировать», расположенной в соответствующей строке.

5.1.3. Основные настройки сети

Во вкладке «Основные настройки сети» отображаются дополнительные глобальные параметры сетевой конфигурации устройства.

Интерфейсы

Устройства

Основные настройки сети

Основные настройки сети

Этот раздел не содержит данных

Применить

Сохранить

Очистить

Рисунок 5 - 21. Интерфейсы. Основные настройки сети

При отсутствии доступных для редактирования параметров в данном разделе отображается сообщение: «Этот раздел не содержит данных».

5.2. Маршрутизация

На странице «Маршрутизация» производится настройка статических маршрутов и правил маршрутизации для протокола IPv4. Данные настройки позволяют определить, через какой интерфейс и шлюз можно достичь определённого хоста или сети.

Страница разделена на две вкладки:

- Статические маршруты IPv4;
- Правила IPv4;

5.2.1. Статические маршруты IPv4

В подразделе «Статические маршруты» отображается таблица уже созданных статических маршрутов.

Маршрутизация

Маршрутизация служит для определения через, какой интерфейс и шлюз можно достичь определенного хоста или сети.

Статические маршруты IPv4

Правила IPv4

Статические маршруты IPv4

Интерфейс	Назначение	Шлюз	Метрика	Таблица	Отключить
Этот раздел не содержит данных					

Добавить

Применить

▼

Сохранить

Очистить

Рисунок 5 - 22. Статические маршруты IPv4

Таблица имеет следующие столбцы:

- Сетевой интерфейс, через который будет отправляться трафик для данного маршрута;
- IP-адрес или сеть назначения;
- IP-адрес шлюза, через который должен передаваться трафик к указанному назначению;
- Метрика маршрута (чем меньше значение, тем выше приоритет);
- Идентификатор таблицы маршрутизации, в которую добавляется маршрут;
- «Отключить» — позволяет временно отключить маршрут без его удаления.

Добавление нового статического маршрута осуществляется нажатием кнопки «Добавить» с последующим указанием параметров маршрута в добавленной строке таблицы.

В общих настройках настраиваются интерфейс, к которому привязан статический маршрут, тип маршрута, сеть назначения и шлюз.

Маршрутизация

Общие настройки	Дополнительные настройки
Интерфейс	не определено Определяет имя логического интерфейса родительского (или главного) интерфейса, которому принадлежит этот маршрут
Тип маршрута	unicast Определяет тип маршрута, который необходимо создать
Назначение	0.0.0.0/0 Сетевой адрес
Шлюз	192.168.0.1 Определяет сетевой шлюз. Если опущено, берется шлюз из родительского интерфейса, если таковой имеется, в противном случае создается маршрут с охватом соединения (link scope). Если установлено значение 0.0.0.0, шлюз не будет определен для маршрута
Заккрыть Сохранить	

Рисунок 5 - 23. Добавление нового маршрута. Общие настройки

В дополнительных настройках настраиваются дополнительные параметры статического маршрута: метрика, MTU, таблица маршрутизации, предпочтительный адрес источника и режим привязки шлюза.

Маршрутизация

Общие настройки	Дополнительные настройки
Метрика	0 Определяет метрику маршрута для использования
MTU	1500 Определяет специальный MTU для этого маршрута
Таблица	не определено Целью правила является идентификатор таблицы поиска: числовой индекс таблицы в диапазоне от 0 до 65535 или символичный псевдоним, объявленный в /etc/iproute2/rt_tables. Специальные псевдонимы local (255), main (254) и default (253) также допустимы
Отправитель	авто Определяет предпочтительный адрес источника при отправке в места назначения, охватываемые целью
On-link маршрут	☐ Если включено, шлюз становится on-link, даже если адрес шлюза не соответствует какому-либо префиксу интерфейса
Заккрыть Сохранить	

Рисунок 5 - 24. Добавление нового маршрута. Дополнительные настройки

5.2.2. Правила IPv4

В подразделе «Правила» отображается таблица уже созданных правил маршрутизации. Правила позволяют управлять выбором таблицы маршрутизации в зависимости от параметров пакета.

Маршрутизация

Маршрутизация служит для определения через, какой интерфейс и шлюз можно достичь определенного хоста или сети.

Статические маршруты IPv4

Правила IPv4

Правила IPv4

Приоритет	Входящий интерфейс	Отправитель	Исходящий интерфейс	Получатель	Таблица	Отключить
Этот раздел не содержит данных						

Добавить

Применить

▼

Сохранить

Очистить

Рисунок 5 - 25. Правила маршрутизации IPv4

Таблица имеет следующие столбцы:

- Числовое значение приоритета, определяющее порядок применения правил (чем меньше число, тем выше приоритет);
- Сетевой интерфейс, с которого поступил пакет (опционально);
- IP-адрес или подсеть источника трафика;
- Сетевой интерфейс, через который должен отправляться пакет (опционально);
- IP-адрес или подсеть назначения трафика;
- Идентификатор таблицы маршрутизации, которая будет использоваться для пакетов, соответствующих данному правилу;
- «Отключить» — позволяет временно отключить правило без его удаления.

Для добавления нового правила маршрутизации предназначена кнопка «Добавить».

В общих настройках настраиваются параметры IP-правила: приоритет, тип действия, условия сопоставления, а также таблица маршрутизации, в которую будет направлен трафик при совпадении условий.

Маршрутизация

Общие настройки	Дополнительные настройки
Приоритет	30000 Определяет порядок следования IP-правил
Тип правила	unicast Определяет целевое действие маршрутизации для правила
Входящий интерфейс	не определено Определяет имя входящего логического интерфейса
Отправитель	0.0.0.0/0 Определяет подсеть источника для сопоставления (CIDR-нотация)
Исходящий интерфейс	не определено Определяет имя исходящего логического интерфейса
Получатель	0.0.0.0/0 Определяет подсеть назначения для сопоставления (CIDR-нотация)
Таблица	не определено Целью правила является идентификатор таблицы поиска: числовой индекс таблицы в диапазоне от 0 до 65535 или символьный псевдоним, объявленный в /etc/iproute2/rt_tables. Специальные псевдонимы local (255), main (254) и default (253) также допустимы

ЗакрытьСохранить

Рисунок 5 - 26. Добавление нового правила. Общие настройки

В дополнительных настройках настраиваются расширенные параметры IP-правила: условия сопоставления трафика, действия и дополнительные модификаторы.

Маршрутизация

Общие настройки	Дополнительные настройки
Перейти к правилу	80000 Целью правила является переход к другому правилу, определенному значением его приоритета
Метка межсетевого экрана	0x1/0xf Определяет fwmark и, опционально, его маску для соответствия. Например, 0xFF для соответствия метке 255 или 0x0/0x1 для соответствия любому четному значению метки
Тип сервиса	10 Определяет значение TOS для сопоставления в IP-заголовках
Идентификатор пользователя	1000-1005 Определяет индивидуальный UID или диапазон UID для соответствия. Например, 1000 для соответствия определенному UID или 1000-1005 для соответствия всем UID в указанном диапазоне
Подавитель префикса	24 Отклонять решения о маршрутизации, длина префикса которых меньше или равна указанному значению
Инvertировать совпадение	☐ Если установлено, значение параметров соответствия инвертируется

ЗакрытьСохранить

Рисунок 5 - 27. Добавление нового правила. Дополнительные настройки

5.3. DHCP и DNS

На странице «DHCP и DNS» раздела «Сеть» представлены настройки сетевой службы dnsmasq, которая представляет собой легковесный DNS и DHCP-сервер.

Страница разделена на семь вкладок:

- [Общие настройки](#);

- Файлы resolv и hosts;
- Настройки PXE/TFTP;
- Дополнительные настройки;
- Постоянные аренды;
- Имена устройств;
- Списки IP.

5.3.1. Общие настройки

Общие настройки службы dnsmasq для удобства разделены на группы:

Параметры DNS:

Требуется домен
☒

Не перенаправлять DNS-запросы без точек или частей домена.

Основной
☒

Это единственный DHCP-сервер в локальной сети.

Локальный сервер

Согласно требованиям, имена соответствующие этому домену, никогда не передаются. И разрешаются только из файла DHCP (/etc/config/dhcp) или файла hosts (/etc/hosts).

Локальный домен

Суффикс локального домена, который будет добавлен к DHCP-именам и записи файла hosts (/etc/hosts).

Рисунок 5 - 28. DHCP и DNS. Общие настройки

Параметры журналирования DNS-запросов:

Журналировать запросы
☐

Записывать полученные DNS-запросы в системный журнал.

Рисунок 5 - 29. DHCP и DNS. Общие настройки

Параметры перенаправления запросов DNS:

Перенаправление запросов DNS ✕

+

Список DNS-серверов для перенаправления запросов.

Адреса +

Список доменов для принудительного преобразования в IP-адрес.

Наборы IP адресов +

Список наборов IP-адресов для заполнения указанными IP-адресами доменов.

Защита от DNS Rebinding ☒

Отбрасывать ответы вышестоящего сервера, содержащие адреса [RFC1918](#).

Разрешить localhost ☒

Разрешить ответы внешней сети в диапазоне 127.0.0.0/8 и ::1. Например, для RBL-сервисов.

Белый список доменов +

Список доменов, для которых разрешены ответы RFC1918.

Рисунок 5 - 30. DHCP и DNS. Общие настройки

Дополнительные настройки DNS:

Только локальный DNS ☒

Ограничение сервиса DNS, для подсетей интерфейса использующего DNS.

Не использовать wildcard ☒

Привязывать динамически к интерфейсам, а не по шаблону адреса (рекомендуется по умолчанию для Linux).

Интерфейс для входящих соединений +

Прослушивать только указанные интерфейсы и интерфейс обратной петли, если не исключено явно.

Исключить интерфейсы +

Запретить прослушивание этих интерфейсов.

Рисунок 5 - 31. DHCP и DNS. Общие настройки

5.3.2. Файлы resolv и hosts

Во вкладке «Файлы resolv и hosts» настраиваются пути к вспомогательным файлам DHCP и DNS, а также дополнительные файлы hosts.

Использовать /etc/ethers ☒

Читать /etc/ethers для настройки DHCP сервера.

Файл аренд

/tmp/dhcp.leases

Файл, где хранятся арендованные DHCP-адреса.

Игнорировать файл resolv ☐

Файл resolv

/tmp/resolv.conf.d/resolv.conf.auto

Файл с вышестоящими DNS-серверами.

Игнорировать содержимое файла «/etc/hosts» ☐

Дополнительный hosts файл

/etc/dnsmasq.hosts

+

Рисунок 5 - 32. DHCP и DNS. Файлы resolv и hosts

5.3.3. Настройки PXE/TFTP

Во вкладке «Настройки PXE/TFTP» страницы «DHCP и DNS» расположены параметры для настройки встроенного TFTP-сервера и PXE-опций загрузки.

Включить TFTP-сервер ☐

Включить встроенный одноэкземплярный сервер TFTP.

Специальные PXE опции загрузки для dnsmasq.

Имя файла	Имя сервера	Адрес сервера	Опции DHCP	Network-ID	Принудительно (Force)	Экземпляр
-----------	-------------	---------------	------------	------------	-----------------------	-----------

Этот раздел не содержит данных

Добавить

Применить

▼

Сохранить

Очистить

Рисунок 5 - 33. DHCP и DNS. Настройки PXE/TFTP

Для добавления новой PXE-опции предназначена кнопка «Добавить». При её нажатии открывается страница редактирования параметров PXE-опции.

Имя файла	pxelinux.0
Хост запрашивает указанный файл с сервера загрузки.	
Имя сервера	myNAS
Имя хоста сервера загрузки	
Адрес сервера	192.168.1.2
IP-адрес сервера загрузки	
Опции DHCP	42,192.168.1.4 +
Параметры для Network-ID (примечание: необходим также Network-ID). Например, 42, 192.168.1.4 для NTP-сервера, 3, 192.168.4.4 для маршрута по умолчанию. 0.0.0 означает «адрес системы, на которой запущен dnsmasq».	
Network-ID	не определено
Применить опции DHCP к этой сети (пусто = все клиенты).	
Принудительно (Force)	☐
Всегда отправлять опции DHCP. Это требуется в некоторых случаях, например, для PXELinux.	
Экземпляр	не определено
Экземпляр dnsmasq, к которому привязан данный раздел загрузки. Если не указано, раздел действителен для всех экземпляров dnsmasq.	

Рисунок 5 - 34. DHCP и DNS. Настройки PXE/TFTP

5.3.4. Дополнительные настройки

Во вкладке «Дополнительные настройки» доступны следующие группы настроек:

Логирование и поведение DHCP/DNS:

Подавить логирование	☐	Подавить логирование стандартной работы этих протоколов.
Выделять IP-адреса последовательно	☐	Выделять IP-адреса последовательно, начинать с меньшего доступного адреса.
Фильтровать частные	☒	Не перенаправлять обратные DNS-запросы для локальных сетей.
Фильтровать бесполезные	☐	Не перенаправлять запросы, которые не могут быть обработаны публичными DNS-серверами.
Локализовывать запросы	☒	Локализовать имя хоста в зависимости от запрашиваемой подсети, если доступно несколько IP-адресов.
Расширять имена узлов	☒	Добавить локальный суффикс домена для имен из файла hosts (/etc/hosts).

Рисунок 5 - 35. DHCP и DNS. Дополнительные настройки

Настройки DNSSEC:

DNSSEC ☐

Требуется поддержка внешней сетью DNSSEC; убедитесь, что ответы не подписанного домена действительно поступают от не подписанных доменов.

DNSSEC проверка без знака ☒

Проверять, действительно ли ответы от неподписанных доменов приходят от неподписанных доменов.

Рисунок 5 - 36. DHCP и DNS. Дополнительные настройки

Настройки копирования:

Отключить кэш отрицательных ответов ☐

Не кэшировать отрицательные ответы, например, для несуществующих доменов.

Размер кэша DNS запроса

1000

Количество кэшированных DNS записей (максимум — 10000, 0 — отключить кэширование).

Рисунок 5 - 37. DHCP и DNS. Дополнительные настройки

Настройка файлов конфигурации:

Дополнительный файл серверов

/etc/dnsmasq.servers

Файл со списком вышестоящих DNS-серверов, опционально специфичных для домена. Например server=/domain/1.2.3.4 или server=1.2.3.4.

Рисунок 5 - 38. DHCP и DNS. Дополнительные настройки

Настройка порядка опроса DNS-серверов:

Строгий порядок ☐

DNS сервера будут опрошены в порядке, определенном в resolvfile файле.

Все серверы ☐

Опрашивать все имеющиеся внешние DNS-серверы.

Рисунок 5 - 39. DHCP и DNS. Дополнительные настройки

Настройка обработки NX-доменов:

Переопределение поддельного NX-домена

64.94.110.11

+

Список IP адресов, поставляющих поддельные результаты домена NX.

Рисунок 5 - 40. DHCP и DNS. Дополнительные настройки

Настройка портов:

DNS порт сервера

Порт для входящих DNS-запросов.

DNS порт запроса

Фиксированный порт для исходящих DNS-запросов.

Рисунок 5 - 41. DHCP и DNS. Дополнительные настройки

Настройка ограничений:

Макс. кол-во аренд DHCP аренды

Максимальное количество активных арендованных DHCP-адресов.

Макс. EDNSO размер пакета

Максимально допустимый размер UDP пакетов EDNSO.

Макс. кол-во одновременных запросов

Максимально допустимое количество одновременных DNS-запросов.

Рисунок 5 - 42. DHCP и DNS. Дополнительные настройки

5.3.5. Постоянные аренды

Постоянная аренда используется для присвоения фиксированных IP-адресов и имён DHCP-клиентам.

Постоянная аренда используется для присвоения фиксированных IP-адресов и имён DHCP-клиентам. Постоянная аренда также необходима для статических интерфейсов, в которых обслуживаются только клиенты с присвоенными адресами. Нажмите кнопку «Добавить», чтобы добавить новую запись аренды. «MAC-адрес» идентифицирует хост, «IPv4-адрес» указывает фиксированный адрес, а «Имя хоста» присваивается в качестве символического имени для запрашивающего хоста. Необязательный параметр «Время аренды адреса» может быть использован для того, чтобы установить индивидуальное время аренды, например «12h», «3d» или «infinite».

Имя	MAC-адрес	IPv4-адрес	Срок аренды адреса	DUID	Суффикс IPv6 (hex)
Этот раздел не содержит данных					

[Добавить](#)

DHCP аренды

Имя	IPv4-адрес	MAC-адрес	До конца аренды
Нет активных арендованных адресов			

DHCPv6 аренды

Устройство	IPv6-адрес	DUID	До конца аренды
Нет активных арендованных адресов			

[Применить](#)
[▼](#)
[Сохранить](#)
[Очистить](#)

Рисунок 5 - 43. DHCP и DNS. Постоянные аренды

Добавление новой постоянной аренды осуществляется нажатием кнопки «Добавить» с последующим указанием параметров постоянной аренды в добавленной строке таблицы.

DHCP и DNS

Имя	
MAC-адрес	не определено
IPv4-адрес	не определено
Срок аренды адреса	
DUID	
Суффикс IPv6 (hex)	

Закрыть

Сохранить

Рисунок 5 - 44. DHCP и DNS. Постоянные аренды

Удалить существующую постоянную аренду можно при помощи кнопки «Удалить», расположенной в строке соответствующей записи.

5.3.6. Имена устройств

Во вкладке «Имена устройств» страницы «DHCP и DNS» производится настройка статических привязок доменных имён к IP-адресам.

DHCP и DNS

Dnsmasq содержит в себе DHCP-сервер и DNS-прокси для сетевых экранов NAT

Общие настройки

Файлы resolv и hosts

Настройки PXE/TFTP

Дополнительные настройки

Постоянные аренды

Имена устройств

Списки IP

Имена устройств используются для привязки доменного имени к IP-адресу. Эта настройка избыточна для устройств с бессрочной арендой, но может быть полезна для перепривязки FQDN.

Имя	IP-адрес
Этот раздел не содержит данных	

Добавить

Применить

▼

Сохранить

Очистить

Рисунок 5 - 45. DHCP и DNS. Постоянные аренды

Для добавления новой привязки предназначена кнопка «Добавить». При её нажатии в таблице появляется новая строка для ввода имени и IP-адреса.

DHCP и DNS

Имя	
IP-адрес	-- Сделайте выбор --

Закрыть

Сохранить

Рисунок 5 - 46. DHCP и DNS. Постоянные аренды

5.3.7. Списки IP

В подразделе «Списки IP» страницы «DHCP и DNS» производится настройка статических привязок доменных имён к наборам IP-адресов.

DHCP и DNS

Dnsmasq содержит в себе DHCP-сервер и DNS-прокси для сетевых экранов NAT

[Общие настройки](#)[Файлы resolv и hosts](#)[Настройки PXE/TFTP](#)[Дополнительные настройки](#)[Постоянные аренды](#)[Имена устройств](#)[Списки IP](#)

Список наборов IP-адресов для заполнения указанными IP-адресами доменов.

Список IP	Домен
Этот раздел не содержит данных	

Добавить

Применить

Сохранить

Очистить

Рисунок 5 - 47. DHCP и DNS. Постоянные аренды

Для добавления новой привязки предназначена кнопка «Добавить». При её нажатии в таблице появляется новая строка для ввода имени набора IP-адресов и домена.

DHCP и DNS

Список IP

+

Домен

+

Закреть

Сохранить

Рисунок 5 - 48. DHCP и DNS. Постоянные аренды

5.4. Диагностика

На странице «Диагностика» реализован интерфейс к некоторым диагностическим сетевым утилитам:

- [Пинг-запрос](#);
- [Трассировка](#);
- [DNS-запрос](#);
- [Внешний IP-адрес](#);
- [ARP сканирование](#);

5.4.1. Пинг-запрос

Выполнение диагностики пинг-запроса для IPv4-адреса соответствует выполнению команды:

```
ping -c 5 -W 1 <адрес>
```

Или для IPv6-адреса:

```
ping6 -c 5 <адрес>
```

Результат выполнения пинг-запроса отображается в текстовом виде под формой ввода. Ниже приведён пример вывода успешного пинг-запроса для адреса ya.ru:

```
PING ya.ru (87.250.250.242): 56 data bytes
64 bytes from 87.250.250.242: seq=0 ttl=48 time=16.959 ms
64 bytes from 87.250.250.242: seq=1 ttl=48 time=17.029 ms
64 bytes from 87.250.250.242: seq=2 ttl=48 time=17.197 ms
64 bytes from 87.250.250.242: seq=3 ttl=48 time=17.338 ms
64 bytes from 87.250.250.242: seq=4 ttl=48 time=16.608 ms
--- ya.ru ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 16.608/17.026/17.338 ms
```

5.4.2. Трассировка

Выполнение трассировки для IPv4-адреса соответствует выполнению команды:

```
tracert -q 1 -w 1 -n <адрес>
```

Или для IPv6-адреса:

```
tracert6 -q 1 -w 2 -n <адрес>
```

Результат выполнения пинг-запроса отображается в текстовом виде под формой ввода. Ниже приведён пример вывода успешной трассировки для адреса ya.ru:

```
tracert to ya.ru (87.250.250.242), 30 hops max, 38 byte packets
 1 192.168.0.1 0.598 ms
 2 10.82.190.5 2.009 ms
 3 212.232.64.221 2.274 ms
 4 212.232.64.209 0.857 ms
 5 212.232.64.85 0.980 ms
 6 212.232.67.218 1.172 ms
 7 188.65.69.56 0.823 ms
 8 188.65.69.65 1.152 ms
 9 46.19.184.17 1.225 ms
10 46.19.184.5 1.090 ms
11 194.226.100.90 1.319 ms
12 *
13 87.250.250.242 17.069 ms
```

5.4.3. DNS-запрос

Выполнение DNS-запроса адреса соответствует выполнению команды:

```
nslookup <адрес>
```

Результат выполнения пинг-запроса отображается в текстовом виде под формой ввода. Ниже приведён пример вывода успешного DNS-запроса для адреса ya.ru:

```
Server: 127.0.0.1
Address: 127.0.0.1#53
Name: ya.ru
Address 1: 87.250.250.242
Address 2: 2a02:6b8::2:242
```

5.4.4. Внешний IP-адрес

«Определить внешний IP-адрес» — кнопка, при нажатии на которую выполняется запрос к внешнему серверу для определения публичного IP-адреса. После выполнения запроса адрес отображается в соответствующем поле.

5.4.5. ARP сканирование

Подраздел «ARP сканирование» позволяет выполнить сканирование локальной сети для обнаружения устройств по протоколу ARP.

5.5. Межсетевой экран

Настройки межсетевого экрана (брандмауэра) расположены на странице «Межсетевой экран» и разделены на вкладки:

- [Общие настройки](#);
- [Перенаправление портов](#);
- [Правила для трафика](#);
- [Правила NAT](#);
- [Пользовательские правила](#);

5.5.1. Общие настройки

Во вкладке «Общие настройки» находятся основные настройки межсетевого экрана и настройка зон.

В общих настройках задаются параметры защиты от SYN-flood, фильтрация некорректных пакетов и политика обработки трафика.

Включить защиту от SYN-flood атак ☒Отбрасывать некорректные пакеты ☐Входящий трафик отвергать ▼Исходящий трафик принимать ▼Перенаправление отвергать ▼

Рисунок 5 - 49. Общие настройки межсетевого экрана

Под общими настройками расположена таблица зон с их основными параметрами.

Зоны

Зона ⇒ Перенаправления	Входящий трафик	Исходящий трафик	Перенаправление	Маскарадинг	
lan ⇒ wan	принимать ▼	принимать ▼	принимать ▼	☐	☰ Изменить Удалить
wan ⇒ REJECT	отвергать ▼	принимать ▼	отвергать ▼	☒	☰ Изменить Удалить
Добавить					

Рисунок 5 - 50. Настройка зон межсетевого экрана.



Чекбокс «Маскарадинг» включает или отключает трансляцию IP-адресов для указанной зоны.

Для редактирования зоны нажмите «Изменить» в соответствующей строке. Настройки зоны на несколько групп.

В группе «Общие настройки» представлены основные параметры зоны и политика перенаправления трафика.

Межсетевой экран - Настройка зон

Общие настройкиДополнительные настройкиОтслеживание соединений (conntrack)Дополнительные аргументы iptables

Страница содержит общие свойства "lan". Режимы 'Входящий трафик' и 'Исходящий трафик' устанавливают политики по умолчанию для трафика, поступающего и покидающего эту зону, в то время как режим 'Перенаправление' описывает политику перенаправления трафика между различными сетями внутри зоны. 'Использовать сети' указывает, какие доступные сети являются членами этой зоны.

Название

lan

Входящий трафик

принимать

Исходящий трафик

принимать

Перенаправление

принимать

Маскарадинг

☐

Ограничение MSS

☐

Охватываемые сети

lan0:lan1:

Данные настройки управляют политиками перенаправления трафика между этой (lan) и другими зонами. Трафиком 'зон-назначения' является перенаправленный трафик 'исходящий из lan'. Трафиком 'зон-источников' является трафик 'направленный в lan'. Перенаправление является 'односторонним', то есть перенаправление из lan в wan 'не' допускает перенаправление трафика из wan в lan.

Разрешить перенаправление в 'зону назначения':

wan(пусто)

Разрешить перенаправление из 'зон источников':

не определено

Закрыть

Сохранить

Рисунок 5 - 51. Настройка зон. Общие настройки

В группе «Дополнительные настройки» настраиваются классификация трафика (по устройствам или подсетям), привязка к протоколу, параметры маскарадинга и журналирование зоны.

Межсетевой экран - Настройка зон

Общие настройкиДополнительные настройкиОтслеживание соединений (conntrack)Дополнительные аргументы iptables

Данные настройки управляют политиками перенаправления трафика между этой (lan) и другими зонами. Трафиком 'зон-назначения' является перенаправленный трафик 'исходящий из lan'. Трафиком 'зон-источников' является трафик 'направленный в lan'. Перенаправление является 'односторонним', то есть перенаправление из lan в wan 'не' допускает перенаправление трафика из wan в lan.

Охватываемые устройства

не определено

Используйте эту опцию для классификации трафика зоны по сетевым устройствам, управляемым не через `uci`.

Охватываемые подсети

Используйте эту опцию для классификации трафика зоны по источнику или подсети назначения вместо сети или устройств.

Использовать протокол

IPv4 и IPv6

Использовать маскарадинг только для указанных подсетей-отправителей

0.0.0.0/0

Использовать маскарадинг только для указанных подсетей-получателей

0.0.0.0/0

Включить журналирование в этой зоне

☐

Закрыть

Сохранить

Рисунок 5 - 52. Настройка зон. Дополнительные настройки

В группе «Отслеживание соединений (conntrack)» настраиваются обработка недействительного трафика и автоматическое назначение помощников отслеживания соединений.

Межсетевой экран - Настройка зон

Общие настройки

Дополнительные настройки

Отслеживание соединений (conntrack)

Дополнительные аргументы iptables

Разрешить «недействительный» трафик ☐

Не устанавливать дополнительные правила для отклонения перенаправляемого трафика с состоянием *недействительный* (*invalid*). Это может потребоваться для сложных настроек асимметричной маршрутизации.

Автоматическое назначение помощников ☒

Автоматическое назначение помощников отслеживания соединений (conntrack) на основе протокола и порта трафика

Закреть

Сохранить

Рисунок 5 - 53. Настройка зон. «Отслеживание соединений (conntrack)»

В группе «Дополнительные аргументы iptables» настраиваются дополнительные аргументы iptables для классификации трафика по источнику и назначению.

Межсетевой экран - Настройка зон

Общие настройки

Дополнительные настройки

Отслеживание соединений (conntrack)

Дополнительные аргументы iptables

Передача аргументов iptables в правилах классификации входящего и исходящего трафика позволяет сопоставлять пакеты, основанные на других критериях, нежели чем интерфейсы или подсети. Эти опции следует использовать с особой осторожностью, так как неверные значения могут привести к нарушению работы правил межсетевого экрана, полностью открывая доступ ко всем службам системы.

Дополнительные аргументы для источника

Дополнительные аргументы iptables для классификации трафика зоны источника, например -p tcp --sport 443 для соответствия только входящему HTTPS трафику.

Дополнительные аргументы для назначения

Дополнительные аргументы iptables для классификации трафика зоны назначения, например -p tcp --dport 443 для соответствия только исходящему HTTPS трафику.

Закреть

Сохранить

Рисунок 5 - 54. Настройка зон. «Дополнительные аргументы iptables»

Для добавления новой зоны предназначена кнопка «Добавить», расположенная снизу таблицы зон. При этом открывается такая же страница редактирования параметров зоны, как и при изменении существующей зоны.

5.5.2. Перенаправление портов

Во вкладке «Перенаправление портов» находятся настройки правил перенаправления портов.

Межсетевой экран - Перенаправление портов

Перенаправленные портов позволяет удалённым компьютерам из Интернета соединяться с компьютером или службой внутри частной локальной сети.

Перенаправление портов

Название	Соответствие	Действие	Включить
Этот раздел не содержит данных			
			Добавить
		Применить	Сохранить
			Очистить

Рисунок 5 - 55. Межсетевой экран. Перенаправление портов

Страница добавления правила перенаправления портов открывается при нажатии кнопки «Добавить». Настройки перенаправления разделены на несколько групп.

В группе «Общие настройки» настраиваются зоны источника и назначения, протоколы (TCP/UDP), внешний и внутренний порт, а также внутренний IP-адрес.

Межсетевой экран - Перенаправление портов - Перенаправление без имени

Общие настройкиДополнительные настройки

Название	Перенаправление без имени		
Протокол	TCP	UDP	▼
Зона источника	wan(пусто) ▼		
Внешний порт	Порт или диапазон портов, входящие подключения на который будут перенаправляться на внутренний порт внутреннего IP-адреса (см. ниже)		
Зона назначения	lan(пусто) ▼		
Внутренний IP-адрес	любой ▼ Перенаправлять трафик на указанный IP-адрес		
Внутренний порт	любой Перенаправлять трафик на указанный порт или диапазон портов внутреннего IP-адреса		

ЗакретьСохранить

Рисунок 5 - 56. Добавление правила перенаправление портов. Общие настройки

В группе «Дополнительные настройки» настраиваются условия фильтрации, параметры NAT Loopback, а также сопоставление с помощником, меткой и ограничениями.

Общие настройки

Дополнительные настройки

MAC-адрес источника

-- добавить MAC-адрес --

Применять правило только для входящего трафика от этих MAC-адресов.

IP-адрес источника

любой

Применять правило только для входящего трафика от этого IP-адреса или диапазона адресов.

Порт источника

любой

Применять правило только для входящего трафика от указанного порта или диапазона портов клиентского хоста

Внешний IP-адрес

любой

Применять правило только для входящих подключений на указанный IP-адрес.

Включить NAT Loopback

☒

IP-адрес источника петли (Loopback)

Использовать внутренний IP-адрес

Определяет, использовать внешний или внутренний IP-адрес для отраженного трафика.

Соответствие помощнику

любой

Сопоставление трафика с помощью указанного помощника отслеживания соединений.

Соответствие метки

Соответствие определённой метке брандмауэра или диапазона различных меток.

Соответствие по ограничениям

без ограничений

Ограничивает сопоставление трафика указанной скорости.

Дополнительные аргументы

Передаёт дополнительные аргументы таблице iptables. Используйте с осторожностью!

Закреть

Сохранить

Рисунок 5 - 57. Добавление правила перенаправление портов. Дополнительные настройки

5.5.3. Правила для трафика

Во вкладке «Правила для трафика» находятся настройки правил межсетевого экрана для входящего, исходящего и перенаправляемого трафика.

Межсетевой экран - Правила для трафика

Правила для трафика определяют политику прохождения пакетов между разными зонами, например, запрет трафика между некоторыми хостами или открытие WAN-портов маршрутизатора.

Правила для трафика

Название	Соответствие	Действие	Включить	
Allow-DHCP-Renew	Входящий IPv4, протокол UDP Из wan В это устройство , порт 68	Разрешить входящий трафик	☒	Изменить Удалить
Allow-Ping	Входящий IPv4, протокол ICMP Из wan В это устройство	Разрешить входящий трафик	☒	Изменить Удалить
Allow-IGMP	Входящий IPv4, протокол IGMP Из wan В это устройство	Разрешить входящий трафик	☒	Изменить Удалить
Allow-DHCPv6	Входящий IPv6, протокол UDP Из wan В это устройство , порт 546	Разрешить входящий трафик	☒	Изменить Удалить
Allow-MLD	Входящий IPv6, протокол ICMP Из wan , IP-адрес fe80::/10 В это устройство	Разрешить входящий трафик	☒	Изменить Удалить
...	Входящий IPv6, протокол ICMP Из wan		☒	Изменить

Рисунок 5 - 58. Правила для трафика межсетевого экрана

Страница редактирования правила для трафика открывается при нажатии кнопки «Изменить» в строке соответствующего правила. Настройки разделены на несколько групп. В группе «Общие настройки» содержатся основные параметры правила для трафика.

Межсетевой экран - Правила для трафика - Allow-DHCP-Renew

Общие настройки	Дополнительные настройки	Временные ограничения
Название	Allow-DHCP-Renew	
Протокол	UDP	
Зона источника	wan(пусто)	
Адрес источника	-- добавить IP-адрес --	
Порт источника	любой	
Зона назначения	Устройство(ввод)	
Адрес назначения	-- добавить IP-адрес --	
Порт назначения	68	
Действие	принимать	
		Заккрыть Сохранить

Рисунок 5 - 59. Правила для трафика. Общие настройки

Группа «Дополнительные настройки» содержит параметры, специфичные для конкретного протокола или типа правила.

Межсетевой экран - Правила для трафика - Allow-DHCP-Renew

Общие настройки	Дополнительные настройки	Временные ограничения
Соответствие устройству	не определено	
Использовать протокол	Только IPv4	
MAC-адрес источника	-- добавить MAC-адрес --	
Соответствие помощнику	любой	
	Сопоставление трафика с помощью указанного помощника отслеживания соединений.	
Соответствие метки		
	Соответствие определённой метке брандмауэра или диапазона различных меток.	
Соответствие DSCP	любой	
	Сопоставляет трафик с указанной DSCP-маркировкой.	
Соответствие по ограничениям	без ограничений	
	Ограничивает сопоставление трафика указанной скорости.	
Дополнительные аргументы		
	Передаёт дополнительные аргументы таблице iptables. Используйте с осторожностью!	
		Заккрыть Сохранить

Рисунок 5 - 60. Правила для трафика. Дополнительные настройки

Группа «Временные ограничения» содержит настройки периода действия правила.

Межсетевой экран - Правила для трафика - Allow-DHCP-Renew

Общие настройки

Дополнительные настройки

Временные ограничения

Дни недели

Любой день

▼

Дни месяца

Любой день

▼

Время начала (чч:мм:сс)

Время окончания (чч:мм:сс)

Дата начала (год-мес-день)

Дата окончания (год-мес-день)

Время UTC

☐

Закреть

Сохранить

Рисунок 5 - 61. Правила для трафика. Временные ограничения

5.5.4. Правила NAT

Во вкладке «Правила NAT» находятся настройки правил трансляции сетевых адресов (NAT).

Межсетевой экран - Правила NAT

Правила NAT позволяют точно контролировать IP-адрес источника в исходящем или перенаправляемом трафике.

Правила NAT

Название	Соответствие	Действие	Включить
Этот раздел не содержит данных			

Добавить

Применить

▼

Сохранить

Очистить

Рисунок 5 - 62. Правила NAT межсетевого экрана

5.5.5. Пользовательские правила

Во вкладке «Пользовательские правила» находятся настройки пользовательских правил межсетевого экрана.

Межсетевой экран - Пользовательские правила

Пользовательские правила позволяют выполнять произвольные команды iptables, которые не охвачены рамками межсетевого экрана. Команды выполняются после каждой перезагрузки межсетевого экрана, сразу после загрузки набора правил по умолчанию.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

Сохранить

Рисунок 5 - 63. Пользовательские правила межсетевого экрана

Chapter 6. VPN

6.1. OpenVPN

Страница «OpenVPN» раздела «VPN» позволяет [управлять](#) экземплярами OpenVPN-серверов и клиентов, [создавать](#) новые конфигурации и [загружать](#) готовые файлы .ovpn.

6.1.1. Экземпляры OpenVPN

В подразделе «Экземпляры OpenVPN» отображается таблица всех настроенных экземпляров OpenVPN с их текущим состоянием.

OpenVPN

Экземпляры OpenVPN

Список настроенных экземпляров OpenVPN и их текущее состояние

Имя	Включено	Запущено	Старт/Стоп	Порт	Протокол		
custom_config	☐	нет	Запустить	-	-	Изменить	Удалить
sample_server	☐	нет	Запустить	1194	udp	Изменить	Удалить
sample_client	☐	нет	Запустить	-	udp	Изменить	Удалить

Рисунок 6 - 1. VPN. Экземпляры OpenVPN

Страница редактирования экземпляра OpenVPN открывается при нажатии кнопки «Изменить» в строке соответствующего экземпляра. На странице представлены основные параметры конфигурации OpenVPN.

verb	3	▼
Задайте детализацию ведения журнала		
port	1194	
Номер локального и удалённого TCP/UDP порта		
server	10.8.0.0 255.255.255.0	
Настроить режим сервера		
keepalive	10 120	
Вспомогательная команда предназначенная для упрощения выражений '-ping' и '-ping-restart' в режиме настройки сервера		
ca	/etc/openvpn/ca.crt (Файл не доступен)	
Центр сертификации		
dh	/etc/openvpn/dh2048.pem (Файл не доступен)	
Файл параметров Диффи Хелмана		
cert	/etc/openvpn/server.crt (Файл не доступен)	
Локальный сертификат		
key	/etc/openvpn/server.key (Файл не доступен)	
Локальный Приватный ключ		
proto	udp ▼	
Использовать протокол		
-- Дополнительно -- ▼		Добавить

Рисунок 6 - 2. VPN. Редактирование экземпляра OpenVPN (на примере «sample_server»)

6.1.2. Конфигурация на основе шаблонов

В подразделе «Конфигурация на основе шаблонов» можно быстро создать новый экземпляр OpenVPN, выбрав один из предустановленных шаблонов.

Конфигурация на основе шаблонов

Имя экземпляра	Выберите шаблон... ▼	Добавить
----------------	----------------------	----------

Рисунок 6 - 3. VPN. Конфигурация на основе шаблонов

6.1.3. Загрузка конфигурационного файла OVPN

В подразделе «Загрузка конфигурационного файла OVPN» можно загрузить готовый конфигурационный файл OpenVPN (с расширением .ovpn) для создания нового экземпляра.

Загрузка конфигуционного файла OVPN

Выберите файл

Файл не выбран

Загрузить

Рисунок 6 - 4. VPN. Загрузка конфигуционного файла OVPN

Chapter 7. Статистика

Раздел «Статистика» главного меню Web-интерфейса позволяет просматривать графики системных параметров, собранные службой collectd и визуализированные с помощью RRDtool. Здесь отображается информация об использовании процессора, сетевых интерфейсов, загрузке системы, оперативной памяти и температуре устройства.

7.1. Графики

Страница «Графики» раздела «Статистика» предназначена для просмотра графиков статистики. В верхней части страницы расположены элементы управления для выбора хоста, временного интервала и частоты обновления.

Страница разделена на `itsnm` подразделов:

- [Статистика](#);
- [CPU](#);
- [Интерфейсы](#);
- [Загрузка системы](#);
- [Оперативная память \(RAM\)](#);
- [Thermal](#).

7.1.1. Статистика

В подразделе «Статистика» расположены элементы управления.

Статистика

titan	▼	Показать хост »
1hour	▼	Показать за промежуток »
Не обновлять	▼	Применить интервал »

Рисунок 7 - 1. Статистика. Элементы управления

- «Показать хост» — выпадающий список для выбора хоста, статистику которого необходимо отобразить;
- «Показать за промежуток» — выпадающий список для выбора временного интервала отображения графиков;
- «Применить интервал» — кнопка для применения выбранного временного интервала;
- «Не обновлять» — выпадающий список для выбора частоты автоматического обновления графиков.

7.1.2. CPU

В подразделе «CPU» отображается график использования процессора для каждого ядра.

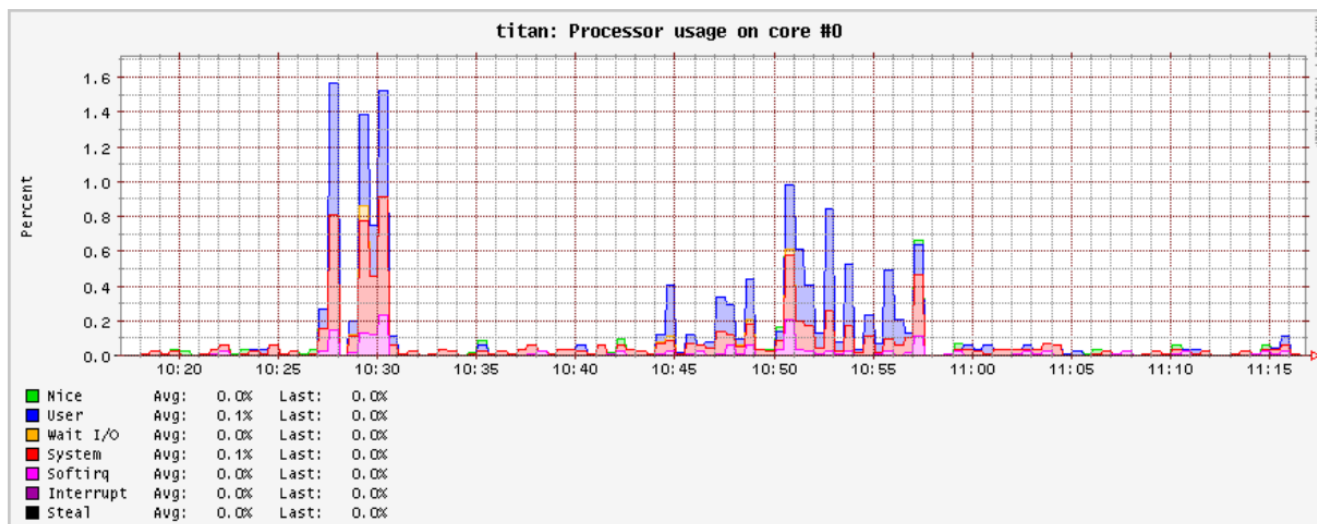


Рисунок 7 - 2. Статистика. График использования CPU (пример для core #0)

На графике показано распределение времени процессора по типам операций:

- Nice — время, затраченное на процессы с изменённым приоритетом;
- User — время выполнения пользовательских процессов;
- Wait I/O — время ожидания операций ввода-вывода;
- System — время выполнения системных вызовов;
- Softirq — время обработки программных прерываний;
- Interrupt — время обработки аппаратных прерываний;
- Steal — время, «украденное» гипервизором (для виртуальных машин).

7.1.3. Интерфейсы

В подразделе «Интерфейсы» отображаются графики сетевой активности для каждого физического интерфейса (eth0, eth1).

Для каждого интерфейса строится два графика:

- Верхний график — скорость передачи и приёма данных в байтах/с;
- Нижний график — количество пакетов в секунду и ошибки.



Рисунок 7 - 3. Статистика. Графики сетевого интерфейса (пример для eth1)

7.1.4. Загрузка системы

В подразделе «Загрузка системы» отображается график средней загрузки системы за различные промежутки времени:

- Средняя загрузка за 1 минуту;
- Средняя загрузка за 5 минут;
- Средняя загрузка за 15 минут.

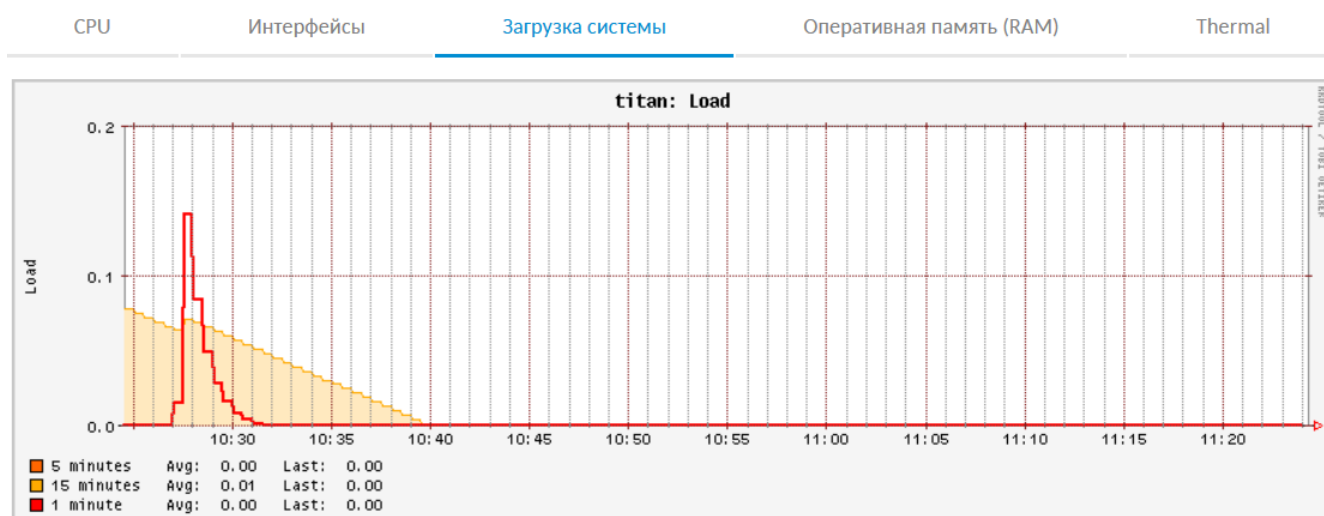


Рисунок 7 - 4. Статистика. График загрузки системы

7.1.5. Оперативная память (RAM)

В подразделе «Оперативная память (RAM)» отображается график использования оперативной памяти с разбивкой по типам:

- Free — свободная память;
- Buffered — память, используемая для буферов;
- Cached — кэшированная память;
- Used — используемая память.

Для каждого типа отображается среднее (Avg) и последнее (Last) значения.

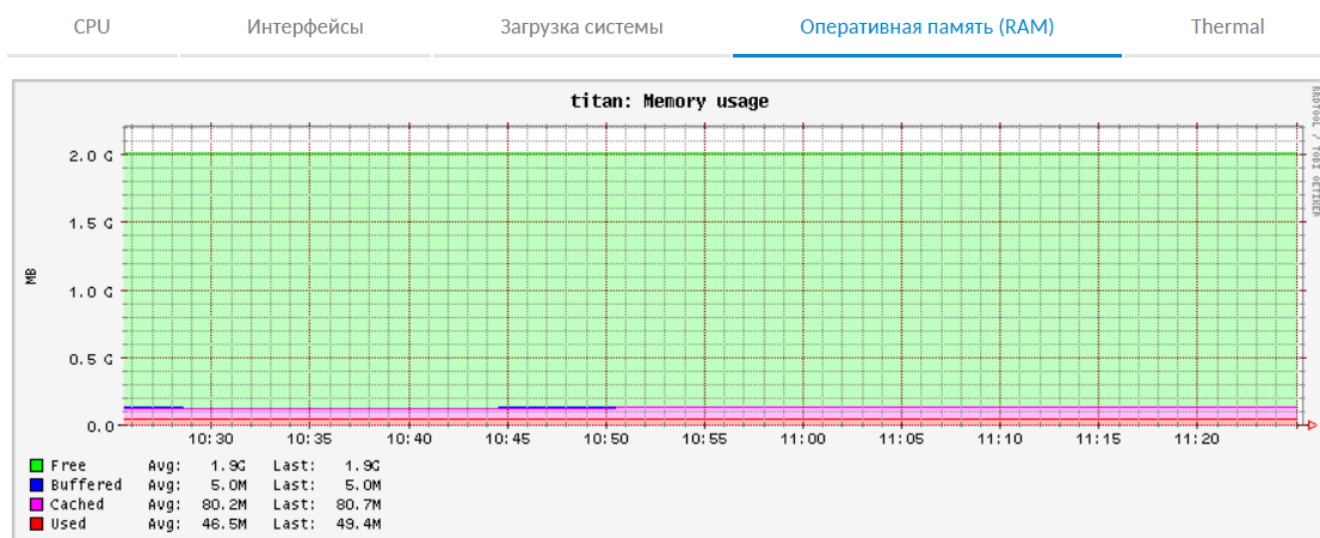


Рисунок 7 - 5. Статистика. График использования оперативной памяти

7.1.6. Thermal

В подразделе «Thermal» отображаются графики температуры устройства для каждого температурного датчика (thermal_zone0, thermal_zone1 и др.). График показывает изменение температуры в градусах Цельсия с течением времени.

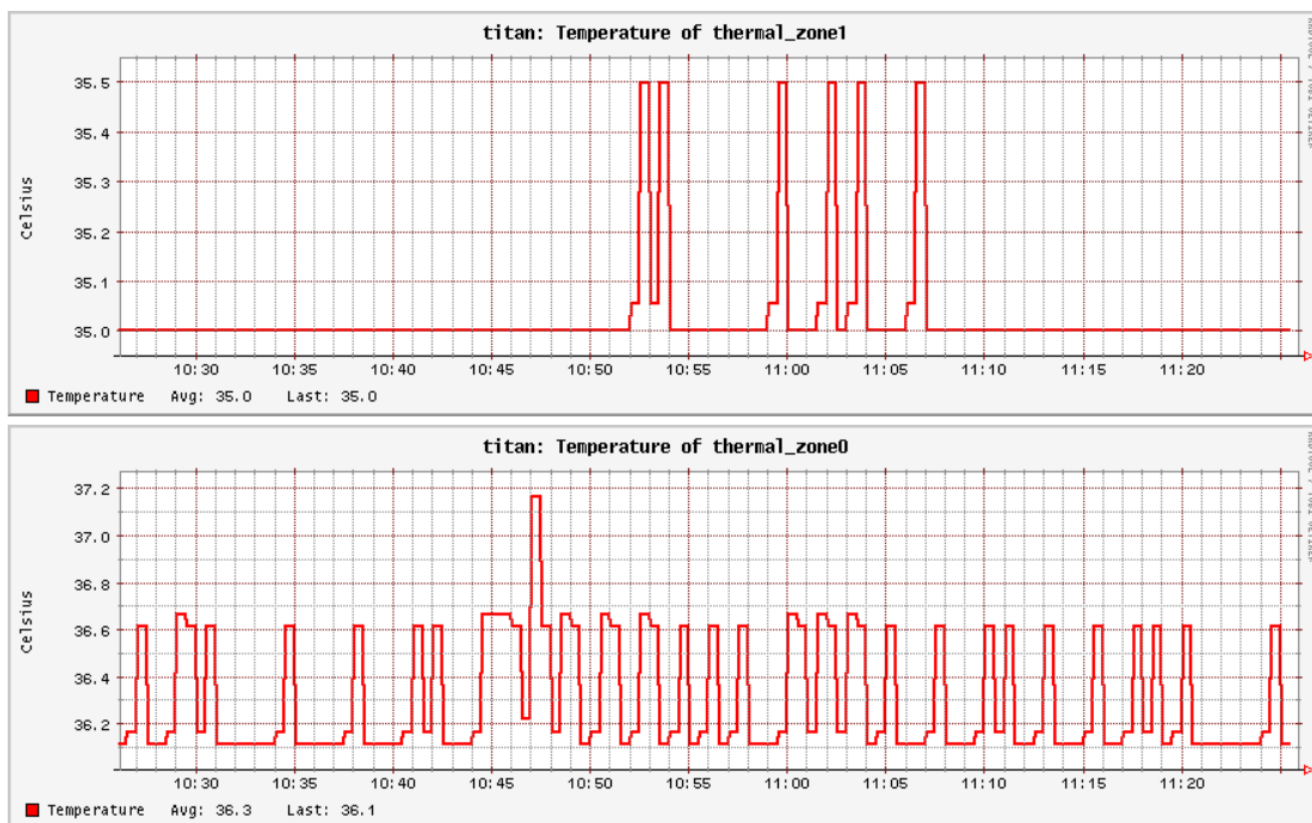


Рисунок 7 - 6. Статистика. Графики температуры (*thermal_zone0* и *thermal_zone1*)

7.2. Настройки статистики

Страница «Настройки collectd» раздела «Статистика» позволяет сконфигурировать службу сбора статистики, а также включить/настроить необходимые плагины.

Страница разделена на четыре вкладки:

- [Настройки collectd](#);
- [Основные плагины](#);
- [Сетевые плагины](#);
- [Плагины вывода](#).

7.2.1. Настройки collectd

Во вкладке «Настройки collectd» задаются общие параметры службы сбора статистики.

Имя	titan
Основная папка приложения	/var/run/collectd
Папка с config файлом	/etc/collectd/conf.d/*.conf
Папка с плагинами collectd	/usr/lib64/collectd
Используемый PID-файл	/var/run/collectd.pid
Файл с определением набора данных	/usr/share/collectd/types.db
Интервал сбора данных	30
	Секунд(ы)
Количество потоков сбора данных	2

Рисунок 7 - 7. Настройки статистики. Collectd.

7.2.2. Основные плагины

Во вкладке «Основные плагины» отображается список плагинов для сбора системной статистики. Если плагин поддерживает дополнительные параметры, для него доступна кнопка «Настроить...».

Страница настройки плагина «CPU» позволяет сконфигурировать параметры сбора статистики об использовании процессора.

Настройка плагина «CPU»

Плагин «CPU» собирает статистику об использовании процессора.

Включить этот плагин	☒
Отдельно для каждого процессора	☒
	При установке данной опции график CPU не будет агрегировать данные всех процессоров в системе
Отдельно для каждого состояния	☒
	При включении, отображаются метрики для каждого состояния (system, user, idle)
Показывать состояние простоя (idle)	☐
	Отображать значения состояния простоя (idle)
Отображать в процентах	☒
	При включении, отображаются значения в процентах

Рисунок 7 - 8. Настройка плагина «CPU»

Страница настройки плагина «Disk» позволяет сконфигурировать параметры сбора статистики использования дисков и разделов

Настройка плагина «Disk»

Плагин «Disk» собирает подробную статистику по выбранным разделам или дискам.

Включить этот плагин

☒

Мониторить диски и разделы

hda1

hdb

-- Сделайте выбор --

×

×

▼

Если ни один диск не будет выбран, будут отслеживаться все.

Собирать статистику со всех кроме указанных

☐

Рисунок 7 - 9. Настройка плагина «Disk»

Страница настройки плагина «Ехес» позволяет сконфигурировать выполнение внешних команд при достижении определённых значений порогов. Плагин «Ехес» выполняет внешнюю команду в случае, когда определённые значения достигают заданного порога.

Настройка плагина «Ехес»

Плагин «Ехес» выполняет внешнюю команду в случае, когда определённые значения достигают заданного порога.

Включить этот плагин

☒

Добавить команду для чтения значений

Скрипт	Пользователь	Группа	
/usr/bin/stat-dhcpusers	nobody	nogroup	Удалить
			Добавить

Здесь вы можете определить внешние команды, которые будут выполнены для чтения определенных значений. Значения будут считаны со стандартного вывода.

Добавить команду уведомления

Скрипт	Пользователь	Группа	
/usr/bin/stat-dhcpusers	nobody	nogroup	Удалить
			Добавить

Здесь вы можете определить внешние команды, которые будут выполнены, когда значения достигнут определенного порога. Значения будут переданы на стандартный ввод вызванным программам.

Рисунок 7 - 10. Настройка плагина «Ехес»

Страница настройки плагина «IRQ» позволяет сконфигурировать параметры сбора статистики по аппаратным прерываниям

Настройка плагина «IRQ»

Плагин «IRQ» собирает статистику по выбранным прерываниям. Если ни одно прерывание не выбрано, сбор статистики будет проводиться по всем прерываниям.

Включить этот плагин

☒

Мониторить прерывания

2

3

4

7

-- Сделайте выбор --

×

×

×

×

▼

Собирать статистику со всех кроме указанных

☐

Рисунок 7 - 11. Настройка плагина «IRQ»

104

Страница настройки плагина «Оперативная память (RAM)» позволяет сконфигурировать параметры сбора статистики об использовании оперативной памяти.

Настройка плагина «Оперативная память (RAM)»

Плагин «Оперативная память (RAM)» собирает статистику об использовании памяти.

Включить этот плагин

☒

Абсолютные значения

☒

При включении, отображаются абсолютные значения

Значения в процентах

☐

При включении, отображаются значения в процентах

Рисунок 7 - 12. Настройка плагина «Оперативная память (RAM)»

Страница настройки плагина «Процессы» позволяет сконфигурировать параметры сбора статистики по выбранным процессам.

Настройка плагина «Процессы»

Плагин «Процессы» собирает информацию, такую как время CPU, ошибки страниц и использование памяти выбранных процессов.

Включить этот плагин

☒

Мониторить процессы

uhttpd

✕

dnsmasq

✕

dropbear

✕

+

Собирать информацию об открытых файловых дескрипторах (CollectFileDescriptor)

☒

Рисунок 7 - 13. Настройка плагина «Процессы»

Страница настройки плагина «Thermal» позволяет сконфигурировать параметры сбора статистики с температурных датчиков устройства.

Настройка плагина «Thermal»

Плагин «Thermal» собирает информацию с температурных сенсоров. Данные будут считываться из /sys/class/thermal/* /temp ('*' обозначает сенсор устройства , как-то thermal_zone1)

Включить этот плагин

☒

Мониторить устройство(а) / зону(ы) нагрева

thermal_zone0

✕

thermal_zone1

✕

+

Если пусто = отслеживать все

Собирать статистику со всех кроме указанных

☐

Рисунок 7 - 14. Настройка плагина «Thermal»

7.2.3. Сетевые плагины

Во вкладке «Сетевые плагины» отображается список плагинов для сбора сетевой статистики. Если плагин поддерживает дополнительные параметры, для него доступна кнопка «Настроить...».

Страница настройки плагина «Интерфейсы» позволяет указать, за какими сетевыми интерфейсами следует собирать статистику.

Настройка плагина «Интерфейсы»

Плагин «Интерфейсы» собирает статистику на выбранных сетевых интерфейсах.

Включить этот плагин ☒

Мониторить интерфейсы

 eth0

 eth1

 usb0

Собирать статистику со всех кроме указанных ☐

Рисунок 7 - 15. Настройка плагина «Интерфейсы»

Страница настройки плагина «Firewall» позволяет собирать статистику с определённых правил межсетевого экрана.

Настройка плагина «Iptables»

Плагин «Iptables» собирает статистику с определённых правил межсетевого экрана.

Включить этот плагин ☒

Соответствие IPv4 правилам iptables

Здесь вы можете указать различные критерии, по которым будут выбраны правила для сбора статистики.

Имя экземпляра	Таблица	Цепочка	Комментарий / номер правила	
LAN-Clients-traffic	nat	luci_fw_postrouting	не определено	Удалить
WLAN-Clients-traffic	nat	luci_fw_postrouting	не определено	Удалить

Добавить селектор правил IPv4

Соответствие IPv6 правилам iptables

Здесь вы можете указать различные критерии, по которым будут выбраны правила для сбора статистики.

Имя экземпляра	Таблица	Цепочка	Комментарий / номер правила
----------------	---------	---------	-----------------------------

Этот раздел не содержит данных

Добавить селектор правил IPv6

Рисунок 7 - 16. Настройка плагина «Firewall»

Страница настройки плагина «Пинг-запрос» позволяет сконфигурировать отправку ICMP-запросов выбранным хостам и измерение времени отклика.

Настройка плагина «Пинг-запрос»

Плагин «Пинг-запрос» посылает ICMP-запросы выбранным хостам и измеряет время отклика.

Включить этот плагин ☒

Мониторить хосты

Тип адреса

TTL для ping-пакетов

Интервал для ping-запросов

Секунд(ы)

Максимальное количество пропущенных пакетов

Если хост не ответил на указанное количество пакетов подряд, повторно разрешить имя хоста в DNS. Это полезно для хостов с динамическим DNS. По умолчанию -1 = отключено.

Рисунок 7 - 17. Настройка плагина «Пинг-запрос»

Страница настройки плагина «TCPConns» позволяет собирать информацию об открытых TCP-соединениях на выбранных портах.

Настройка плагина «TCPConns»

Плагин «TCPConns» собирает информацию об открытых TCP соединениях на выбранных портах.

Включить этот плагин ☒

Собирать статистику со всех портов для входящих соединений ☐

Мониторить локальные порты

Мониторить удаленные порты

Рисунок 7 - 18. Настройка плагина «TCPConns»

7.2.4. Плагины вывода

Во вкладке «Плагины вывода» отображается список плагинов, определяющих, куда и как сохранять собранную статистику. Если плагин поддерживает дополнительные параметры, для него доступна кнопка «Настроить...».

Страница настройки плагина «RRDTool» позволяет сконфигурировать параметры сохранения статистики в RRD-файлы.

Настройка плагина «RRDTool»

Плагин «RRDTool» сохраняет статистику в формате RRD для последующего построения диаграмм.

Внимание: установка неверных параметров может привести к высокому потреблению памяти устройства. Это может привести к зависанию устройства!

Включить этот плагин

☒

Папка с данными

/tmp/rrd

Внимание: все операции осуществляются под пользователем «nobody», соответственно все файлы *.rrd и папки будут доступны любому пользователю.

Базовый интервал между данными в RRD (StepSize)

30

Секунд(ы)

Максимальное количество секунд между двумя обновлениями (HeartBeat)

60

Секунд(ы)

Создавать только средние RRA

☒

позволяет уменьшить размер RRD

Сохраняемые промежутки времени

1hour

×

1day

×

1week

×

1month

×

1year

×

+

Список временных интервалов для хранения в базе данных RRD. Например, «1hour 1day 14day». Допустимые типы временных интервалов: min, h, hour(s), d, day(s), w, week(s), m, month(s), y, year(s)

Количество «поколений» данных в архиве RRA

288

Часть интервала консолидации, которая может состоять из неопределенных значений (*UNKNOWN*), если консолидированное значение может быть определено (известно)

0.1

Кэшировать собранную статистику в течении

0

Секунд(ы)

Сбросить кэш после

0

Секунд(ы)

Рисунок 7 - 19. Настройка плагина «RRDTool»

Страница настройки плагина «Network» позволяет отправлять статистику по сети на удалённый сервер collectd.

Настройка плагина «Сеть»

Плагин «Сеть» предоставляет возможность сетевого обмена данными между разными сервисами collectd. Collectd может работать в режиме сервера или клиента. В режиме клиента, локальная статистика передается collectd-серверу, в режиме сервера collectd собирает статистику с удаленных хостов.

Включить этот плагин ☒

ТTL для сетевых пакетов

Максимальный размер пакета
Установка максимального размера датаграмм, отправляемых по сети

Включить пересылку ☐
Перенаправление между локальным адресом и адресом сервера

Включить статистику ☐
Собирать статистику о самом сетевом плагине

Прослушивать интерфейсы

Хост для входящих соединений	Порт
Этот раздел не содержит данных	

[Добавить](#)

Строка задает интерфейсы, на которых collectd будет обрабатывать входящие соединения.

Интерфейсы сервера

Хост сервера	Порт сервера
Этот раздел не содержит данных	

[Добавить](#)

Строка задает сервера, на которые будет передаваться локальная статистика.

Рисунок 7 - 20. Настройка плагина «Network»

В подразделе «Прослушивать интерфейсы» задаются интерфейсы, на которых collectd будет обрабатывать входящие соединения (режим сервера).

В подразделе «Интерфейсы сервера» задаются серверы, на которые будет передаваться локальная статистика (режим клиента).

Страница настройки плагина «Syslog» позволяет сконфигурировать отправку сообщений collectd в системный журнал.

Настройка плагина «Syslog»

Плагин «SysLog» получает сообщения от служб и отправляет их в syslog.

Включить этот плагин ☒

Уровень журналирования
Устанавливает уровень журналирования syslog.

Уровень уведомлений
Определяет, какие уведомления должны быть отправлены в syslog.

Рисунок 7 - 21. Настройка плагина «Syslog»