Маршрутизатор (RedBox)

TOPAZ FW

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

ПЛСТ.465277.385 РЭ

Technology

Москва

ОГЛАВЛЕНИЕ

1 ОПИСАНИЕ И РАБОТА 4
1.1 Назначение изделия 4
1.2 Модификации и условные обозначения 4
1.3 Технические характеристики 5
1.3.1 Конструкция 5
1.3.2 Рабочие условия эксплуатации 6
1.3.3 Безопасность и электромагнитная совместимость 6
1.3.4 Надежность 12
1.3.5 Питание 13
1.3.6 Характеристики устройства 13
1.3.7 Синхронизация времени 14
1.3.8 Интерфейсы передачи данных 14
1.4 Комплектность 15
1.5 Устройство и работа 15
1.5.1 Функциональные возможности 15
1.5.2 Встроенная система безопасности 16
1.5.3 Работа кнопок и индикаторов в модификации MR 17
1.6 Конфигурирование устройства 17
1.6.1 Подключение к командной строке 17
1.6.2 Общие сведения про интерфейс командной строки 19
1.6.1 Структура командной строки 21
1.7 Подменю System 21
1.7.1 VRF 21
1.7.2 GRE туннели 22
1.7.3 Loopback интерфейсы 23
1.7.4 VLAN интерфейсы 23
1.7.5 Bridge интерфейс 24
1.7.6 PRP интерфейс 25
1.7.7 Режим работы RedBox 25
1.7.8 Работа с конфигурацией устройства 26
1.7.9 Сброс к заводским настройкам 26
1.8 Подсистема router 26
1.8.1 Настройки интерфейсов 26
1.8.2 BGPv4 28
1.8.3 L3VPN на основе MP-BGP (VPNv4) 31
1.8.4 MPLS 32
1.8.5 OSPF 34

1.8.6 Статическая маршрутизация....36
1.8.7 VRRP....38
1.9 Настройка правил межсетевого экрана....40
1.9.1 Правила и действия....40
1.9.2 Таблицы iptables....41
1.9.3 Утилита iptables....42
1.9.4 Пример использования....43
1.10 Настройка функций безопасности....45
1.10.1 Конфигурирование порта управления....45
1.10.2 Подсистема регистрации событий безопасности....45
1.10.3 Подсистема проверки целостности....47
1.10.4 Подсистема криптозащиты каналов связи....53
1.10.5 Подсистема аудита....53
1.11 Работа в режиме RedBox....65
2 МАРКИРОВКА И ПЛОМБИРОВАНИЕ....65
3 УПАКОВКА....66
4 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ....66
5 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ....66
6 УТИЛИЗАЦИЯ....67
7 ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ....67
7.1 Эксплуатационные ограничения и меры безопасности....67
7.2 Монтаж....68
7.2.1 Подготовка к монтажу....68
7.2.2 Установка на DIN-рейку....68
7.2.3 Внешние подключения....68
7.2.4 Шина T-BUS....69
7.2.5 Подключение питания....70
7.2.6 Монтаж модификации MR....71
7.2.7 Подключение к сети Ethernet....75
7.2.8 Горячая замена блока питания в модификации MR....77
ПРИЛОЖЕНИЕ А (Назначение контактов и портов)....79
ПРИЛОЖЕНИЕ Б (Назначение кнопок и индикаторов)....80
ПРИЛОЖЕНИЕ В (Внешний вид устройства)....81
ПРИЛОЖЕНИЕ Г (Подключение к устройству с помощью утилиты PuTTY)....83
ПРИЛОЖЕНИЕ Д (Модификации устройства)....85

Настоящее руководство по эксплуатации (РЭ) предназначено для ознакомления со сведениями о конструкции, принципе действия, технических характеристиках маршрутизаторов (RedBox) **TOPAZ FW** (далее по тексту – маршрутизатор, изделие, устройство) и его составных частях, содержит указания, необходимые для правильной и безопасной эксплуатации, технического обслуживания, ремонта, хранения и транспортирования, а также схемы подключения устройства к цепям питания, цепям сигнализации и интерфейсам передачи данных.

Перед началом работы с устройством необходимо ознакомиться с настоящим РЭ.

РЭ предназначено для эксплуатационного персонала и инженеров-проектировщиков автоматизированных систем.



В СВЯЗИ С ПОСТОЯННОЙ РАБОТОЙ ПО СОВЕРШЕНСТВОВАНИЮ ИЗДЕЛИЯ, В КОНСТРУКЦИЮ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МОГУТ БЫТЬ ВНЕСЕНЫ ИЗМЕНЕНИЯ, НЕ УХУДШАЮЩИЕ ЕГО ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И НЕ ОТРАЖЕННЫЕ В НАСТОЯЩЕМ ДОКУМЕНТЕ.

1 ОПИСАНИЕ И РАБОТА

1.1 Назначение изделия

Маршрутизаторы TOPAZ FW предназначены для маршрутизации и передачи данных в технологических сетях объектов промышленности и электроэнергетики, в том числе в системах автоматизации, телемеханики и высокоавтоматизированных подстанций с применением МЭК 61850. Маршрутизаторы обеспечивают пересылку пакетов между сегментами сети с использованием статической и динамической маршрутизации.

RedBox (Redundancy Box) — программно конфигурируемый режим маршрутизаторов платформы MX681, предназначенный для подключения устройств или сегментов сети, не поддерживающих PRP, к двум параллельным сетям PRP. Маршрутизаторы платформы MX710 не поддерживают режим RedBox.

1.2 Модификации и условные обозначения

Функциональные возможности устройства, количество и тип интерфейсов передачи данных определяются конструктивным исполнением, типом платформы и количеством/типом плат расширений. Количество и тип интерфейсов передачи данных устройства, а также наличие дополнительных функциональных возможностей зависят от конкретного исполнения.

Полная расшифровка условных обозначений устройства приведена в таблице 1.

Для формирования условного обозначения устройства необходимо вписать на место каждой позиции соответствующий код. Квадратными скобками выделены позиции, на место которых можно вписать одновременно несколько вариантов кода.

Таблица 1 – Расшифровка условного обозначения устройства

TOPAZ FW A [B-…-Bx]-C-D-E		
Позиция	**Код**	**Расшифровка**
A	MX681 Exx[1)]	Платформа MX681. Exx — общее количество портов Ethernet маршрутизатора, не более 32
	MX710	Платформа MX710
Коммуникационные порты Ethernet [2)]		
B	nGTxSFP[3)]	n комбинированных портов Ethernet RJ-45/SFP
	nGTx	n портов Ethernet RJ-45 со скоростью передачи данных до 1000 Мбит/с
	nTx	n портов Ethernet RJ-45 со скоростью передачи данных до 100 Мбит/с
Конструктивное исполнение		
C	–	Пластиковый корпус платформы MX681; код конструктивного исполнения в обозначении не указывают
	MR	Металлический корпус для установки в стойку 19 дюймов: высотой 1U для платформы MX681 или 2U для платформы MX710

TOPAZ FW A [B-…-Bx]-C-D-E		
Позиция	**Код**	**Расшифровка**
Каналы питания		
D	2HV	Два независимых встроенных источника питания 220 В переменного или постоянного тока; применяется для исполнения в пластиковом корпусе
	2PW	Два слота для сменных блоков питания[4]; применяется для конструктивного исполнения MR
Дискретные входы и выходы		
E	DGN	Наличие “сухих контактов” сигнализации питания и неисправности

Примечания:

1) E(xx) - общее количество (xx) портов Ethernet устройства, задается в заказном обозначении. Максимальное суммарное количество портов Ethernet – 32.
2) n – количество портов соответствующего типа, задается в заказном обозначении.
3) SFP-модули заказываются дополнительно:
   - TOPAZ SFP-100-01-MM – 100 мегабитный многомодовый SFP-модуль
   - TOPAZ SFP-100-01-SM – 100 мегабитный одномодовый SFP-модуль
   - TOPAZ SFP-1G-10-SM – гигабитный одномодовый SFP-модуль, дальность передачи 10 км
   - TOPAZ SFP-1G-15-SM – гигабитный одномодовый SFP-модуль, дальность передачи 15 км
   - TOPAZ SFP-1G-40-SM – гигабитный одномодовый SFP-модуль, дальность передачи 40 км
   - TOPAZ SFP-1G-01-MM – гигабитный многомодовый SFP-модуль, дальность передачи 1 км
   - TOPAZ SFP-1G-02-MM – гигабитный многомодовый SFP-модуль, дальность передачи 2 км.
4) Для исполнения MR с кодом 2PW блоки питания заказываются отдельно. Доступны к заказу следующие блоки питания:
   - TOPAZ PW220/100W-MR;
   - TOPAZ PW110/100W-MR;
   - TOPAZ PW48/100W-MR;
   - TOPAZ PW24/100W-MR.

Устройство выпускается в модификациях, приведенных в приложении Д.

1.3 Технические характеристики

1.3.1 Конструкция

Маршрутизаторы платформы MX681 без кода конструктивного исполнения выполнены в пластиковом корпусе, не поддерживающем горение, с креплением для установки на DIN-рейку. Вентиляционные отверстия корпуса расположены в верхней и нижней частях корпуса. Габаритные размеры (Ш × В × Г) — не более 180 × 99 × 124 мм. Масса — не более 1,0 кг.

Номера плат и блоков питания указаны на верхней и нижней панелях устройства. Платы с оптическими портами Ethernet имеют дополнительную маркировку на передней панели: **SM** – одномодовое оптоволокно, **MM** – многомодовое оптоволокно.

Маршрутизаторы платформы MX681 с кодом конструктивного исполнения MR выполнены в металлическом корпусе высотой 1U для установки в стойку 19 дюймов. Габаритные размеры (Ш × В × Г) — не более 480 × 44,5 × 394 мм. Масса — не более 5,0 кг.

Маршрутизаторы платформы MX710 выполнены в металлическом корпусе высотой 2U для установки в стойку 19 дюймов. Габаритные размеры (Ш × В × Г) — не более 480 × 89 × 394 мм. Масса — не более 6,5 кг.

Степень защиты маршрутизаторов от проникновения внутрь твёрдых частиц, пыли и воды — не ниже IP20 по ГОСТ 14254-2015.

Внешний вид, описание входов, выходов и индикаторов устройства приведены в Приложении В настоящего руководства.

1.3.2 Рабочие условия эксплуатации

Рабочие условия эксплуатации приведены в таблице 2.

Таблица 2 – Рабочие условия эксплуатации

Параметр	Значение
Температура окружающего воздуха, °С	от минус 40 до плюс 70
Относительная влажность воздуха при температуре 30 °С и ниже, %	до 100 без долговременной конденсации внутри оболочки
Атмосферное давление воздуха, кПа	от 73,3 до 106,7
Высота над уровнем моря, м	не более 2000
Тип атмосферы, по ГОСТ 15150	промышленная, II
Синусоидальная вибрация: - диапазон частот, Гц - максимальная амплитуда ускорения, м·с$^{-2}$ (g)	 0,5 – 100 10 (1)
Удары одиночного действия: - пиковое ударное ускорение, м·с$^{-2}$ (g) - длительность действия ударного ускорения, мс	 100 (10) 2-20
Сейсмостойкость, баллов по МСК	9
Срок сохраняемости	1 год
Условия хранения, по ГОСТ 15150 - температура окружающего воздуха, °С - относительная влажность при температуре 25°С, %	2 от минус 50 до плюс 50 до 98
Транспортирование	- автомобильным транспортом, закрытым брезентом; - в закрытых железнодорожных вагонах, трюмах речного транспорта; - в негерметизированных отсеках самолетов при пониженном атмосферном давлении 12 кПа (90 мм рт.ст.)
Условия транспортирования: - температура окружающего воздуха, °С - относительная влажность при температуре 25°С, % - атмосферное давление, кПа - воздействия механических факторов, по ГОСТ 23216	 от минус 50 до плюс 50 до 100 от 12 до 106,7 Очень легкие (ОЛ)

По рабочим условиям эксплуатации (климатическим воздействиям) устройство соответствует изделиям группы С2 по ГОСТ Р 52931-2008.

Устройства пригодны для эксплуатации в условиях климатических исполнений по ГОСТ 15150: УХЛ 4, УХЛ 3.1, а также УХЛ 2.1, но при этом нижнее значение температуры окружающего воздуха должно быть не ниже минус 40 °С. Для работы при более низких температурах комплектное изделие должно оснащаться системой поддержания заданных параметров микроклимата.

Устройства пригодны для эксплуатации при рабочих значениях механических внешних воздействующих факторов (ВВФ) – по ГОСТ 30631-99 для групп механического исполнения М43, М40, М39, М38, М6.

Эксплуатация устройств допускается на высотах до 2000 метров над уровнем моря.

1.3.3 Безопасность и электромагнитная совместимость

Маршрутизаторы соответствуют требованиям электромагнитной совместимости ГОСТ Р 51317.6.5-2006, ГОСТ IEC 61000-6-5-2017 и требованиям ГОСТ Р МЭК 61850-3-2005 в части электромагнитной совместимости. Виды, уровни и параметры воздействий определяются типом порта, установленным блоком питания и условиями подключения. При воздействии помех с уровнями, приведенными в

таблице 3, маршрутизаторы устойчиво функционируют в соответствии с назначением без ухудшения установленных показателей и прекращения выполнения заявленных функций (критерий качества функционирования А).

Уровень индустриальных радиопомех, создаваемых маршрутизатором, не превышает норм, установленных для класса А по ГОСТ 30805.22-2013.

На корпусе маршрутизатора предусмотрен контакт для подключения кабеля защитного заземления. Сопротивление между контактом защитного заземления и каждой доступной прикосновению металлической нетоковедущей частью, которая может оказаться под напряжением, — не более 0,1 Ом.

Электрическое сопротивление изоляции между независимыми цепями, а также между каждой независимой цепью и корпусом маршрутизатора в нормальных климатических условиях — не менее 100 МОм при воздействующем напряжении 500 В постоянного тока.

Электрическая прочность изоляции маршрутизаторов соответствует следующим значениям:

– входные и выходные цепи с номинальным напряжением до 60 В, включая линии связи и изолированные вторичные цепи, выдерживают в течение 60 с испытательное напряжение промышленной частоты 0,5 кВ и импульсное напряжение 1,0/50 мкс амплитудой 1 кВ;

– цепи электропитания постоянного тока с номинальным напряжением до 60 В выдерживают в течение 60 с испытательное напряжение промышленной частоты 1 кВ и импульсное напряжение 1,0/50 мкс амплитудой 2 кВ;

– цепи электропитания с номинальным напряжением свыше 60 В выдерживают в течение 60 с испытательное напряжение промышленной частоты 2,5 кВ и импульсное напряжение 1,0/50 мкс амплитудой 5 кВ.

Испытания проводят между каждой независимой цепью и корпусом маршрутизатора при соединённых между собой выводах испытываемой цепи. Пробой и перекрытие изоляции не допускаются.

Устройство соответствует требованиям технических регламентов Таможенного союза ТР ТС 004/2011 «О безопасности низковольтного оборудования», ТР ТС 020/2011 «Электромагнитная совместимость технических средств».

В части защиты от поражения электрическим током устройство соответствует требованиям к классу защиты от поражения электрическим током — I по ГОСТ 12.2.091-2012 и ГОСТ 12.2.007.0-75.

Таблица 3 - Виды и уровни выдерживаемых электромагнитных воздействий

№ п/п	Вид электромагнитных воздействий на помехоустойчивость	Значение
	Порт корпуса	
1.	**Устойчивость к магнитному полю промышленной частоты по ГОСТ IEC 61000-4-8-2013:**	
	• степень жесткости	СЖ 5
	• напряженность непрерывного МППЧ, А/м	100
	• напряженность кратковременного (1 с) МППЧ, А/м	1000
2.	**Устойчивость к радиочастотному электромагнитному полю по ГОСТ 30804.4.3:**	
	• степень жесткости	СЖ 3
	• напряженность испытательного поля, В/м	10
	• полоса частот немодулированного сигнала, МГц	80-1000 и 1400-6000

3.	**Устойчивость к импульсному магнитному полю по ГОСТ IEC 61000-4-9-2022:**	
	• степень жесткости	СЖ 5
	• напряженность ИМП, А/м	1000
4.	**Устойчивость к затухающему колебательному магнитному полю по ГОСТ IEC 61000-4-10-2022 (100 кГц, 1МГц):**	
	• степень жесткости	СЖ 5
	• напряженность ЗКМП (пиковое значение), А/м	100
5.	**Устойчивость к электростатическим разрядам по ГОСТ 30804.4.2:**	
	• степень жесткости	СЖ 5
	• контактный: испытательное напряжение, кВ	8
	• воздушный: испытательное напряжение, кВ	15
	Сигнальные порты	
6.	**Устойчивость к колебательным затухающему помехам по ГОСТ IEC 61000-4-12-2016 и ГОСТ IEC 61000-4-12-2016:**	
	• повторяющиеся КЗП (сигнальные порты полевого соединения):	
	- степень жесткости - частота колебаний	СЖ 2 100 кГц; 1 МГц
	- по схеме «провод-провод»: испытательное напряжение, кВ	0,5
	- по схеме «провод-земля»: испытательное напряжение, кВ	1
	• одиночные КЗП (сигнальные порты полевого соединения):	
	- степень жесткости	СЖ 3
	- по схеме «провод-провод»: испытательное напряжение, кВ	1
	- по схеме «провод-земля»: испытательное напряжение, кВ	2
7.	**Устойчивость к микросекундным импульсным помехам большой энергии по ГОСТ IEC 61000-4-5-2017:**	
	• сигнальные порты полевое соединение:	
	- по схеме «провод-провод»: степень жесткости / амплитуда импульсов, кВ	СЖ 2 / 1
	- по схеме «провод-земля»: степень жесткости / амплитуда импульсов, кВ	СЖ 3 / 2
	• сигнальные порты локальное соединение:	

	- по схеме «провод-провод»: степень жесткости / амплитуда импульсов, кВ	СЖ1 / 0,5
	- по схеме «провод-земля»: степень жесткости / амплитуда импульсов, кВ	СЖ2 / 1
8.	**Устойчивость к наносекундным импульсным помехам по ГОСТ 30804.4.4:**	
	• сигнальные порты локального соединения: степень жесткости / амплитуда импульсов, кВ	СЖ 3 / 1
	• сигнальные порты полевого соединения: степень жесткости / амплитуда импульсов, кВ	СЖ 4 / 2
9.	**Устойчивость к кондуктивным помехам, в полосе частот от 150 кГц до 80 МГц по ГОСТ IEC 61000-4-6-2022:**	
	все сигнальные порты:	
	• степень жесткости	СЖ3
	• испытательное напряжение, В	10
10.	**Устойчивость к кондуктивным помехам в полосе частот от 0 до 150 кГц по ГОСТ IEC 61000-4-16-2023:**	
	• сигнальные порты полевого соединения:	
	• степень жесткости	СЖ4
	• длительная помеха, испытательное напряжение / частота	30 В / 50 Гц 30-3-30 В / 15 Гц – 150 кГц
	• кратковременная (1 с) помеха, испытательное напряжение / частота	300 В / 50 Гц
	Порты электропитания постоянного тока (входные)	
11.	**Провалы напряжения по ГОСТ IEC 61000-4-29-2016**	30 % (1 с) 60 % (0.1 с)
	Прерывания напряжения по ГОСТ IEC 61000-4-29-2016	100 % (0.5 с)
12.	**Устойчивость к пульсациям напряжения электропитания постоянного тока по ГОСТ Р 51317.4.17-2000**	СЖ 3 Не выше 10 %
13.	**Устойчивость к кондуктивным помехам в полосе частот от 0 до 150 кГц по ГОСТ IEC 61000-4-16-2023**	
	• степень жесткости	СЖ4
	• длительная помеха, испытательное напряжение / частота	30 В / 50 Гц 30-3-30 В / 15 Гц – 150 кГц

	• кратковременная (1 с) помеха, испытательное напряжение / частота	300 В / 50 Гц
14.	**Устойчивость к микросекундным импульсным помехам большой энергии 1/50 мкс по ГОСТ IEC 61000-4-5-2017**	
	• порты ниже 60 В:	
	- по схеме «провод-провод»: степень жесткости / амплитуда импульсов	СЖ 2 / 1 кВ
	- по схеме «провод-земля»: степень жесткости / амплитуда импульсов	СЖ 3 / 2 кВ
	• порты выше 60 В:	
	- по схеме «провод-провод»: степень жесткости / амплитуда импульсов	СЖ 3 / 2 кВ
	- по схеме «провод-земля»: степень жесткости / амплитуда импульсов	СЖ4 / 4 кВ
15.	**Устойчивость к наносекундным импульсным помехам (частота повторения импульсов 5 и 100 кГц) по ГОСТ 30804.4.4-2013**	СЖ 4 / 4 кВ
16.	**Устойчивость к кондуктивным помехам, в полосе частот от 150 кГц до 80 МГц по ГОСТ IEC 61000-4-6-2022**	СЖ 3 / 10 В
17.	**Устойчивость к колебательным затухающим помехам по ГОСТ IEC 61000-4-12-2016 и ГОСТ IEC 61000-4-12-2016:**	
	• повторяющиеся КЗП для портов ниже 60 В	
	- степень жесткости - частота колебаний	СЖ 2 100 кГц; 1 МГц
	- по схеме «провод-провод»: испытательное напряжение, кВ	0,5
	- по схеме «провод-земля»: испытательное напряжение, кВ	1
	• одиночные КЗП для портов ниже 60 В:	
	- степень жесткости	СЖ 3
	- по схеме «провод-провод»: испытательное напряжение, кВ	1
	- по схеме «провод-земля»: испытательное напряжение, кВ	2
	• повторяющиеся КЗП для портов выше 60 В	
	- степень жесткости - частота колебаний	СЖ 3 100 кГц; 1 МГц
	- по схеме «провод-провод»: испытательное напряжение, кВ	1
	- по схеме «провод-земля»: испытательное напряжение, кВ	2,5
	• одиночные КЗП для портов ниже 60 В	

	- степень жесткости	СЖ 4
	- по схеме «провод-провод»: испытательное напряжение, кВ	2
	- по схеме «провод-земля»: испытательное напряжение, кВ	4
	Порты электропитания переменного тока	
18.	**Провалы напряжения электропитания (при фазовых углах 0, 90, 270 градусов) по ГОСТ 30804.4.11-2013**	Δ U 30 % (25 периодов) Δ U 60 % (50 периодов)
19.	**Прерывания напряжения по ГОСТ 30804.4.11-2013**	Δ U 100 % (50 периодов)
20.	**Устойчивость к изменениям частоты питания в сети переменного тока по ГОСТ Р 51317.4.28-2000**	(±3) % (при tp=10 с), (+ 4)% / (-6) % (при tp=10 с) и (±15) % (при tp =1 с)
21.	**Устойчивость к кондуктивным помехам, в полосе частот от 150 кГц до 80 МГц по ГОСТ IEC 61000-4-6-2022**	СЖ 3 / 10 В
22.	**Устойчивость к кондуктивным помехам в полосе частот от 0 до 150 кГц по ГОСТ IEC 61000-4-16-2023**	
	• степень жесткости	СЖ4
	• длительная помеха, испытательное напряжение / частота	30 В / 50 Гц 30-3-30 В / 15 Гц – 150 кГц
	• кратковременная (1 с) помеха, испытательное напряжение / частота	300 В / 50 Гц
23.	**Устойчивость к колебательным затухающим помехам (при фазовых углах 0, 90 и 270 градусов) по ГОСТ IEC 61000-4-12-2016 и ГОСТ IEC 61000-4-18-2016**	
	• повторяющиеся КЗП	
	- степень жесткости - частота колебаний	СЖ 3 100 кГц; 1 МГц
	- по схеме «провод-провод»: испытательное напряжение, кВ	1
	- по схеме «провод-земля»: испытательное напряжение, кВ	2,5
	• одиночные КЗП:	
	- степень жесткости	СЖ 4
	- по схеме «провод-провод»: испытательное напряжение, кВ	2
	- по схеме «провод-земля»: испытательное напряжение, кВ	4
24.	**Устойчивость к искажениям синусоидальности напряжения электропитания, включая передачу сигналов по электрическим сетям по ГОСТ 30804.4.13-2013**	Класс 3 Не более 12 %

25.	**Устойчивость к колебаниям напряжения электропитания по ГОСТ Р 51317.4.14-2000**	СЖ 3 ΔU = ±0.12Uн
26.	**Устойчивость к наносекундным импульсным помехам (частота повторения импульсов 5 и 100 кГц) по ГОСТ 30804.4.4-2013**	СЖ 4 / 4 кВ
27.	**Устойчивость к микросекундным импульсным помехам большой энергии 1/50 мкс по ГОСТ IEC 61000-4-5-2017**	
	- по схеме «провод-провод»: степень жесткости / испытательное напряжение, кВ	СЖ 3 /2 кВ
	- по схеме «провод-земля»: степень жесткости / испытательное напряжение, кВ	СЖ 4 / 4 кВ
	Порт функционального заземления	
28.	**Устойчивость к наносекундным импульсным помехам (частота повторения импульсов 5 и 100 кГц) (ввод помехи применением емкостных ключей связи) по ГОСТ 30804.4.4-2013**	СЖ 4 / 4 кВ
29.	**Устойчивость к кондуктивным помехам, в полосе частот от 150 кГц до 80 МГц по ГОСТ IEC 61000-4-6-2022**	СЖ 3 / 10 В
30.	**Устойчивость к токам кратковременных синусоидальных помех частотой 50 Гц в цепях защитного и сигнального заземления по ГОСТ 32137-2025**	СЖ 4 / 200 А
31.	**Устойчивость к токам микросекундных импульсных помех в цепях защитного и сигнального заземления по ГОСТ 32137-2025**	СЖ 4 / 200 А
	Помехоэмиссия	
32.	**Радиопомехи от оборудования по ГОСТ 30805.22-2013 класс А:**	
	Напряжение радиопомех. Квазипиковое значение: - в диапазоне 0,15-0,5 МГц - в диапазоне 0,5-30 МГц Напряжение радиопомех. Среднее значение: - в диапазоне 0,15-0,5 МГц - в диапазоне 0,5-30 МГц Напряжённость поля радиопомех (Квазипиковое значение) -в диапазоне 30 -230 МГц -в диапазоне 230 -1000 МГц	 79 дБ(мкВ); 73 дБ(мкВ). 66 дБ(мкВ); 60 дБ(мкВ). 40 дБ(мкВ/м); 47 дБ(мкВ/м).

1.3.4 Надежность

Устройство является восстанавливаемым, ремонтируемым изделием, предназначенным для круглосуточной эксплуатации в стационарных условиях в производственных помещениях. Режим работы устройства непрерывный. Продолжительность непрерывной работы не ограничена. Средняя наработка на отказ— не менее 200 000 ч. Средний срок службы — не менее 30 лет. Среднее время восстановления работоспособности на объекте эксплуатации (без учета времени прибытия персонала) — не более 30 мин. Готовность каналов передачи данных — не менее 0,9998 без учета повреждений кабеля связи.

1.3.5 Питание

Количество и тип каналов питания устройства зависят от исполнения по питанию. Характеристики каналов питания приведены в таблице 4.

В исполнениях MR с кодом 2PW при наличии двух установленных БП обеспечивается горячая замена одного БП без прерывания передачи данных. Подробнее описано в п. 7.2.8.

Таблица 4 – Характеристики питания

Наименование параметра	Значение		
Количество каналов питания	до 2		
Каналы питания по кодировке исполнения:	Применяемые БП	Номинальное значение	Рабочий диапазон
- (кодировка отсутствует)[1)]	-	24/48 В (DC)	от 10 до 60 В (DC)
2HV[1)]	-	220 В (AC/DC)	90 – 265 В (AC) 110 – 365 В (DC)
2PW[2)]	TOPAZ PW24/100W-MR	24 В (DC)	10 – 36 В (DC)
	TOPAZ PW48/100W-MR	48 В (DC)	18 – 75 В (DC)
	TOPAZ PW110/100W-MR	110 В (AC/DC)	90–265 В (AC); 88–365 В (DC)
	TOPAZ PW220/100W-MR	220 В (AC/DC)	90–265 В (AC); 110–365 В (DC)
Частотный диапазон напряжения питания 220 В, Гц	от 45 до 55		
Ток потребления канала питания 220 В, не более, А	0,4		
Примечание: 1) Для исполнений в пластиковом корпусе 2) Для исполнения MR			

Устройство обеспечивает нормальную работу при произвольном изменении напряжения питания в пределах рабочего диапазона. Кратковременные перерывы питания не влияют на работу устройства. При нарушении питания устройство корректно завершает свою работу, а при восстановлении напряжения питания устройство переходит в рабочий режим автоматически. Под корректным завершением работы в данном случае понимается отсутствие передачи ложной информации и потери конфигурационной информации. Время установления рабочего режима при восстановлении питания не более 10 с.

Конфигурация устройства сохраняется в энергонезависимой памяти, которая обеспечивает сохранение параметров при отсутствии напряжения питания в течение 30 лет.

Примечание Устройства с БП, рассчитанными на 220 В AC/DC, необходимо подключать через автоматические выключатели.

1.3.6 Характеристики устройства

Технические характеристики устройства приведены в таблице 5.

Таблица 5 – Характеристики устройства

Наименование параметра	Значение
Операционная система	ТОС TOPAZ Linux
Слот для Flash-карты [1)]	microSD
Примечания: 1) Отсутствует в модификации MR	

1.3.7 Синхронизация времени

Характеристики синхронизации времени приведены в таблице 6.

Таблица 6 – Характеристики синхронизации времени

Наименование параметра	Значение
Уход локальных часов без внешнего питания, с / сутки, не более	± 1
Уход локальных часов при отсутствии синхронизации по сигналам точного времени, с / сутки, не более	± 0,5
Точность синхронизации времени: - по протоколам ГОСТ Р МЭК 60870-5-101/104 - по протоколам NTP, SNTP	 ±2 мс ±100 мкс

1.3.8 Интерфейсы передачи данных

Количество и тип интерфейсов передачи данных указываются в условном обозначении устройства.

Типы Ethernet-интерфейсов, разъёмов и поддерживаемые скорости передачи данных приведены в таблице 7. Дополнительные характеристики оптического SFP-интерфейса комбо-портов GTxSFP приведены в таблице 8.

Таблица 7 – Технические характеристики интерфейса Ethernet

Код	Тип разъема	Скорость передачи данных, Мбит/с
nGTx	RJ-45	10/100/1000
nGTxSFP	Комбо-порт RJ-45/SFP	SFP: 100 или 1000 (зависит от типа SFP-модуля) RJ-45: 10/100/1000
nTx	RJ-45	10/100

Таблица 8 – Характеристики оптического SFP-интерфейса Ethernet

Наименование параметра	Значение
Физическая реализация	Сменный SFP-трансивер в SFP-интерфейсе комбо-порта GTxSFP
Поддерживаемые стандарты	100BASE-FX; 1000BASE-X
Параметры оптического интерфейса	Определяются типом установленного SFP-трансивера
Цифровой диагностический мониторинг	При применении SFP-трансивера с поддержкой цифрового диагностического мониторинга маршрутизатор обеспечивает считывание значений оптической мощности передатчика Tx и приёмника Rx

Примечание Комбо-порт GTXSFP работает в режиме автоматического переключения. При одновременном подключении ко входу RJ-45 и SFP активен только вход SFP.
Примечание Скорость передачи данных порта SFP соответствует скорости передачи данных SFP-модуля.

Таблица 9 – Поддерживаемые технологии Ethernet

Технологии	Описание
Поддерживаемые стандарты	IEEE 802.3 10BaseT; IEEE 802.3u 100BASE-TX, 100BASE-FX; IEEE 802.3z 1000BASE-X; IEEE 802.3ab 1000BASE-T; IEEE 802.3x управление потоком; IEEE 802.3az Ethernet с энергосберегающим режимом; IEEE 802.1D-2004 STP, QoS; IEEE 802.1d STP;

Технологии	Описание
	IEEE 802.1w RSTP; IEEE 802.1s MSTP; IEEE 802.1Q тегирование трафика.
Промышленные протоколы	Ethernet/IP; ГОСТ Р МЭК 60870-5-104; Modbus/TCP; IEC 61850
Управление	SSH; Console – CLI; Web
Протоколы фильтрации трафика	VLAN на основе портов
Протоколы резервирования сети	STP/RSTP/MSTP; PRP; HSR
Информационная безопасность	Authentication Certificate - SSL Certificate/SSH Key Regenerate; 802.1X – Port Based; Port Security – Static MAC Port Lock
Протоколы синхронизации времени	ГОСТ Р МЭК 60870-5-104; NTP/SNTP Server/Client

1.4 Комплектность

Комплект поставки конкретного маршрутизатора указывается в паспорте устройства.

В базовый комплект поставки входят:

- маршрутизатор (RedBox) TOPAZ FW;
- паспорт.

Наличие и количество штекеров, клеммных блоков, шинных соединителей T-BUS, SFP-модулей и иных принадлежностей определяются конкретным исполнением и заказом и указываются в индивидуальном паспорте устройства. SFP-модули поставляются отдельно, если иное не предусмотрено заказом.

Эксплуатационная документация доступна на сайте: http://www.tpz.ru.

1.5 Устройство и работа

1.5.1 Функциональные возможности

Устройство является сетевым маршрутизатором, реализующим функции маршрутизации, коммутации, резервирования сети и межсетевого экранирования. Функции информационной безопасности устройства приведены в 1.5.2 и разделе 1.10 настоящего РЭ.

Устройство работает под управлением технологической операционной системы TOPAZ Linux и реализует следующие базовые функции:

- прием информации по цифровым каналам связи;
- выполнение прикладных программ;
- автоматическое накопление, хранение и передача информации по цифровым каналам связи;
- ведение системного времени и его автоматическая коррекция/синхронизация по сигналам точного времени, по протоколам NTP и SNTP;
- синхронизации времени подконтрольных устройств;
- самодиагностика и тестирование работоспособности первичных преобразователей (датчиков);
- ведение журнала событий.

В «Журнале событий» устройства автоматически фиксируются время и даты наступления следующих событий:

- попыток несанкционированного доступа;
- фактов изменения данных;
- перезапуск устройства;
- фактов корректировки времени с обязательной фиксацией времени до и после коррекции или величины коррекции времени, на которую было скорректировано устройство;
- результатов самодиагностики;
- отключения питания.

Таблица 10 – Функциональные возможности маршрутизатора

Технологии	Описание
Межсетевой экран	статическая фильтрация пакетов; фильтрация по IP адресам, протоколам и портам; трансляция адресов источника и назначения NAT; отслеживание TCP сессий, контроль корректности установления соединения; поддержка фильтрации с использованием адресных листов
Маршрутизация	статическая маршрутизация; маршрутизация на основе политик; маршрутизация на основе правил для интерфейсов; динамическая маршрутизация: RIP v1/v2, OSPFv2, BGPv4; IP/MPLS; резервирование маршрутизаторов по протоколу VRRP
Коммутация	поддержка STP/RSTP/MSTP поддержка VLAN IEEE802.1q
VPN	IPsec с использованием туннельного и транспортного режимов, авторизация по сертификату или PSK ключу, протоколы AH/ESP аппаратная поддержка шифрования AES с 128/256-битным ключом протоколы туннелирования: OpenVPN, GRE, L3VPN MBGP
DHCP	DHCP-сервер/клиент, DHCP-relay; статические и динамические диапазоны адресов; поддержка конфигурируемых опций DHCP.
Утилиты	ping; traceroute; iperf; tcpdump; ssh
Прочие функции	поддержка Radius/Tacacs аутентификации; LLDP sFTP сервер; сервер/клиент синхронизации времени NTP.
Технология PRP	устройство поддерживает протокол бесшовного резервирования PRP IEC 62439-3 в качестве устройства DAN (Double Attached Node), а также может выступать в роли RedBox (Redundancy Box) (только для платформы MX681)

Настройка, управление и контроль работы устройства осуществляется с использованием персонального компьютера, подключаемого через сеть Ethernet, либо через консоль (виртуальный COM-порт).

1.5.2 Встроенная система безопасности

Встроенная система информационной безопасности устройства реализует следующие функции:

- идентификацию и аутентификацию пользователей;
- разграничение прав доступа пользователей;
- передачу данных с использованием СКЗИ;
- межсетевое экранирование;
- регистрацию событий безопасности и их отправку в централизованные системы мониторинга;
- контроль целостности системных файлов.

Система включает следующие подсистемы:

- подсистема регистрации событий безопасности;
- подсистема проверки целостности;
- подсистема криптозащиты каналов связи;
- подсистема аудита.

Описание настройки функций информационной безопасности устройства приведено в разделе 1.10 настоящего РЭ.

1.5.3 Работа кнопок и индикаторов в модификации MR

На передней панели устройства расположены светодиодные индикаторы, отображающие работу устройства. Названия и количество индикаторов зависят от модификации и заказного обозначения устройства.

На передней панели устройства также расположены кнопки, для нажатия которых используют заострённый предмет.

- Кнопка **RS** предназначена для перезагрузки устройства без отключения питания. Кнопка **RS** может отсутствовать.
- Кнопка **RB** предназначена для активации загрузчика с SD-карты при одновременном нажатии с кнопкой **RS**. В случае отсутствия кнопки **RS** активация загрузчика с SD-карты осуществляется посредством нажатия кнопки **RB**.

Информация о работе кнопок и индикаторов в различных исполнениях устройства содержится в приложении Б.

1.6 Конфигурирование устройства

1.6.1 Подключение к командной строке

Конфигурирование устройства с помощью командной строки возможно через серийную консоль (порт USB на лицевой стороне устройства) либо через порт Ethernet по протоколу ssh.

Таблица 11 – Варианты доступа к настройкам устройства

Протокол	Описание	Требуемое ПО
SSH	Защищенный протокол передачи данных. Аналог протокола Telnet с шифрованием трафика при авторизации и работе с консолью.	UNIX – утилита ssh (стандартный SSH-клиент UNIX); Windows – PuTTY, WinSCP, openssh
Серийная консоль	Подключение через консольный USB-порт устройства (virtual COM-port).	UNIX – утилита minicom; Windows XP – HyperTerminal (встроенное ПО); Windows 7, 8, 10 – PuTTY или аналог

Конфигурирование устройства через SSH-соединение или серийную консоль можно осуществлять с помощью одной из терминальных программ. В приложении Г настоящего РЭ приведен пример подключения к устройству с помощью одной из таких программ.

ВНИМАНИЕ! ПРИ КОНФИГУРИРОВАНИИ УСТРОЙСТВА РЕКОМЕНДУЕТСЯ УДЕЛИТЬ ОСОБОЕ ВНИМАНИЕ НАСТРОЙКАМ ДОСТУПА ПО ПРОТОКОЛУ SSH. ОТ СЛОЖНОСТИ ПАРОЛЕЙ, РАЗРЕШЕНИЯ УДАЛЕННОГО ДОСТУПА, ИСПОЛЬЗУЕМЫХ ПОРТОВ СЕТЕВЫХ СЛУЖБ, НАСТРОЕК МЕЖСЕТЕВОГО ЭКРАНА И ДРУГИХ НАСТРОЕК СЕТЕВЫХ СЛУЖБ ЗАВИСИТ БЕЗОПАСНОСТЬ УСТРОЙСТВА И ПОДКЛЮЧЕННЫХ К НЕМУ УСТРОЙСТВ.

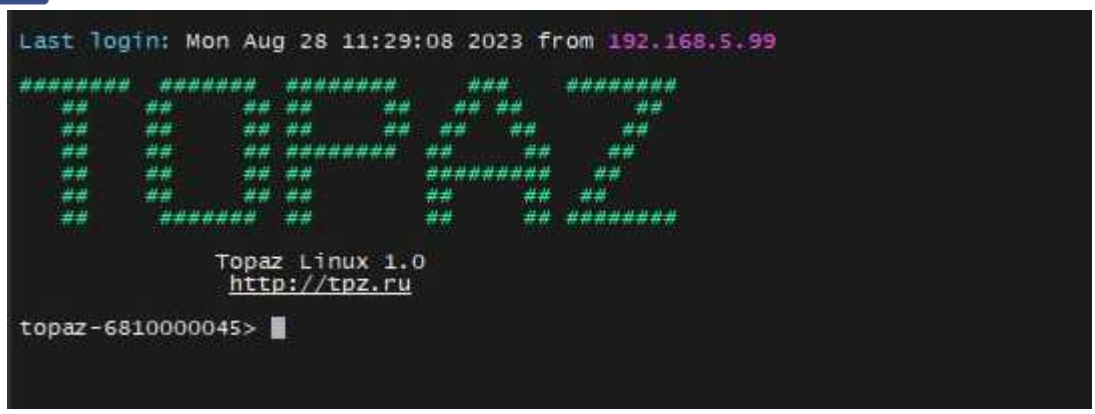


Рисунок 1 – Экран приветствия командной строки

1.6.1.1 Подключение через серийную консоль

При подключении устройства через консольный порт (USB) в системе появится виртуальный последовательный COM-порт, который можно использовать для соединения персонального компьютера с устройством. Для того, чтобы узнать номер порта, перейдите в «Диспетчер устройств» Windows и откройте вкладку «Порты». После чего, убедившись, что на устройство подано питание, соедините устройство с компьютером. Во вкладке «Порты» появится новый последовательный порт.

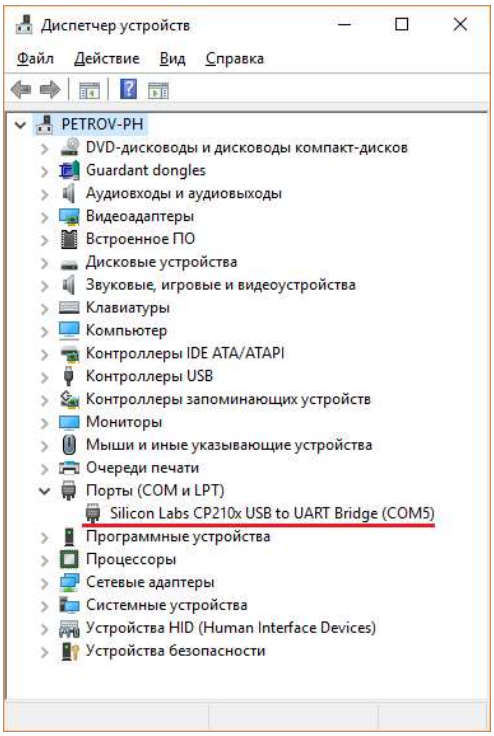


Рисунок 2 – Отображение устройства в диспетчере устройств Windows

Примечание Номер виртуального COM-порта присваивается операционной системой автоматически, поэтому на вашем компьютере он может отличаться от указанного в примере.

Последовательный порт консоли предоставляет пользователю удобный способ подключения к устройству, особенно при первом подключении и настройке устройства. Связь осуществляется по прямому последовательному соединению и пользователю не нужно знать IP адреса Ethernet-портов для того, чтобы подключиться к устройству.

При подключении через консольный порт для управления устройством используется интерфейс командной строки.

Параметры передачи данных по виртуальному COM-порту приведены в таблице ниже.

Таблица 12 – Параметры соединения с устройством по виртуальному COM-порту

Параметр	Значение
Скорость передачи / Baudrate	115 200 bps
Биты данных / Data bits	8
Стоповые биты / Stop bits	1
Контроль четности / Parity	None
Управление потоком / Flow Control	None

1.6.1.2 Подключение через порт Ethernet по протоколу SSH

Дистанционное конфигурирование и управление должны выполняться по протоколу SSH.

1.6.1.3 Авторизация на устройстве

При первом входе на устройство необходимо использовать следующие параметры доступа:

Login: admin
Password: admin

По умолчанию в системе создан один привилегированный пользователь с правами администратора – admin, в процессе конфигурирования рекомендуется сменить пароль по умолчанию.

Устройство поддерживает создание новых пользователей с правами администратора и ограниченными парвами конфигурирования (info). Также авторизация пользователей доступна через сервера Radius/Tacacs.

1.6.2 Общие сведения про интерфейс командной строки

Управление параметрами маршрутизатора осуществляется через интерфейс командной строки (CLI). CLI построен на базе командного интерпретатора и поддерживает иерархические режимы работы, контекстную справку, сокращённый ввод команд и автоматическое дополнение команд по клавише Tab. В зависимости от режима доступны команды просмотра состояния, изменения конфигурации и управления отдельными протоколами маршрутизации. Приведённые ниже приглашения командной строки являются примерами; их вид зависит от имени устройства и настроек программного обеспечения.

1.6.2.1 Режимы командной строки

Таблица 13 – Режимы командной строки

Команда / клавиша	Назначение
router>	Пользовательский режим (если предусмотрен настройками доступа)
router#	Привилегированный режим выполнения команд
router(config)#	Режим глобального конфигурирования
router(config-if)#	Режим конфигурирования интерфейса
router(config-router)#	Режим конфигурирования протокола маршрутизации.

Для перехода в режим глобального конфигурирования из привилегированного режима используется команда **`configure terminal`**. Для возврата на предыдущий уровень используется **`exit`**, для завершения конфигурирования и возврата в привилегированный режим — **`end`**.

```
router# configure terminal
router(config)# interface eth1
router(config-if)# exit
router(config)# end
router#
```

1.6.2.2 Выполнение команд с использованием do

Команда **do** позволяет выполнить команду исполнительного режима, не выходя из текущего режима конфигурирования. Ключевое слово **do** вводится перед командой, которую необходимо выполнить.

Синтаксис команды:

```
do COMMAND
```

COMMAND — команда исполнительного режима, доступная для выполнения в данном контексте.

Во время настройки интерфейса можно проверить его состояние, не покидая режим конфигурирования:

```
router# configure terminal
router(config)# interface eth1
router(config-if)# description Uplink
router(config-if)# do show interface eth1
```

Аналогично можно просмотреть текущую конфигурацию:

```
router(config-if)# do show running-config
```

Использование **do** не изменяет текущий режим конфигурирования: после выполнения команды пользователь остаётся в прежнем режиме.

1.6.2.3 Автоматическое дополнение команд (Tab)

Клавиша Tab используется для автоматического дополнения вводимых ключевых слов и, где это поддерживается, других элементов команды. Если введённая последовательность однозначно определяет продолжение, CLI дополняет её до соответствующего слова.

Пример использования

В режиме глобального конфигурирования введите начало команды:

```
router(config)# inter
```

Нажмите клавишу Tab. При однозначном соответствии CLI дополнит ключевое слово до **interface**. Затем можно указать имя интерфейса:

```
router(config)# interface eth1
```

Если введённый фрагмент соответствует нескольким вариантам, автоматическое дополнение может не выполняться; поведение вывода вариантов зависит от версии CLI. В этом случае необходимо ввести дополнительные символы или воспользоваться контекстной справкой.

1.6.2.4 Контекстная справка (?)

Символ **?** используется для получения списка доступных команд, ключевых слов или аргументов в текущем контексте. В отличие от Tab, контекстная справка предназначена для просмотра допустимых вариантов ввода и их кратких описаний.

Примеры использования

```
router# ?
router(config)# ?
router(config)# interface ?
```

Набор отображаемых вариантов зависит от текущего режима и доступных функций. Для получения справки по следующему аргументу вводят пробел после завершённого ключевого слова и затем **?**.

1.6.2.5 Сокращённый ввод команд

CLI допускает ввод сокращений ключевых слов при условии, что сокращение однозначно определяет команду в текущем режиме. Если введённое сокращение неоднозначно, команду необходимо уточнить.

```
router# conf t
router(config)# int eth1
```

В эксплуатационной документации рекомендуется приводить полные формы команд. Сокращения удобно использовать при интерактивной настройке, однако они могут становиться неоднозначными при изменении состава команд в разных версиях программного обеспечения.

1.6.1 Структура командной строки

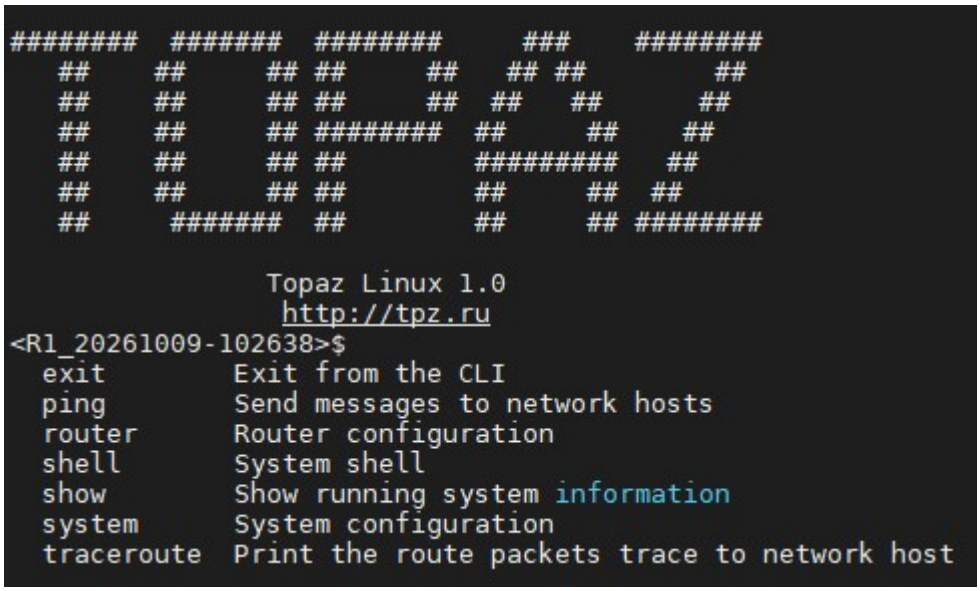


Рисунок 3 - Структура командной строки

```
Exit – выход из текущего подменю
Ping – утилита ping
Router- меню конфигурирования функций маршрутизатора и сетевых интерфейсов
Shell – подменю ТОС TOPAZ Linux
Show – команды просмотра
System – подменю системы
Traceroute – утилита для трассировки
```

1.7 Подменю System

Далее будут описаны настройки устройства, выполняемые в подменю system.

1.7.1 VRF

VRF (Virtual Routing and Forwarding) – технология, которая позволяет изолировать маршрутную информацию, принадлежащую различным классам (например, маршруты разных сервисов).

Для создания VRF необходимо войти в меню System:

```
system
```

Потом запустить режим конфигурации:

```
configure terminal
```

Далее для создания VRF:

```
vrf interface table-id <VRF table id>
```

<VRF table id> - уникальный идентификатор таблицы VRF, число от 1 до 252 (идентификаторы от 253 до 255 зарезервированы). Будет создан интерфейс **vrf<VRF table id>** и открыто подменю интерфейса VRF со строкой приглашения вида **config-vrf<VRF table id>.**

В подменю интерфейса VRF можно задать интерфейсы для указанного VRF:

```
interface <Network interface>
```

<Network interface> - имя сетевого интерфейса, по нажатию “TAB” будут предложены возможные варианты.

```
topaz-6810000045> system
topaz-6810000045# configure terminal
topaz-6810000045(config)# vrf interface table-id 100
topaz-6810000045(config-vrf100)# interface
eth0   eth1   eth2   lo     vrf100
topaz-6810000045(config-vrf100)# interface eth0
topaz-6810000045(config-vrf100)# exit
topaz-6810000045(config)# do show running-config
!
hostname topaz-6810000045
!
vrf interface table-id 100
 interface eth0
topaz-6810000045(config)#
```

Рисунок 4 - Подменю интерфейса VRF

Для удаления интерфейса из VRF, в подменю **config-vrf<VRF table id>** ввести команду

```
no interface <Network interface>
```

Для удаления VRF ввести команду

```
no vrf interface table-id <VRF table id>
```

```
topaz-6810000045(config-vrf100)# no interface eth0
topaz-6810000045(config-vrf100)# no vrf interface table-id 100
topaz-6810000045(config)#
```

Рисунок 5 - Удаление VRF

Примечание Нельзя отнести уже созданный интерфейс, имеющий IP адрес, в VRF, нужно сначала удалить с интерфейса IP адрес, добавить в VRF и далее присвоить интерфейсу IP адрес.

1.7.2 GRE туннели

Для создания GRE туннеля запустить режим конфигурации в подменю **system**:

```
configure terminal
```

Дать команду

```
tunnel tun-id <Tunnel id> mode <GRE mode>
```

<Tunnel id> - номер-идентификатор интерфейса от 1 до 255, **<GRE mode>** - режим работы туннеля, **gre** или **gretap**, в режиме **gretap** туннель может работать с кадрами канального уровня, интерфейс можно добавить в **bridge**.

В результате исполнения команды будет создан туннельный интерфейс **tun<Tunnel id>**, и открыто подменю интерфейса со строкой приглашения вида **config-if-tun<Tunnel id>.**

В подменю интерфейса необходимо задать локальный IP-адрес и IP-адрес удалённой стороны:

```
local <A.B.C.D>
remote <A.B.C.D>
```

Здесь же можно настроить ключ:

```
key <Key>
```

<Key> - 32-битное число, одинаковое для всех участников тоннеля.

Можно задать установку TTL для туннелированных пакетов:

```
ttl <TTL value>
```

Команда **no ttl** отключит эту опцию, TTL туннелированных пакетов не будет изменяться.

```
topaz-6810000045# configure terminal
topaz-6810000045(config)# tunnel tun-id 1 mode gre
topaz-6810000045(config-if-tun1)#local 10.10.10.10
topaz-6810000045(config-if-tun1)# remote 20.20.20.20
topaz-6810000045(config-if-tun1)# ttl 64
topaz-6810000045(config-if-tun1)# key 0xffffffff
topaz-6810000045(config-if-tun1)# exit
topaz-6810000045(config)# do show running-config
!
hostname topaz-6810000045
!
tunnel tun-id 1 mode gre
 key 0xffffffff
 local 10.10.10.10
 remote 20.20.20.20
 ttl 64
!
```

Рисунок 6 - Создание GRE туннеля

Для удаления туннельного интерфейса используется команда

```
no tunnel tun-id <Tunnel id>
```

```
topaz-6810000045(config-if-tun1)# no tunnel tun-id 1
topaz-6810000045(config)#
```

Рисунок 7 - Удаление туннельного интерфейса

Настройка IP-адресации для GRE интерфейса производится в меню **router**.

1.7.3 Loopback интерфейсы

Запустить режим конфигурации в подменю system:

```
configure terminal
```

Дать команду:

```
loopback id <lo id>
```

<lo id> - номер-идентификатор loopback-интерфейса.

```
topaz-6810000045(config)# loopback id 10
topaz-6810000045(config-lo10)# do show running-config
!
hostname topaz-6810000045
!
loopback id 10
```

Рисунок 8 - loopback-интерфейс

Для удаления loopback-интерфейса используется команда

```
no loopback id <lo id>
```

```
topaz-6810000045(config-lo10)# no loopback id 10
topaz-6810000045(config)#
```

Рисунок 9 - Удаление loopback-интерфейса

Настройка IP-адресации производится в меню **router**.

1.7.4 VLAN интерфейсы

Запустить режим конфигурации:

```
configure terminal
```

Дать команду:

```
vlan interface <ethernet/bridge> <Network interface> vlan-id <VLAN id>
```

<ethernet/bridge> - выбор типа интерфейса, **<Network interface>** - имя сетевого интерфейса, к которому будет привязан VLAN-интерфейс, по нажатию “TAB” будут показаны доступные варианты, **<VLAN id>** - идентификатор VLAN. В результате исполнения команды будет создан VLAN-интерфейс **<Network interface>.<VLAN id>**.

```
topaz-6810000045# configure terminal
topaz-6810000045(config)# vlan interface
ethernet bridge
topaz-6810000045(config)# vlan interface ethernet
eth1 eth2 eth0
topaz-6810000045(config)# vlan interface ethernet eth0 vlan-id
  Number in the range 1-4094  VLAN id

topaz-6810000045(config)# vlan interface ethernet eth0 vlan-id 10
topaz-6810000045(config-if-eth0.10)# do show running-config
!
hostname topaz-6810000045
!
vlan interface ethernet eth0 vlan-id 10
topaz-6810000045(config-if-eth0.10)#
```

Рисунок 10 - VLAN-интерфейс

Для удаления VLAN-интерфейса используется команда

```
no vlan interface <ethernet/bridge> <Network interface> vlan-id <VLAN id>
```

```
topaz-6810000045(config-if-eth0.10)# no vlan interface ethernet eth0 vlan-id 10
topaz-6810000045(config)#
```

Рисунок 11 - Удаление VLAN-интерфейса

Настройка IP-адресации производится в меню **router**.

1.7.5 Bridge интерфейс

Bridge интерфейс позволяет объединять несколько интерфейсов в режим «коммутатора»

Запустить режим конфигурации:

```
configure terminal
```

Дать команду:

```
bridge interface group-id <Bridge group id>
```

<Bridge group id> - номер-идентификатор интерфейса от 1 до 255. В результате работы команды будет создан bridge-интерфейс **br<Bridge group id>**, и открыто подменю интерфейса со строкой приглашения вида **config-if-br<Bridge group id>.** В подменю интерфейса можно добавить интерфейсы в этот bridge:

```
interface <ethernet/tunnel> <Network interface>
```

<ethernet/tunnel> - выбор типа интерфейса, **<Network interface>** - имя сетевого интерфейса, по нажатию “TAB” будут показаны доступные варианты.

Можно включить Spanning Tree Protocol:

```
stp <classic/rapid>
```

Отключить Spanning Tree Protocol можно командой **no stp**

```
topaz-6810000045(config)# bridge interface group-id 1
topaz-6810000045(config-if-br1)# interface
ethernet tunnel
topaz-6810000045(config-if-br1)# interface tunnel tun1
topaz-6810000045(config-if-br1)# interface ethernet
eth1 eth2 eth0
topaz-6810000045(config-if-br1)# interface ethernet eth1
topaz-6810000045(config-if-br1)# stp
classic rapid
topaz-6810000045(config-if-br1)# stp rapid
topaz-6810000045(config-if-br1)# do show running-config
!
hostname topaz-6810000045
!
tunnel tun-id 1 mode gretap
 local 10.10.10.10
 remote 20.20.20.20
 ttl 64
!
bridge interface group-id 1
 interface ethernet eth1
 interface tunnel tun1
 stp rapid
topaz-6810000045(config-if-br1)#
```

Рисунок 12 - Отключение Spanning Tree Protocol

Удалить bridge-интерфейс можно командой

```
no bridge interface group-id <Bridge group id>
```

```
topaz-6810000045(config-if-br1)# no bridge interface group-id 1
topaz-6810000045(config)#
```

Рисунок 13 - Удаление bridge-интерфейса

Настройка IP-адресации производится в меню **router**.

1.7.6 PRP интерфейс

Интерфейс PRP используется для подключения к сети с протоколом бесшовного резервирования PRP (Parallel Redundancy Protocol IEC 62439-3). Устройство может быть узлом DANP.

Запустить режим конфигурации:

```
configure terminal
```

Дать команду:

```
prp interface id <prp id> port_a <Network interface> port_b <Network interface>
```

port_a – интерфейс для подключения к сети «А»,
port_b – интерфейс для подключения к сети «Б»
<Network interface> - имя сетевого интерфейса в системе, по нажатию “TAB” будут показаны доступные варианты, для корректной работы требуется выбирать физические интерфейсы в системе.
В результате исполнения команды будет создан интерфейс **prp0 (id 0)**.

1.7.7 Режим работы RedBox

Для аппаратной платформы TOPAZ FW MX681 поддерживается режим работы RedBox для сетей с использованием протокола бесшовного резервирования PRP (IEC 62439-3).

RedBox подключает узлы SAN к двум независимым сетям PRP (А и Б) и выполняет для них функции двухпортового узла DANP: передаёт кадры в обе сети, а полученные копии сводит к одной для SAN устройств.

Запустить режим конфигурации:

```
configure terminal
```

Дать команду:

```
rb interface port_a <Network interface> port_b <Network interface> interlink <Network interface>
```

port_a – интерфейс для подключения к сети «А»,

port_b – интерфейс для подключения к сети «Б»,

interlink – интерфейс для подключения SAN устройства,

<Network interface> - имя сетевого интерфейса в системе, по нажатию “TAB” будут показаны доступные варианты, для корректной работы требуется выбирать физические интерфейсы в системе.

В результате исполнения команды будет создан интерфейс **RB (RedBox).**



Примечание Для режима Redbox задействуются 3 сетевые интерфейса на устройстве, интерфейсы нельзя использовать как независимые порты и назначать IP адресацию, IP адреса присваиваются созданному интерфейсу RB. В системе можно создать только один интерфейс RedBox.

1.7.8 Работа с конфигурацией устройства

Сохранение конфигурации устройства осуществляется из подменю **system** с помощью команды **write**, после ее выполнения конфигурация сохраняется в энергонезависимую память устройства.

Просмотр текущей конфигурации устройства осуществляется с помощью команды

```
show running-config
```

Просмотр текущей сохраненной конфигурации

```
show startup-config
```

1.7.9 Сброс к заводским настройкам

Для сброса к заводским настройкам с удалением всей конфигурации в подменю **system** необходимо выполнить команду

```
restore default-config
```

1.8 Подсистема router

В данной подсистеме настраивается IP адресация для интерфейсов, статические маршруты, протоколы динамической маршрутизации, VRRP, фильтрация маршрутов, а также протокол MPLS.

1.8.1 Настройки интерфейсов

Для настройки интерфейсов предусмотрены следующие функции:

- назначение и удаление IPv4- и IPv6-адресов;
- включение и отключение интерфейсов;
- назначение текстового описания;
- настройка параметра пропускной способности, используемого протоколами маршрутизации;
- управление отслеживанием состояния физического соединения;
- управление поддержкой многоадресной передачи;
- настройка параметров MPLS и Traffic Engineering;
- просмотр текущего состояния и параметров интерфейсов.

Таблица 14 - Команды настройки сетевых интерфейсов

Команда	Описание
interface IFNAME	Переход в режим конфигурирования указанного интерфейса
description DESCRIPTION	Назначение текстового описания интерфейса
ip address ADDRESS/PREFIX	Назначение IPv4-адреса
ipv6 address ADDRESS/PREFIX	Назначение IPv6-адреса
Shutdown/ no shutdown	Отключение / включение интерфейса
link-detect / no link-detect	Управление отслеживанием состояния соединения
bandwidth VALUE	Установка расчётной пропускной способности
mpls enable / mpls disable	Управление обработкой MPLS

1.8.1.1 Настройка IP адресации

Для назначения IPv4-адреса используется команда

```
ip address ADDRESS/PREFIX
```

где:

ADDRESS — IPv4-адрес,

PREFIX — длина префикса от 0 до 32.

Для удаления адреса используется

```
no ip address ADDRESS/PREFIX
```

Для IPv6 используются команды **ipv6 address ADDRESS/PREFIX** и **no ipv6 address ADDRESS/PREFIX**, длина префикса — от 0 до 128.

Интерфейсу могут быть назначены IPv4- и IPv6-адреса одновременно.

```
router# configure terminal
router(config)# interface eth1
router(config-if)# ip address 192.0.2.1/24
router(config-if)# ipv6 address 2001:db8:1::1/64
router(config-if)# no shutdown
router(config-if)# exit
```

1.8.1.2 Управление административным состоянием

Команда **Shutdown** административно отключает интерфейс; команда **no shutdown** отменяет отключение. Фактическая доступность интерфейса также зависит от физического соединения, драйвера и операционной системы.

```
router(config)# interface eth1
router(config-if)# shutdown
router(config-if)# no shutdown
```

1.8.1.3 Настройка описания интерфейса

Команда **description DESCRIPTION** задаёт произвольное текстовое описание назначения интерфейса, например подключённого оборудования или канала связи.

```
router(config)# interface eth1
router(config-if)# description Uplink_to_Core_Router
```

1.8.1.4 Настройка пропускной способности

Команда **bandwidth VALUE** задаёт значение пропускной способности, используемое протоколами маршрутизации для расчёта метрик. Команда не меняет физическую скорость соединения и не ограничивает трафик.

```
router(config)# interface eth1
router(config-if)# bandwidth 1000
```

1.8.1.5 Отслеживание состояния соединения

Механизм **link-detect** позволяет учитывать состояние соединения, предоставляемое драйвером интерфейса. Для включения используется **link-detect**, для отключения — **no link-detect**. В заводской конфигурации механизм включён по умолчанию.

```
router(config)# interface eth1
router(config-if)# link-detect
```

1.8.1.6 Обработка MPLS

Команды **mpls enable** и **mpls disable** управляют обработкой MPLS на интерфейсе. Включение MPLS не выполняет автоматически настройку протоколов распределения меток.

```
router(config)# interface eth1
router(config-if)# mpls enable
```

1.8.1.7 Просмотр состояния интерфейсов

Таблица 15 - Просмотр состояния интерфейсов

Команда	Назначение
show interface	Информация обо всех интерфейсах
show interface IFNAME	Подробная информация об интерфейсе
show interface brief	Краткая информация

```
router# show interface eth1
router# show interface brief
```

1.8.2 BGPv4

BGP (Border Gateway Protocol — протокол междоменной маршрутизации, используемый для обмена маршрутами между автономными системами (AS), а также внутри одной AS. В этом разделе приведён порядок настройки соседства BGPv4 для семейства адресов IPv4 unicast, публикации IPv4-префиксов и проверки состояния сеанса.

1.8.2.1 Термины и обозначения

Таблица 16 - Термины и обозначения BGP

Термин	Описание
BGPv4	BGP для обмена маршрутами IPv4, адресное семейство IPv4 unicast задаётся контекстом address-family ipv4 unicast.
AS / ASN	Автономная система / её номер. В примерах используются 65001 и 65002.
eBGP	Соседство между маршрутизаторами с разными номерами AS.
iBGP	Соседство между маршрутизаторами с одним номером AS.
AFI/SAFI	Тип адресов и тип пересылаемой информации. Для этого раздела — IPv4 / unicast.
Префикс	IPv4-сеть с длиной маски, например 198.51.100.0/24.
RIB	База маршрутизации; таблица маршрутов, используемая протоколами и маршрутизатором.

Route-map / prefix-list	Механизмы политики маршрутизации и фильтрации префиксов.

1.8.2.2 Предварительные условия

- Проверьте IP-адреса интерфейсов и наличие IP-достижимости до адреса BGP-соседа. Для соседства через **loopback** требуется предварительно обеспечить маршрут до loopback-адреса в обе стороны.
- Согласуйте локальный и удалённый ASN, адреса соседей, нужные префиксы, направления фильтрации и политику **next-hop** с администратором соседнего узла.
- Перед изменениями сохраните текущую конфигурацию и предусмотрите способ восстановления доступа, если изменение повлияет на маршрут управления.

1.8.2.3 Общий алгоритм настройки

- Указать локальный ASN, **router-id** и адрес соседнего маршрутизатора.
- Создать BGP-процесс командой **router bgp** и объявить соседство через **neighbor remote-as**.
- При необходимости задать источник TCP-соединения командой **neighbor update-source**.
- В контексте **address-family ipv4 unicast** активировать соседа и задать публикацию собственных префиксов командой **network**.
- При необходимости определить **prefix-list** и **route-map**, затем применить политику к входящим или исходящим маршрутам соседа.
- Для **iBGP** при соответствующей схеме маршрутизации рассмотреть **neighbor next-hop-self**.
- Проверить конфигурацию, состояние BGP-сеанса, полученные и отправленные маршруты
- Сохранить конфигурацию.

1.8.2.4 Основные команды конфигурирования

Таблица 17 - Основные команды конфигурирования

Команда	Назначение и параметры
router bgp ASN	Создаёт или открывает процесс BGP с локальным номером автономной системы ASN.
bgp router-id A.B.C.D	Задаёт идентификатор BGP-маршрутизатора в формате IPv4. Выберите стабильное уникальное значение в пределах домена маршрутизации.
neighbor A.B.C.D remote-as ASN	Объявляет BGP-соседа по IPv4-адресу и задаёт номер удалённой AS. Совпадающий локальный/удалённый ASN соответствует iBGP, различный — eBGP.
neighbor A.B.C.D update-source IFACE|A.B.C.D	Задаёт локальный интерфейс или адрес источника для BGP-соединения. Используйте, например, при peering через loopback; поддерживаемую форму аргумента уточните в справке установленной версии.
address-family ipv4 unicast	Входит в контекст обмена маршрутами IPv4 unicast.
neighbor A.B.C.D activate	Активирует соседа для выбранного адресного семейства. Указывайте в контексте address-family, если это требуется используемым режимом/версией.
network PREFIX	Добавляет IPv4-префикс к объявлениям BGP для текущего address-family. Публикация зависит от наличия соответствующего маршрута в RIB и поведения import-check в данной версии/режиме.

neighbor A.B.C.D next-hop-self	При отправке маршрута соседу заменяет next-hop на адрес текущего маршрутизатора; обычно применяется в iBGP-схеме, когда соседу иначе недоступен исходный next-hop.
neighbor A.B.C.D route-map NAME in|out	Применяет именованную политику к входящим или исходящим маршрутам конкретного соседа.
ip prefix-list NAME seq N permit|deny PREFIX/LEN	Создаёт правило списка префиксов. Для диапазона длин масок могут применяться ge и le; проверьте точный синтаксис и допустимые значения для версии.

1.8.2.5 Настройка eBGP для IPv4 unicast

Пример:
Локальный маршрутизатор использует AS 65001 и адрес 192.0.2.1;
Сосед — AS 65002 и адрес 192.0.2.2.
Префикс 198.51.100.0/24 указан как пример отдаваемого маршрута

```
configure terminal
router bgp 65001
bgp router-id 192.0.2.1
neighbor 192.0.2.2 remote-as 65002
address-family ipv4 unicast
neighbor 192.0.2.2 activate
network 198.51.100.0/24
exit-address-family
exit
end
```

1.8.2.6 Настройка iBGP для IPv4 unicast

В iBGP локальный и удалённый маршрутизаторы используют один ASN. Ниже приведён фрагмент для соседа 10.0.0.2 в той же AS 65001. Предполагается, что loopback0 уже настроен и между loopback-адресами есть связность.

```
configure terminal
router bgp 65001
bgp router-id 10.0.0.1
neighbor 10.0.0.2 remote-as 65001
neighbor 10.0.0.2 update-source lo1
address-family ipv4 unicast
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 next-hop-self
exit-address-family
exit
end
```

1.8.2.7 Просмотр состояния BGP сессий

Таблица 18 - Просмотр состояния BGP сессий

Команда	Назначение
show bgp summary	Состояние сеанса: состояние соседа, длительность соединения, счётчики и число принятых / отправленных префиксов.
show bgp ipv4 unicast	Таблица BGP IPv4 unicast и выбранные маршруты.
show bgp ipv4 unicast neighbors A.B.C.D	Сведения о конкретном соседе и параметрах сеанса; доступные поля могут различаться по версии.

1.8.3 L3VPN на основе MP-BGP (VPNv4)

MP-BGP (Multiprotocol BGP) расширяет BGP механизмами обмена NLRI для разных адресных семейств. В типовой MPLS L3VPN-схеме PE-маршрутизаторы (Provider Edge) обмениваются VPN-IPv4 маршрутами через семейство IPv4 VPN (VPNv4), используется специальный address-family ipv4 vpn. Маршруты клиентских сетей находятся в отдельных VRF, экспортируются в VPN RIB с RD, RT и VPN label, а на удалённом PE импортируются в VRF по совпадающему RT.

1.8.3.1 Предварительные условия

Создайте VRF на маршрутизаторе в подменю system и привяжите к ней клиентские интерфейсы.

Обеспечьте IP-достижимость между loopback-адресами PE и настройте MP-BGP-соседство между ними. В типовой схеме PE обмениваются VPNv4 внутри одной AS (iBGP), напрямую или через route reflector.

Настройте и проверьте распределение транспортных меток и поддержку MPLS на всех участвующих линках/узлах. Одного VPNv4 BGP-соседства недостаточно для пересылки пользовательского трафика.

Согласуйте для каждой VRF уникальные RD, экспортируемые RT и RT импорта, а также способ получения маршрутов от CE: статические маршруты, BGP или другой разрешённый протокол.

1.8.3.2 Пример MP-BGP соседства PE—PE

Пример для PE с ASN 65000, router-id 192.0.2.1 и удалённым PE 192.0.2.2 с VPNv4-маршрутами; адреса loopback и транспортная MPLS-связность должны быть настроены отдельно.

```
configure terminal
router bgp 65000
bgp router-id 192.0.2.1
neighbor 192.0.2.2 remote-as 65000
address-family ipv4 vpn
neighbor 192.0.2.2 activate
exit-address-family
exit
end
```

1.8.3.3 Пример VRF и обмена маршрутами с VPN RIB

Ниже показан BGP-фрагмент для клиентской VRF vrf10. Предполагается, что VRF vrf10 создана в маршрутизаторе, а клиентский префикс 10.10.10.0/24 уже присутствует в её таблице маршрутизации. Номера ASN, RD и RT условные; в рабочей сети используйте согласованные значения.

```
configure terminal
router bgp 65000 vrf vrf10
address-family ipv4 unicast
rd vpn export 65000:101
rt vpn export 65000:100
rt vpn import 65000:100
label vpn export auto
export vpn
import vpn
exit-address-family
exit
end
```

Параметры задаются в контексте IPv4 unicast соответствующей VRF. **`export vpn`** включает передачу маршрутов из VRF в VPN RIB; **`import vpn`** — импорт из VPN RIB по RT. Если маршруты клиентской сети будут получаться динамически от CE (Customer Edge), настройте PE—CE протокол в этой VRF и его политику отдельно.

1.8.3.4 Команды L3VPN и проверки

Таблица 19 - Команды L3VPN и проверки

Команда	Назначение
router bgp ASN vrf VRFNAME	Открывает BGP-контекст VRF. VRFNAME должна бытьсоздана на маршрутизаторе
address-family ipv4 vpn	Включает контекст VPNv4 (IPv4 VPN SAFI) в глобальном BGP-процессе.
rd vpn export ASN:NN	Задаёт RD для маршрутов, экспортируемых из текущей VRF в VPN RIB.
rt vpn export RTLIST	Назначает экспортируемый Route Target (или список RT) VPN-маршрутам этой VRF.
rt vpn import RTLIST	Задаёт RT, по которым VPN-маршруты импортируются в текущую VRF.
label vpn export auto	Запрашивает автоматическое назначение VPN label через Zebra; команда и режим должны поддерживаться установленной версией.
export vpn / import vpn	Включает экспорт из VRF в VPN RIB и импорт из VPN RIB в VRF соответственно.
show bgp ipv4 vpn summary	Показывает состояние соседств для семейства IPv4 VPN, если такая форма команды поддерживается версией.
show bgp ipv4 vpn rd all	Показывает VPNv4 маршруты по всем RD.
show ip route vrf VRFNAME	Показывает маршруты в таблице, указанной VRF; убедитесь, что импортированные клиентские префиксы установлены в нужную таблицу.

При диагностике последовательно проверьте:

- BGP-соседство VPNv4;
- наличие VPNv4 маршрута с ожидаемыми RD, RT и меткой;
- совпадение export RT удалённой VRF с import RT локальной VRF;
- появление маршрута в VRF RIB;
- разрешение next-hop и работоспособность MPLS-транспорта.

1.8.4 MPLS

MPLS (Multiprotocol Label Switching) — технология передачи пакетов по меткам. На входе в MPLS-сеть к пакету добавляется метка, транзитные маршрутизаторы заменяют её на следующую, а на выходе метка снимается; это позволяет пересылать трафик по заранее известному пути через ядро сети. Для обмена метками используется протокол LDP.

LDP (Label Distribution Protocol) автоматически обменивается MPLS-метками между соседними маршрутизаторами. В типовой сети провайдера LDP вместе с IGP формирует транспортные LSP: IGP обеспечивает IP-достижимость адресов маршрутизаторов, а LDP распространяет соответствующие метки для пересылки через MPLS-ядро.

1.8.4.1 Основные термины

Таблица 20 - Основные термины LDP

Термин	Описание
LDP-сосед	Маршрутизатор, с которым установлено LDP-соседство и ведётся обмен метками
LSR ID / LDP Router ID	Идентификатор LDP-маршрутизатора; должен быть стабильным и достижимым в транспортной сети

LDP Discovery	Обнаружение соседей Hello-сообщениями на интерфейсах, где включён LDP
Label binding	Связь FEC/префикса с MPLS-меткой, объявленная локально или полученная от соседа
FEC	Класс эквивалентной пересылки; в типовой конфигурации LDP для IPv4 соответствует IP-префиксу
Транспортный LSP	Путь по MPLS-ядру, по которому пакет с меткой доставляется к следующему узлу/PE

1.8.4.2 Предварительные условия

- Настройте IGP или другой предусмотренный проектом способ IP-достижимости между LDP Router ID и адресами транспортных интерфейсов. LDP не распространяет маршруты IGP.
- Проверьте, что MPLS forwarding поддерживается и включён на интерфейсах MPLS-ядра.
- Согласуйте адрес LDP Router ID, транспортный адрес, интерфейсы, область распространения меток и способ защиты соседства. LDP следует включать только на интерфейсах транспортной сети, предусмотренных проектом.

1.8.4.3 Алгоритм настройки

- Проверьте IP-адреса транспортных интерфейсов и IP-маршрутизацию между маршрутизаторами ядра.
- Задайте **`LDP Router ID`**.
- В адресном семействе IPv4 укажите транспортный адрес **`discovery`** и перечислите интерфейсы, на которых разрешено LDP-обнаружение.
- На соседних маршрутизаторах настройте совместимые параметры и включите LDP на соответствующих линках.
- Проверьте активность интерфейсов LDP, обнаружение и состояние соседей, затем проверьте полученные **`label bindings`** и MPLS-таблицу.
- Проверьте сквозную MPLS-пересылку и достижимость целевых FEC.

1.8.4.4 Основные команды

Таблица 21 - Основные команды

Команда	Назначение и параметры
mpls ldp	Входит в контекст конфигурирования LDP
router-id A.B.C.D	Задаёт LDP Router ID
address-family ipv4	Входит в контекст LDP для IPv4
discovery transport-address A.B.C.D	Задаёт IPv4-адрес, используемый как транспортный адрес LDP в данном address-family
interface IFNAME	Включает LDP discovery на указанном интерфейсе. Интерфейс должен быть транспортным и поддерживать MPLS
neighbor A.B.C.D password TEXT	Необязательная аутентификация LDP-соседа, если поддерживается и согласована на обоих концах

1.8.4.5 Пример включения LDP

Пример для маршрутизатора ядра с Router ID и транспортным адресом 10.0.0.1. Имена eth1 и eth2 условные. Настройка IGP, IP-адресов интерфейсов выполняется отдельно.

```
configure terminal
mpls ldp
 router-id 10.0.0.1
```

```
 address-family ipv4
  discovery transport-address 10.0.0.1
  interface eth1
  interface eth2
 exit-address-family
exit
end
```

1.8.4.6 Проверка состояния

Таблица 22 - Проверка состояния

Команда	Что проверяется
show mpls ldp neighbor	Обнаруженные LDP-соседи, их идентификаторы, состояние и время работы соседства
show mpls ldp neighbor A.B.C.D detail	Подробные сведения о конкретном соседе; доступные поля зависят от версии
show mpls ldp discovery	Информация об обнаружении LDP-соседей
show mpls ldp ipv4 interface	Интерфейсы IPv4, на которых работает LDP, и состояние discovery
show mpls ldp ipv4 binding	Локальные и полученные от соседей соответствия префиксов и меток
show mpls table	Таблица MPLS-меток, установленная в dataplane
show ip route	Проверка IP-маршрутов к LDP Router ID и целевым префиксам

Рабочее соседство отображается со статусом OPERATIONAL. Проверяйте, что ожидаемые интерфейсы активны, сосед обнаружен, нужные метки получены и соответствующие записи присутствуют в MPLS-таблице. Наличие LDP-соседства без корректной IP-маршрутизации или MPLS-записей не подтверждает сквозную пересылку пакетов

1.8.5 OSPF

OSPFv2 — протокол внутренней маршрутизации, который обменивается сведениями о топологии внутри автономной системы. Маршрутизаторы формируют базу состояния каналов (LSDB), вычисляют кратчайшие пути алгоритмом SPF и устанавливают выбранные маршруты в таблицу маршрутизации.

1.8.5.1 Основные термины

Таблица 23 - Основные термины OSPF

Термин	Описание
OSPF Router ID	32-битный идентификатор маршрутизатора в формате IPv4. Он идентифицирует узел в OSPF и не обязан совпадать с адресом активного интерфейса
Area	Область OSPF, внутри которой маршрутизаторы обмениваются детальными LSAs. Магистральная область имеет ID 0.0.0.0.
LSDB	База объявлений состояния каналов, синхронизируемая между соседями в одной области
Сосед / смежность	Сосед обнаруживается по Hello-пакетам; на подходящих типах сетей маршрутизаторы устанавливают полную смежность и синхронизируют LSDB
Cost	Метрика OSPF для интерфейса/пути. При прочих равных меньшая суммарная стоимость предпочтительнее
DR / BDR	Designated Router и Backup DR на широковещательных сетях; сокращают число смежностей. На point-to-point линках выбор DR/BDR не выполняется

1.8.5.2 Предварительные условия

- Согласуйте **Area ID**, тип области, тип сети на интерфейсе, аутентификацию и параметры **Hello/Dead** с соседним маршрутизатором.
- Выберите уникальный **Router ID.** Убедитесь, что маршрутизаторы, которым нужно обмениваться маршрутами, имеют связность между интерфейсами.
- Определите, какие интерфейсы должны формировать соседства, а какие следует объявлять в OSPF без отправки Hello-пакетов. Для клиентских и пользовательских сегментов обычно проверяют необходимость passive-interface.

1.8.5.3 Алгоритм настройки

1. Проверьте IPv4-адреса и связность на OSPF-линках.
2. Создайте процесс **router ospf** и задайте стабильный **Router ID.**
3. Назначьте интерфейсы областям OSPF одним поддерживаемым способом: командами **network** в контексте **router ospf** либо командами **ip ospf area** в настройке интерфейса.
4. Настройте пассивные интерфейсы, метрики и согласованные параметры безопасности/таймеров, если это требуется проектом.
5. Проверьте состояние интерфейсов и соседей, синхронизацию LSDB и появление ожидаемых OSPF-маршрутов.
6. Сохраните конфигурацию

1.8.5.4 Пример настройки

Пример для маршрутизатора с Router ID 10.255.0.1. Сеть 192.0.2.0/30 — пример транзитного линка в Area 0.0.0.0; 198.51.100.0/24 — подключённый сегмент, который следует объявлять, но на котором не нужно устанавливать соседство.

```
configure terminal
router ospf
 ospf router-id 10.255.0.1
 network 192.0.2.0/30 area 0.0.0.0
 network 198.51.100.0/24 area 0.0.0.0
 passive-interface eth2
exit
end
```

Вместо команд **network** можно назначить область непосредственно интерфейсам. Пример ниже является альтернативой предыдущему способу. Не используйте оба способа одновременно на одном маршрутизаторе.

```
configure terminal
interface eth1
 ip ospf area 0.0.0.0
exit
interface eth2
 ip ospf area 0.0.0.0
 ip ospf passive
exit
router ospf
 ospf router-id 10.255.0.1
exit
end
```

1.8.5.5 Проверка состояния

Таблица 24 - Проверка состояния

Команда	Что проверяется
show ip ospf	Состояние процесса OSPF, Router ID и общая информация
show ip ospf interface [IFNAME]	Область, состояние интерфейса, таймеры, стоимость и параметры OSPF
show ip ospf neighbor	Список соседей и состояние смежностей
show ip ospf neighbor detail	Подробности о соседях, если форма поддерживается установленной версией
show ip ospf database	Содержимое/сводка LSDB
show ip ospf route	Маршруты, вычисленные OSPF после SPF
show ip route	Общая таблица маршрутизации; используйте её для проверки выбранных маршрутов и их источника

На **point-to-point** или **broadcast** сегменте с ожидаемым соседом проверьте переход смежности в **FULL**; на **broadcast**-сегменте состояния с DR/BDR могут отображаться иначе в зависимости от роли маршрутизатора. Затем убедитесь, что нужные маршруты видны в OSPF и установлены в RIB.

1.8.6 Статическая маршрутизация

Статическая маршрутизация задаёт маршрут вручную, администратор указывает префикс назначения и следующий узел или выходной интерфейс. Статические маршруты подходят для небольших или предсказуемых сетей, маршрута по умолчанию.

1.8.6.1 Основные термины

Таблица 25 - Основные термины статической маршрутизации

Термин	Описание
Префикс назначения	Сеть или адрес, к которому задаётся маршрут, например 203.0.113.0/24.
Следующий узел (next-hop)	IP-адрес маршрутизатора, которому передаётся пакет для дальнейшей доставки.
Маршрут по умолчанию	Маршрут 0.0.0.0/0, применяемый, если нет более специфичного маршрута.
Administrative distance	Приоритет источника маршрута, для static route обычно используется значение по умолчанию 1; большее значение может использоваться для резервного статического маршрута.
ECMP	Пересылка по нескольким равноправным next-hop для одного префикса

1.8.6.2 Предварительные условия

- Проверьте, что адрес **next-hop** достижим через активный интерфейс или другой маршрут.
- Для **default route** согласуйте адрес вышестоящего маршрутизатора и порядок резервирования. Наличие резервного маршрута не означает автоматическое обнаружение отказа удалённого сервиса, если **next-hop** остаётся достижимым.
- Перед изменением маршрута управления зафиксируйте текущий путь и подготовьте безопасный способ восстановления доступа.

1.8.6.3 Алгоритм настройки

1. Определите префикс назначения, основной **next-hop** и, если требуется, резервный путь.

2. Убедитесь в IP-достижимости **next-hop** и наличии правильного выходного интерфейса.
3. Добавьте маршрут командой **ip route** в конфигурации подменю **router**; для отдельной VRF укажите контекст VRF.
4. Проверьте наличие запись в таблице маршрутизации.
5. Проверьте фактическую пересылку трафика средствами платформы и при необходимости оцените контроль достижимости **next-hop**, например по ICMP.
6. Удаляйте маршрут командой **no ip route** с тем же префиксом и идентификатором **next-hop**.

1.8.6.4 Основные команды

Таблица 26 - Основные команды

Команда	Назначение и параметры
ip route PREFIX GATEWAY [DISTANCE]	Добавляет IPv4-маршрут через IP-адрес следующего узла. PREFIX задаётся с длиной маски, DISTANCE — необязательный административный приоритет
ip route PREFIX IFNAME [DISTANCE]	Добавляет маршрут через выходной интерфейс; применяйте с учётом типа канала и возможности однозначно определить next-hop
ip route PREFIX GATEWAY IFNAME [DISTANCE]	Задаёт и адрес следующего узла, и выходной интерфейс
ip route 0.0.0.0/0 GATEWAY [DISTANCE]	Добавляет маршрут IPv4 по умолчанию через указанный next-hop
ip route PREFIX GATEWAY ... vrf VRFNAME	Задаёт маршрут в конкретной VRF
no ip route PREFIX GATEWAY	Удаляет статический маршрут/next-hop. Для multipath удаляйте соответствующий next-hop, не затрагивая остальные
show ip route [PREFIX]	Показывает маршруты; используйте код источника S и состояние выбранного маршрута
show static routes [vrf NAME]	Показывает конфигурацию staticd и состояние next-hop, включая причины, по которым next-hop не установлен

1.8.6.5 Пример конфигурации

Пример направляет сеть 203.0.113.0/24 через основной шлюз 192.0.2.1. Второй шлюз 198.51.100.1 задан с большей **distance** как запасной путь.

```
configure terminal
ip route 203.0.113.0/24 192.0.2.1
ip route 203.0.113.0/24 198.51.100.1 200
ip route 0.0.0.0/0 192.0.2.1
end
```

Маршрут с меньшей **distance** предпочтительнее при прочих равных. Резервный статический маршрут выбирается, когда основной путь становится недоступен для разрешения **next-hop** или удаляется из таблицы. Если требуется обнаруживать отказ дальше непосредственного **next-hop**, используйте специально настроенный механизм контроля достижимости, например, BFD.

1.8.6.6 Проверка и диагностика

```
show ip route
show ip route 203.0.113.0/24
show static routes
```

В зависимости от вывода указанных команд, ниже приведены примеры диагностики.

Таблица 27 - Диагностика

Что наблюдается	Что проверить
Маршрут отсутствует в show ip route	Наличие команды в running-config; корректность префикса; разрешение next-hop; состояние интерфейса и VRF.
Маршрут настроен, но next-hop inactive	Результат show static routes, наличие маршрута до next-hop, существование/активность интерфейса и принадлежность нужной VRF.
Маршрут есть в RIB, но трафик не проходит	Выбран ли маршрут, установлен ли он в FIB, доступен ли следующий узел, корректны ли обратный маршрут, ACL/firewall и MTU.
Резервный маршрут не выбирается	Сравните administrative distance, проверьте, что основной next-hop действительно признан недоступным; сама потеря удалённого сервиса может не менять статический маршрут без отдельного мониторинга.

1.8.7 VRRP

VRRP (Virtual Router Redundancy Protocol) обеспечивает резервирование шлюза по умолчанию для узлов одного IP-сегмента. Несколько маршрутизаторов используют общий виртуальный IP-адрес; один из них работает в состоянии Master и обслуживает виртуальный адрес, остальные находятся в Backup и принимают роль Master при отказе текущего.

1.8.7.1 Основные термины

Таблица 28 - Основные термины

Термин	Описание
VRID	Идентификатор виртуального маршрутизатора в диапазоне 1–255. Узлы одной группы должны использовать одинаковый VRID на общем сегменте.
Virtual IP	Общий IPv4-адрес шлюза, используемый клиентами. На каждом участнике группы список виртуальных IP должен соответствовать проекту.
Master / Backup	Master обслуживает виртуальный адрес и отправляет объявления VRRP; Backup отслеживает объявления и готов принять роль.
Priority	Приоритет выбора Master. Задаётся в диапазоне 1–254; при равных значениях учитывается основной IP-адрес маршрутизатора.
Advertisement interval	Интервал отправки объявлений VRRP. Значение должно быть согласовано между участниками группы.
Preempt	Режим, при котором узел с более высоким приоритетом может занять роль Master после восстановления.

1.8.7.2 Предварительные условия

- Маршрутизатор использует **`macvlan`** для виртуального MAC-адреса VRRP и не создаёт необходимые системные macvlan-интерфейсы автоматически. Их требуется настроить в подменю system через vr; виртуальные IP должны быть назначены соответствующим macvlan-интерфейсам до активации VRRP.

- Участники одной группы должны быть подключены к одному L2-сегменту, иметь одинаковый VRID, версию протокола, виртуальные IP и согласованный интервал объявлений. Назначьте приоритеты согласно плану переключения.
- Проверьте фильтрацию трафика VRRP в L2-сети и на узлах.

1.8.7.3 Алгоритм настройки

1. Подготовьте общий L2-сегмент, базовые интерфейсы и системные macvlan-интерфейсы с виртуальными MAC и адресами.
2. На каждом маршрутизаторе создайте VRRP-группу с одним и тем же VRID и версией протокола на соответствующем интерфейсе.
3. Задайте общий виртуальный IPv4-адрес и согласованный интервал объявлений; настройте приоритеты для выбора предпочтительного Master.
4. Проверьте состояние show vrrp на каждом участнике и подтвердите, что один участник стал Master, а остальные — Backup.
5. Проверьте доступность шлюза клиентами и плановое переключение в согласованном испытании; убедитесь, что маршрутизация за пределами LAN настроена отдельно.

1.8.7.4 Основные команды

Таблица 29 - Основные команды

Команда	Назначение и параметры
interface IFNAME	Открывает контекст интерфейса, на котором настроена VRRP-группа.
vrrp VRID version 2|3	Создаёт группу с заданным VRID и выбирает версию протокола. Если версия не указана, VRRPv3 по умолчанию.
vrrp VRID ip A.B.C.D	Добавляет виртуальный IPv4-адрес. Этот адрес должен быть предварительно назначен соответствующему системному macvlan-интерфейсу.
vrrp VRID priority 1–254	Задаёт приоритет участника. Более высокий приоритет обычно выбирает Master; значение 255 зарезервировано для текущего владельца адреса по спецификации и не задаётся этой командой.
vrrp VRID advertisement-interval MS	Задаёт интервал объявлений в миллисекундах; документирует диапазон 10–40950 мс с шагом 10 мс.
vrrp VRID preempt	Включает режим вытеснения. Он включён по умолчанию
vrrp VRID shutdown / no vrrp VRID shutdown	Административно останавливает VRRP-группу
show vrrp [interface IFNAME] [VRID]	Показывает состояние VRRP-групп, включая роль, приоритет, виртуальные адреса и счётчики объявлений.

1.8.7.5 Пример конфигурации

Пример для интерфейса eth0, VRID 5 и виртуального адреса 10.0.2.16. Значения и имя интерфейса условные. До применения подготовьте macvlan.

```
configure terminal
interface eth0
 vrrp 5 version 3
 vrrp 5 priority 200
```

```
 vrrp 5 advertisement-interval 1000
 vrrp 5 ip 10.0.2.16
exit
end
```

На резервном маршрутизаторе используйте тот же VRID, версию, виртуальный IP и интервал; задайте другой приоритет, например, 150. Оба участника должны видеть объявления друг друга в общем сегменте. VRRP активируется после добавления IP-команды; если требуется отложить запуск, примените административный shutdown и снимите его после подготовки.

1.8.7.6 Проверка состояния

```
show vrrp
show vrrp interface eth0
show vrrp interface eth0 5
```

Таблица 30 - Проверка состояния

Проверка	Ожидаемый результат
Состояние группы	На одном участнике отображается Master, на остальных — Backup.
VRID и виртуальный IP	Участники используют ожидаемые одинаковые значения на соответствующем сегменте.
Приоритет и preempt	Роль Master соответствует плану выбора; после восстановления при необходимости происходит ожидаемое вытеснение.
Объявления	Счётчики передачи и приёма объявлений меняются в соответствии с ролью и интервалом.
Системные macvlan	Виртуальные интерфейсы существуют и имеют требуемые MAC/IP; FRR не создаёт их автоматически.
Клиентская пересылка	Клиенты используют Virtual IP как шлюз; маршруты к внешним сетям и обратная маршрутизация проверяются отдельно.

1.9 Настройка правил межсетевого экрана

Управление трафиком осуществляется с помощью утилиты **iptables** (утилита командной строки, являющая стандартным интерфейсом управления работой межсетевого экрана). Межсетевой экран работает по принципу цепочек правил. Для использования утилиты **iptables** необходимо войти в режим Shell:

```
shell
```

1.9.1 Правила и действия

Для каждого типа пакетов можно установить набор правил, которые по очереди будут проверяться на соответствие с пакетом, и если пакет соответствует, то применять к нему указанное в правиле действие. Правила образуют цепочку, поэтому input, output и forward называют цепочками правил. Действий может быть несколько:

- **ACCEPT** - разрешить прохождение пакета дальше по цепочке правил;
- **DROP** - удалить пакет;

- **REJECT** - отклонить пакет, отправителю будет отправлено сообщение, что пакет был отклонен;
- **LOG** - сделать запись о пакете в лог файл;
- **QUEUE** - отправить пакет пользовательскому приложению.

Обрабатываемые пакеты проходят через заданные пользователем цепочки правил до тех пор, пока не будут приняты (**ACCEPT**), отклонены (**REJECT**) или не обработаны (**DROP**).

Правила могут проверять любые соответствия, например, по ip, по порту получателя или отправителя, заголовкам пакета и многому другому. Если пакет не подходит ни одному из правил, то к нему применяется действие по умолчанию, обычно ACCEPT.

Кроме перечисленных выше, есть еще две дополнительные цепочки правил:

- **prerouting** - в эту цепочку пакет попадает перед обработкой iptables;
- **postrouting** - сюда попадают все проходящие пакеты, которые уже прошли цепочку forward.

1.9.2 Таблицы iptables

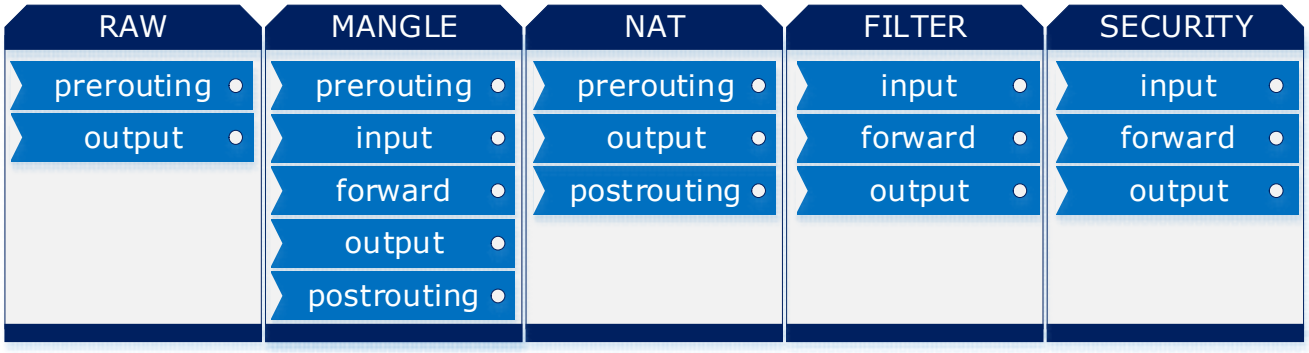


Рисунок 14 - Таблицы iptables

В системе есть несколько таблиц, и все они имеют стандартный набор цепочек input, forward и output. Таблицы предназначены для выполнения разных действий над пакетами, например для модификации или фильтрации. Фильтрация пакетов iptables осуществляется в таблице filter.

Таблица Filter предназначена для фильтрации трафика, то есть разрешения и запрета пакетов и соединений. Для таблицы Filter существуют три базовых цепочки:

INPUT – цепочка для входящих пакетов;

FORWARD – цепочка для перенаправляемых пакетов;

OUTPUT – цепочка для отправляемых пакетов.

Таблица NAT предназначена для операций stateful-преобразования (преобразования на основании данных о соединении) сетевых адресов и портов обрабатываемых пакетов. Для таблицы NAT существуют две базовых цепочки:

PREROUTING – в эту цепочку пакеты попадают до принятия решения о маршрутизации;

POSTROUTING – через эту цепочку проходят все исходящие пакеты;

OUTPUT – через эту цепочку проходят пакеты, сгенерированные процессами хоста.

Таблица Mangle предназначена для операций по классификации и маркировке пакетов и соединений, а также модификации заголовков пакетов (поля TTL и TOS). Для таблицы Mangle существуют следующие базовые цепочки:

PREROUTING — позволяет модифицировать пакет до принятия решения о маршрутизации;

INPUT — позволяет модифицировать пакет, предназначенный самому хосту;

FORWARD — цепочка, позволяющая модифицировать транзитные пакеты;

OUTPUT — позволяет модифицировать пакеты, исходящие от хоста;

POSTROUTING — дает возможность модифицировать все исходящие пакеты, как сгенерированные самим хостом, так и транзитные.

Талица Raw предназначена для выполнения действий с пакетами до их обработки системой conntrack (отслеживание состояний соединений). Для таблицы Raw существуют следующие базовые цепочки:

PREROUTING — в эту цепочку входящие пакеты попадают раньше, чем в любую другую из цепочек iptables, и до обработки их системой conntrack;
OUTPUT — аналогично для пакетов, сгенерированных хостом.

1.9.3 Утилита iptables

Утилита **iptables** предназначена для управления таблицами маршрутизации и NAT.

1.9.3.1 Синтаксис

```
iptables [-t <таблица>] [<опции>]
```

Таблица 31 - Таблицы утилиты iptables

Таблица	Описание
filter	Таблица по умолчанию. Данная таблица содержит предопределённые цепочки INPUT (для входящих), FORWARD (для перенаправляемых пакетов) и OUTPUT (для исходящих пакетов)
nat	Данная таблица используется для пакетов, устанавливающих новое соединение. В ней содержится три предопределённых цепочки: PREROUTING (для изменения входящих пакетов), OUTPUT (для изменения локально сгенерированных пакетов перед их отправлением) и POSTROUTING (для изменения всех исходящих пакетов)
mangle	Данная таблица используется для специальных изменений пакетов. В ней содержатся цепочки PREROUTING (для изменения входящих пакетов до их перенаправления-маршрутизации), OUTPUT (для изменения локально сгенерированных пакетов перед их маршрутизацией), INPUT (для изменения входящих пакетов), FORWARD (для изменения перенаправляемых пакетов) и POSTROUTING (для изменения исходящих пакетов)
raw	Используется преимущественно для создания исключений в слежении за соединениями совместно с целью NOTRACK. Таблица содержит следующие предопределённые цепочки: PREROUTING (для пакетов, приходящих из сетевых интерфейсов) OUTPUT (для пакетов, генерируемых локальными процессами)

Таблица 32 – Опции команды iptables

Опция	Описание
Основные	
-A	добавить правило в цепочку;
-C	проверить все правила;
-D	удалить правило;
-I	вставить правило с нужным номером;
-L	вывести все правила в текущей цепочке;
-S	вывести все правила;
-F	очистить все правила;
-N	создать цепочку;

Опция	Описание
-X	удалить цепочку;
-P	установить действие по умолчанию.
Дополнительные	
-p	указать протокол, один из tcp, udp, udplite, icmp, icmpv6, esp, ah, sctp, mh;
-s	указать ip адрес устройства-отправителя пакета;
-d	указать ip адрес получателя;
-i	входной сетевой интерфейс;
-o	исходящий сетевой интерфейс;
-j	выбрать действие, если правило подошло

1.9.4 Пример использования

1.9.4.1 Основные действия

Отобразить статус:

```
iptables -L -n -v
```

Отобразить список правил с номерами строк:

```
iptables -n -L -v --line-numbers
```

Отобразить цепочку правил OUTPUT:

```
iptables -L OUTPUT -n -v --line-numbers
```

Удалить все правила:

```
iptables -F
```

Заблокировать все входящие запросы порта 80:

```
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -i emp -p tcp --dport 80 -j DROP
```

1.9.4.2 Список правил

Просмотр правил iptables:

```
 iptables -L
```

Просмотр правил с указанием интересующей цепочки:

```
 iptables -L INPUT
```

1.9.4.3 Очистка правил

Очистка правил:

```
  iptables -F
```

Очистка правил только для определенной цепочки:

```
iptables -F Input
```

1.9.4.4 Правила по умолчанию

Если для пакета не подходит ни одно правило, то для него применяется действие по умолчанию. Его можно задать с помощью опции -p:

```
iptables -p INPUT ACCEPT
iptables -p OUTPUT ACCEPT
iptables -p FORWARD DROP
```

Разрешить цепочки INPUT и OUTPUT, но запретить FORWARD:

```
iptables -L
```

1.9.4.5 Блокировка пакетов

Для блокировки пакетов можно использовать действие DROP. Фильтровать пакеты, которые нужно заблокировать можно по различным критериям, например, протоколу, ip адресу, маске сети, порту и тд.

Пример команды, которая позволяет добавить правило iptables для блокировки всех входящих пакетов от ip 10.10.10.10:

```
iptables -A INPUT -s 10.10.10.10 -j DROP
```

Пример команды, которая позволяет добавить правило iptables для блокировки всех исходящих пакетов на этот же адрес:

```
iptables -A OUTPUT -s 10.10.10.10 -j DROP
```

Пример команды, которая блокирует диапазон ip. Маска сети 10.10.10.0/24. Это все адреса начиная с 10.10.10.0 до 10.10.10.255:

```
iptables -A INPUT -s 10.10.10.0/24 -j DROP
```

Расширенный вариант маски:

```
iptables -A INPUT -s 10.10.10.0/255.255.255.0 -j DROP
```

Заблокировать все входящие соединения ssh:

```
iptables -A INPUT -p tcp --dport ssh -s 10.10.10.10 -j DROP
```

1.9.4.6 Удаление правил

Удаление правил **iptables** выполняется так же, как и создание новых. При этом вместо опции **-A** используется опция **-D**.

Вывести список правил:

```
iptables -L
```

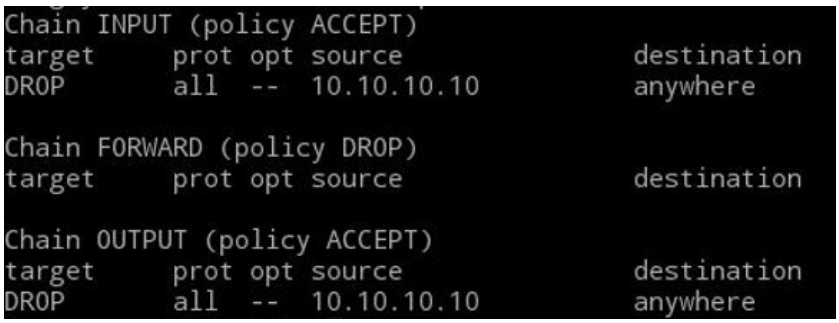


Рисунок 15 - Удаление правил iptables

Удалить правило **iptables**, которое было создано вторым:

```
iptables -D OUTPUT -s 10.10.10.10 -j DROP
```

Полностью очистить **iptables** выполнив команду с опцией **-F**:

```
iptables -F
```

Сохранить настройки **iptables** можно выполнив команду:

```
iptables-cfg-save
```

Восстановить ранее сохранённые настройки **iptables** можно выполнив команду:

```
iptables-cfg-restore
```

Просмотреть ранее сохранённые настройки **iptables** можно выполнив команду:

```
iptables-cfg-show
```

1.10 Настройка функций безопасности

1.10.1 Конфигурирование порта управления

Для обеспечения требований безопасности необходимо ограничить возможность удаленного управления устройством по протоколу SSH. Подключение должно быть разрешено только через специально выделенный порт управления, либо отключено. Настройка порта управления осуществляется при помощи утилиты.

Пример:

```
#Разрешить входящие соединения по протоколу SSH только на интерфейсе eth0
iptables –A INPUT –I eth0 –p TCP --dport 22 -J ACCEPT
…
…
…
iptables –P INPUT DROP
```

1.10.2 Подсистема регистрации событий безопасности

Подсистема реализована системной службой **syslogd**, которая осуществляет журналирование событий, происходящих в системе и сообщений ядра системы, а также поддерживает отправку событий на удаленный сервер по протоколу **syslog**.

Для настройки отправки событий необходимо указать источник, объем событий и адрес централизованной системы мониторинга. Настройки данных параметров хранятся в конфигурационном файле syslog.conf

Главным конфигурационным файлом службы **syslogd** является **syslog.conf**. Файл **syslog.conf** представляет собой **набор правил**. Каждое **правило** представляет из себя строку, состоящую из *селектора* и *действия*, разделенных пробелом или табуляцией. **Селектор** представляет собой запись в виде <*источник*>.<*приоритет*>. (*источник* иногда именуют - *категорией*) **Селектор** может состоять из нескольких записей <*источник*>.<*приоритет*>, разделенных символом ";". Можно указывать несколько источников в одном селекторе (через запятую). Поле **«действие»** устанавливает журналируемое действие для селектора.

Сообщения, предназначенные для записи в журнал, проверяются на соответствие шаблонам, определяемым селектором. Если сообщение соответствует шаблону, выполняется указанное в правиле действие.

Сообщение с уровнем, *равным* или *выше* указанного в селекторе, и источником, *равным указанному* в селекторе, считается *подходящим*. **Звездочка перед** точкой соответствует *любому источнику*, **после** точки - *любому уровню*. Слово **none** после точки - никакому уровню для данного источника. Можно указывать несколько источников в одном селекторе (через запятую).

Источник (категория) может быть следующим:

- 0 - **kern** - Сообщения ядра
- 1 - **user** - Сообщения пользовательских программ
- 2 - **mail** - Сообщения от почтовой системы.
- 3 - **daemon** - Сообщения от тех системных служб, не имеющих категорий.
- 4 - **auth** – Сообщения, связанные с авторизацией пользователей (безопасность/права доступа: login, su и т.д.)
- 5 - **syslog** – Сообщения системы протоколирования.
- 6 - **lpr** - Сообщения от системы печати.
- 7 - **news** - Сообщения от сервера новостей (не используется).
- 8 - **uucp** - Сообщения от UNIX-to-UNIX Copy Protocol (не используется).
- 9 - **cron** - Сообщения от системного планировщика.
- 10 - **authpriv** - Сообщения, связанные с авторизацией пользователей, доступные только определенным пользователям.
- 11 - **ftp** - Сообщения FTP сервера.
- 12 - **NTP** - сообщения сервера времени
- 13 - **log audit**
- 14 - **log alert**
- 15 - **clock daemon -** сообщения службы времени
- с 16 по 23 **local0 - local7** Зарезервированные категории для использования администратором системы. Категория local7 обычно используется для сообщений, генерируемых на этапе загрузки системы.
- **mark** (не имеющая цифрового эквивалента) - присваивается отдельным сообщениям, формируемым самим сервисом syslogd

Приоритет (степени важности) сообщений имеет 8 уровней, которые кодируются числами от 0 до 7:

- 0 - **emerg** (старое название **PANIC**) - Чрезвычайная ситуация. Система неработоспособна.

- 1 - **alert -** Тревога! Требуется немедленное вмешательство.
- 2 - **crit -** Критическая ошибка (критическое состояние).
- 3 - **err** (старое название **ERROR**) - Сообщение об ошибке.
- 4 - **warning** (старое название **WARN**) - Предупреждение.
- 5 - **notice -** Информация о каком-то нормальном, но важном событии.
- 6 - **info -** Информационное сообщение.
- 7 - **debug -** Сообщения, формируемые в процессе отладки.

Согласно **действию,** указанному в правиле, сообщение может быть записано в следующие назначения:

Обычный файл

Задается полным путем, начиная со слеша (/).

Удаленная машина

Для отправки сообщений на другой хост, необходимо перед адресатом добавить символ @.

```
# Пример конфигурационного файла syslogd.
# Все сообщения перенаправляются на
# удалённую сетевую машину.
*.*          @192.168.10.10
```

1.10.3 Подсистема проверки целостности

Проверка целостности системных файлов осуществляется автоматически с периодичностью раз в сутки утилитой **afick**. Ручной контроль целостности осуществляется посредством команды **afick** с ключом **-k**.

На этапах ввода системы в опытную, промышленную эксплуатацию необходимо пересоздать базу данных с контрольными суммами файлов и настроить отправку данных на централизованный сервер мониторинга событий безопасности (в случае необходимости).

1.10.3.1 Утилита afick

Afick — утилита, помогающая при обнаружении вторжений, а также позволяющая контролировать общую целостность системы.

Afick контролирует изменения в файловой системе и сразу сообщает о них, таким образом, предоставляя вам выбор решить, действительно ли ожидались эти изменения. Эта информация может помочь вам в расследовании инцидента, когда необходимо определить, какие были произведены изменения в системе в результате взлома.

В процессе установки **Afick** формирует базу данных файлов, каталогов и соответствующих им MD5 контрольных сумм. Файлы и каталоги, включенные в эту базу данных, выбираются соответственно входным данным из файла конфигурации **Afick**, называемого **afick.conf**, после того, как **Afick** установит этот файл в **/etc** каталог. Файл конфигурации **afick.conf** имеет простую синтаксическую структуру. По вашему усмотрению Вы можете очень быстро добавить или удалить типы файлов, каталоги, и т.д. Ниже приведено содержимое файла **afick.conf**.

Обратите внимание, что элементы в файле конфигурации чувствительны к регистру.

```
# afick config sample file

# directives

#############
```

database:=/var/lib/afick/afick - Определяет какую базу данных будет использовать Afick

 # report_url := stdout - Определяет куда Afick будет выводить результаты своей работы

 # verbose := no

 # warn_dead_symlinks := no

 # report_full_newdel := no

 # warn_missing_file := no

 # running_files := no

 # timing := no

 # text files

exclude_suffix := log LOG html htm HTM txt TXT xml - Определяет, что Afick должен игнорировать текстовые файлы с такими расширениями.

 # help files

exclude_suffix := hlp pod chm - Определяет, что Afick должен игнорировать файлы справки с такими расширениями

 # old files

exclude_suffix := tmp old bak - Определяет, что Afick должен игнорировать временные файлы с такими расширениями

 # fonts

exclude_suffix := fon ttf TTF - Определяет, что Afick должен игнорировать файлы шрифтов с такими расширениями

 # images

exclude_suffix := bmp BMP jpg JPG gif png ico - Определяет, что Afick должен игнорировать файлы изображений с такими расширениями

 # audio

exclude_suffix := wav WAV mp3 avi - Определяет, что Afick должен игнорировать медиа файлы с такими расширениями

 # macros

########

 # used by cron

@@define MAILTO root - Определяет пользователя, которому будут отсылаться отчеты по работе Afick.

@@define LINES 1000 - Определяет максимальное количество строк в отчете

 # list the file or directories to scan

 # syntaxe :

 # file action

 # to have action on file (see below

 # ! file

```
# to remove file from scan
# file with blank character have to be quoted
# action : a list of item to check - Ниже описаны опции, определяющие какие атрибуты файлов нужно контролировать.
# md5 : md5 checksum
# d : device
# i : inode
# p : permissions
# n : number of links
# u : user
# g : group
# s : size
# b : number of blocks
# m : mtime
# c : ctime
# a : atime
#R: p+d+i+n+u+g+s+m+c+md5
#L: p+d+i+n+u+g
# action alias may be configured with
# your_alias = another_alias|item[+item][-item]
# all is a pre-defined alias for all items except "a"
# alias :
#########
DIR = p+i+n+u+g
ETC = p+d+i+u+g+s+md5
Logs = p+n+u+
MyRule = p+d+i+n+u+g+s+b+md5+m .
# files to scan
###############
=/ DIR - Проверка с использованием описанных выше правил для каталогов
#
/bin MyRule
/boot MyRule
!/boot/map - Игнорируется указанный каталог.
!/boot/System.map - Игнорируется указанный файл
/etc ETC
```

```
/etc/mtab ETC - i
/etc/adjtime ETC - md5
/etc/aliases.db ETC - md5
/etc/mail/statistics ETC - md5
!/etc/map
!/etc/webmin/sysstats/modules/
!/etc/cups/certs/0
/lib MyRule
/lib/modules MyRule -m
/root MyRule
!/root/.viminfo
!/root/.bash_history
!/root/.mc
/sbin MyRule
/usr/bin MyRule
/usr/sbin MyRule
/usr/lib MyRule
/usr/local/bin MyRule
/usr/local/sbin MyRule
/usr/local/lib MyRule
/var/ftp MyRule
/var/log Logs
/var/www MyRule
```

1.10.3.2 Пример использования

В данном разделе приведен пример, в котором к проверке целостности **Afick** добавляется основной каталог системы. К примеру, если необходимо, чтобы файлы в основном каталоге проверялись на изменения при монопольном доступе, изменение прав доступа, изменения размера файлов и времени последнего обращения к файлу.

Для начала нужно создать новый элемент, под разделом **#alias** в файле конфигурации **afick.conf**, как показано ниже:

```
HOME = u+g+p+m+s
```

Затем в разделе **#files to scan** необходимо добавить следующую строку:

```
/home/yourusername HOME
```

Теперь, при следующем запуске, **Afick** добавит данный каталог в свою базу данных и будет контролировать находящиеся в нем файлы, согласно заданным критериям. Если нужно, чтобы изменения применились немедленно, то можно запустить **Afick** вручную, используя следующую команду:

```
Afick -- update
```

Иначе придется ждать запуска крон задачи **Afick**. Эта задача добавляется автоматически во время инсталляции программы и запускается один раз в день. Результаты работы данного задания будет получен по электронной почте на адрес, указанный в разделе **MAILTO** файла конфигурации **afick.conf**. Используя почтового клиента, можно будет увидеть ежедневный отчет приблизительно в следующем виде:

```
This is an automated report generated by Another File Integrity Checker on
+localhost.localdomain at 07:46:07 AM on 02/25/2004.
Output of the daily afick run:
new file : /var/log/afick/afick.log.2
new file : /var/log/afick/error.log.2
deleted file : /etc/sysconfig/iptables
changed file : /etc/adjtime
changed file : /etc/aliases.db
changed file : /etc/mail/statistics
changed file : /etc/prelink.cache
changed file : /etc/printcap
detailed changes
changed file : /etc/adjtime
MD5 : 7+bTDZQbxsTXEJXhyI2GCw ao6a/yDwoBR8GSL1AKlWXQ
changed file : /etc/aliases.db
MD5 :GT/eP5D+B8apNoa7L5CLRw soh7MnLDuQw4gI9KHlhpTA
changed file : /etc/mail/statistics
MD5 :oshq17jZ2a0o5pYhVBRgwQ vb69gMWXvpIEEZ4fmOl9/Q
changed file : /etc/prelink.cache
MD5 : SKh/403FRMUqBNdCIInQ9A zeC+5EPFfWBR4OeT7xZdbw
changed file : /etc/printcap
MD5 : b5e3g2//bGaxeCxVyRJqaw QFY1NJGy/kdt32B1YV0TXQ
filesize : 194 581
```

В примере выше **Afick** сообщает, что некоторые файлы были изменены, созданы или удалены. Также показаны начальные и текущие контрольные суммы файлов, и сообщается, что в одном из файлов был изменен его размер. Afick проконтролирует наличие изменений в файле, сравнивая его атрибуты с атрибутами, которые были сохранены при последнем запуске **Afick.** Примером этого могут служить файлы в папке **/usr/bin** или в **/sbin**. Как правило эти файлы изменяются не часто, если только их не изменили, обновляя программу (в противном случае они не останутся неизменны).

Следует обратить внимание на то, где сохраняется вашу базу данных **Afick** (по умолчанию — **/var/lib/afick/**), так как возможно возникновение ситуации, когда система была взломана, ну это не было зафиксировано, так как была нарушена целостность базы данных. Возможным решением данного вопроса может быть сохранение базы на защищенных от записи носителях (например, CD-ROM), после чего изменить файл конфигурации **afick.conf**, чтобы указать на выбранное вами место сохранения базы.

1.10.3.3 Проведение процедуры контроля целостности ОС

Для **сертифицированной редакции** в состав репозитория ОС включена база данных утилиты контроля целостности afick, которая содержит перечень контролируемых бинарных исполняемых файлов изделия, согласно документации на изделие. Для самостоятельной проверки целостности ОС необходимо сделать следующее:

1. Запустить проверку файлов ОС командой:

```
# afick -k

...

new file : /var/lib/afick/redos/redos.ctr

new file : /var/lib/afick/redos/redos.db

deleted file : /lib/modules/4.19.79-1.el7.x86_64.debug/kernel/arch/x86/crypto/aegis128-aesni.ko

...

deleted file : /var/lib/afick/afick.db

        parent_date             : Fri Apr 24 09:17:05 2020

changed file : /etc/afick.conf

        md5                     : 03bf42d0327b3f2fe195d0eca359b1ec   addfc78d95514
1718f78df7587ae3ceb

        filemode                : 100600      100644

        filesize                : 924772      924774

# Hash database : 6793 files scanned, 6320 changed (new : 2; delete : 6317; change
d : 1; dangling : 0; exclude_suffix : 0; exclude_prefix : 0; exclude_re : 0; degra
ded : 3)

# ###################################################################

# MD5 hash of /var/lib/afick/redos/redos => oRTAm4SAHdk9vwSktXz88A

# user time : 12.73; system time : 3.14; real time : 27
```

2. После завершения проверки проанализировать полученные данные. Новые файлы можно не принимать во внимание.

```
new : 2
```

Удалённые файлы в отчете можно не учитывать — это объясняется тем, что БД afick снимается для всех контролируемых файлов, а в используемом экземпляре ОС могут использоваться не все пакеты.

```
delete : 6317
```

Интерес в первую очередь представляют изменённые файлы.

```
changed : 1
```

3. Проанализировать подробный отчёт в выводе утилиты выше и оценить, допустимы ли данные изменения файлов.

```
changed file : /etc/afick.conf

        md5                     : 03bf42d0327b3f2fe195d0eca359b1ec   addfc78d95514
```

```
1718f78df7587ae3ceb
        filemode                : 100600      100644
        filesize                : 924772      924774
```

В приведенном примере был изменен конфигурационный файл утилиты **afick**. Это считается допустимым изменением, так как на эталонной ОС конфигурация **afick** по умолчанию не настроена. Скачанный конфигурационный файл, содержащийся в пакете БД **afick**, заменил файл, поставляемый с утилитой. Других изменений в системе нет, значит, можно сделать вывод о целостности ОС.

1.10.4 Подсистема криптозащиты каналов связи

Устройство поддерживает следующие решения: Infotecs ViPNet VPN, ТСС Diamond VPN, OpenVPN, IPSec, PPTP VPN, L2TP.

Настройка СКЗИ Infotecs ViPNet VPN, ТСС Diamond VPN осуществляется согласно инструкции производителя СКЗИ.

1.10.5 Подсистема аудита

В устройстве реализована подсистема аудита, которая позволяет осуществлять аудит:

- запуск и завершение работы системы;
- чтение, запись и изменение прав доступа к файлам;
- инициация сетевых соединений;
- попытки неудачной авторизации в системе;
- изменение сетевых настроек;
- изменение информации о пользователях и группах;
- запуск и остановка приложений;
- выполнение системных вызовов.

Подсистема реализована на базе сервиса **auditd**. Просмотр результатов аудита осуществляется утилитами:

- **aureport** - инструмент для генерации итоговых отчетов на основе логов демона аудита;
- **ausearch** - поиск по журналу аудита;
- **auditctl** - инструмент для управления аудитом, предоставляемого Linux ядром.

1.10.5.1 Сервис auditd

1.10.5.1.1 Описание

auditd - это прикладной компонент системы аудита Linux. Он ведёт протокол аудита на диске. Для просмотра протоколов предназначены команды **ausearch** и **aureport.** Команда **auditctl** позволяет настраивать правила аудита. Кроме того, при загрузке загружаются правила из файла */etc/audit.rules*. Некоторые параметры самого демона можно изменить в файле **auditd.conf.**

1.10.5.1.2 Синтаксис

```
auditd [-f] [-l] [-n]
```

Таблица 33 – Опции сервиса auditd

Опция	Описание
-f	Не переходить в фоновый режим (для отладки). Сообщения программы будут направляться в стандартный вывод для ошибок (stderr), а не в файл

Опция	Описание
-l	Включить следование по символическим ссылкам при поиске конфигурационных файлов
-n	Не создавать дочерний процесс. Для запуска из inittab

1.10.5.1.3 Сигналы

Таблица 34 – Сигналы сервиса auditd

Опция	Описание
SIGHUP	Перезагрузить конфигурацию - загрузить файл конфигурации с диска. Если в файле не окажется синтаксических ошибок, внесенные в него изменения вступят в силу. При этом в протокол будет добавлена запись о событии DAEMON_CONFIG. В противном случае действия службы будут зависеть от параметров space_left_action, admin_space_left_action, disk_full_action, disk_error_action файла auditd.conf
SIGTERM	Прекратить обработку событий аудита и завершить работу, о чём предварительно занести запись в протокол
SIGUSR1	Создать новый файл для протокола, перенумеровав старые файлы или удалив часть из них, в зависимости от параметра max_log_size_action

1.10.5.1.4 Файлы

/etc/audit/auditd.conf - файл конфигурации демона аудита **/etc/audit/audit.rules** - правила аудита (загружается при запуске службы).

1.10.5.2 Утилита ausearch

Программа **ausearch** является инструментом поиска по журналу аудита. **ausearch** может также принимать данные со стандартного ввода (**stdin**) до тех пор, пока на входе будут необработанные данные логов. Все условия, указанные в параметрах, объединяются логическим И. К примеру, при указании **-m** и **-ui** в качестве параметров будут показаны события, соответствующие заданному типу и идентификатору пользователя.

1.10.5.2.1 Синтаксис

```
ausearch [опции]
```

1.10.5.2.2 Опции

Таблица 35 – Опции утилиты ausearch

Опция	Описание
-a, **--event** *audit-event-id*	Искать события с заданным *идентификатором события*. Сообщения обычно начинаются примерно так: msg=audit(1116360555.329:2401771). Идентификатор события - это число после ':'. Все события аудита, связанные с одним системным вызовом имеют одинаковый идентификатор.
-c, **--comm** *comm-name*	Искать события с заданным *comm name*. comm name - имя исполняемого файла задачи.
-f, **--file** *file-name*	Искать события с заданным *именем файла*.

Опция	Описание
-ga, **--gid-all** *all-group-id*	Искать события с заданным эффективным или обычным *идентификатором группы*.
-ge, **--gid-effective** *effective-group-id*	Искать события с заданным *эффективным идентификатором группы* или именем группы.
-gi, **--gid** *group-id*	Искать события с заданным *идентификатором группы* или именем группы.
-h, **--help**	Справка
-hn, **--host** *host-name*	Искать события с заданным *именем узла*. Имя узла может быть именем узла, полным доменным именем или цифровым сетевым адресом.
-i, **--interpret**	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет оттранслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущен **ausearch**. Т.е. если вы переименовали учетные записи пользователей или не имеете таких же учетных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение.
-if, **--input** *file-name*	Использовать указанный *файл* вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
-k, **--key** *key-string*	Искать события с заданным *ключевым словом*.
-m, **--message** *message-type* | *comma-sep-message-type-list*	Искать события с заданным *типом*. Вы можете указать *список значений, разделенных запятыми*. Можно указать несуществующий в событиях тип **ALL**, который позволяет получить все сообщения системы аудита. Список допустимых типов большой и будет показан, если указать эту опцию без значения. Тип сообщения может быть строкой или числом. В списке значений этого параметра в качестве разделителя используются запятые и пробелы недопустимы.
-o, **--object** *SE-Linux-context-string*	Искать события с заданным *контекстом* (объектом).
-p, **--pid** *process-id*	Искать события с заданным *идентификатором процесса*.
-pp, **--ppid** *parent-process-id*	Искать события с заданным *идентификатором родительского процесса*.
-r, **--raw**	Необработанный вывод. Используется для извлечения записей для дальнейшего анализа.
-sc, **--success** *syscall-name-or-value*	Искать события с заданным *системным вызовом*. Вы можете указать его номер или имя. Если вы указали имя, оно будет проверено на машине, где запущен **ausearch**.
-se, **--context** *SE-Linux-context-string*	Искать события с заданным *контекстом SELinux* (stcontext/subject или *tcontext*/object).
-su, **--subject** *SE-Linux-context-string*	Искать события с заданным контекстом SELinux - *scontext* (subject).
-sv, **--success** *success-value*	Искать события с заданным *флагом успешного выполнения*. Допустимые значения: **yes (успешно)** и **no**(неудачно).

Опция	Описание
-te, **--end** [*end-date*] [*end-time*]	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (**today**). Если не указано время, то подразумевается текущий момент (**now**). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: **now** (сейчас), **recent**, **today**, **yesterday**, **this-week**, **this-month**, **this-year**. **today** означает первую секунду после полуночи текущего дня. **recent** - 10 минут назад. **yesterday** - первую секунду после полуночи предыдущего дня. **this-week** означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. **localtime**). **this-month** означает первую секунду после полуночи первого числа текущего месяца. **this-year** означает первую секунду после полуночи первого числа первого месяца текущего года.
-ts, **--start** [*start-date*] [*start-time*]	Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (**today**). Если не указано время, то подразумевается полночь (**midnight**). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: **now** (сейчас), **recent**, **today**, **yesterday**, **this-week**, **this-month**, **this-year**. **today** означает первую секунду после полуночи текущего дня. **recent** - 10 минут назад. **yesterday** - первую секунду после полуночи предыдущего дня. **this-week** означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. **localtime**). **this-month** означает первую секунду после полуночи первого числа текущего месяца. **this-year** означает первую секунду после полуночи первого числа первого месяца текущего года.
-tm, **--terminal** *terminal*	Искать события с заданным *терминалом*. Некоторые демоны (такие как cron и atd) используют имя демона как имя терминала.
-ua, **--uid-all** *all-user-id*	Искать события, у которых любой из идентификатора пользователя, эффективного идентификатора пользователя или loginuid (auid) совпадают с заданным *идентификатором пользователя*.
-ue, **--uid-effective** *effective-user-id*	Искать события с заданным *эффективным идентификатором пользователя*.
-ui, **--uid** *user-id*	Искать события с заданным *идентификатором пользователя*.
-ul, **--loginuid** *login-id*	Искать события с заданным *идентификатором пользователя*. Все программы, которые его используют, должны использовать pam_loginuid.
-v, **--verbose**	Показать версию и выйти
-w, **--word**	Совпадение с полным словом. Поддерживается для имени файла, имени узла, терминала и контекста SELinux.
-x, **--executable** *executable*	Искать события с заданным *именем исполняемой программы*.

1.10.5.3 Утилита aureport

aureport - это инструмент, который генерирует итоговые отчеты на основе логов демона аудита. **aureport** может также принимать данные со стандартного ввода (**stdin**) до тех пор, пока на входе будут необработанные данные логов. В шапке каждого отчета для каждого столбца есть заголовок - это облегчает понимание данных. Все отчеты, кроме основного итогового отчета, содержат номера событий аудита. Используя их, вы можете найти полные данные о событии с помощью **ausearch -a** *номер события*. Если в отчете слишком много данных, можно задать время начала и время окончания для уточнения временного промежутка. Отчеты, генерируемые **aureport**, могут быть использованы как исходный материал для получения более развернутых отчетов.

1.10.5.3.1 Синтаксис

```
aureport [опции]
```

1.10.5.3.2 Опции

Таблица 36 – Опции утилиты aureport

Опция	Описание
-au, **--auth**	Отчет о всех попытках аутентификации
-a, **--avc**	Отчет о всех avc сообщениях
-c, **--config**	Отчет об изменениях конфигурации
-cr, **--crypto**	Отчет о событиях, связанных с шифрованием
-e, **--event**	Отчет о событиях
-f, **--file**	Отчет о файлах
--failed	Для обработки в отчетах выбирать только неудачные события. По умолчанию показываются и удачные и неудачные события.
-h, **--host**	Отчет о хостах
-i, **--interpret**	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет оттранслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущен **aureport**. Т.е. если вы переименовали учетные записи пользователей или не имеете таких же учетных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение.
-if, **--input** *файл*	Использовать указанный *файл* вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
-l, **--login**	Отчет о попытках входа в систему
-m, **--mods**	Отчет об изменениях пользовательских учетных записей.
-ma, **--mac**	Отчет о событиях в системе обеспечивающей мандатное управление доступом - Mandatory Access Control (MAC).
-p, **--pid**	Отчет о процессах
-r, **--response**	Отчет о реакциях на аномальные события
-s, **--syscall**	Отчеты о системных вызовах
--success	Для обработки в отчетах выбирать только удачные события. По умолчанию показываются и удачные и неудачные события.

Опция	Описание
--summary	Генерировать итоговый отчет, который дает информацию только о количестве элементов в том или ином отчете. Такой режим есть не у всех отчетов.
-t, **--log**	Этот параметр генерирует отчет о временных рамках каждого отчета.
-te, **--end** [*дата*] [*время*]	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (**today**). Если не указано время, то подразумевается текущий момент (**now**). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: **now** (сейчас), **recent**, **today**, **yesterday**, **this-week**, **this-month**, **this-year**. **today** означает первую секунду после полуночи текущего дня. **recent** - 10 минут назад. **yesterday** - первую секунду после полуночи предыдущего дня. **this-week** означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. **localtime**). **this-month** означает первую секунду после полуночи первого числа текущего месяца. **this-year** означает первую секунду после полуночи первого числа первого месяца текущего года.
-tm, **--terminal**	Отчет о терминалах
-ts, **--start** [*дата*] [*время*]	Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (**today**). Если не указано время, то подразумевается полночь (**midnight**). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: **now** (сейчас), **recent**, **today**, **yesterday**, **this-week**, **this-month**, **this-year**. **today** означает первую секунду после полуночи текущего дня. **recent** - 10 минут назад. **yesterday** - первую секунду после полуночи предыдущего дня. **this-week** означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. **localtime**). **this-month** означает первую секунду после полуночи первого числа текущего месяца. **this-year** означает первую секунду после полуночи первого числа первого месяца текущего года.
-u, **--user**	Отчет о пользователях
-v, **--version**	Вывести версию программы и выйти
-x, **--executable**	Отчет об исполняемых объектах

1.10.5.4 Утилита auditctl

auditctl используется для контроля поведения, получения состояния и добавления/удаления правил аудита, предоставляемого ядром Linux версии 2.6.

1.10.5.4.1 Синтаксис

```
auditctl [опции]
```

1.10.5.4.2 Опции

Таблица 37 – Опции утилиты auditctl

Опция	Описание
-b *backlog*	Установить максимальное количество доступных для аудита буферов, ожидающих обработки (значение в ядре по умолчанию - 64). Если все буфера заняты, то флаг сбоя будет выставлен ядром для его дальнейшей обработки.
-e [**0**..**2**]	Установить флаг блокировки. **0** позволит на время отключить аудит, включить его обратно можно, передав **1** как параметр. Если установлено значение опции **2**, то защитить конфигурацию аудита от изменений. Каждый, кто захочет воспользоваться этой возможностью, может поставить эту команду последней в audit.rules. После этой команды все попытки изменить конфигурацию будут отвергнуты с уведомлением в журналах аудита. В этом случае, чтобы задействовать новую конфигурацию аудита, необходимо перезагрузить систему аудита.
-f [**0**..**2**]	Установить способ обработки для флага сбоя. **0**=silent **1**=printk **2**=panic. Эта опция позволяет определить каким образом ядро будет обрабатывать критические ошибки. Например, флаг сбоя выставляется при следующих условиях: ошибки передачи в пространство демона аудита, превышение лимита буферов, ожидающих обработки, выход за пределы памяти ядра, превышение лимита скорости выдачи сообщений. Значение по умолчанию: **1**. Для систем с повышенными требованиями к безопасности, значение **2** может быть более предпочтительно.
-h	Краткая помощь по аргументам командной строки.
-i	Игнорировать ошибки при чтении правил из файла.
-l	Вывести список всех правил по одному правилу в строке.
-k *ключ*	Установить на правило ключ фильтрации. Ключ фильтрации - это произвольная текстовая строка длиной не больше 31 символа. Ключ помогает уникально идентифицировать записи, генерируемые в хода аудита за точкой наблюдения.
-m *текст*	Послать в систему аудита пользовательское сообщение. Это может быть сделано только из-под учетной записи root.
-p [**r**|**w**|**x**|**a**]	Установить фильтр прав доступа для точки наблюдения. **r**=чтение, **w**=запись, **x**=исполнение, **a**=изменение атрибута. Не путайте эти права доступа с обычными правами доступа к файлу - они определяют типы системных вызовов, которые выполняют данные действия. Заметьте, системные вызовы read и write не включены в этот набор, поскольку логи аудита были бы перегружены информацией о работе этих вызовов.
-r *частота*	Установить ограничение скорости выдачи сообщений в секунду (**0** - нет ограничения). Если эта *частота* не нулевая и она превышается в ходе аудита, флаг сбоя выставляется ядром для выполнения соответствующего действия. Значение по умолчанию: 0.
-R *файл*	Читать правила из *файла*. Правила должны быть расположены по одному в строке и в том порядке, в каком они должны исполняться. Следующие ограничения накладываются на файл: владельцем должен быть root и доступ на чтение должен быть только у него. Файл может содержать комментарии, начинающиеся с символа '#'. Правила,

Опция	Описание
	расположенные в файле, идентичны тем, что набираются в командной строке, без указания 'auditctl'.
-s	Получить статус аудита.
-a *список*,*действие*	Добавить правило с указанным *действием* к концу *списка*. Заметьте, что запятая разделяет эти два значения. Отсутствие запятой вызовет ошибку. Ниже описаны имена доступных списков:
task	Добавить правило к списку, отвечающему за процессы. Этот список правил используется только во время создания процесса - когда родительский процесс вызывает fork() или clone(). При использовании этого списка вы можете использовать только те поля, которые известны во время создания процесса: uid, gid и т.д.
entry	Добавить правило к списку, отвечающему за точки входа системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам входа системных вызовов.
exit	Добавить правило к списку, отвечающему за точки выхода из системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам выхода из системных вызовов.
user	Добавить правило, отвечающего за список фильтрации пользовательских сообщений. Этот список используется ядром, чтобы отфильтровать события, приходящие из пользовательского пространства, перед тем как они будут переданы демону аудита. Необходимо отметить, что только следующие поля могут быть использованы: uid, auid, gid и pid. Все остальные поля будут обработаны, как если бы они не совпали.
exclude	Добавить правило к списку, отвечающего за фильтрацию событий определенного типа. Этот список используется, чтобы отфильтровывать ненужные события. Например, если вы не хотите видеть avc сообщения, вы должны использовать этот список. Тип сообщения задается в поле msgtype. Ниже описаны доступные *действия* для правил:
never	Аудит не будет генерировать никаких записей. Это может быть использовано для подавления генерации событий. Обычно необходимо подавлять генерацию в верху списка, а не внизу, т.к. событие инициируется на первом совпавшем правиле.
always	Установить контекст аудита. Всегда заполнять его во время входа в системный вызов, и всегда генерировать запись во время выхода из системного вызова.
-A *список*,*действие*	Добавить правило с указанным *действием* в начало *списка*.
-d *список*,*действие*	Удалить правило с указанным *действием* из *списка*. Правило удаляется только в том случае, если полностью совпали и имя системного вызова и поля сравнения.
-D	Удалить все правила и точки наблюдения.
-S [*Имя или номер системного вызова*|**all**]	Любой *номер* или *имя* системного вызова может быть использован. Также возможно использование ключевого слова *all*. Если какой-либо процесс выполняет указанный системный вызов, то аудит генерирует соответствующую запись. Если значения полей сравнения заданы, а системный вызов не указан, правило будет применяться ко всем

Опция	Описание
	системным вызовам. В одном правиле может быть задано несколько системных вызовов - это положительно сказывается на производительности, поскольку заменяет обработку нескольких правил.
-F [*n*=*v* | *n***!**=*v* | *n*<*v* | *n*>*v* | *n*<=*v* | *n*>=*v* | *n***&**=*v* | *n***&=***v*]	Задать поле сравнения для правила. Атрибуты поля следующие: объект, операция, значение. Вы можете задать до 64 полей сравнения в одной команде. Каждое новое поле должно начинаться с **-F**. Аудит будет генерировать запись, если произошло совпадение по всем полями сравнения. Допустимо использование одного из следующих 8 операторов: равно, не равно, меньше, больше, меньше либо равно, больше либо равно, битовая маска (*n***&***v*) и битовая проверка (*n***&=***v*). Битовая проверка выполняет операцию 'and' над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию 'and'. Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя - программа автоматически получит идентификатор пользователя из его имени. То же самое можно сказать и про имя группы. Поля сравнения могут быть заданы для следующих объектов:
a0, a1, a2, a3	Четыре первых аргумента, переданных системному вызову. Строковые аргументы не поддерживаются. Это связано с тем, что ядро должно получать указатель на строку, а проверка поля по значению адреса указателя не желательна. Таким образом, вы должны использовать только цифровые значения.
arch	Архитектура процессора, на котором выполняется системный вызов. Используйте 'uname -m', чтобы определить архитектуру. Если вы не знаете архитектуру вашей машины, но хотите использовать таблицу 32-х битных системных вызовов, и ваша машина поддерживает 32 бита, вы можете использовать **b32**. Подобно этому **b64** может быть использовано для использования таблицы 64-х битных системных вызовов.
auid	Это аббревиатура: audit uid - идентификатор пользователя, использованный для входа в систему.
devmajor	Главный номер устройства (Device Major Number)
devminor	Вспомогательный номер устройства (Device Minor Number)
egid	Действительный идентификатор группы
euid	Действительный идентификатор пользователя
exit	Значение, возвращаемое системным вызовом при выходе.
fsgid	Идентификатор группы, применяемый к файловой системе.
fsuid	Идентификатор пользователя, применяемый к файловой системе.
gid	Идентификатор группы
Идентификатор группы	**inode**
inode	Номер inode
key	Альтернативный способ установить ключ фильтрации. Смотри выше описание опции **-k**.
msgtype	Используется для проверки совпадения с числом, описывающим тип сообщения. Может быть использован только в списке **exclude**.
obj_user	Имя пользователя-владельца ресурса (в контексте SELinux)

Опция	Описание
obj_role	Роль ресурса (в контексте SELinux)
obj_type	Тип ресурса (в контексте SELinux)
obj_lev_low	Нижний уровень ресурса (в контексте SELinux)
obj_lev_high	Верхний уровень ресурса (в контексте SELinux)
path	Полный путь к файлу для точки наблюдения. Смотри ниже описание опции "**-w**". Может быть использован только в списке **exit**.
perm	Фильтр прав доступа для файловых операций. Смотри выше описание опции "**-p**". Может быть использован только в списке **exit**.
pers	Персональный номер операционной системы.
pid	Идентификатор процесса
ppid	Идентификатор родительского процесса.
subj_user	Имя пользователя-владельца процесса (в контексте SELinux)
subj_role	Роль процесса (в контексте SELinux)
subj_type	Тип процесса (в контексте SELinux)
subj_sen	Чувствительность процесса (в контексте SELinux)
subj_clr	Допуск процесса (в контексте SELinux)
sgid	Установленный идентификатор группы
success	Если значение, возвращаемое системным вызовом, больше либо равно 0, данный объект будет равен "true/yes", иначе "false/no". При создании правила используйте 1 вместо "true/yes" и 0 вместо "false/no".
suid	Установленный идентификатор пользователя
uid	Идентификатор пользователя
-w *путь*	Добавить точку наблюдения за файловым объектом, находящемуся по указанному *пути*. Вы не можете добавлять точку наблюдения к каталогу верхнего уровня - это запрещено ядром. Групповые символы (wildcards) также не могут быть использованы, попытки их использования будут генерировать предупреждающее сообщение. Внутренне точки наблюдения реализованы как слежение за inode. Таким образом, если вы установите точку наблюдения за каталогом, вы увидите файловые события, которые в действительности будут означать обновления метаданных этой inode, и вы можете не увидеть событий, непосредственно связанных с файлами. Если вам необходимо следить за всеми файлами в каталоге, рекомендуется создавать индивидуальную точку наблюдения для каждого файла. В противоположность к правилам аудита системных вызовов, точки наблюдения не оказывают влияния на производительность, связанную с количеством правил, посылаемых в ядро.
-W *путь*	Удалить точку наблюдения за файловым объектом, находящемуся по указанному *пути*.

1.10.5.4.3 Примеры использования для контроля поведения, получения состояния

Чтобы увидеть все системные вызовы, используемые определенным процессом:

```
auditctl -a entry,always -S all -F pid=1005
```

Чтобы увидеть все файлы, открытые определенным пользователем:

```
auditctl -a exit,always -S open -F auid=510
```

Чтобы увидеть неудачные попытки вызова системной функции 'open':

```
auditctl -a exit,always -S open -F success!=0
```

1.10.5.4.4 Создание правил

Список опций команды auditctl для создания правил (подробное описание опций приведено в таблице 37):

- **-l** — вывести список имеющихся правил;
- **-a** — добавить новое правило;
- **-d** — удалить правило из списка;
- **-D** — удалить все имеющиеся правила.

Чтобы создать новое правило, нужно выполнить команду вида:

```
$ auditctl -a <список>, <действие> -S <имя системного вызова> -F <фильтры>
```

Сначала после опции -a указывается список, в который нужно добавить правило. Всего существует 5 таких списков:

- **task** — события, связанные с созданием новых процессов;
- **entry** — события, которые имеют место при входе в системный вызов;
- **exit** — события, которые имеют место при выходе из системного вызова;
- **user** — события, использующие параметры пользовательского пространства;
- **exclude** — используется для исключения событий.

Затем указывается, что нужно делать после наступления события. Здесь возможны два варианта: **always** (события будут записываться в журнал) и **never** (не будут).

После опции **-S** идёт имя системного вызова, при котором событие нужно перехватить (**open**, **close** и т.п.).

После опции **-F** указываются дополнительные параметры фильтрации. Например, если нам требуется вести аудит обращений к файлам из каталога **/etc**, правило будет выглядеть так:

```
$ auditctl -a exit,always -S open -F path =/etc/
```

Можно установить и дополнительный фильтр:

```
$ auditctl -a exit,always -S open -F path =/etc/ -F perm = aw
```

Аббревиатура aw означает следующее: **a** — изменение атрибута (**attribute change**), **w** — запись (**write**). Формулировка **perm = aw** указывает, что для директории **/etc** нужно отслеживать все факты изменения атрибутов (**a — attribute change**) и **w (w — write)**.

При настройке слежения за отдельными файлами можно опустить опцию **-S**, например:

```
$ auditctl -a exit,always -F path =/etc/ -F perm = aw
```

1.10.5.5 Файлы правил

Правила можно не только задавать через командную строку, но и прописывать в файле **etc/audit/audit.rules**.

Начинается этот файл с так называемых метаправил, в которых задаются общие настройки журналирования:

```
# удаляем все ранее созданные правила
-D


# задаём количество буферов, в которых будут храниться сообщения
-b 320


# указываем, что делать в критической ситуации (например, при переполнении буферов ): 0 - ничего не делать; 1 - отправлять сообщение в dmesg, 2 - отправлять ядро в панику
-f 1
```

Далее следуют пользовательские правила. Их синтаксис предельно прост: достаточно просто перечислить соответствующие опции команды `auditctl`. Рассмотрим пример типового конфигурационного файла:

```
# отслеживать системные вызовы unlink () и rmdir()
-a exit,always -S unlink -S rmdir


# отслеживать системные вызовы open () от пользователя с UID 1001
-a exit,always -S open -F loginuid=1001


# отслеживать доступ к файлам паролей и групп и попытки их изменения:
-w /etc/group -p wa
-w /etc/passwd -p wa
```

```
-w /etc/shadow -p wa
-w /etc/ers -p wa

# отслеживать доступ к следующей директории:
-w /etc/my_directory -p r

# закрыть доступ к конфигурационному файлу для предотвращения изменений
-e 2
```

Изменения конфигурации вступят в силу после перезапуска демона **auditd**:

```
$  service auditd restart
```

1.11 Работа в режиме RedBox

Маршрутизаторы платформы MX681 дополнительно могут использоваться в режиме RedBox для подключения устройств или сегментов сети, не поддерживающих PRP, к двум параллельным сетям PRP. Режим RedBox задаётся программно (см. п. 1.9 настоящего РЭ) и не требует отдельной аппаратной платы. Маршрутизаторы платформы MX710 режим RedBox не поддерживают.

Конкретное назначение физических портов устанавливают программно в соответствии с эксплуатационной документацией. Для исполнений MX681 с интерфейсами 2GTxSFP-1GTx два порта GTxSFP могут использоваться для подключения к сетям A и B, а порт GTx — в качестве порта interlink.

Примечание Порты Interlink не поддерживают STP/RSTP протоколы и не пересылают BPDU пакеты, использование избыточных соединений приведет к широковещательному шторму и нарушению работы сети. Используйте interlink порты для подключения оконечных SAN устройств или сетей без кольцевой топологии.

2 МАРКИРОВКА И ПЛОМБИРОВАНИЕ

Вся обязательная информация по маркировке нанесена на лицевой, задней или боковой (в зависимости от конструктивного исполнения) панелях. Маркировка выполнена способом, обеспечивающим ее сохранность на все время эксплуатации устройства.

Перечень информации, содержащейся в маркировке на лицевой панели:

- наименование и условное обозначение;
- назначение светодиодов устройства;
- назначение клеммных соединений и разъемов устройства.

Перечень информации, содержащейся в маркировке на боковой или задней панели:

- наименование и условное обозначение;
- товарный знак;
- номер технических условий;
- наименование предприятия-изготовителя и контактный телефон;
- порядковый номер по системе нумерации предприятия-изготовителя;
- дата изготовления.

Для предотвращения несанкционированного доступа к внутренним электрическим элементам корпус устройства пломбируется путем нанесения на стыковочный шов саморазрушающейся наклейки.

3 УПАКОВКА

Маршрутизатор вместе с предусмотренными комплектом поставки принадлежностями и эксплуатационной документацией упаковывается предприятием-изготовителем в индивидуальную или групповую упаковку из гофрированного картона.

Упаковка соответствует ГОСТ 33781, вид II.

Маршрутизатор перед упаковыванием помещается в пакет из полиэтиленовой пленки.

При размещении маршрутизатора в упаковке обеспечивается дополнительная защита (амортизация) при помощи ложементов из вспененного полиэтилена. Ложементы обеспечивают зазор между упаковкой и коммутатором от 10 до 50 мм и исключают свободное перемещение внутри упаковки.

Упаковка исключает свободное перемещение изделия и обеспечивает его защиту от механических повреждений и загрязнения при транспортировании и хранении в установленных условиях.

На упаковке наносится следующая маркировка в соответствии с ГОСТ 14192:

- Хрупкое.
- Осторожно;
- Беречь от влаги;
- Верх;
- Штабелирование ограничено.

Эксплуатационная документация вкладывается в пакет из полиэтиленовой плёнки и укладывается в упаковку с изделиями.

4 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

Техническое обслуживание устройства заключается в профилактических осмотрах.

При профилактическом осмотре должны быть выполнены следующие работы:

- проверка обрыва или повреждения изоляции проводов и кабелей;
- проверка надежности присоединения проводов и кабелей;
- проверка отсутствия видимых механических повреждений, а также пыли и грязи на корпусе устройства.

Периодичность профилактических осмотров устройства устанавливается потребителем, но не реже 1 раз в год.

Эксплуатация устройства с повреждениями категорически запрещается.

5 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ

Транспортирование маршрутизаторов в упаковке предприятия-изготовителя допускается автомобильным транспортом, закрытым брезентом, в закрытых железнодорожных вагонах, трюмах речного транспорта и в негерметизированных отсеках самолётов.

Маршрутизаторы в упакованном виде устойчивы при транспортировании к температуре окружающего воздуха от минус 50 до плюс 50 °С и относительной влажности воздуха 100 % при температуре плюс 25 °С. При транспортировании в негерметизированных отсеках самолётов маршрутизаторы должны быть устойчивы к пониженному атмосферному давлению 12 кПа при температуре минус 50 °С.

Размещение и крепление упакованных маршрутизаторов в транспортных средствах выполняют так, чтобы обеспечивать их устойчивое положение и исключать удары друг о друга и о стенки транспортного средства.

Упакованные маршрутизаторы укладывают в штабели в соответствии с правилами и нормами, действующими на соответствующем виде транспорта, не допуская деформации транспортной тары при возможных механических перегрузках.

При погрузке и выгрузке запрещается бросать и кантовать устройства.

После транспортирования при отрицательных температурах вскрытие упаковки допускается не ранее чем через 12 ч после размещения устройства в отапливаемом помещении. Перед использованием после такого транспортирования общая продолжительность выдержки устройства в нормальных климатических условиях должна составлять не менее 24 ч.

Маршрутизаторы в упакованном виде допускается хранить в неотапливаемых складских помещениях при температуре от минус 50 до плюс 40 °С и среднемесячном значении относительной влажности 80 % при температуре плюс 20 °С.

В атмосфере помещения не должны присутствовать пары агрессивных жидкостей и агрессивные газы.

Допускается кратковременное повышение относительной влажности до 98 % при температуре ниже плюс 25 °С без конденсации влаги, суммарно не более одного месяца в год.

Срок хранения маршрутизаторов — один год с момента отгрузки, включая время транспортирования.

6 УТИЛИЗАЦИЯ

Маршрутизатор при хранении, транспортировании, эксплуатации не оказывает недопустимого вредного воздействия на окружающую среду и организм человека.

После окончания срока службы маршрутизатор подлежит демонтажу и утилизации как радиоэлектронная аппаратура в соответствии с нормами региона эксплуатации.

7 ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ

7.1 Эксплуатационные ограничения и меры безопасности

К эксплуатации устройства должны допускаться лица, изучившие настоящее руководство по эксплуатации и обладающие базовыми знаниями основ работы стеков протоколов TCP/IP, принципов построения сетей передачи данных, практическими навыками по первоначальной настройке (подключение по консоли, задание IP-адресов, управление учетными записями), резервному копированию и восстановлению конфигурационных файлов и образов ОС маршрутизатора, настройке статической маршрутизации и базовых протоколов динамической маршрутизации (например, OSPF в одной зоне), настройке базовой безопасности (ACL, SSH).

Устройство должно размещаться вне взрывоопасных зон при соблюдении рабочих условий эксплуатации. При этом устройство должно быть защищено от прямого воздействия атмосферных осадков. Способ установки определяется конструктивным исполнением: маршрутизатор платформы MX681 в пластиковом корпусе устанавливают на стандартную металлическую DIN-рейку шириной 35 мм; маршрутизаторы в исполнении MR устанавливают в стандартную телекоммуникационную стойку 19 дюймов с фиксацией винтами через монтажные элементы корпуса.

Для нормального охлаждения устройства, а также для удобства монтажа и обслуживания, при монтаже устройства сверху и снизу необходимо предусмотреть свободное пространство не менее 100 мм. Принудительная вентиляция не требуется.





- Производитель не несет ответственности за ущерб, вызванный неправильным монтажом, нарушением правил эксплуатации или использованием оборудования не по назначению.
- Во время монтажа, эксплуатации и технического обслуживания оборудования необходимо соблюдать «Правила технической эксплуатации электроустановок потребителей».
- Монтаж и эксплуатацию оборудования должен проводить квалифицированный персонал, имеющий группу по электробезопасности не ниже 3 и аттестованный в установленном порядке на право проведения работ в электроустановках потребителей до 1000 В.
- На лице, проводящем монтаж, лежит ответственность за производство работ в соответствии с настоящим руководством, требованиями безопасности и электромагнитной совместимости.
- В случае возникновения неисправности необходимо отключить питание от устройства, демонтировать и передать его в ремонт производителю.

7.2 Монтаж

7.2.1 Подготовка к монтажу

После транспортирования при отрицательных температурах распаковывание устройства допускается не ранее чем через 12 ч после размещения устройства в отапливаемом помещении. Перед использованием после такого транспортирования общая продолжительность выдержки устройства в нормальных климатических условиях должна составлять не менее 24 ч.

При распаковывании следует соблюдать следующий порядок операций:

- открыть коробку;
- из коробки извлечь:
  - документацию;
  - вложенные принадлежности, если они предусмотрены паспортом или спецификацией поставки;
  - ложементы с устройством;
- произвести внешний осмотр устройства.
  - проверить отсутствие видимых внешних повреждений корпуса и внешних разъемов;
  - внутри устройства не должно быть незакрепленных предметов;
  - маркировка устройства, комплектующих изделий должна легко читаться и не иметь повреждений.

В случае выявления повреждений их необходимо зафиксировать (фото- или видеофиксация), составить АКТ и уведомить поставщика.

7.2.2 Установка на DIN-рейку

Маршрутизатор платформы MX681 в пластиковом корпусе устанавливается на монтажную рейку (DIN-профиль 35 мм) в следующей последовательности:

- корпус устройства ставится на рейку, цепляясь верхними выступами;
- корпус опускается вниз относительно верхнего выступа до щелчка.



ВНИМАНИЕ! МОНТАЖНАЯ РЕЙКА ДОЛЖНА БЫТЬ ЗАЗЕМЛЕНА.

7.2.3 Внешние подключения

Внешние подключения осуществляются с помощью разъемов MSTBT 2,5/4-ST либо аналогов проводами сечением до 1,5 мм^2.



Рисунок 16 – Внешний вид разъема MSTBT 2,5/4-ST

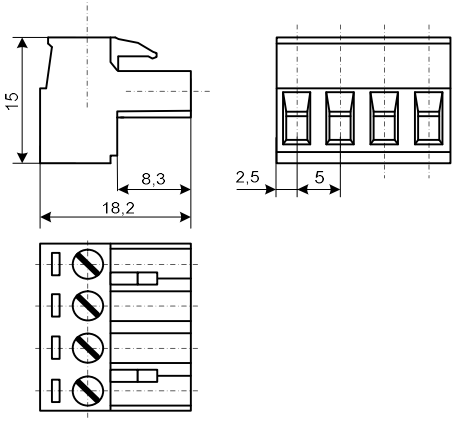


Рисунок 17 – Габаритные размеры разъема MSTBT 2,5/4-ST

ВНИМАНИЕ! ПОДКЛЮЧЕНИЕ К КЛЕММАМ УСТРОЙСТВА ПРОИЗВОДИТЬ ПРИ ОБЕСТОЧЕННОМ ОБОРУДОВАНИИ

ВНИМАНИЕ! ПРИ ПРОВЕРКЕ ГОТОВНОСТИ К РАБОТЕ ПРОВЕРИТЬ ПРАВИЛЬНОСТЬ ПОДКЛЮЧЕНИЙ, КРЕПЛЕНИЕ КЛЕММНИКОВ.

7.2.4 Шина T-BUS

Шина T-BUS представляет собой пятипроводную шину, составляемую из произвольного количества единичных Т-образных шинных соединителей ME 22,5 T-BUS 1,5/5-ST-3,81 либо аналогичных, крепящихся к DIN-рейке с помощью защелок.

Шина T-BUS предназначена для обеспечения питания установленных на ней устройств TOPAZ. Установленные на шине T-BUS устройства, поддерживающие передачу данных по интерфейсу RS-485, также объединяются в единую линию связи RS-485 типа «общая шина».

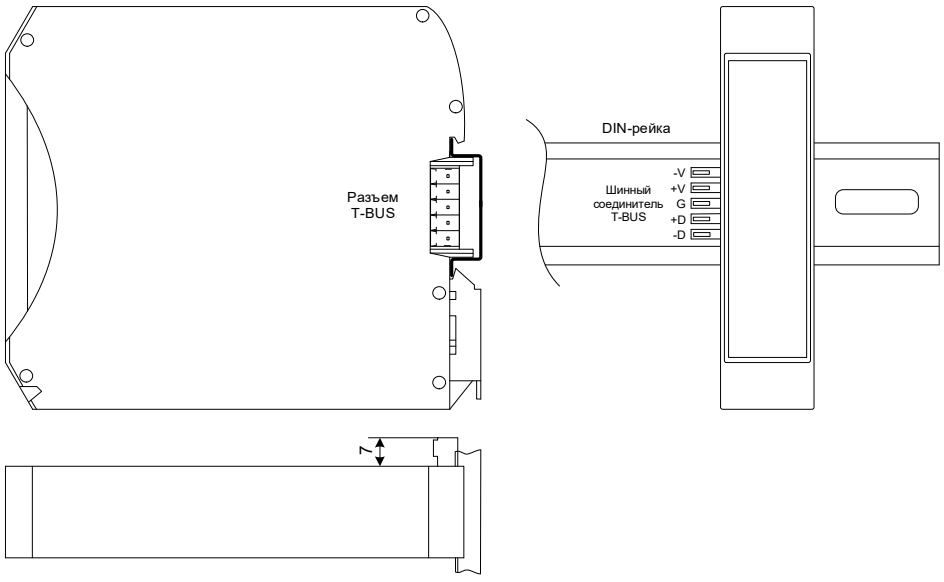


Рисунок 18 – Размещение устройства на DIN-рейке с шиной T-BUS

ВНИМАНИЕ! ПРИ УСТАНОВКЕ УСТРОЙСТВА НА ШИНУ T-BUS НЕОБХОДИМО КОНТРОЛИРОВАТЬ ПОЛОЖЕНИЕ КЛЕММ ШИННОГО СОЕДИНИТЕЛЯ T-BUS ОТНОСИТЕЛЬНО РАЗЪЕМА T-BUS НА ТЫЛЬНОЙ СТОРОНЕ КОРПУСА УСТРОЙСТВА.

Для подключения монтажных проводов к шине T-BUS используют аналоги следующих штекерных соединителей MC 1,5/5 ST 3,81 или IMC 1,5/5 ST 3,81, в зависимости от удобной стороны подвода проводов к шине. На рисунке ниже приведен внешний вид шины T-BUS в сборе, где:

A – шинный соединитель ME 22,5 T-BUS 1,5/5-ST-3,81
B – штекерный соединитель (розетка) MC 1,5/5-ST-3,81
C – штекерный соединитель (вилка) IMC 1,5/5-ST-3,81

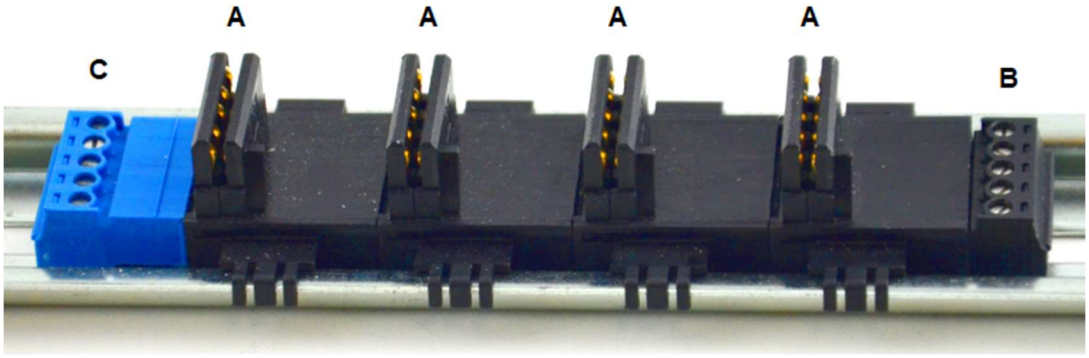


Рисунок 19 – Внешний вид шины T-BUS

Примечание Штекер IMC 1,5/5-ST-3,81 и его аналоги не входят в стандартный комплект поставки устройства.

7.2.5 Подключение питания

Количество и тип каналов питания устройства зависят от исполнения по питанию, согласно условному обозначению устройства. При наличии напряжения питания на канале питания загорится индикатор **PWR**.

При подключении источника питания постоянного тока к каналу питания 220 В полярность значения не имеет.

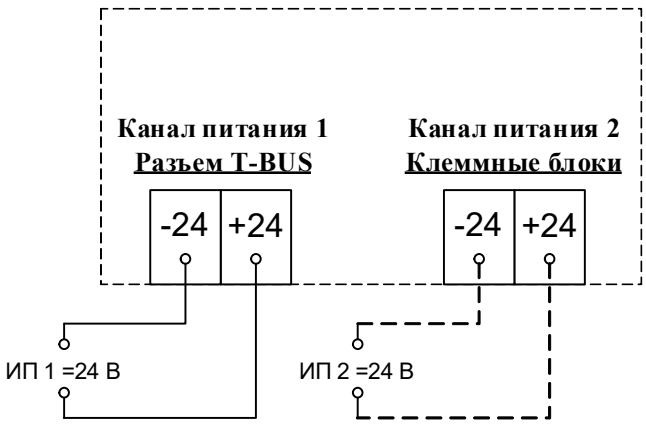


Рисунок 20 – Схема подключения питания 24 В постоянного тока

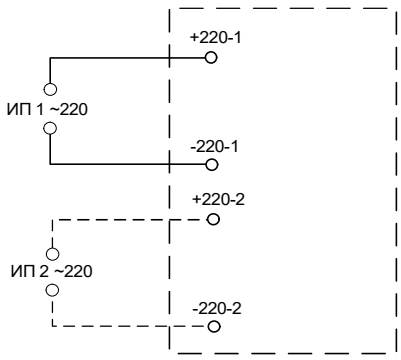


Рисунок 21 – Схема подключения питания устройств исполнения HV (2HV)

ВНИМАНИЕ! ОДНОВРЕМЕННОЕ ПОДКЛЮЧЕНИЕ К СЕТИ ПИТАНИЯ 24 В И 220 В НЕ ДОПУСКАЕТСЯ!

ВНИМАНИЕ! СЕТЬ ПИТАНИЯ (≈/= 220 В) ДОЛЖНА ИМЕТЬ ПРОВОД ЗАЗЕМЛЕНИЯ.

7.2.5.1 Питание шины T-BUS

Номинальное напряжение питания шины T-BUS: 24 В постоянного тока. Подача питания на шину T-BUS осуществляется одним из следующих способов:

- от внешнего источника питания, подключенного к шине с помощью штекера;
- от источника питания TOPAZ, установленного на шине.

ВНИМАНИЕ! НЕОБХОДИМО УЧИТЫВАТЬ, ЧТО НОМИНАЛЬНОЕ ЗНАЧЕНИЕ НАПРЯЖЕНИЯ ПИТАНИЯ ШИНЫ T-BUS ДОЛЖНО ВХОДИТЬ В ДОПУСТИМЫЙ ДИАПАЗОН ПИТАНИЯ ДЛЯ КАЖДОГО УСТРОЙСТВА TOPAZ, УСТАНОВЛЕННОГО НА ШИНЕ. НОМИНАЛЬНЫЕ ЗНАЧЕНИЯ И ДОПУСТИМЫЕ ДИАПАЗОНЫ ПИТАНИЯ УСТРОЙСТВ TOPAZ ПРИВЕДЕНЫ В РУКОВОДСТВАХ ПО ЭКСПЛУАТАЦИИ НА СООТВЕТСТВУЮЩИЕ УСТРОЙСТВА.

ВНИМАНИЕ! ЗАПРЕЩЕНО ПОДАВАТЬ НА ШИНУ T-BUS ВНЕШНЕЕ НАПРЯЖЕНИЕ ПИТАНИЯ, ПРЕВЫШАЮЩЕЕ ВЕРХНЮЮ ГРАНИЦУ РАБОЧЕГО ДИАПАЗОНА ДЛЯ НОМИНАЛЬНОГО НАПРЯЖЕНИЯ 24 В ПОСТОЯННОГО ТОКА.

ПОДКЛЮЧЕНИЕ К ШИНЕ T-BUS ИСТОЧНИКА С НОМИНАЛЬНЫМ ВЫХОДНЫМ НАПРЯЖЕНИЕМ 220 В ПОСТОЯННОГО / ПЕРЕМЕННОГО ТОКА ПРИВЕДЕТ К ВЫХОДУ ИЗ СТРОЯ ВСЕХ ПОДКЛЮЧЕННЫХ К ШИНЕ УСТРОЙСТВ!

7.2.6 Монтаж модификации MR

7.2.6.1 Установка в стойку 19”

Маршрутизатор платформы MX681 в исполнении MR устанавливается в стойку 19 дюймов и занимает 1U по высоте. Маршрутизатор платформы MX710 устанавливается в стойку 19 дюймов и занимает 2U по высоте.

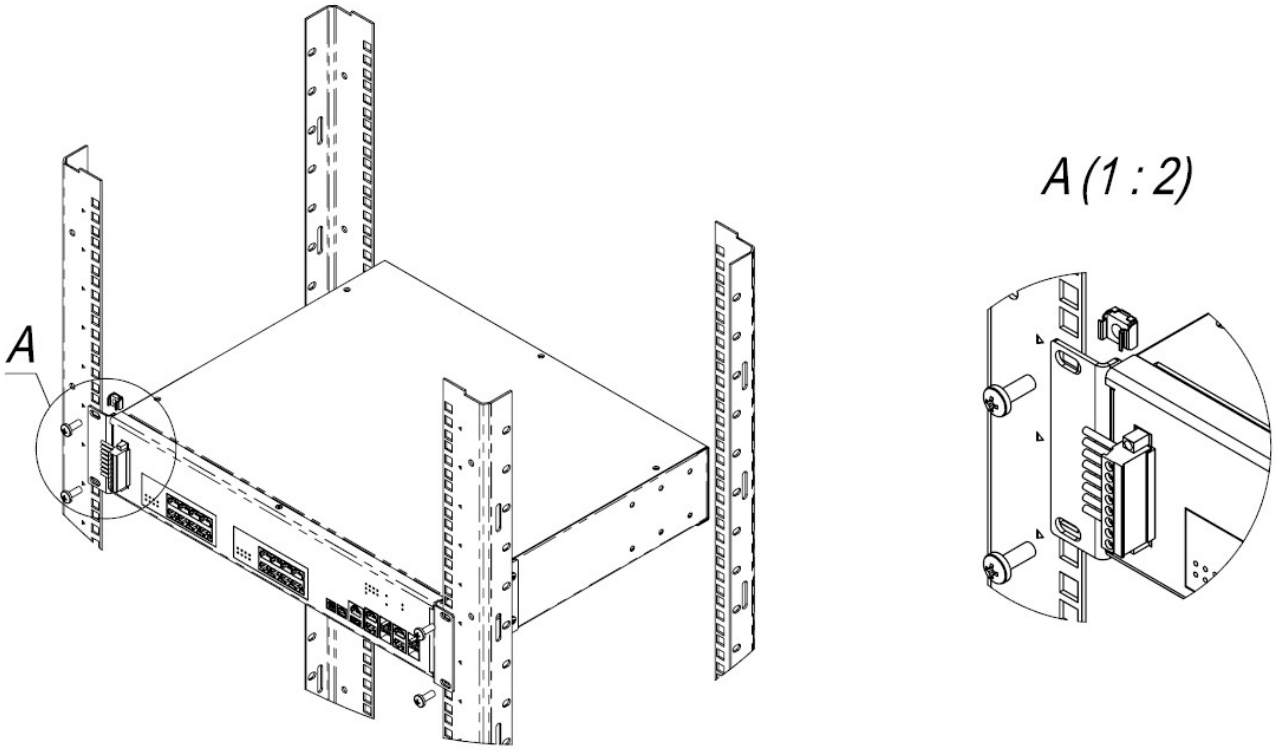


Рисунок 22 - Размещение устройства в стойку 19”. Крышка клеммного блока ввода питания условно не показана

7.2.6.2 Подключение питания

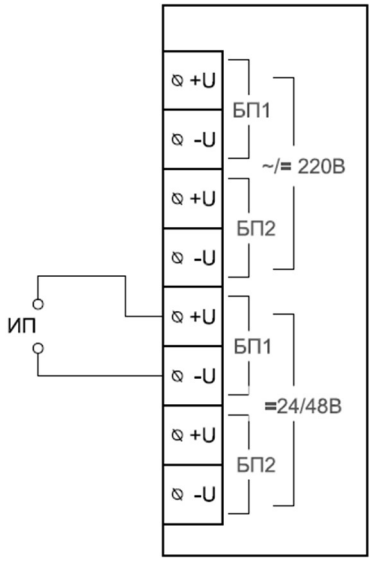
Входы питания модификации MR располагаются на клеммном блоке. В зависимости от исполнения, устройство может иметь следующие входы питания, каждый из которых обозначен соответствующей маркировкой:

- вход питания для первого блока питания (БП1), если на его вход требуется подавать 24 В постоянного тока;
- вход питания для второго блока питания (БП2), если на его вход требуется подавать 24 В постоянного тока;
- вход питания для первого блока питания (БП1), если на его вход требуется подавать 48 В постоянного тока;
- вход питания для второго блока питания (БП2), если на его вход требуется подавать 48 В постоянного тока;
- вход питания для первого блока питания (БП1), если на его вход требуется подавать 220 В постоянного или переменного тока;
- вход питания для второго блока питания (БП2), если на его вход требуется подавать 220 В постоянного или переменного тока.

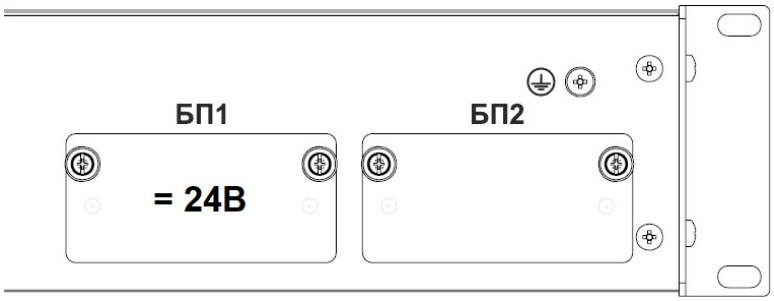
Напряжение, на которое рассчитан каждый блок питания, указано на блоках питания. Тип и количество блоков питания определяются заказным обозначением.

ВНИМАНИЕ! ПОДАЧА НАПРЯЖЕНИЯ 220 В (AC/DC) НА ВХОД ПИТАНИЯ 24 В (DC) или 24/48 В (DC) ПРИВЕДЕТ К УСТРОЙСТВА ИЗ СТРОЯ И АННУЛЯЦИИ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ ПРОИЗВОДИТЕЛЯ.

Схемы подключения электропитания различных исполнений по питанию и соответствующая маркировка блоков питания приведены на рисунках ниже.

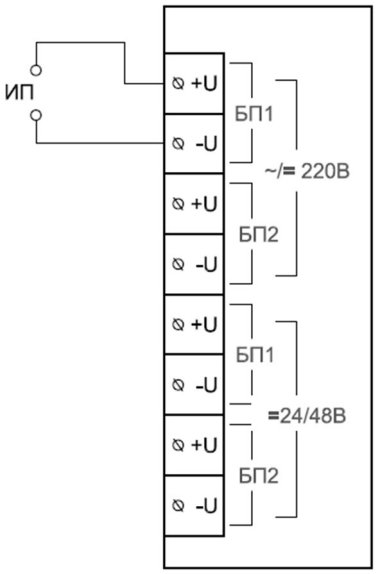


а) Схема подключения питания

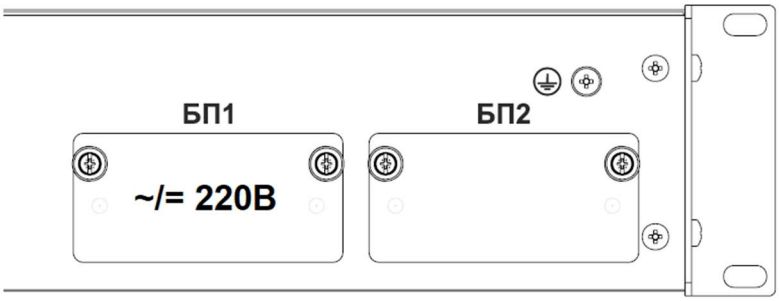


б) Маркировка блоков питания. Крышки отсека БП маркировки не имеют

Рисунок 23 – Пример подключения одного блока питания TOPAZ PW24/100W-MR и соответствующая маркировка отсеков для блоков питания

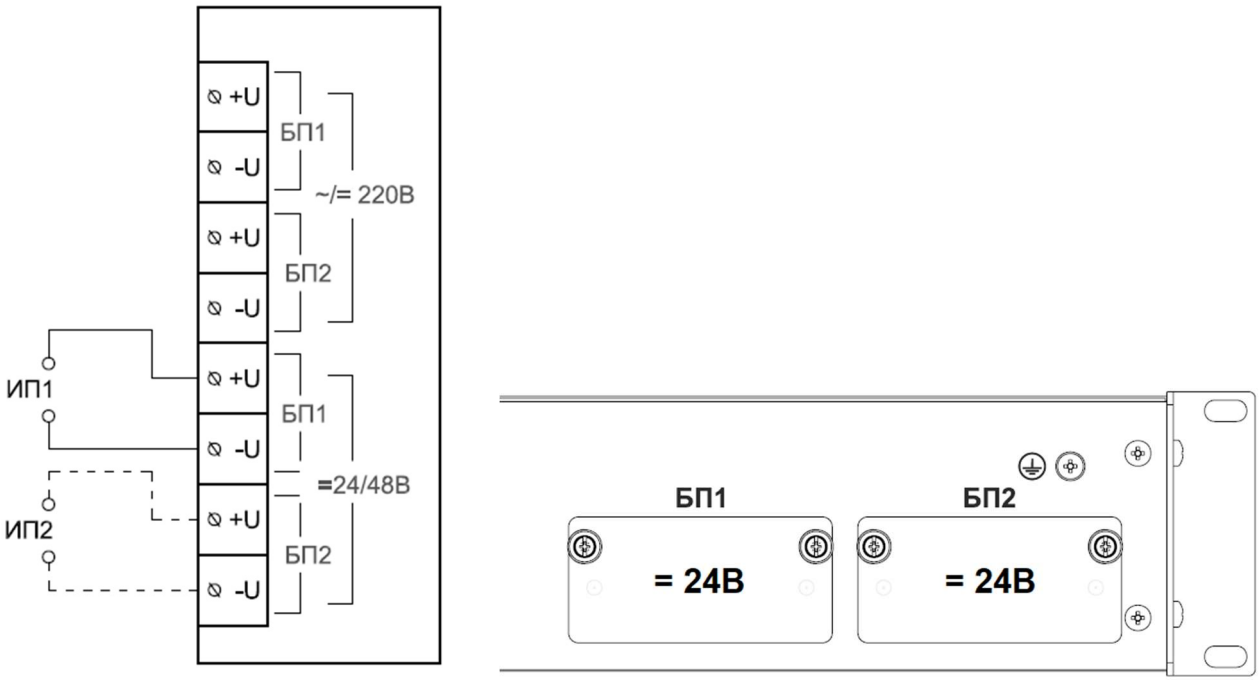


а) Схема подключения питания



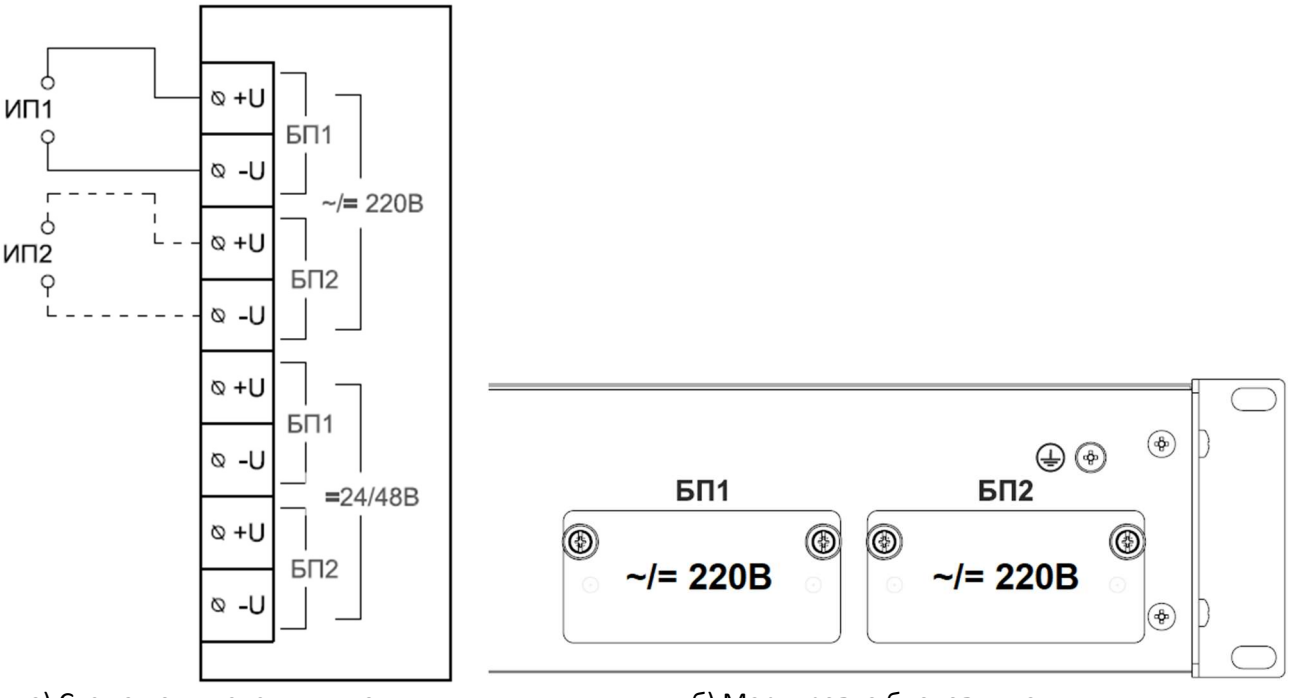
б) Маркировка блоков питания. Крышки отсека БП маркировки не имеют

Рисунок 24 – Пример подключения одного блока питания TOPAZ PW220/100W-MR и соответствующая маркировка отсеков для блоков питания



а) Схема подключения питания б) Маркировка блоков питания

Рисунок 25 – Пример подключения двух блоков питания TOPAZ PW24/100W-MR и маркировки БП1 и БП2



а) Схема подключения питания б) Маркировка блоков питания

Рисунок 26 – Пример подключения двух блоков питания TOPAZ PW220/100W-MR и маркировки БП1 и БП2

7.2.6.3 Подключение цепей сигнализации

Внешний вид клемм для подключения цепей сигнализации представлен на рисунке ниже.

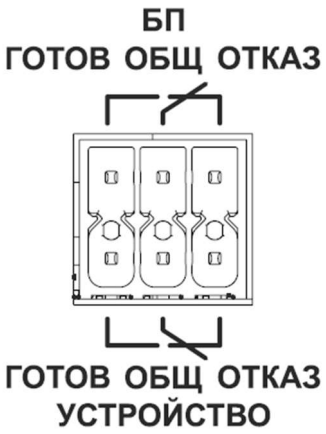


Рисунок 27 - Внешний вид клемм для подключения цепей сигнализации

Подключение цепей сигнализации представлено на схемах ниже.

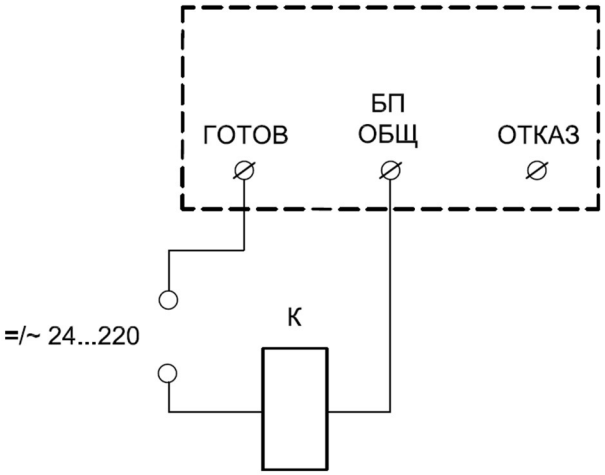


Рисунок 28 – Схема подключения цепей для проверки состояния каналов питания

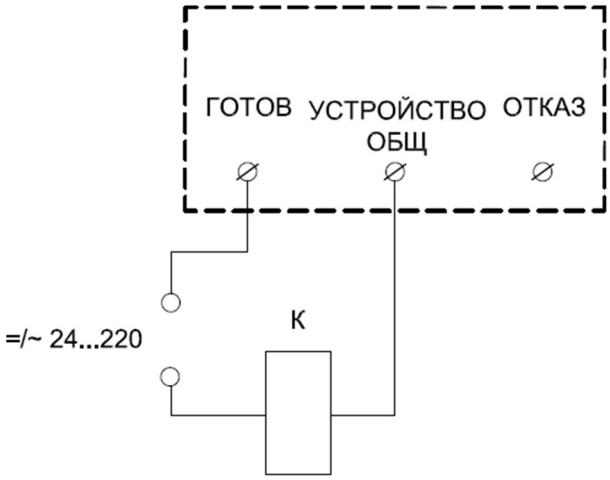


Рисунок 29 – Схема подключения цепей для диагностики исправности маршрутизатора

7.2.7 Подключение к сети Ethernet

Подключение к сети Ethernet осуществляют с использованием коммутаторов, объединенных в локальную технологическую сеть.

7.2.7.1 Подключение оптоволоконных портов Ethernet

Схема подключения оптического интерфейса Ethernet определяется типом установленного SFP-трансивера и количеством используемых им оптических волокон. Для двухволоконного SFP-трансивера используют две оптические линии; Tx-порт устройства 1 соединяют с Rx-портом устройства 2, а Rx-порт устройства 1 — с Tx-портом устройства 2. При подключении кабеля рекомендуется обозначить две стороны одной и той же линии одинаковой буквой (A-A, B-B, как показано на рисунке 30).

Для одноволоконного SFP-трансивера используют одно оптическое волокно; подключение выполняют в соответствии с технической документацией применяемого SFP-трансивера. На рисунке 30 приведена двухволоконная схема подключения.

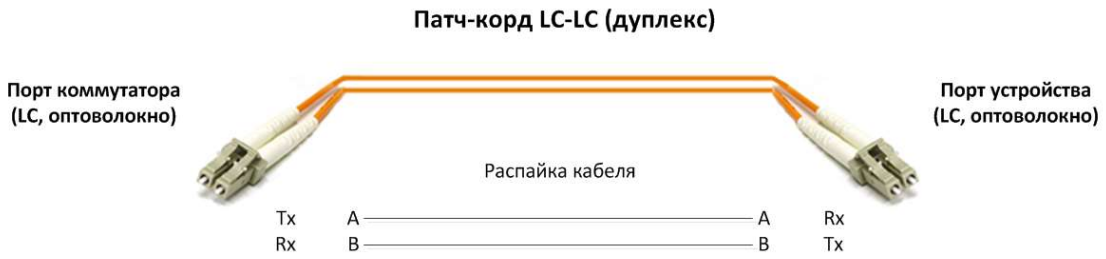


Рисунок 30 – Схема подключения оптоволоконного кабеля

ВНИМАНИЕ! УСТРОЙСТВО ЯВЛЯЕТСЯ ПРОДУКТОМ КЛАССА CLASS 1 LASER/LED. ИЗБЕГАЙТЕ ПРЯМОГО ПОПАДАНИЯ В ГЛАЗ ИЗЛУЧЕНИЯ LASER/LED.

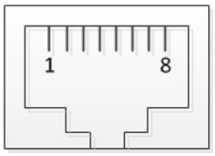
7.2.7.2 Подключение Ethernet-портов 10BASE-T/100BASE-TX

Порты 10BASE-T/100BASE-TX, расположенные на передней панели, используются для подключения Ethernet-устройств.

На рисунке ниже приведена схема расположения контактов для портов MDI (подключение устройств пользователя) и MDI-X (подключение коммутаторов/концентраторов), а также показана распайка прямого и перекрестного Ethernet-кабелей.

Таблица 38 – Назначение контактов

Контакт	Сигнал
порт MDI	
1	Tx+
2	Tx-
3	Rx+
6	Rx-
порт MDI-X	
1	Rx+
2	Rx-
3	Tx+
6	Tx-



8-контактный порт RJ45

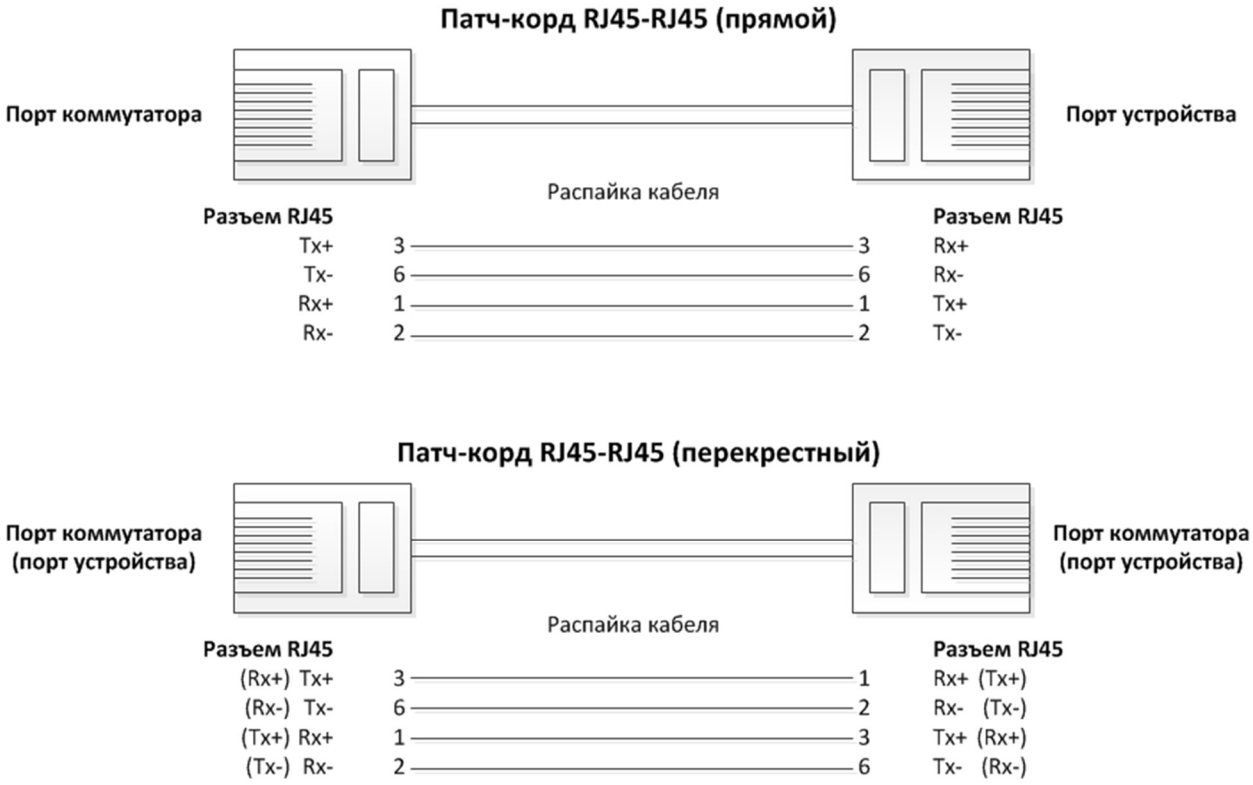


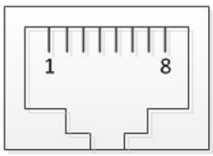
Рисунок 31 – Схема соответствия контактов

7.2.7.3 Подключение Ethernet-портов 1000BASE-T

Данные по интерфейсу 1000BASE-T передаются по четырём витым парам.

Таблица 39 – Назначение контактов

Контакт	Сигнал
порт MDI/MDI-X	
1	TRD (0) +
2	TRD (0) -
3	TRD (1) +
4	TRD (2) +
5	TRD (2) -
6	TRD (1) -
7	TRD (3) +
8	TRD (3) -



8-контактный порт RJ45

7.2.8 Горячая замена блока питания в модификации MR

При наличии двух установленных БП устройство поддерживает функцию горячей замены блоков питания. Для замены БП не требуется отключать цепи питания от соответствующих клемм.

Примечание Для БП, рассчитанного на 220 В AC/DC, необходимо предварительно отключить питание. Включение/отключение питания производится путем перевода соответствующего автоматического выключателя БП в положение «включено» / «отключено».

Горячую замену БП необходимо осуществлять в следующем порядке:

1) в случае, если применен БП на 220 В AC/DC, отключить питание заменяемого БП и убедиться в отсутствии напряжения на заменяемом БП (соответствующий индикатор **БП1** или **БП2** на передней панели устройства не активен);
2) открутить два фиксирующих винта заменяемого БП;
3) извлечь заменяемый БП;
4) установить новый БП на место заменяемого;
5) убедиться, что новый БП вставлен до упора (дополнительные усилия прилагать нельзя);
6) вручную закрутить фиксирующие винты нового БП;
7) в случае, если БП рассчитан на 220 В AC/DC, включить питание нового БП;
8) убедиться в наличии напряжения на новом БП (соответствующий индикатор БП1 или БП2 на передней панели устройства активен).

ПРИЛОЖЕНИЕ А

(Назначение контактов и портов)

Таблица А.1 – Обозначения клемм и портов стандартной модификации

Обозначение	Описание
Разъем T-BUS	
-24	Канал питания №1
+24	
Клеммный блок	
-24	Канал питания №2
+24	
Питание напряжением переменного тока	
~ 220 В	Клеммы питания 220 В
Заземление	
⏚	клемма заземления
Интерфейс конфигурирования	
USB	USB порт для подключения через консоль
Интерфейс Ethernet	
LANn	Порт Ethernet, где n номер порта

Таблица А.2 – Назначение клемм и портов модификации MR

Обозначение			Назначение
Каналы питания 220 В			
~/= 220V	**БП1**	**+U**	Вход от источника питания 220 В №1
		-U	
	БП2	**+U**	Вход от источника питания 220 В №2
		-U	
Каналы питания 24/48 В			
= 24/48V	**БП1**	**+U**	Вход от источника питания 24/48 В №1
		-U	
	БП2	**+U**	Вход от источника питания 24/48 В №2
		-U	
Реле сигнализации питания			
БП ОБЩ			Общий контакт
ГОТОВ			Нормально разомкнутый контакт (отсутствие неисправностей)
ОТКАЗ			Нормально замкнутый контакт (наличие неисправностей)
Реле сигнализации работы устройства			
УСТРОЙСТВО ОБЩ			Общий контакт
ГОТОВ			Нормально разомкнутый контакт (отсутствие неисправностей)
ОТКАЗ			Нормально замкнутый контакт реле (наличие неисправностей)
Порты			
КОНСОЛЬ			Порт USB
			Порт Ethernet

ПРИЛОЖЕНИЕ Б

(Назначение кнопок и индикаторов)

Таблица Б.1 – Обозначения кнопок и светодиодных индикаторов стандартной модификации

Обозначение	Описание
Кнопки (в наличии RS и RB)	
RS	Перезагрузка устройства
RB	Активация загрузчика с SD-карты при одновременном нажатии с кнопкой RS
Кнопки (в наличии RB)	
RB	Активация загрузчика с SD-карты
Индикаторы	
PWR	Наличие питания
RDY	Состояние готовности устройства

Таблица Б.2 – Назначение светодиодных индикаторов модификации MR

Наименование индикатора		Режим работы	Описание
Модули питания и ЦП			
ГОТОВ (или **ГОТ**)		не светится	Устройство не работает
		мигает	Устройство функционирует нормально
АВАРИЯ		светится непрерывно	Устройство неисправно
		не светится	Устройство исправно
КОНСОЛЬ		светится непрерывно	Наличие подключения к устройству
		не светится	Отсутствует подключение
СВЯЗЬ	**П1**	светится непрерывно	Наличие подключения к порту П1
		не светится	Отсутствует подключение к порту П1
	П2	светится непрерывно	Наличие подключения к порту П2
		не светится	Отсутствует подключение к порту П2
	П3	светится непрерывно	Наличие подключения к порту П3
		не светится	Отсутствует подключение к порту П3
	П4	светится непрерывно	Наличие подключения к порту П4
		не светится	Отсутствует подключение к порту П4
SFP	**П1**	светится непрерывно	Наличие подключения к порту П1 (SFP)
		не светится	Отсутствует подключение к порту П1 (SFP)
	П2	светится непрерывно	Наличие подключения к порту П2 (SFP)
		не светится	Отсутствует подключение к порту П2 (SFP)
	П3	светится непрерывно	Наличие подключения к порту П3 (SFP)
		не светится	Отсутствует подключение к порту П3 (SFP)
	П4	светится непрерывно	Наличие подключения к порту П4 (SFP)
		не светится	Отсутствует подключение к порту П4 (SFP)
БП1		светится непрерывно	Наличие питания от блока питания 1
		не светится	Отсутствие питания от блока питания
БП2		светится непрерывно	Наличие питания от блока питания 2
		не светится	Отсутствие питания от блока питания

ПРИЛОЖЕНИЕ В
(Внешний вид устройства)







Рисунок В.1 – Внешний вид TOPAZ FW MX710 4GTxSFP-16Tx-MR-2PW



Рисунок В.2 – Внешний вид маршрутизатора TOPAZ FW платформы MX681 в пластиковом корпусе

Примечание Рисунки В.1 и В.2 приведены в качестве примера внешнего вида отдельных модификаций. Внешний вид, расположение элементов индикации и интерфейсных разъемов могут отличаться в зависимости от конкретной модификации изделия.

ПРИЛОЖЕНИЕ Г

(Подключение к устройству с помощью утилиты PuTTY)

Утилита PuTTY – одна из распространенных бесплатных программ, не требующая установки. В данном разделе приведено описание подключения к устройству с помощью данной утилиты.

Сайт разработчика:
http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html.
Ссылка непосредственно на исполняемый файл программы:
https://the.earth.li/~sgtatham/putty/latest/x86/putty.exe.

Подключение через серийный порт

После запуска программы PuTTY откроется окно настройки, где во вкладке **Session** необходимо выбрать тип соединения **Serial** и его основные параметры (номер виртуального порта будет отличаться от приведенного в примере в зависимости от вашей системы):

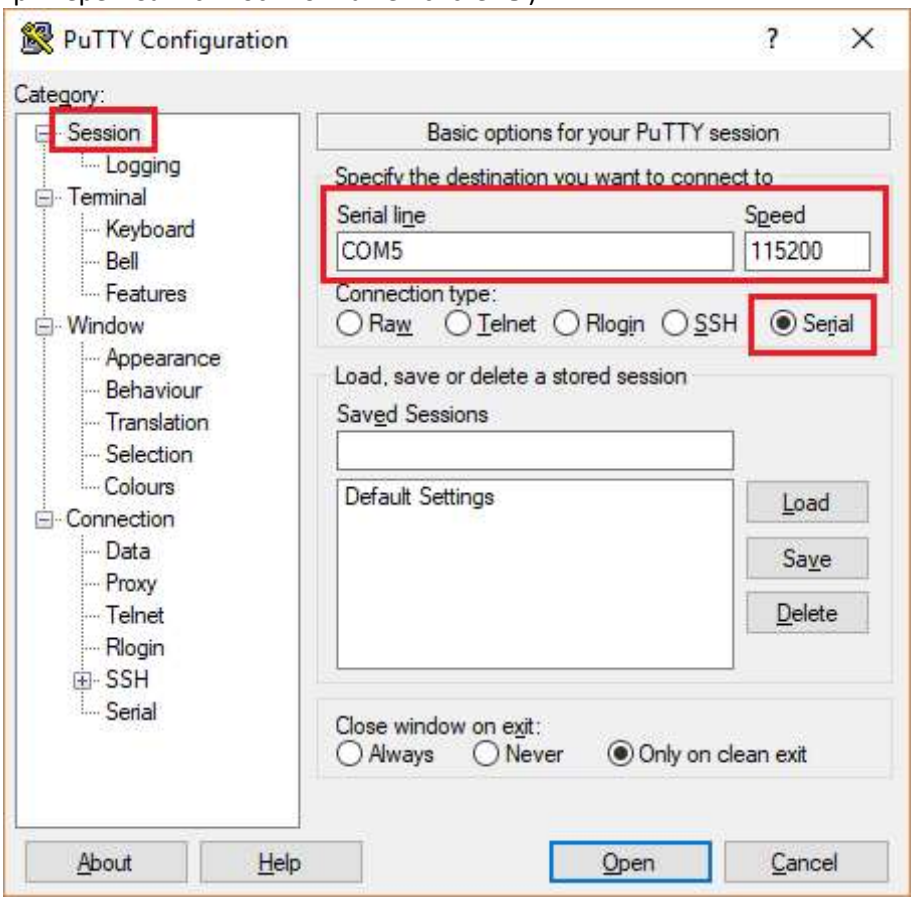


Рисунок Г.1 – Задаваемые настройки раздела Session (сессия)

В настройках соединения (**Connection**) – выбрать последовательный порт (**Serial**) и установить параметры соединения:

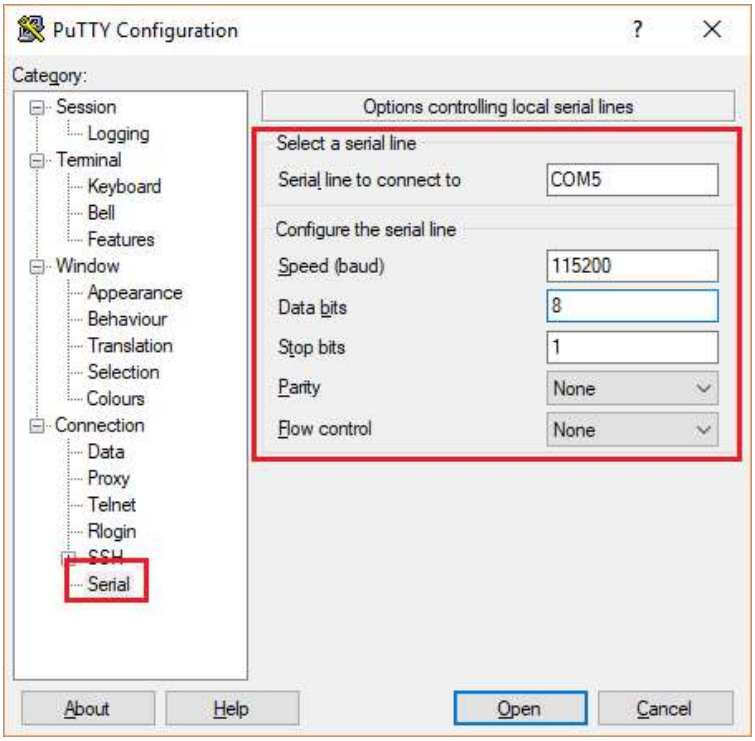


Рисунок Г.2 – Задаваемые настройки раздела Serial (серийный порт)

После настройки параметров последовательного порта необходимо нажать кнопку «Открыть» (Open) для установки соединения и вызова окна консоли.

Подключение через Ethernet-порт

Для подключения к устройству по протоколу SSH, во вкладке **Session** необходимо выбрать тип соединения **SSH** и его основные параметры:

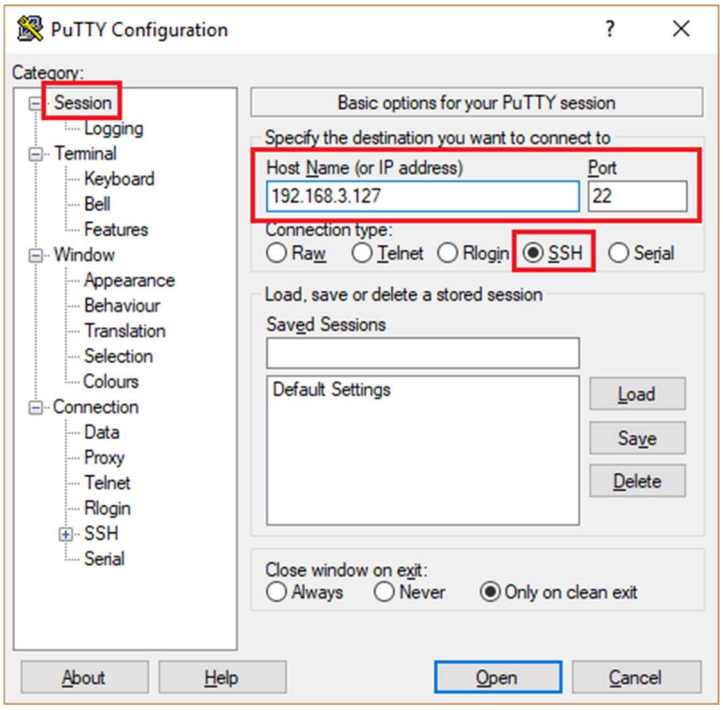


Рисунок Г.3 – Задаваемые настройки раздела Session (сессия)

После настройки параметров SSH-соединения необходимо нажать кнопку «Открыть» (Open) для установки соединения и вызова окна консоли.

ПРИЛОЖЕНИЕ Д
(Модификации устройства)

Таблица Д.1 – Типовые модификации устройства

Платформа	Модификация
MX681	Маршрутизатор TOPAZ FW MX681 E10 2GTxSFP-8Tx-MR-2PW-DGN
	Маршрутизатор TOPAZ FW MX681 E3 2GTxSFP-1GTx-2HV-DGN
	Маршрутизатор TOPAZ FW MX681 E3 2GTxSFP-1GTx-MR-2PW-DGN
MX710	Маршрутизатор TOPAZ FW MX710 4GTxSFP-MR-2PW-DGN
	Маршрутизатор TOPAZ FW MX710 4GTxSFP-8Tx-MR-2PW-DGN
	Маршрутизатор TOPAZ FW MX710 4GTxSFP-16Tx-MR-2PW-DGN