

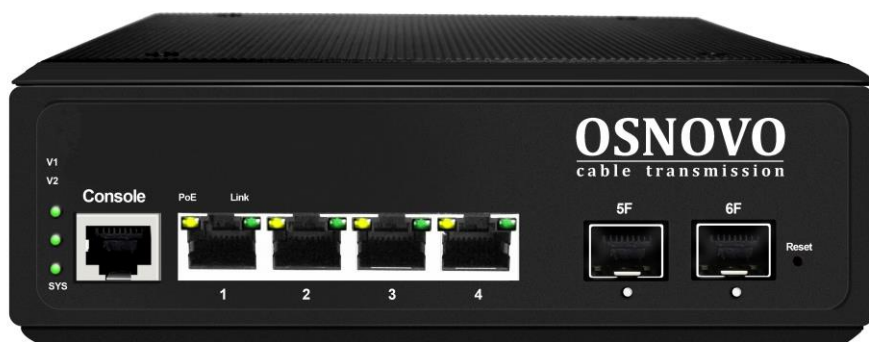
OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Управляемый (L2+) PoE коммутатор на 6
портов

SW-80402-IL(port 90W,360W)



Прежде чем приступить к эксплуатации изделия,
внимательно прочтите настоящее руководство

www.osnovo.ru

Содержание

1. Назначение.....	4
2. Комплектация*	4
3. Особенности оборудования	5
4. Внешний вид и описание элементов	5
5. Подключение.....	7
6. Проверка работоспособности системы	10
7. Подготовка перед управлением коммутатором через WEB.	11
8. Подготовка перед управлением коммутатором через порт CONSOLE	14
9. Подготовка перед управлением коммутатором через Telnet/SSH	16
10. Управление через WEB интерфейс.....	18
10.1 Основные сведения.....	18
10.2 Главное меню WEB интерфейса	19
10.3 Network Admin (Настройка сетевых параметров и администрирование) ...	20
10.3.1 IP Configuration (Настройка IP адреса)	20
10.3.2 SNTP Configuration (Настройка протокола времени SNTP)	21
10.3.3 SNMP Configuration (Настройка протокола управления SNMP).....	22
10.3.4 System Log Configuration (Настройка системного журнала)	24
10.4 Port Configure (Конфигурирование портов).....	25
10.4.1 Port Configuration (Настройка портов).....	25
10.4.2 Link aggregation (Агрегация каналов).....	26
10.4.3 Port Mirroring (Зеркалирование портов)	29
10.4.4. Thermal Protection Configuration (Температурная защита)	30
10.5 PoE Configuration (Конфигурация PoE)	31
10.5.1 PoE Setting (Настройки PoE).....	32
10.5.2 PD Alive (Функция антизависания для PoE устройств).....	33
10.5.3 PoE Status (Состояние PoE на портах)	34
10.6 Advanced Configure (Расширенные настройки)	34
10.6.1 VLAN (Настройка VLAN)	34
10.6.2 Port Isolation (Изоляция портов)	39

10.6.3 STP (Протокол связующего дерева).....	40
10.6.4 MAC Address Table (Таблица MAC адресов).....	43
10.6.5 IGMP Snooping.....	44
10.6.6 ERPS (Протокол ERPS)	47
10.6.7 LLDP (Настройка протокола LLDP)	50
10.6.8 Loop Protection (Защита от сетевых петель)	51
10.7 QoS (Приоритезация трафика).....	52
10.7.1 QoS Port Classification (Классификация портов с помощью QoS).....	53
10.7.2 Port Policing (Функция ограничения скорости на портах).....	54
10.7.3 Storm Control Configuration (Настройка защиты от сетевого шторма).....	55
10.8 Security Configure (Настройки безопасности)	56
10.8.1 Password (Пароль)	56
10.8.2 802.1X.....	56
10.8.3 DHCP Snooping (Защита от атак с использованием DHCP)	58
10.8.4 IP&MAC Source Guard	59
10.8.5 ARP Inspection (Проверка ARP пакетов).....	62
10.8.6 ACL (Правила контроля доступа).....	65
10.9 Diagnostics (Инструменты диагностики и мониторинга).....	68
10.9.1 Ping Test (Тестирование соединения с помощью PING)	68
10.9.2 Cable Diagnostics (Проверка кабеля)	70
10.9.3 CPU Load (Загрузка CPU коммутатора).....	70
10.10 Maintenance (Обслуживание).....	71
10.10.1 Restart Device (Перезагрузка коммутатора)	71
10.10.2 Factory Defaults (Возврат к заводским настройкам).....	71
10.10.3 Firmware Upgrade (Обновление прошивки)	72
10.10.4 Firmware Select (Выбор текущей прошивки коммутатора)	72
10.10.5 Configuration (Текущая конфигурация).....	73
11. Технические характеристики*	76
12. Гарантия	78

1. Назначение

Управляемый (L2+) PoE коммутатор на 6 портов SW-80402-IL(port 90W,360W) предназначен для объединения сетевых устройств, запитывания их по технологии PoE и передачи данных между ними в условиях эксплуатации в промышленных условиях.

Промышленный коммутатор (далее по тексту - коммутатор) оснащен 4-мя портами Gigabit Ethernet (10/100/1000Base-T) с PoE, а также 2-мя Gigabit Ethernet SFP-слотами (100/1000Base-FX).

К каждому из 4 основных портов коммутатора можно подключать мощные PoE-устройства с потреблением до 90 Вт (общая выходная мощность на 4 порта до 360 Вт). Порты соответствуют стандартам IEEE 802.3af/at/bt и автоматически определяют подключаемые PoE-устройства.

В коммутаторе предусмотрена функция проверки статуса подключенного PoE устройства (PD Alive). Данная функция активируется через WEB интерфейс и позволяет диагностировать в автоматическом режиме «зависание» подключенных PoE устройств и перезагружать их путем переподачи PoE питания.

Коммутатор гибко настраивается через WEB-интерфейс и имеет множество функций L2+ уровня, таких как VLAN, IGMP snooping, QoS и др.

Кроме того коммутатор поддерживает автоматическое определение MDI/MDIX (Auto Negotiation) на всех портах – распознает тип подключенного сетевого устройства и при необходимости меняет контакты передачи данных, что позволяет использовать кабели, обжатые любым способом (кроссовые и прямые).

Коммутатор SW-80402-IL(port 90W,360W) рекомендуется использовать, если есть необходимость объединить несколько сетевых устройств (например, IP-камеры, в том числе с мощной подсветкой и обогревом) в одну сеть и передать к ним питание по кабелю витой пары (PoE) в условиях эксплуатации на промышленных объектах.

2. Комплектация*

1. Коммутатор SW-80402-IL(port 90W,360W) – 1 шт;
2. Клемма 6pin (под винт) – 1 шт;
3. Краткое руководство по эксплуатации – 1 шт;
4. Упаковка – 1 шт;

3. Особенности оборудования

- Поддерживает стандарты PoE IEEE 802.3af/at/bt . Мощность портов до 90Вт (общая мощность 360Вт на 4 порта);
- Предназначен для организации сети в условиях эксплуатации на промышленных объектах;
- Расширенный диапазон рабочих температур: -40... +75 °С;
- Грозозащита медных портов;
- Управление через WEB интерфейс;
- Поддержка функций L2 (VLAN,QOS,LACP,LLDP,IGMP snooping);
- Поддержка кольцевой топологии подключения;
- PD Alive – функция для автоматической диагностики и перезагрузки зависших PoE устройств.

4. Внешний вид и описание элементов

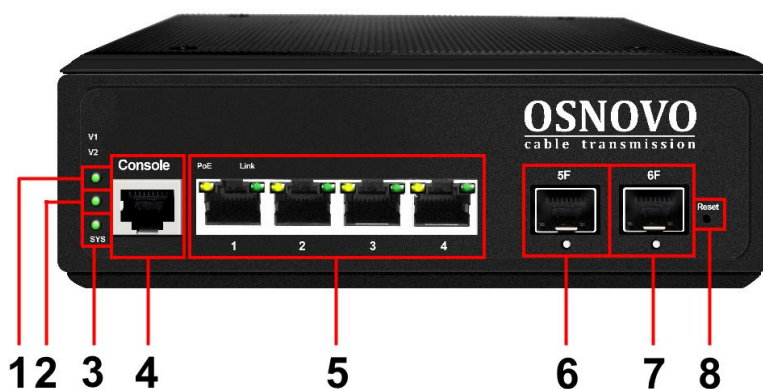


Рис.1 Коммутатор SW-80402-IL(port 90W,360W), разъемы, кнопки и индикаторы

Таб. 1 Коммутатор SW-80402-IL(port 90W,360W), назначение внутренних элементов

№ п/п	Обозначение	Назначение
1	V1	LED-индикатор подключения основного БП <u>Горит зеленым</u> – питание подается. <u>Не горит</u> – питание на входе отсутствует.
2	V2	LED-индикатор подключения резервного БП <u>Горит зеленым</u> – питание подается. <u>Не горит</u> – питание на входе отсутствует.
3	SYS	LED индикатор работы коммутатора. <u>Мигает</u> – работа в штатном режиме; <u>Горит</u> – аварийная ситуация (зависание коммутатора); <u>Быстро мигает</u> – идет загрузка прошивки.
4	Console	Разъем RJ-45 для подключения коммутатора к COM порту. Позволяет загружать в коммутатор прошивку в случае аварийной ситуации
5	PoE Link 1 2 3 4	Разъемы RJ-45 с 1 по 4й для подключения сетевых устройств на скорости 10/100/1000 Мбит/с и запитывания их по технологии PoE (до 90 Вт на порт) LED-индикаторы: <u>Горит желтым</u> – подключено PoE устройство. <u>Не горит</u> – подключено устройство без PoE или питание PoE не подается (неисправность). <u>Горит/Мигает зеленым</u> – подключено устройство, идет передача данных.
6	5F	SFP-слот (№1) для подключения коммутатора к оптической линии связи на скорости 100/1000 Мбит/с, используя SFP-модули 155Мбит/с или 1,25 Гбит/с (приобретаются отдельно). LED индикаторы активности SFP портов: <u>Мигает зеленым</u> – к порту подключено устройство, порт активен, идет передача данных.

№ п/п	Обозначение	Назначение
		<u>Горит зеленым</u> – к порту подключено устройство. Передачи данных нет.
7	6F	SFP-слот (№2) для подключения коммутатора к оптической линии связи на скорости 100/1000 Мбит/с, используя SFP-модули 155Мбит/с или 1,25 Гбит/с (приобретаются отдельно). LED индикаторы активности SFP портов: <u>Мигает зеленым</u> – к порту подключено устройство, порт активен, идет передача данных. <u>Горит зеленым</u> – к порту подключено устройство. Передачи данных нет.
8	Reset	Кнопка для сброса настроек коммутатора к заводским. Необходимо продолжительное нажатие ~3 сек при включенном питании.

5. Подключение

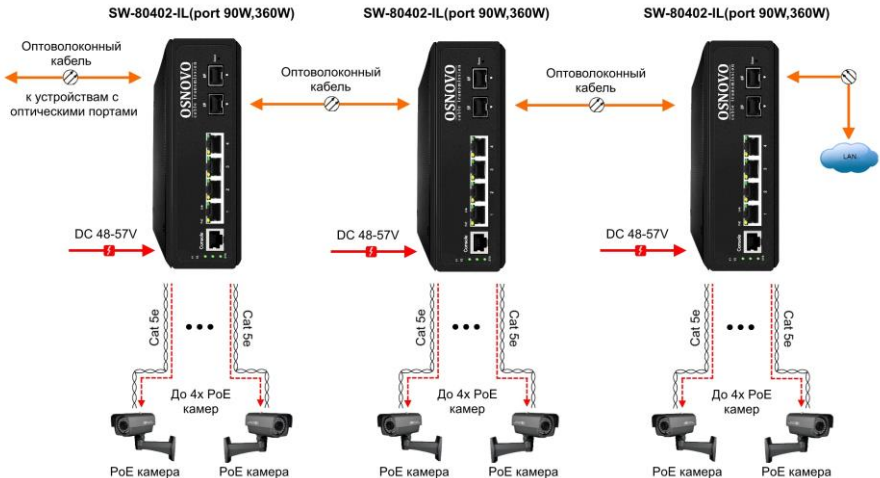


Рис. 2 Схема подключения коммутатора SW-80402-IL(port 90W,360W) каскадом

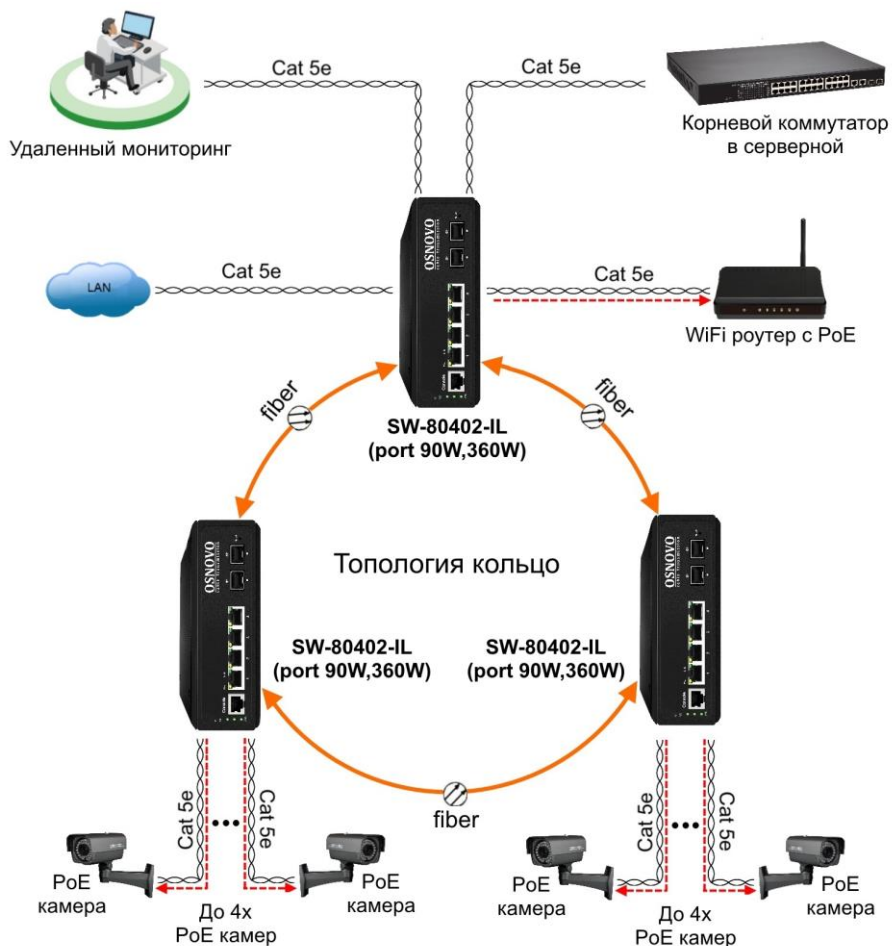


Рис.3 Схема подключения коммутатора SW-80402-IL(port 90W,360W) в топологии «кольцо»

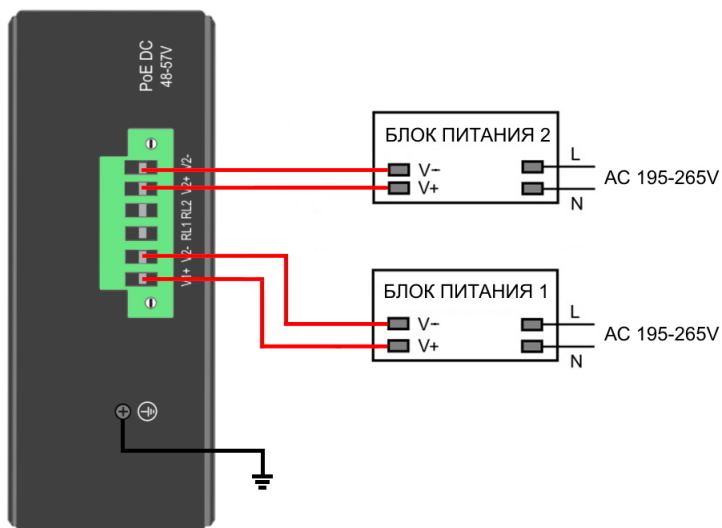


Рис.4 Схема подключения блоков питания (основной V1 и резервный V2) к коммутатору SW-80402-IL(port 90W,360W)

Внимание!

Перед установкой и подключением коммутатора отключите питание. Для подключения коммутатора к сети питания используйте подходящие блоки питания DC 48-57V (в комплект поставки не входят). При подключении БП к коммутатору строго соблюдайте полярность.

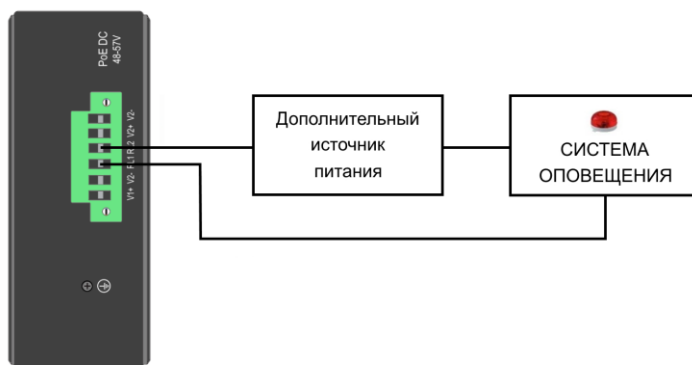


Рис.5 Схема подключения системы оповещения к коммутатору SW-80402-IL(port 90W,360W)

Внимание!

Релейный выход (RL1, RL2 нормально разомкнутые контакты) поддерживает управление исполнительными устройствами мощностью не более 24Вт. Напряжение источника питания, подключенного к релейному выходу, не должно превышать 24В, постоянный ток, проходящий через реле, не должен превышать 1А.

6. Проверка работоспособности системы

После подключения кабелей к разъёмам и подачи питания можно убедиться в работоспособности коммутатора.

Подключите коммутатор между двумя ПК с известными IP-адресами, располагающимися в одной подсети, например, 192.168.2.2 и 192.168.2.3.

На первом компьютере (192.168.2.2) запустите командную строку (выполните команду cmd) и в появившемся окне введите команду:

ping 192.168.2.3

Если все подключено правильно, на экране монитора отобразится ответ от второго компьютера. Это свидетельствует об исправности коммутатора.

Если ответ ping не получен («Время запроса истекло»), то следует проверить соединительный кабель и IP-адреса компьютеров. Если не все пакеты были приняты, это может свидетельствовать:

- о низком качестве кабеля витой пары;
- о неисправности коммутатора;
- о помехах в линии.

Примечание:

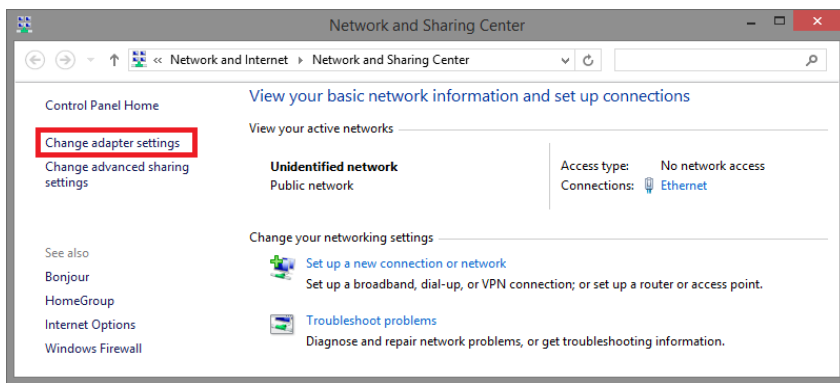
Причины потери в оптической линии могут быть вызваны:

- неисправностью SFP-модулей;
- изгибами кабеля;
- большим количеством узлов сварки;
- неисправностью или неоднородностью оптоволокну.

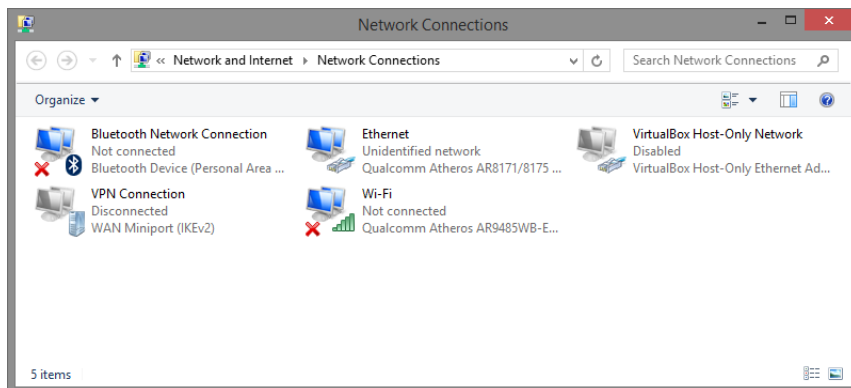
7. Подготовка перед управлением коммутатором через WEB.

Здесь будет показана детальная настройка сети для ПК под управлением Windows 8 (похожий интерфейс у Windows7 и Windows Vista).

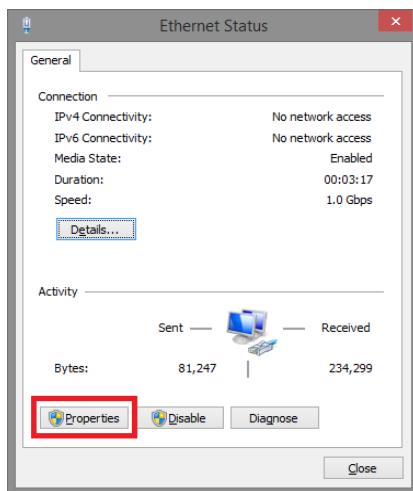
1. Откройте «Центр управления сетями и общим доступом» (Network and Sharing in Control Panel) и нажмите «Изменение параметров адаптера» (Change adapter setting) как на рисунке ниже.



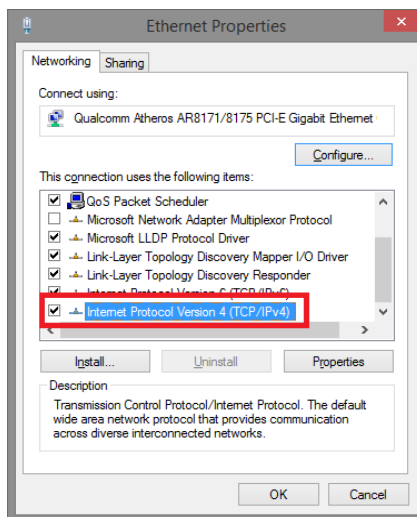
2. В появившемся окне «Сетевые подключения» (Network Connections) отображены все сетевые подключения, доступные вашему ПК. Сделайте двойной клик на подключении, которое вы используете для сети Ethernet



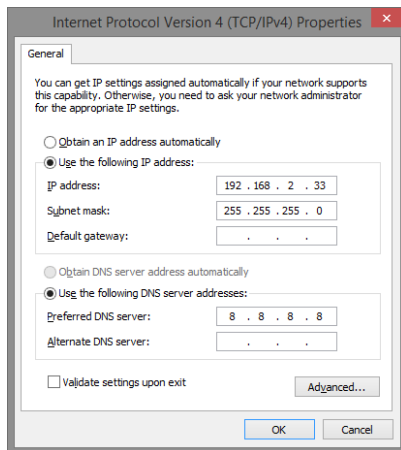
3. В появившемся окне «Состояние - Подключение по локальной сети» (Ethernet Status) нажмите кнопку «Свойства» (Properties) как показано ниже.



4. В появившемся окне «Подключение по локальной сети – Свойства» сделайте двойной клик на «протокол интернета версии IP V4 (TCP/IPv4)» как показано ниже



5. В появившемся окне «Протокол интернета версии IP V4 (TCP/IPv4)» сконфигурируйте IP адрес вашего ПК и маску подсети как показано ниже



По умолчанию IP адрес коммутатора:

192.168.2.1

Вы можете задать любой IP адрес в поле «IP адрес», в той же подсети, что и IP адрес коммутатора. Нажмите кнопку ОК, чтобы сохранить и применить настройки.

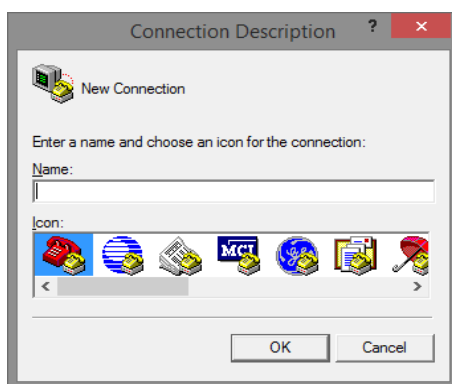
Теперь вы можете использовать любой браузер для входа в меню настроек коммутатора.

- Login: **admin**
- Password: **system**

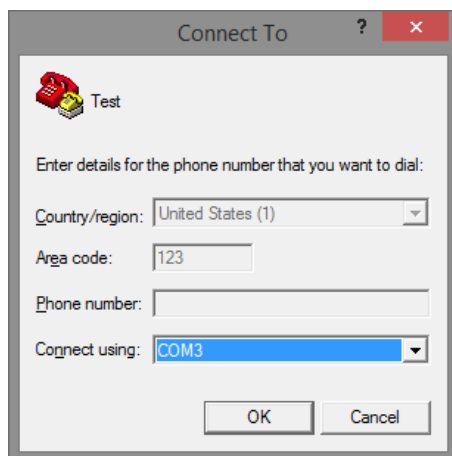
8. Подготовка перед управлением коммутатором через порт CONSOLE

Скачайте и установите на ПК, с которого будет проводиться конфигурирование коммутатора программу-эмулятор HyperTerminal или PuTTY. После установки необходимого ПО используйте следующую пошаговую инструкцию:

1. Соедините порт Console коммутатора с COM-портом компьютера с помощью кабеля.
2. Запустите HyperTerminal на ПК.
3. Задайте имя для нового консольного подключения.

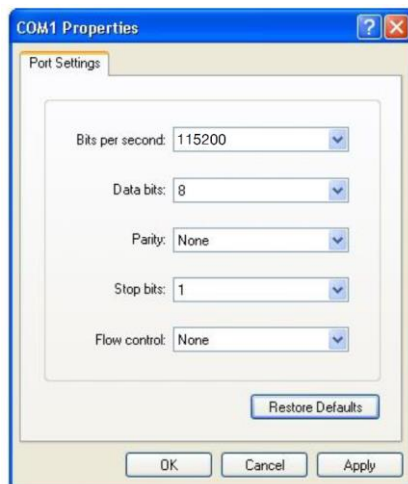


4. Выберите COM-порт, к которому подключен коммутатор.



5. Настройте COM-порт следующим образом:

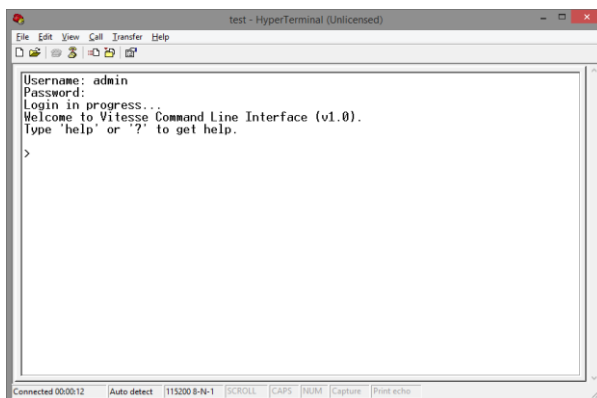
- ✓ Скорость передачи данных (Baud Rate) – 115200;
- ✓ Биты данных (Data bits) – 8;
- ✓ Четность (Parity) – нет;
- ✓ Стоп биты (Stop bits) – 1;
- ✓ Управление потоком (flow control) – нет.



6. Система предложит войти Вам в интерфейс CLI (управление через командную строку).

По умолчанию:

- Login: admin
- Password: system



9. Подготовка перед управлением коммутатором через Telnet/SSH

Протоколы Telnet и SSH предоставляют пользователю текстовый интерфейс командной строки для управления коммутатором (CLI). Но только SSH обеспечивает создание безопасного канала с полным шифрованием передаваемых данных.

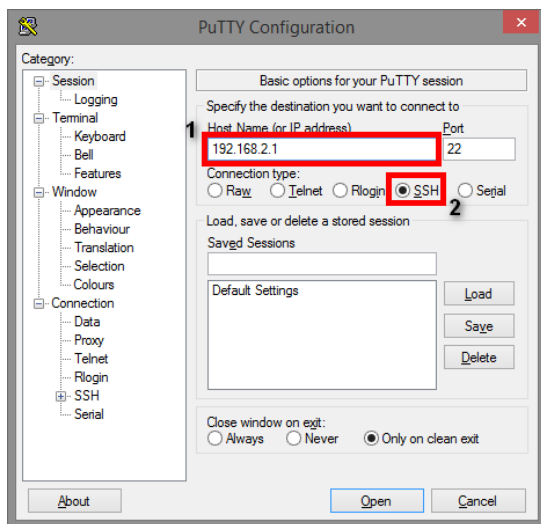
Чтобы получить доступ к CLI коммутатора через Telnet/SSH, ваш ПК и коммутатор должны находиться в одной сети. Подробнее, как это сделать рассматривалось в разделе инструкции «Подготовка перед управлением коммутатором через WEB-интерфейс».

Telnet интерфейс встроен в командную строку CMD семейства операционных систем Microsoft Windows. SSH интерфейс доступен только с помощью программы эмулятора SSH терминала. Ниже показано, как получить доступ к CLI коммутатора через SSH с помощью программы PuTTY.

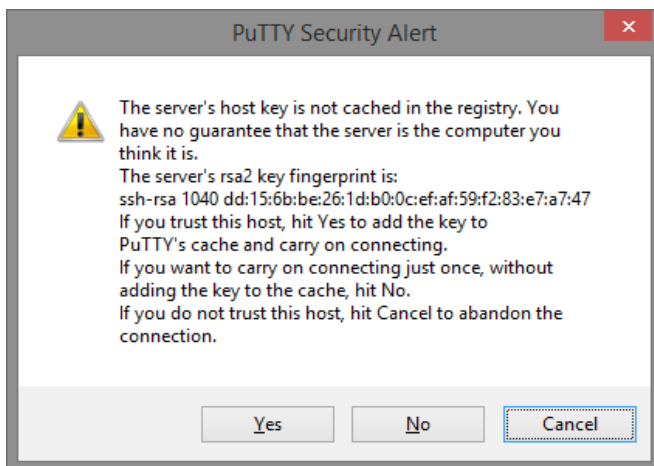
1. Зайдите в меню PuTTY Configuration. Введите IP адрес коммутатора в поле Имя хоста (Host Name) (или IP адрес). По умолчанию IP адрес коммутатора:

192.168.2.1

2. Выберите тип подключения (Connection type) – SSH.



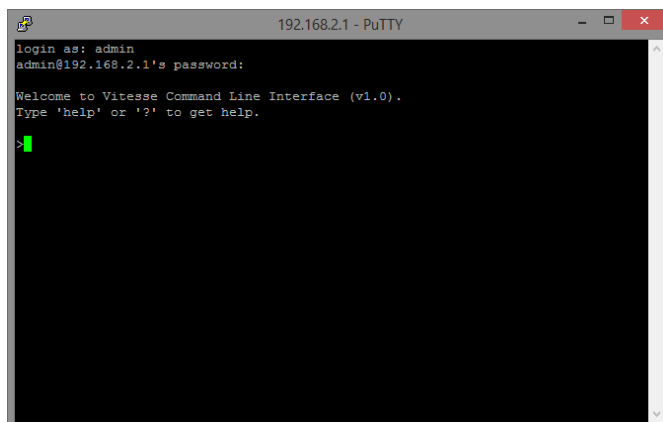
3. Если вы подключаетесь к коммутатору через SSH впервые, вы увидите окно PuTTY Security Alert. Нажмите Yes (Да) для продолжения.



4. PuTTY обеспечит вам доступ к управлению коммутатором после того как Telnet/SSH подключение будет установлено.

По умолчанию:

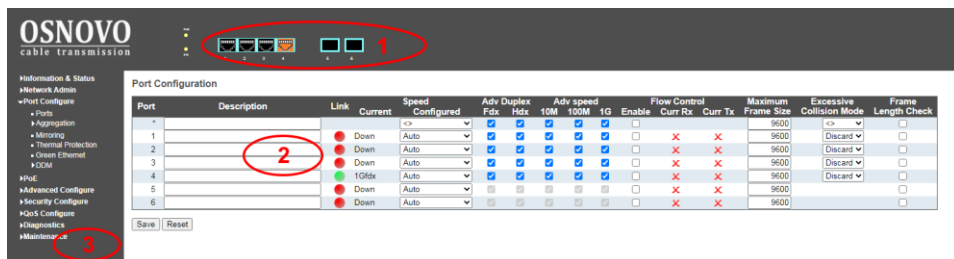
- Login: admin
- Password: system



10. Управление через WEB интерфейс.

10.1 Основные сведения

WEB интерфейс коммутатора представлен на рисунке ниже:



Визуально WEB интерфейс состоит из 3 частей:

Часть 1* (Part 1)	Индикаторы портов, включая PoE статус и статус соединения. Выбор языка. Документ справки.
Часть 2 (Part 2)	Основной интерфейс, где доступны настройки и отображается статистика по тем или иным параметрам.
Часть 3 (Part 3)	Главное меню WEB интерфейса. Содержит перечень доступных настроек, режимов, инструментов для мониторинга сети, а также инструментов для обслуживания коммутатора.

* WEB интерфейс отображает схему всех портов коммутатора. Различные цвета на схеме означают, что порт/порты находятся в том или ином состоянии.



Скорость порта 100Мбит/с



Скорость порта 1000 Мбит/с



Нет соединения

10.2 Главное меню WEB интерфейса

С помощью встроенного в коммутатор WEB интерфейса Вы можете гибко настраивать системные параметры, скорость портов, отслеживать состояние сети и многое другое.

Все инструменты и настройки собраны в группы и подгруппы. Основных групп 9:

Information&Status (Общая информация и статус) – пользователи могут проверить общую информацию о коммутаторе, статус, как долго коммутатор находится включенным и тд.

Network Admin (Настройка сетевых параметров и администрирование) – пользователи могут проверить и настроить параметры, относящиеся к сети в данном пункте главного меню WEB интерфейса коммутатора.

Port Configure (Конфигурирование портов коммутатора) – пользователи могут проверить и настроить определенные параметры портов в данном пункте главного меню WEB интерфейса коммутатора.

PoE – пользователи могут проверить и настроить определенные параметры PoE для портов в данном пункте главного меню WEB интерфейса коммутатора.

Advanced Configure (Расширенные настройки) – пользователи могут проверить и настроить L2 и L2+ функции коммутатора в данном пункте главного меню WEB интерфейса.

Security Configure (Настройки безопасности) – пользователи могут проверить и настроить параметры безопасности для коммутатора в данном пункте главного меню WEB интерфейса.

QoS (Управление очередями) – пользователи могут проверить и настроить параметры режима управления очередями QoS в данном пункте главного меню WEB интерфейса.

Diagnostics (Инструменты для диагностики) – пользователи могут воспользоваться инструментами для диагностики сети (Ping), диагностики

кабеля, а также проверить загрузку CPU коммутатора в данном пункте главного меню WEB интерфейса.

Maintenance (Обслуживание) – пользователи могут воспользоваться инструментами обслуживания коммутатора (сброс к заводским настройкам, обновление прошивки, загрузка и сохранение текущей конфигурации, перезагрузка коммутатора) в данном пункте главного меню WEB интерфейса.

10.3 Network Admin (Настройка сетевых параметров и администрирование)

10.3.1 IP Configuration (Настройка IP адреса)

Примечание: IP адрес коммутатора по умолчанию 192.168.2.1 Маска подсети по умолчанию 255.255.255.0(24)

Выберите подраздел главного меню WEB интерфейса коммутатора: *Network Admin > IP*

Information & Status

Network Admin

- IP
- SNTP
- SNMP
- SysLog

Port Configure

PoE

Advanced Configure

Security Configure

IP Configuration

IP Interfaces

Delete	VLAN	IPv4 DHCP			IPv4	
		Enable	Fallback	Current Lease	Address	Mask Length
☐	1	☐	0		192.168.2.1	24

Add Interface

SaveReset

Port Name	Отображает системное имя порта
VLAN	VLAN для доступа к управлению коммутатором
IPv4 DHCP	- Если включено, это означает, что порт VLAN запускает IPv4 DHCP клиент, чтобы динамически получать IPv4 адреса коммутатора. В противном случае он будет использовать статический IP адрес. - Откат (в секундах) означает время ожидания для коммутатора для получения динамического IP адреса с помощью DHCP. Значение 0 – отменяет время ожидания. - Текущая аренда, поле отображает текущий IP адрес, полученный от DHCP

IPv4	- Адрес: статический IP адрес, введенный пользователем. - Длина маски: статическая IPv4 маска для подсети, введенная пользователем.
------	--

Нажмите Add Interface, чтобы задать новые настройки для VLAN и IP адреса. Нажмите Save, чтобы сохранить настройки.

Примечание: Для управления коммутатором используется VLAN1 по умолчанию. Если пользователю необходима другая VLAN, для управления коммутатором, пожалуйста, добавьте VLAN в соответствующем меню WEB интерфейса, а также добавьте порт в эту VLAN.

10.3.2 SNTP Configuration (Настройка протокола времени SNTP)

SNTP это акроним от Simple Network Time Protocol – протокол синхронизации часов с настройками ПК. Вы можете выбрать определенный SNTP сервер и настроить GMT временную зону.

Выберите подраздел главного меню WEB интерфейса коммутатора:
Network Admin > SNTP

Mode	Нажмите на выпадающее меню, чтобы выбрать Enabled или Disabled Enabled (вкл) – включает режим SNTP. В данном режиме агент отправляет и принимает SNTP сообщения между клиентами и сервером, когда они находятся не в одной подсети. Disabled (выкл) – отключает режим SNTP.
SNTP Server	После ввода IP адреса SNTP сервера, SNTP информация будет получена с этого сервера.

Нажмите Save, чтобы сохранить настройки.

10.3.3 SNMP Configuration (Настройка протокола управления SNMP)

Simple Network Management Protocol (SNMP) это протокол прикладного уровня, который облегчает обмен информацией управления между сетевыми устройствами. SNMP позволяет сетевым администраторам управлять производительностью сети, находить и решать проблемы с сетью, планировать расширение сети.

Коммутатор поддерживает SNMPv1, v2c. Различные версии SNMP обеспечивают разный уровень безопасности для управления станциями и сетевыми устройствами.

В SNMP v1 и v2c для аутентификации пользователей используется «Community String». Функционал этой строки схож с функционалом пароля. Приложение SNMP удаленного пользователя и SNMP коммутатора должны использовать одно и тоже значение Community String. Пакеты SNMP от любых неавторизованных сайтов будут игнорироваться (отбрасываться).

Community String по умолчанию для коммутатора имеет значение:

1. public – позволяет аутентификацию станции управления для чтения MIB объектов.
2. private – позволяет аутентификацию станции управления для чтения, записи и изменения MIB объектов.

Trap

Используется агентом для асинхронного информирования NMS (станция управления) о каком-либо событии. Эти события могут быть очень серьезными, такими, как перезагрузка (кто-то случайно выключил коммутатор), или просто, общая информация, такая как изменение статуса порта. Коммутатор создает информацию о ловушке (Trap), а затем отправляет ее получателю или администратору сети. Типичная ловушка включает в себя информацию о ошибках аутентификации, сетевых изменениях.

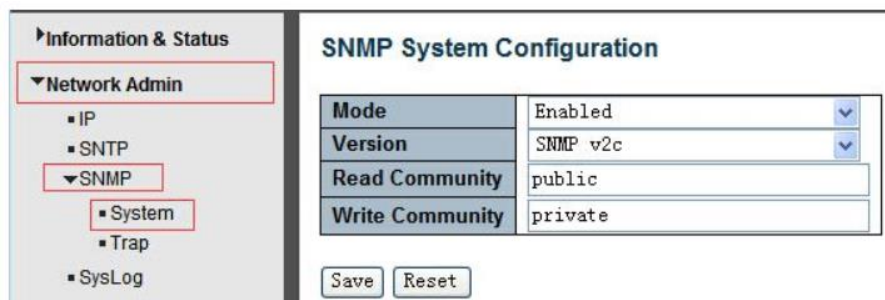
MIB

Это коллекция управляемых объектов, находящихся в виртуальном хранилище информации. Коллекции связанных управляемых объектов определены в определенных модулях MIB. Коммутатор использует стандартный модуль управления информацией MIB-II. Таким образом, значение объекта MIB может быть прочитано любым программным обеспечением, управляемым через SNMP протокол.

10.3.3.1 SNMP System Configuration (Настройка SNMP для системы)

Вы можете включить или выключить данную функцию в разделе

Admin>SNMP>System



Mode	Включение/выключение SNMP функции
Version	Нажмите на выпадающее меню, чтобы выбрать версию протокола SNMP v2c или v1
Read Community	Позволяет аутентификацию станции управления для чтения MIB объектов.
Write Community	Позволяет аутентификацию станции управления для чтения, записи и изменения MIB объектов

10.3.3.2 SNMP Trap Configuration (Настройка SNMP Trap)

Вы можете включить или выключить данную функцию и настроить ее в следующем разделе

Network Admin>SNMP>Trap

Information & Status

Network Admin

IP

SNTP

SNMP

System

Trap

SysLog

Port Configure

PoE

Advanced Configure

Security Configure

Trap Configuration

Global Settings

Mode Disabled

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
Add New Entry					
Save Reset					

10.3.4 System Log Configuration (Настройка системного журнала)

Вы можете настроить системный журнал коммутатора перейдя в нужный раздел основного меню WEB интерфейса

Network Admin > Syslog

Information & Status

Network Admin

IP

SNTP

SNMP

SysLog

Port Configure

System Log Configuration

Server Mode	Disabled
Server Address	192.168.2.100
Syslog Level	Info

Save Reset

Server Mode	Вкл/выкл функцию системного журнала для SNMP . Если включено, коммутатор отправляет копию журнала на сторонний сервер
Server Address	Сервер, на который отправляется копия системного журнала
Syslog Level	Info – информация, предупреждения и ошибки Warning – только предупреждения и ошибки Errors – только ошибки

10.4 Port Configure (Конфигурирование портов)

10.4.1 Port Configuration (Настройка портов)

Данный раздел WEB интерфейса содержит перечень настроек для портов коммутатора.

Port Configure>Ports

▼Port Configure • Ports ►Aggregation • Mirroring • Thermal Protection • Green Ethernet	Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
			Current	Configured	Current Rx	Current Tx	Configured		
	*		◇				☐	9600	◇
	1	● Down	Auto		×	×	☐	9600	Discard
	2	● 100fdx	Auto		×	×	☐	9600	Discard
3	● Down	Auto		×	×	☐	9600	Discard	

Link	Красный цвет означает, что соединения нет. Зеленый – соединение есть.
Speed	Выбор скорости и режима работы (дуплекс/полудуплекс) для порта Disabled – порт отключен. Auto – позволяет порту автоматически выбирать наиболее подходящие параметры для подключенного устройства. FDX – дуплекс. По умолчанию для скорости 1000Мбит/с HDX – полудуплекс 1000-X_AMS – означает, что порт является оптическим или комбо-портом и оптический порт – основной. Также есть другие аналогичные параметры: 10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000-X
Flow Control	Механизм управления потоком. Полнодуплексные порты используют 802.3x протокол для управления потоком, полудуплексные порты используют backpressure управление потоком. По умолчанию данный механизм для портов – отключен.
Maximum Frame Size	Поле, где задается максимальный размер передаваемых/принимаемых пакетов. По умолчанию размер – 9600, чтобы обеспечить поддержку Jumbo frames.

Нажмите Save, чтобы сохранить настройки.

10.4.2 Link aggregation (Агрегация каналов)

Агрегация каналов, это метод, который связывает определенные физические порты вместе, как один логический порт, чтобы увеличить общую пропускную способность.

Коммутатор поддерживает до 13 групп агрегации каналов. От 2 до 8 портов в виде единого логического порта.

Примечание: Если какой-либо порт в группе агрегации каналов отключен, пакет данных, отправленный на отключенный порт будет распределять нагрузку на другой подключенный порт в этой группе агрегации.

10.4.2.1 Static Aggregation (Статическая Агрегация)

В этом разделе WEB интерфейса коммутатора пользователь может настроить статическую агрегацию для портов.

Port Configure > Aggregation > Static

Information & Status

Network Admin

Port Configure

Ports

Aggregation

Static

LACP

Mirroring

Thermal Protection

Green Ethernet

PoE

Advanced Configure

Security Configure

QoS Configure

Diagnostics

Maintenance

Aggregation Mode Configuration

Hash Code Contributors

Source MAC Address

Destination MAC Address

IP Address

TCP/UDP Port Number

Aggregation Group Configuration

Group ID	Port Members																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Normal	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
13	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

Aggregation Mode Configuration	Этот режим является алгоритмом хеширования потока между портами LAG (группа агрегированных портов или Link Aggregation Group)
Group ID	ID группы статической агрегации
Port Members	Коммутатор поддерживает до 13 групп агрегации, от 2 до 8 портов в одной группе.

Нажмите Save, чтобы сохранить настройки.

Примечание: Статическая агрегация позволяет одновременно объединять не более 8 портов в одну статическую группу.

10.4.2.2 LACP Aggregation (Агрегация на основе LACP)

LACP – Протокол управления агрегацией каналов. Агрегация каналов позволяет объединять до восьми портов в одно выделенное соединение (логический порт).

Эта функция может расширить пропускную способность устройства. Работа LACP требует включения дуплексного режима на портах.

Для получения более подробной информации ознакомьтесь со стандартом IEEE 802.3ad.

Port Configure > Aggregation > LACP

Information & Status

Network Admin

Port Configure

Ports

Aggregation

Static

LACP

Mirroring

Thermal Protection

Green Ethernet

LACP Port Configuration

Port	LACP Enabled	Key	Role	Timeout	Prio
*	☐	<>	<>	<>	32768
1	☐	Auto	Active	Fast	32768
2	☐	Auto	Active	Fast	32768
3	☐	Auto	Active	Fast	32768
4	☐	Auto	Active	Fast	32768
5	☐	Auto	Active	Fast	32768

LACP	Включение/выключение поддержки протокола LACP на порте
Key	Значение ключа, полученное портом, находится в диапазоне 1-65535. Auto настройка задаст ключ в зависимости от скорости физического канала, 10Mb = 1, 100Mb = 2, 1Gb = 3. Specific настройка позволяет вводить значение ключа вручную. Порты с одинаковым значением ключа могут быть участниками одной группы агрегации, а порты с разными ключами – не могут.
Role	Данное поле отвечает за состояние активности LACP. Active – передача пакетов LACP каждую секунду Passive – ожидание пакетов LACP.
Timeout	Данное поле отвечает за промежуток времени между передачей BPDU Fast – отправка пакетов LACP каждую секунду Slow – 30 сек ожидания перед отправкой пакета LACP
Prio	Данное поле контролирует приоритет порта. Если партнер LACP хочет сформировать большую группу, чем устройство поддерживает, то параметр Prio будет контролировать, какие порты будут в активной роли, а какие в резервной роли. Меньшее значение параметра Prio означает больший приоритет.

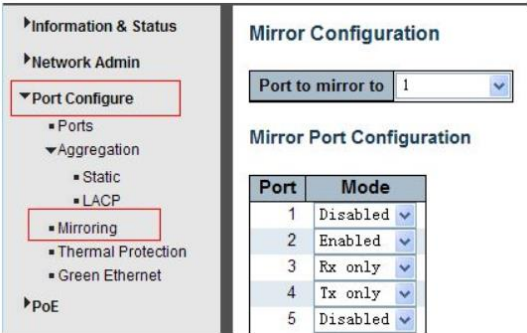
Нажмите Save, чтобы сохранить настройки.

10.4.3 Port Mirroring (Зеркалирование портов)

Функция зеркалирования портов обеспечивает мониторинг сетевого трафика, копия которого (входящие или исходящие пакеты) пересылается с одного порта сетевого коммутатора на другой порт, где трафик может быть исследован.

Это позволяет администратору сети отслеживать производительность коммутатора и при необходимости изменять его настройки.

Port Configure > Mirroring



Port mirror to	Пакеты с портов, для которых включено зеркалирование rx или tx будут доступны на этом порте. Disabled – отключает зеркалирование
Mode	Выбор режима зеркалирования для порта источника. Rx only – пакеты, полученные на этом порте будут отправлены за порт-зеркало (mirror port). Исходящие пакеты зеркалироваться не будут. Tx only – пакеты, исходящие с этого порта будут отправлены за порт-зеркало (mirror port). Получаемые пакеты зеркалироваться не будут. Disabled – все пакеты (tx и rx) не будут зеркалироваться Enabled – все пакеты (tx и rx) будут отправлены на порт-зеркало.

Нажмите Save, чтобы сохранить настройки.

10.4.4. Thermal Protection Configuration (Температурная защита)

Температурная защита предотвращает перегрев портов. Когда коммутатор определяет порт, на котором температура выше заданной, происходит отключение порта.

Port Configuration > Thermal Protection

Information & Status

Network Admin

Port Configure

Ports

Aggregation

Mirroring

Thermal Protection

Green Ethernet

PoE

Advanced Configure

Security Configure

QoS Configure

Diagnostics

Maintenance

Thermal Protection Configuration

Temperature settings for priority groups

Priority	Temperature
0	255 °C
1	255 °C
2	255 °C
3	255 °C

Port priorities

Port	Priority
*	<> ▾
1	0 ▾
2	0 ▾
3	0 ▾

Temperature settings for priority groups	Коммутатор поддерживает 4 группы температурной защиты. Каждая может быть настроена на свою максимальную температуру.
Port priorities	Поле определяет принадлежность порта к той или иной группе температурной защиты.

Нажмите Save, чтобы сохранить настройки.

Примечание: по умолчанию все порты коммутатора находят в группе приоритета 0, с максимальной температурой 255 C

10.5 PoE Configuration (Конфигурация PoE)

Power Over Ethernet (PoE) – функция, позволяющая устройствам получать питание и данные по одному кабелю в сети Ethernet.

Таковыми устройствами могут быть PoE IP камеры, точки доступа, телефоны VoIP. Наличие данной функции позволяет снизить затраты на создание сетевой инфраструктуры.

PoE – определяется стандартом IEEE 802.3af/at. Поэтому обычно не возникает сложностей с питанием удаленного устройства, если оно поддерживает/совместимо с данными стандартами.

PD – запрашиваемое устройство, например PoE IP камера.

PSE – устройство обеспечивающее питание удаленного PD

Процесс подачи питания PoE состоит из нескольких шагов:

- 1) Определение. PSE устройство отправляет сигнал с минимальным напряжением, чтобы определить совместимо ли удаленное PD устройство со стандартами IEEE 802.3af/at. Если удаленное устройство совместимо происходит следующий шаг.
- 2) Классификация PD устройства. PSE устройство определяет необходимую мощность для удаленного PD устройства.
- 3) После первых двух шагов PSE устройство начинает подавать в линию полное напряжение и мощность (44-57V, мощность af – 15.4Вт макс, at – 25.5Вт макс.)
- 4) Отключение. Если удаленное PD устройство отключилось, или пользователь отключил его с помощью управления через WEB, PSE устройство в течение 300-400 мс прекращает подачу напряжения PoE в линию.

10.5.1 PoE Setting (Настройки PoE)

Настройки PoE находятся в следующем разделе WEB интерфейса коммутатора.

PoE > PoE Setting

Power Over Ethernet Configuration

Reserved Power determined by

☒ Auto☐ Manual

Power Management Mode

☒ Actual Consumption☐ Reserved Power

Capacitor Detection

☒ Disabled☐ Enabled

PoE Power Supply Configuration

Primary Power Supply [W]

250

PoE Port Configuration

Port	PoE Mode	Priority	PD Alive Check	Maximum Power [W]	Description
*	C>	C>	C>	15.4	
1	PoE+	Low	ON	15.4	
2	PoE+	Low	ON	15.4	
3	PoE+	Low	ON	15.4	
4	PoE+	Low	ON	15.4	
5	PoE+	Low	ON	15.4	
6	PoE+	Low	ON	15.4	
7	PoE+	Low	ON	15.4	
8	PoE+	Low	ON	15.4	

Save

Reset

Reserved
Power
determined by

Коммутатор поддерживает 2 режима для определения мощности на порте

Auto – коммутатор автоматически определяет мощность на порте в зависимости от класса подключенного PoE устройства.

Manual – вручную – максимальная доступная на порте мощность задается пользователем.

Power
Management
Mode

Коммутатор поддерживает 2 режима управления питанием.

1. Реальное потребление. В этом режиме общая мощность (PoE бюджет) делится на все порты. Порт с наименьшим приоритетом будет выключен, если мощность превысит бюджет PoE. Если все порты имеют одинаковое значение приоритета – будет отключен порт с крайним номером.

2. Зарезервированная мощность. В этом режиме, если мощность превысит PoE бюджет коммутатора, порт к которому будет подключено новое PoE устройство не будет активен.

Primary Power Supply	Пользователи могут настраивать PoE бюджет всего коммутатора (не более значения по умолчанию). Значение по умолчанию 370 W
PoE Mode	Режим PoE на портах. По умолчанию – 802.3at (PoE+)
Priority	Значение определяющее приоритет порта. Может принимать 3 значения Low – низкий приоритет High – высокий приоритет Critical – критически важный приоритет
Maximum Power (W)	В ручном режиме выставляется значение максимальной доступной мощности на порте.

Нажмите Save, чтобы сохранить настройки.

10.5.2 PD Alive (Функция антизависания для PoE устройств)

Настройки данной функции находятся в следующем разделе WEB интерфейса коммутатора:

PoE > PoE Setting

Power Over Ethernet Configuration

Reserved Power determined by

☒ Auto
☐ Manual

Power Management Mode

☒ Actual Consumption
☐ Reserved Power

Capacitor Detection

☒ Disabled
☐ Enabled

PoE Power Supply Configuration

Primary Power Supply [W]

250

PoE Port Configuration

Port	PoE Mode	Priority	PD Alive Check	Maximum Power [W]	Description
*	<>	<>	<>	15.4	
1	PoE+	Low	ON	15.4	
2	PoE+	Low	ON	15.4	
3	PoE+	Low	ON	15.4	
4	PoE+	Low	ON	15.4	

Save

Reset

Функция работает полностью в автоматическом режиме после ее активации на порте/портах. Срабатывание происходит через 120 сек после того, как коммутатором было зафиксировано состояние «зависания» на порте/портах. Сработка происходит 1 раз.

10.5.3 PoE Status (Состояние PoE на портах)

Позволяет отслеживать состояние PoE на всех портах. Находится в разделе

PoE > PoE Status

Information & Status

Network Admin

Port Configure

PoE

PoE Setting

PoE Status

Advanced Configure

Security Configure

QoS Configure

Diagnostics

Maintenance

Power Over Ethernet Status

Auto-refresh ☐ Refresh

Local Port	Description	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
2	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
3	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
4	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
5	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
6	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
7	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
8	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
9	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
10	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
11	-	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled

10.6 Advanced Configure (Расширенные настройки)

10.6.1 VLAN (Настройка VLAN)

VLAN – виртуальная локальная сеть – представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения.

VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе, даже если они не находятся в одной физической сети.

Настройки находятся в разделе

Advanced Configure > VLANs

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

MAC Table

VLANs

Port Isolation

Loop Protection

Spanning Tree

MEP

ERPS

IGMP Snooping

LLDP

Global VLAN Configuration

Allowed Access VLANs

1

Ethertype for Custom S-ports

88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	↕	1	↕	☒	↕	↕	1	
1	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	

Allowed VLANs	В этом поле отображаются созданные VLAN ID. По умолчанию значение – 1. Если вы хотите создать новую VLAN, измените значение на новое.
Ethertype for Custom S-ports	В этом поле указывается значение ethertype / TPID (в шестнадцатеричном формате). Параметр действует для всех портов, тип которых (Port Type) установлен как S-Custom-Port
Mode	Режим порта (по умолчанию Access) определяет основное поведение порта. Порт может находиться в одном из трех режимов, как описано ниже. Всякий раз, когда выбран определенный режим, остальные поля в этой строке будут либо недоступны или сделаны изменяемыми в зависимости от рассматриваемого режима. Затененные поля показывают значение, которое порт получит при применении режима. <u>Access</u>. Порты с этим режимом обычно используют для подключения к конечным станциям. Имеют следующие характеристики: - Порт участник Access VLAN (по умолчанию 1) - Порт принимает пакеты типа untagged и C-tagged - Отбрасывает все пакеты, которые не классифицированы для доступа к Access VLAN - На выходе все пакеты, относящиеся к Access VLAN будут передаваться, как untagged. Другие (динамически добавленные VLANы) будут передаваться, как tagged. <u>Trunk</u>. Trunk (магистральные) порты могут

	одновременно передавать трафик по нескольким сетям VLAN и обычно используются для подключения к другим коммутаторам. Имеют следующие характеристики: - По умолчанию, trunk порт является участником всех VLAN (1-4094) - VLANы, участником которых является trunk порт, могут быть ограничены через поле Allowed VLANs - Пакеты, относящиеся к VLAN, участником которой порт не является – отбрасываются. - По умолчанию все пакеты, кроме пакетов относящихся к Port VLAN (Native VLAN) будут помечены (tagged) на выходе. - Маркирование пакетов на выходе (тегирование) может быть изменено, чтобы пометить все пакеты. В таком случае, только tagged пакеты будут приниматься на входе. <u>Hybrid</u>. Такие порты во многом напоминают trunk порты, но имеют дополнительные настройки. – Порт может быть настроен так, чтобы VLAN tag не распознавался, C-tag и S-tag поддерживались. - Фильтрация на входе могла контролироваться. - Прием пакетов на входе и настройка исходящего тегирования могут настраиваться независимо.
Port VLAN	Поле определяет идентификатор VLAN порта (PVID). Разрешенные VLAN находятся в диапазоне от 1 до 4094, по умолчанию 1

Port Type	Порты в гибридном режиме позволяют изменять тип порта. <u>Unaware</u>. На входе все пакеты, независимо от того помечены ли они VLAN tag или нет, будут отнесены к VLAN Port, возможные метки (теги) будут удалены на выходе. <u>C-port</u>. На входе пакеты с тегом VLAN с TPID = 0x8100 будут классифицированы по VLAN ID, содержащемуся в метке. Если пакет помечен, как приоритетный, он будет классифицирован Port VLAN. Если пакеты должны быть помечены на выходе, они будут помечаться C-tag меткой. <u>S-port</u>. На входе пакеты с тегом VLAN с TPID = 0x8100 или 0x88A8 будут классифицированы по VLAN ID, содержащемуся в метке. Если пакет помечен, как приоритетный, он будет классифицирован Port VLAN. Если пакеты должны быть помечены на выходе, они будут помечаться S-tag меткой. <u>S-Custom-Port</u>. На входе пакеты с тегом VLAN с TPID = 0x8100 или Ethertype, настроенный для Custom-S портов будут классифицированы по VLAN ID, содержащемуся в метке. Если пакет не помечен или пакет помечен, как приоритетный, он будет классифицирован Port VLAN. Если пакеты должны быть помечены на выходе, они будут помечаться заданной S-tag меткой.
Ingress Filter	Гибридные порты позволяют менять входную фильтрацию. Access и Trunk порты всегда имеют включенную входную фильтрацию. Если входная фильтрация включена (флажок установлен), пакеты относящиеся к VLAN, в которой порт не является участником – будут отброшены. Если входная фильтрация выключена, пакеты относящиеся к VLAN, в которой порт не является участником – будут приняты и обработаны коммутатором.
Ingress Acceptance	Гибридные порты позволяют менять тип пакетов, принимаемых на входе. <u>Tagged and Untagged</u>. Все типы пакетов с меткой или

	без будут приниматься. <u>Tagged only.</u> Только помеченные пакеты будут приниматься на входе. Пакеты без метки будут отброшены. <u>Untagged only.</u> Только пакеты без метки будут приниматься на входе. Пакеты с меткой будут отброшены.
Egress Tagging	Порты в Trunk и Hybrid режимах могут контролировать присваивание метки на выходе <u>Untag Port VLAN.</u> Пакеты относящиеся к Port VLAN будут передаваться без метки. Остальные пакеты получают соответствующую метку. <u>Tag All.</u> Все пакеты, относящиеся к Port VLAN или нет будут передаваться с меткой. <u>Untag All.</u> Все пакеты, относящиеся к Port VLAN или нет будут передаваться без метки. Только для Hybrid режима.
Allowed VLANs	Порты в режимах Trunk и Hybrid могут контролировать в какой VLAN они могут быть участниками. Access порты могут быть участниками только одной VLAN (Access VLAN). По умолчанию Trunk и Hybrid порты могут быть участниками всех VLAN 1-4094. Поле может быть пустым, что означает принадлежность порта ко всем VLAN.
Forbidden VLANs	Порт может быть настроен таким образом, чтобы не быть участником ни одной из VLAN. По умолчанию поле пустое, что означает принадлежность порта ко всем VLAN.

Нажмите Save, чтобы сохранить настройки.

10.6.2 Port Isolation (Изоляция портов)

Изоляция портов ограничивает обмен трафиком между портами. Функция похоже на VLAN, но имеет более строгие правила.

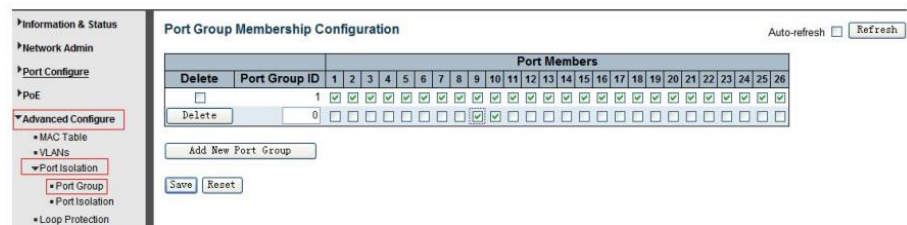
10.6.2.1 Port Group (Группа портов)

Коммутатор поддерживает формирование групп портов. Порты участники группы могут обмениваться данными.

Примечание: Порт может принадлежать к нескольким группам. Данные могут быть переданы между любыми портами, которые принадлежат одной группе портов

Настройки групп находятся в следующем разделе:

Advanced Configure > Port Isolation > Port Group



Port members	Отметьте порты, которые будут принадлежать одной группе.
--------------	--

Нажмите Add new Port Group, чтобы создать новую группу. Delete – чтобы удалить группу. Save – чтобы сохранить текущие настройки.

10.6.2.2 Port Isolation (Изоляция портов)

Настройка изоляции портов находится в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > Port isolation > Port Isolation

Port Number																									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
☐	☐	☐	☐	☐	☐	☐	☐	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

Auto-refresh ☐ Refresh

Port number	Отметьте порты, которые будут изолированы.
-------------	--

Нажмите Save, чтобы сохранить настройки.

10.6.3 STP (Протокол связующего дерева)

Spaning Tree Protocol (STP) – или протокол связующего дерева используется для обнаружения и исправления сетевых петель. Он обеспечивает запасные соединения между коммутаторами, мостами и маршрутизаторами.

STP позволяет коммутатору взаимодействовать с другими bridge устройствами сети, гарантируя существование только одного маршрута между любыми двумя станциями в сети, и обеспечивая наличие резервных соединений, которые автоматически используются, когда основное соединение по каким-либо причинам перестает существовать.

10.6.3.1 STP Bridge Settings (Настройка протокола STP)

Настройки протокола STP находятся в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > Spanning Tree > Bridge Settings

STP Bridge Configuration

Basic Settings

Protocol Version	RSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Save Reset

Protocol Version	Нажмите на выпадающее меню чтобы выбрать версию протокола STP: STP – Spanning Tree Protocol (IEEE 802.1D) RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
Bridge Priority	Контроль приоритета моста (bridge). Меньшее значение имеет больший приоритет. Приоритет моста + MSTI связан с 6-байтовым MAC адресом коммутатора формирует идентификатор моста (bridge).
Forward Delay (4-30)	Задержка перед отправкой. Значение может быть в диапазоне от 4 до 30 сек. По умолчанию – 15 сек.
Max age (6-40)	Максимальное время жизни информации отправленной мостом, пока он имеет роль корневого моста (root bridge). Допустимые значения находятся в диапазоне от 6 до 40 сек. Значение по умолчанию – 20 сек.
Maximum Hop Count (6-40)	Эта настройка определяет количество необходимых переходов (hop'ов) для MSTI информации, сформированной на границе MSTI. Также это значение определяет как много мостов в роли корневого моста могут передавать BPDU информацию. Допустимые значения находятся в диапазоне от 6 до 40 переходов.
Transmit Hold Count (1-10)	Количество BPDU пакетов, которые корневой порт (bridge port) может отправлять за 1 секунду. Если необходимо, может быть организована задержка перед отправкой следующего BPDU пакета. Доступные значения от 1 до 10 BPDU пакетов в секунду. Значение по умолчанию – 6.

Нажмите Save, чтобы сохранить настройки.

10.6.3.2 STP Bridge Port (Выбор bridge порта)

Настройки STP bridge для портов находятся в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > Spanning Tree > Bridge Ports

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Forced True

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
1	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
2	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
3	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
4	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto

STP enabled	Отметьте, чтобы включить STP на порте.
Path Cost	Поле определяет стоимость пути (path cost) для порта. Auto – стоимость пути высчитывается на основе физической скорости порта, используя значения, рекомендуемые 802.1D. Specific – стоимость пути, задаваемая пользователем. Стоимость пути используется для построения актуальной топологии сети. Порты с меньшим значением используются как forwarding порты. Доступные значения в диапазоне от 1 до 200000000
Priority	Поле определяет приоритет порта.
Auto Edge	Отметьте, чтобы превратить порт в Auto Edge
Restricted Role	Отметьте, чтобы превратить порт в Restricted Role
Restricted TCN	Отметьте, чтобы превратить порт в Restricted TCN

BPDU Guide	Отметьте, чтобы активировать BPDU Guide. Когда порт получает BPDU пакет, он переходит в состояние «Disable», т.е. отключается.
Point-to-point	Поле отвечает за организацию соединения точка-точка. Агрегированные порты всегда находятся в состоянии Point-to-point

Нажмите Save, чтобы сохранить настройки.

10.6.4 MAC Address Table (Таблица MAC адресов)

Настройки таблицы MAC адресов находятся в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > MAC Table

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

MAC Table

VLANs

Port Isolation

Loop Protection

Spanning Tree

MEP

ERPS

IGMP Snooping

LLDP

Security Configure

QoS Configure

Diagnostics

Maintenance

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging

Aging Time

300

seconds

MAC Table Learning

	Port Members																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Auto	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Disable	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Secure	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Static MAC Table Configuration

	Port Members																											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Delete	1	00-00-00-00-00-00	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Add New Static Entry

Save

Reset

Disable Automatic Aging	Если этот чекбокс отмечен, функция автоматического устаревания отключена.
Aging Time	Время, после которого запись помещенная в таблицу будет исключена из нее. Диапазон 10-1000000 сек. Значение по умолчанию – 300 сек.

MAC Table Learning	Коммутатор поддерживает 3 типа запоминания (learning) MAC адресов в таблицу Auto – порт автоматически запоминает MAC адреса. Disable – порт не запоминает MAC адреса Secure – порт пересылает данные только, если используется статический MAC адрес.
Static MAC Table Configuration	Статические записи MAC адресов отображаются в этой таблице. Нажмите «Add New Static Entry» (добавить новую статическую запись), чтобы создать новую запись.

Нажмите Save, чтобы сохранить настройки.

10.6.5 IGMP Snooping

Internet Group Management Protocol (IGMP) – позволяет хостами маршрутизаторам обмениваться информацией о multicast группам. IGMP Snooping это функция коммутатора, которая отвечает за контроль IGMP сообщениями. Главная цель IGMP Snooping – ограничить пересылку multicast пакетов только для портов, которые являются членами multicast групп.

10.6.5.1 Basic Information

Общая информация о IGMP настройках находится в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > IGMP Snooping > Basic Configuration

- Information & Status
- Network Admin
- Port Configure
- PoE
- Advanced Configure
 - MAC Table
 - VLANs
 - Port Isolation
 - Loop Protection
 - Spanning Tree
 - MEP
 - ERPS
 - IGMP Snooping
 - Basic Configuration
 - VLAN Configuration
 - LLDP

IGMP Snooping Configuration

Global Configuration

Snooping Enabled ☐

Unregistered IPMCv4 Flooding Enabled ☒

Port Related Configuration

Port	Router Port	Fast Leave
*	☐	☐
1	☐	☐
2	☐	☐
3	☐	☐
4	☐	☐
5	☐	☐
6	☐	☐
7	☐	☐
8	☐	☐
9	☐	☐

Snooping Enabled	Вкл/выкл функции IGMP Snooping. Значение по умолчанию – отключено (disabled)
Unregistred IPMCv4 Flooding Enabled	Отметьте чекбокс, чтобы включить функцию Unregistred IPMCv4 Flooding.
Router Port	Поле определяет, какие порты будут отмечены, как router порты. Router порт в коммутаторе ведет к multicast устройству или устройству, запрашивающему IGMP. Если в качестве router порта выбран порт агрегированной группы, то вся группа портов будет выполнять роль router портов.
Fast Leave	Данная настройка отвечает за удаление MAC адреса немедленно после получения сообщения для группы.

Нажмите Save, чтобы сохранить настройки.

10.6.5.2 IGMP Snooping VLAN Configuration (Настройка IGMP Snooping для VLAN)

Настройка IGMP Snooping для VLAN находится в следующем разделе WEB интерфейсе коммутатора:

Advanced Configure > IGMP Snooping > VLAN Configuration

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

MAC Table

VLANs

Port Isolation

Loop Protection

Spanning Tree

MEP

ERPS

IGMP Snooping

Basic Configuration

VLAN Configuration

LLDP

IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address
Delete	1	☐	☒	0.0.0.0

Add New IGMP VLAN

SaveReset

Snooping Enabled	Включение IGMP для VLAN. 32 VLAN могут быть отмечены для IGMP Snooping
Querier Election	Включить вступление IGMP Querier в VLAN.
Querier Address	Поле определяет IPv4 адрес источника, использующего IP заголовок для IGMP. По умолчанию это поле равно 192.0.2.1

Нажмите Save, чтобы сохранить настройки.

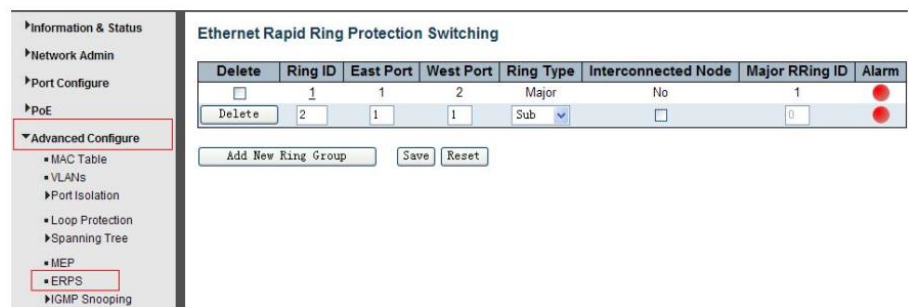
10.6.6 ERPS (Протокол ERPS)

ERPS – специальный протокол для защиты коммутатора от сетевых петель при использовании в кольцевой топологии. Время восстановления топологии при использовании этого протокола < 50ms.

Примечание: Перед использованием ERPS необходимо отключить STP на портах, так как они являются взаимоисключающими.

Раздел с настройками ERPS находится по адресу:

Advanced Configure > ERPS



Ring ID	Идентификатор ERPS Ring
East Port	Номер порта, который участвует в Ring Protection
West Port	Номер другого порта, который участвует в Ring Protection
Ring Type	Доступен выбор Major Ring – основное кольцо Sub Ring – вспомогательное кольцо По умолчанию тип кольца – Major Ring.

Interconnected Node	В топологии «мультикольцо», Interconnected Node – это узел соединяющий 2 или более колец.
Major Ring ID	В топологии «одно кольцо», Major Ring ID имеет тоже самое значение, что и Ring ID. В топологии «мультикольцо», субкольцо имеет тот же тип, что и Major Ring ID
R-APS VLAN (1-4094)	Поле определяет VLAN для R-APS VLAN'ов.

Нажмите Save, чтобы сохранить настройки.

После нажатия на номер под полем «Ring ID» открывается страница WEB интерфейса, как на рисунке ниже:

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

MAC Table

VLANs

Port Isolation

Loop Protection

Spanning Tree

MEP

ERPS

IGMP Snooping

LLDP

Security Configure

QoS Configure

Diagnostics

Maintenance

Rapid Ring Configuration 1

Auto-refresh ☐ Refresh

Instance Data

Ring ID	East Port	West Port	East Port SF MEP	West Port SF MEP	East Port APS MEP	West Port APS MEP	Ring Type
1	1	2	1	2	1	2	Major Ring

Instance Configuration

Configured	WTR(Wait to Restore) Time	Revertive	VLAN config
☒	1min	☒	VLAN Config

RPL Configuration

RPL Role	RPL Port	Clear
None	None	☐

Instance State

Protection State	East Port	West Port	Transmit APS	East Port Receive APS	West Port Receive APS	WTR Remaining	RPL Un-blocked	No APS Received	East Port Block Status	West Port Block Status	FOP Alarm
Protected	SF	OK	SF	BPR0		0	☒	☒	Blocked	Unblocked	☒

Save Reset

WTR (Wait to restore) Time (1-12)	Нажмите на выпадающее меню, чтобы выбрать время до восстановления R-APS. Доступный диапазон значений 1-12 мин. По умолчанию – 1 мин.
Revertive	Отметьте чекбокс, чтобы задать статус Revertive для R-APS
VLAN Config	После нажатия на VLAN Config, это приведет на страницу Rapid Ring VLAN Configuration

RPL Role	Нажмите на выпадающее меню, чтобы выбрать роль: None – без роли RPL Owner – владелец RPL RPL Neighbor – «сосед» RPL
RPL Port	Нажмите на выпадающее меню, чтобы выбрать тип порта None – не выбрано East port West port

Нажмите Save, чтобы сохранить настройки.

После нажатия на VLAN Config открывается страница WEB интерфейса настройки Rapid Ring VLAN, как на рисунке ниже:

Delete	VLAN ID
☐	1

Нажмите Add New Entry, чтобы добавить новую запись.

Нажмите Save, чтобы сохранить настройки.

10.6.7 LLDP (Настройка протокола LLDP)

Link Layer Discovery Protocol (LLDP) – протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения. Описание протокола приводится в стандарте IEEE 802.1AB.

Настройки данного протокола находятся в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > LLDP

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

MAC Table

VLANs

Port Isolation

Loop Protection

Spanning Tree

MEP

ERPS

IGMP Snooping

LLDP

Security Configure

QoS Configure

Diagnostics

Maintenance

LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Port Configuration

Port	Mode	Optional TLVs				
		Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☒	☒	☒	☒	☒
1	Disabled	☒	☒	☒	☒	☒
2	Disabled	☒	☒	☒	☒	☒
3	Disabled	☒	☒	☒	☒	☒
4	Disabled	☒	☒	☒	☒	☒
5	Disabled	☒	☒	☒	☒	☒
6	Disabled	☒	☒	☒	☒	☒

LLDP Parameters

В данном поле есть возможность настроить текущие LLDP настройки для порта:

TX interval

Tx Hold

Tx Delay

Tx Remit

Mode	Выбор LLDP сообщений для режима отправки и приема. Tx Only Rx Only Enabled Disabled
Optional TLVs	Поле отвечающее за настройку информации, которая включена в TLV поле публикуемых сообщений. Port Descr Sys Name Sys Descr Sys Capa Mgmt Addr

Нажмите Save, чтобы сохранить настройки.

10.6.8 Loop Protection (Защита от сетевых петель)

Данный раздел WEB интерфейса коммутатора предоставляет доступ к настройкам защиты от сетевых петель во время broadcast или multicast шторма.

Advanced Configure > Loop Protection

- Information & Status
- Network Admin
- Port Configure
- PoE
- Advanced Configure
 - MAC Table
 - VLANs
 - Port Isolation
 - Loop Protection
 - Spanning Tree
 - MEP
 - ERPS
 - IGMP Snooping
 - LLDP

Loop Protection Configuration

General Settings

Global Configuration

Enable Loop Protection	Disable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☐	<>	<>
1	☐	Shutdown Port	Enable
2	☐	Shutdown Port and Log	Disable
3	☐	Log Only	Enable

Global Configuration	Вкл/выкл защиты от сетевых петель. Transmission time – значение в сек, отвечающее за показатель Loop Protection Interval Time Shutdown Time – значение в сек для настройки порта Shutdown Time
Enable	Отметьте чекбокс, чтобы активировать Loop Protection на порте.
Action	Действие, применяющееся к порту, на котором замечена сетевая петля. Shutdown port – отключение порта Shutdown port and log – отключение порта и запись в журнал Log only – только запись в журнал.
Tx Mode	Вкл/выкл Режимы передачи Tx

Нажмите Save, чтобы сохранить настройки.

10.7 QoS (Приоритезация трафика)

Quality of Service (QoS) – технология предоставления различным классам трафика различных приоритетов в обслуживании.

QoS позволяет задавать различные уровни сетевого обслуживания для разных типов трафика, таких как мультимедийный, видео, и прочие типы. С помощью QoS можно понижать приоритет обработки трафика, который не является важным.

10.7.1 QoS Port Classification (Классификация портов с помощью QoS)

Настроить разные классы для портов можно в следующем разделе WEB интерфейса коммутатора:

QoS Configure > Port Classification

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

Security Configure

QoS Configure

Port Classification

Port Policing

Port Scheduler

Port Shaping

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Address Mode
*	<>	<>	<>	<>	<>
1	0	0	0	1	Source
2	1	1	1	0	Destination
3	2	0	2	0	Source
4	3	0	3	0	Destination
5	4	0	4	0	Source
6	5	0	5	0	Source
7	6	0	6	0	Source
8	7	0	7	0	Source

CoS	Поле отвечает класс обслуживания. Диапазон от 0 до 7, где 0 (самый низкий приоритет), а 7 (самый высокий приоритет). <i>Примечание: По умолчанию значение CoS изменяется динамически.</i>
DPL	Поле отвечает за Drop Precedence Level
PCP	Поле отвечает за значение PCP. Все пакеты классифицируются на основе PCP.
DEI	Поле отвечает за значение DEI по умолчанию. Все пакеты классифицируются на основе DEI.
Address Mode	IP/MAC режим

Нажмите Save, чтобы сохранить настройки.

10.7.2 Port Policing (Функция ограничения скорости на портах)

Данная функция находится в следующем разделе WEB интерфейса коммутатора:

QoS Configure > Port Policing

Port	Enabled	Rate	Unit	Flow Control
*	☐	500	<>	☐
1	☒	500	kbps	☒
2	☐	500	Mbps	☐
3	☒	500	fps	☒
4	☐	500	kfps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐

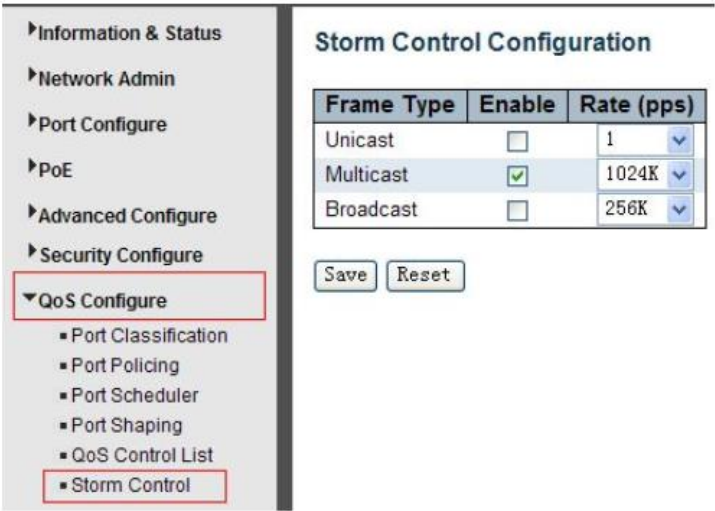
Enabled	Отметьте чекбокс, чтобы активировать функцию Port Policing для порта
Rate	Значение по умолчанию 500. Диапазон возможных значений 100-1000000, если в поле Unit выбрано kbps (Кбит/с) или fps (пакетов в сек) и 1-3300, если в поле Unit выбрано mbps (Мбит/с) или kfps (тысяч пакетов/сек)
Unit	Значение по умолчанию – kbps (Кбит/с)
Flow Control	Если управление потоком включено и порт находится в таком режиме, то отправляются пакеты «паузы», вместо отбрасывания пакетов.

Нажмите Save, чтобы сохранить настройки.

10.7.3 Storm Control Configuration (Настройка защиты от сетевого шторма)

Данная функция находится в следующем разделе WEB интерфейса коммутатора:

QoS Configure > Storm Control



Frame Type	Коммутатор поддерживает до 3 типов пакетов, которые могут нести угрозу в виде сетевого шторма: Unicast Unknown Multicast Broadcast
Enable	Отметьте чекбокс, чтобы включить защиту от сетевого шторма
Rate (pps)	Скорость пропускания пакетов в сек (pps). Доступные значения: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, 1024K.

Нажмите Save, чтобы сохранить настройки.

10.8 Security Configure (Настройки безопасности)

10.8.1 Password (Пароль)

Пароль системы можно поменять в данном разделе WEB интерфейса коммутатора:

Security Configure > Password

The screenshot shows the 'System Password' configuration page. On the left, a sidebar menu lists various configuration sections: Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, and Security Configure. The 'Security Configure' section is expanded, showing sub-items: Password, SSH, HTTPS, and Port Security Limit. The 'Password' sub-item is selected. The main content area is titled 'System Password' and contains three input fields labeled 'Old Password', 'New Password', and 'Confirm New Password'. Below these fields is a 'Save' button.

Нажмите Save, чтобы сохранить настройки.

10.8.2 802.1X

Стандарт IEEE 802.1X определяет протокол контроля доступа и аутентификации, который ограничивает права неавторизованных компьютеров, подключенных к коммутатору.

Сервер аутентификации проверяет каждый компьютер перед тем, как тот сможет воспользоваться сервисами, которые предоставляет ему коммутатор. До тех пор, пока компьютер не аутентифицировался, он может использовать только протокол EAPOL (англ. extensible authentication protocol over LAN) и только после успешной аутентификации весь остальной трафик сможет проходить через тот порт коммутатора, к которому подключен данный компьютер.

Коммутатор поддерживает протокол контроля доступа на основе IEEE 802.1X. Настройки находятся в следующем разделе WEB интерфейса коммутатора:

Security Configure > 802.1X

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

Security Configure

Password

SSH

HTTPS

Port Security Limit

802.1X

ACL

DHCP

IP&MAC Source Guard

ARP Inspection

AAA

Network Access Server Configuration

System Configuration

Mode	Disabled	
Reauthentication Enabled	☐	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds

Port Configuration

Port	Admin State	Port State	Restart	
*	<>			
1	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize

System Configuration	В этом поле пользователь может вкл/выкл 802.1X или повторную аутентификацию, а также настроить период повторной аутентификации, таймаут для EAPOL, период устаревания и время удержания.
Port Configuration	В выпадающем меню можно выбрать настройки для состояния портов: Force Authorized – ускоренная авторизация Force Unauthorized 802.1X – авторизация на базе протокола 802.1X Mac Based Auth – авторизация на базе MAC адреса

Нажмите Save, чтобы сохранить настройки.

10.8.3 DHCP Snooping (Защита от атак с использованием DHCP)

10.8.3.1 About DHCP Snooping (Описание функции DHCP Snooping)

DHCP snooping — функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Например, атаки с подменой DHCP-сервера в сети или атаки DHCP starvation, которая заставляет DHCP-сервер выдать все существующие на сервере адреса злоумышленнику.

DHCP snooping регулирует только сообщения DHCP и не может повлиять напрямую на трафик пользователей или другие протоколы. Некоторые функции коммутаторов, не имеющие непосредственного отношения к DHCP, могут выполнять проверки на основании таблицы привязок DHCP snooping (DHCP snooping binding database). В их числе:

- ✓ Dynamic ARP Protection (Inspection) — проверка ARP-пакетов, направленная на борьбу с ARP-spoofing,
- ✓ IP Source Guard — выполняет проверку IP-адреса отправителя в IP-пакетах, предназначенная для борьбы с IP-spoofingом.

DHCP snooping позволяет:

- ✓ защитить клиентов в сети от получения адреса от неавторизованного DHCP-сервера,
- ✓ регулировать какие сообщения протокола DHCP отбрасывать, какие перенаправлять и на какие порты.

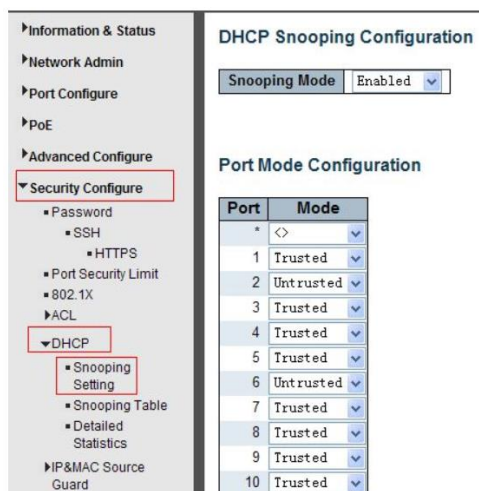
Для правильной работы DHCP snooping, необходимо указать какие порты коммутатора будут доверенными (trusted), а какие — нет (untrusted, в дальнейшем — ненадёжными):

- ✓ Ненадёжные (Untrusted) — порты, к которым подключены клиенты. DHCP-ответы, приходящие с этих портов отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database).
- ✓ Доверенные (Trusted) — порты коммутатора, к которым подключен другой коммутатор или DHCP-сервер. DHCP-пакеты, полученные с доверенных портов не отбрасываются.

10.8.3.2 DHCP Snooping Configure (Настройка DHCP Snooping)

Настройки функции DHCP Snooping находятся в следующем разделе WEB интерфейса коммутатора:

Security Configure > DHCP > Snooping Settings



DHCP Snooping Mode	Нажмите на выпадающее меню, чтобы вкл/выкл DHCP Snooping
Port Mode	Поле отображает режим DHCP Snooping для портов: Trusted – доверенные порты Untrusted – недоверенные порты Подробнее в пункте 8.8.3.1 About DHCP Snooping

Нажмите Save, чтобы сохранить настройки.

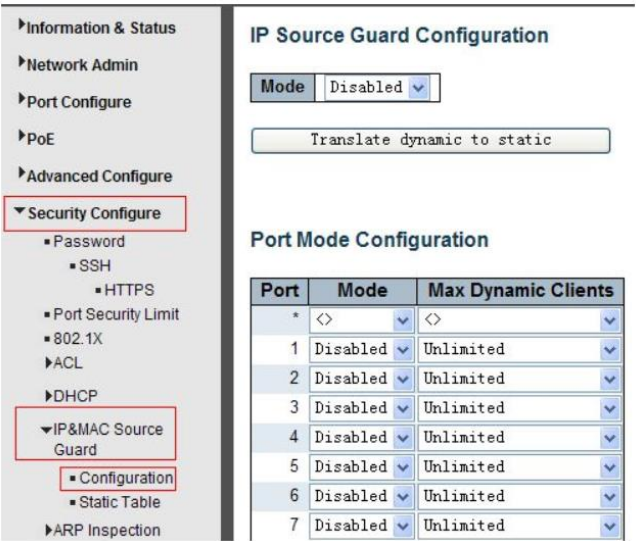
10.8.4 IP&MAC Source Guard

Функция коммутатора, которая ограничивает IP-трафик на интерфейсах 2го уровня, фильтруя трафик на основании таблицы привязок DHCP snooping и статических соответствий. Функция используется для борьбы с IP-spoofingom.

10.8.4.1 Port Configuration (Настройка IP&MAC Source Guard для портов)

Настроить функцию IP&MAC Source Guard для портов можно в следующем разделе WEB интерфейса коммутатора:

Security Configure > IP & MAC Source Guard > Configuration



Global Mode	Нажмите на выпадающее меню, чтобы вкл/выкл функцию IP&MAC Source Guard глобально.
Port Mode	Нажмите на выпадающее меню, чтобы вкл/выкл функцию IP&MAC Source Guard для выбранного порта.
Max Dynamic Clients	Нажмите на выпадающее меню, чтобы выбрать максимальное количество динамических клиентов. Доступные значения: Unlimited, 0, 1, 2.

Нажмите Save, чтобы сохранить настройки.

10.8.4.2 Static Table (Таблица статических соответствий)

На данной странице WEB интерфейса коммутатора есть возможность вручную настроить Таблицу статических соответствий для функции IP&MAC Source Guard. Все настройки доступны здесь:

Security Configure > IP&MAC Source Guard > Static Table

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

Add New Entry

Save Reset

Port	Нажмите на выпадающее меню, чтобы выбрать порт
VLAN	Нажмите на выпадающее меню, чтобы выбрать VLAN ID
IP Address	Поле с IP адресом
MAC Address	Поле с MAC адресом

Нажмите Save, чтобы сохранить настройки.

10.8.5 ARP Inspection (Проверка ARP пакетов)

Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Например, атаки ARP-spoofing, позволяющей перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена.

Dynamic ARP Inspection (Protection) регулирует только сообщения протокола ARP и не может повлиять напрямую на трафик пользователей или другие протоколы.

10.8.5.1 Port Configuration (Настройка ARP Inspection для портов)

Пользователь может настроить ARP Inspection для конкретного порта на этой странице WEB интерфейса коммутатора:

Security Configure > ARP Inspection > Port Configuration

ARP Inspection Configuration

Mode: Disabled

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None

Global Mode	Нажмите на выпадающее меню, чтобы вкл/выкл ARP Inspection глобально.
Port Mode	Нажмите на выпадающее меню, чтобы вкл/выкл ARP Inspection для портов.
Check VLAN	Если необходимо включить ARP Inspection для VLAN, активируйте (enable) функцию в выпадающем меню «Check VLAN». Значение по умолчанию – отключено (disable).
Log Type	None – журнал ARP Inspection не ведется. Deny – журнал ведется для заблокированных записей. Permit – журнал ведется для разрешенных записей. ALL – журнал ведется для всех типов записей.

Нажмите Save, чтобы сохранить настройки.

10.8.5.2 VLAN Configuration (Настройка ARP Inspection для VLAN)

Настройки ARP Inspection для VLAN находятся в следующем разделе WEB интерфейса коммутатора:

Security Configure > ARP Inspection > VLAN Configuration

VLAN Mode Configuration

Start from VLAN with entries per page.

Delete	VLAN ID	Log Type
Delete	1	None

VLAN ID	Отображает VLAN ID для текущей VLAN
Log Type	None – журнал ARP Inspection не ведется. Deny – журнал ведется для заблокированных записей. Permit – журнал ведется для разрешенных записей. ALL – журнал ведется для всех типов записей.

Нажмите Save, чтобы сохранить настройки.

10.8.5.3 Static Table (Таблица соответствий для ARP Inspection)

Пользователь может самостоятельно настроить таблицу соответствий для ARP Inspection. Соответствующие настройки находятся в следующем разделе WEB интерфейса коммутатора:

Security Configure > ARP Inspection > Static Table

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Add New Entry

Save Reset

Port	Нажмите на выпадающее меню, чтобы выбрать порт
VLAN	Выберите VLAN ID для настраиваемой VLAN
IP Address	Укажите IP адрес
MAC Address	Укажите MAC адрес

Нажмите Save, чтобы сохранить настройки.

10.8.6 ACL (Правила контроля доступа)

Access Control List или ACL — список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).

10.8.6.1 ACL Port Configure (Настройка ACL для портов)

Настройки правил контроля доступа (ACL) находятся в соответствующем разделе:

Security Configure > ACL > Ports

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

Security Configure

• Password

• SSH

• HTTPS

• Port Security Limit

• 802.1X

ACL

• Ports

• Rate Limiters

• Access Control List

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	247562
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1	Disabled	Disabled	Disabled	Enabled	0

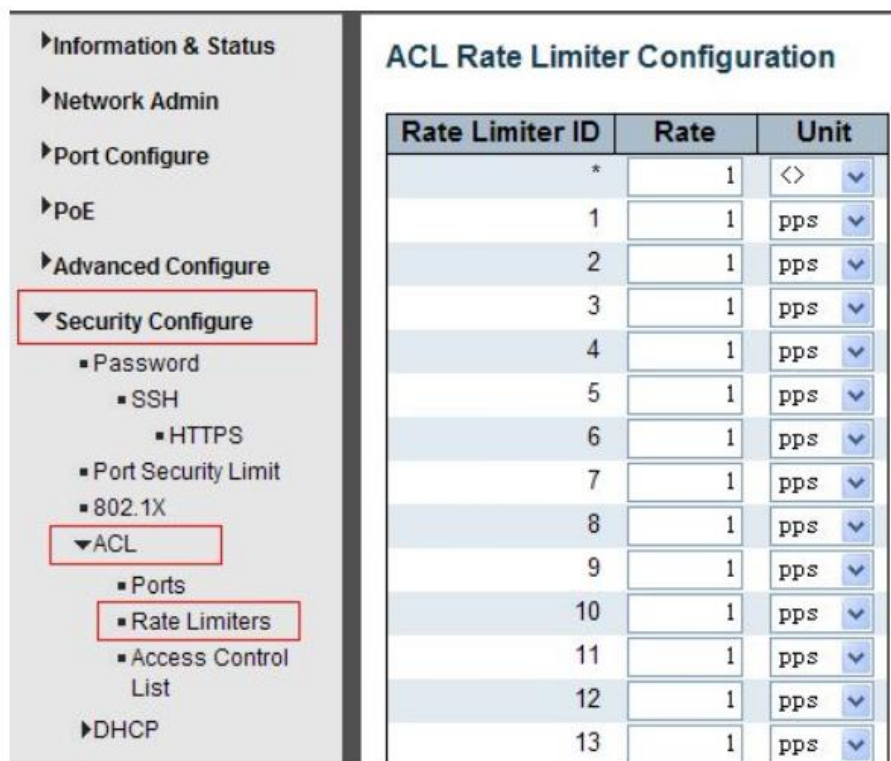
Action	Permit – разрешает выбранному порту пропускать данные Deny – запрещает выбранному порту пропускать данные
Rate Limiter ID	Ограничитель пропускной способности портов. Настройки находятся в соответствующем разделе.
Port Redirect	Выбор порта, пакеты с которого будут перенаправлены. Значение по умолчанию – Disabled (отключено)
Mirror	Поле определяет параметры зеркалирования на настраиваемом порте. Доступные значения Enabled – включено Disabled – отключено Значение по умолчанию – Disabled
Logging	Включение/выключение ведения журнала записей
Shut Down	Enabled – если пакеты будут получены на этом порте, порт будет выключен. Disabled – порт не будет выключен при получении пакетов. Значение по умолчанию – Disabled. <i>Примечание: данная функция работает, только если размер пакета меньше 1518 (без VLAN тэгов)</i>
State	Enabled – для открытия порта используются правила ACL заданные пользователем Disabled – для закрытия порта используются правила ACL заданные пользователем Значение по умолчанию – Enabled
Counter	Количество пакетов удовлетворяющих заданным правилам

Нажмите Save, чтобы сохранить настройки.

10.8.6.2 Rate Limiter Configuration (Настройка ограничителя пропускной способности портов)

Пользователь может настроить правила ACL для ограничителя пропускной способности для портов в соответствующем разделе WEB интерфейса коммутатора:

Security Configure > ACL > Rate Limiter



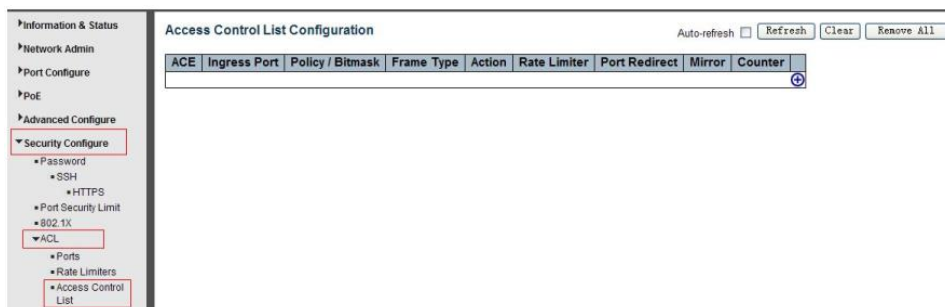
Rate Limiter ID	Rate	Unit
*	1	<> ▼
1	1	pps ▼
2	1	pps ▼
3	1	pps ▼
4	1	pps ▼
5	1	pps ▼
6	1	pps ▼
7	1	pps ▼
8	1	pps ▼
9	1	pps ▼
10	1	pps ▼
11	1	pps ▼
12	1	pps ▼
13	1	pps ▼

Нажмите Save, чтобы сохранить настройки.

10.8.6.3 Access Control List Configuration (Настройка ACL)

Пользователь может гибко настроить ACL в соответствующем разделе WEB интерфейса коммутатора:

Security Configure > ACL > Access Control List



Чтобы добавить и изменить запись нажмите кнопку «+»

10.9 Diagnostics (Инструменты диагностики и мониторинга)

10.9.1 Ping Test (Тестирование соединения с помощью PING)

PING это небольшой модуль, который взаимодействует с ECHO пакетами от IP адреса, который принадлежит удаленному устройству.

Данный инструмент находится в соответствующем разделе WEB интерфейса коммутатора:

Diagnostics > Ping

- Information & Status
- Network Admin
- Port Configure
- PoE
- Advanced Configure
- Security Configure
- QoS Configure
- Diagnostics**
 - Ping**
 - Cable Diagnostics
 - CPU Load

ICMP Ping

IP Address

0.0.0.0

Ping Length

56

Ping Count

5

Ping Interval

1

Start

IP Address	IP адрес удаленного адресата, который необходимо проверить
Ping Length	Число от 1 до 1452. Значение по умолчанию – 56
Ping Count	Количество отправляемых PING запросов. От 1 до 60.
Ping Interval	Интервал между отправкой PING запросов.

Нажмите кнопку «Start», чтобы приступить к тестированию с помощью Ping

10.9.2 Cable Diagnostics (Проверка кабеля)

Диагностика кабеля доступна только для медных кабелей, совместимых с 10/100/1000BaseT. Инструмент позволяет определить длину кабеля и его состояние.

Diagnostics > Cable Diagnostics

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

Security Configure

QoS Configure

Diagnostics

Ping

Cable Diagnostics

CPU Load

VeriPHY Cable Diagnostics

Port All

Start

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	Open	0	Open	0	Open	0	Open	0
2	OK	6	OK	6	--	0	--	0
3	Open	0	Open	0	Open	0	Open	0
4	Open	0	Open	0	Open	0	Open	0

Нажмите кнопку «Start», чтобы приступить к диагностике.

10.9.3 CPU Load (Загрузка CPU коммутатора)

На данной странице WEB интерфейса находится график загрузки CPU коммутатора в реальный момент времени.

Diagnostics > CPU Load

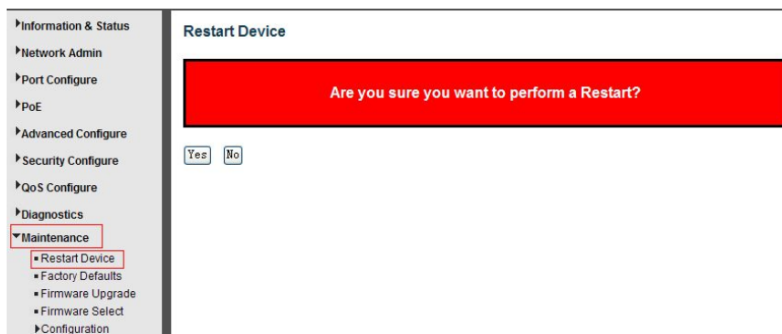


10.10 Maintenance (Обслуживание)

10.10.1 Restart Device (Перезагрузка коммутатора)

На данной странице WEB интерфейса находится инструмент для удаленной перезагрузки коммутатора.

Maintenance > Restart Device



Yes – перезагрузка коммутатора

10.10.2 Factory Defaults (Возврат к заводским настройкам)

На данной странице WEB интерфейса находится инструмент для возврата коммутатора к заводским настройкам.

Maintenance > Factory Defaults

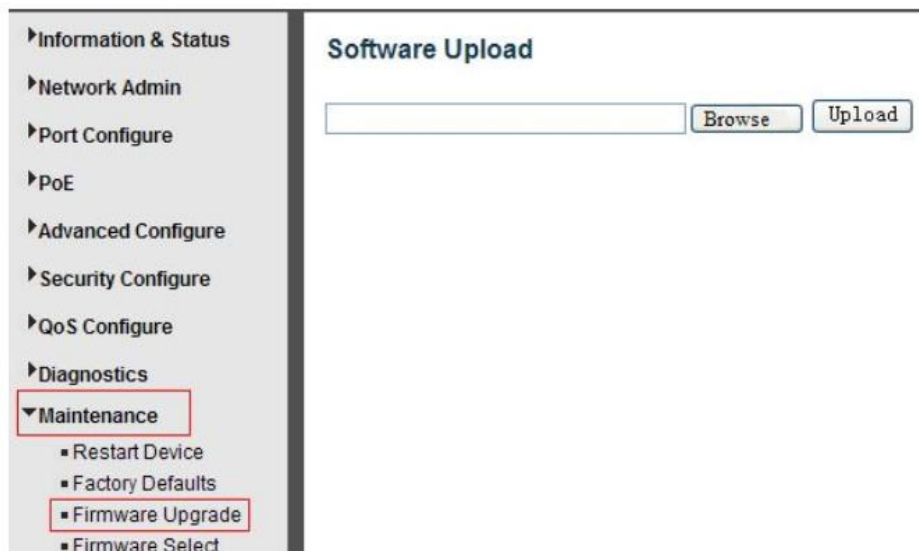


Yes – сброс настроек коммутатора к заводским.

10.10.3 Firmware Upgrade (Обновление прошивки)

На данной странице WEB интерфейса находится инструмент для обновления прошивки коммутатора.

Maintenance > Firmware Upgrade



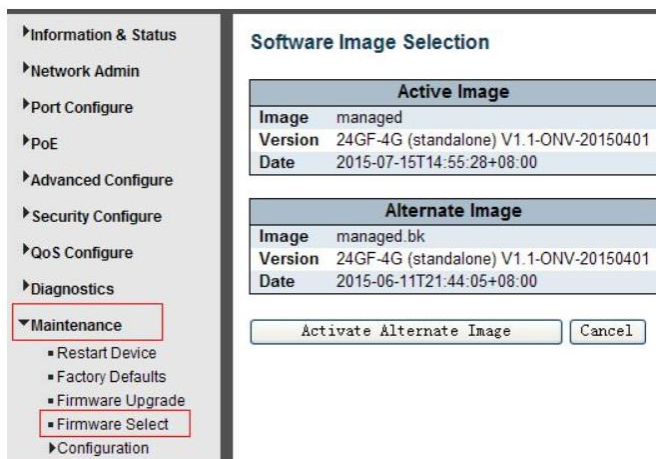
Нажмите Browse, выберите файл с прошивкой. Нажмите Upload, чтобы загрузить прошивку в коммутатор.

10.10.4 Firmware Select (Выбор текущей прошивки коммутатора)

Коммутатор позволяет выбрать один из 2х образов текущей прошивки коммутатора

Maintenance > Firmware Select

Для выбора альтернативной прошивки нажмите кнопку «Activate Alternate Image»

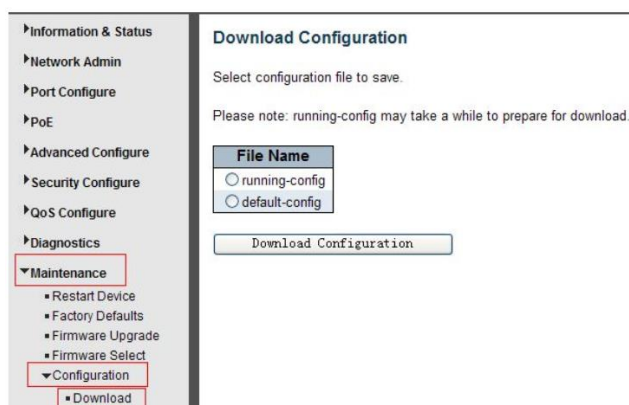


10.10.5 Configuration (Текущая конфигурация)

В данном разделе содержатся инструменты для сохранения и загрузки файла с текущей конфигурацией коммутатора

10.10.5.1 Download (Сохранение файла с текущей конфигурацией коммутатора)

Maintenance > Configuration > Download



Выберите файл с текущей конфигурацией (running config) или конфигурацией по умолчанию (default config), а затем нажмите кнопку «Download Configuration»

10.10.5.2 Upload Configuration (Загрузка файла с конфигурацией)

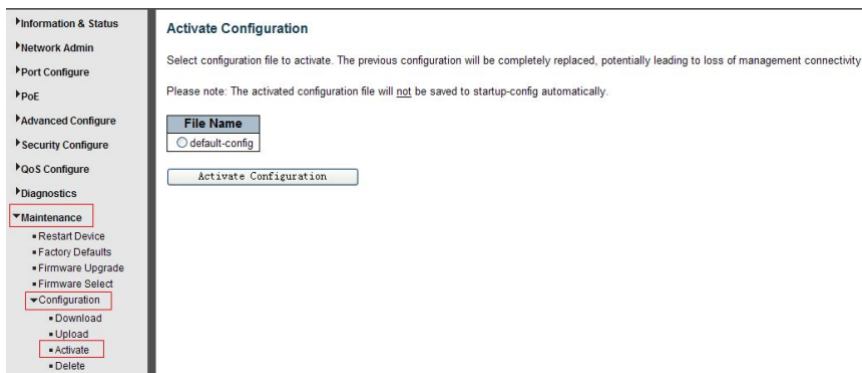
Maintenance > Configuration > Upload

The screenshot displays the 'Upload Configuration' web interface. On the left, a sidebar menu lists various system functions. The 'Maintenance' section is expanded, and the 'Configuration' sub-menu is further expanded, with the 'Upload' option highlighted. The main content area is titled 'Upload Configuration'. It features a 'File To Upload' section with a text input field and a 'Browse' button. Below this is a 'Destination File' section with two tabs: 'File Name' and 'Parameters'. At the bottom of this section is a large 'Upload Configuration' button.

Нажмите кнопку «Browse», чтобы выбрать файл с конфигурацией для коммутатора. Нажмите кнопку «Upload Configuration», чтобы загрузить файл с конфигурацией в коммутатор.

10.10.5.3 Activate Configuration (Активация файла с конфигурацией)

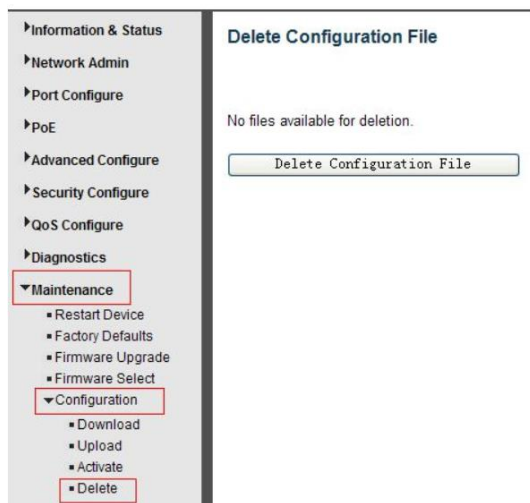
Maintenance > Configuration > Activate



Для активации нажмите кнопку «Activate Configuration»

10.10.5.4 Delete Configuration File (Удаление файла с конфигурацией)

Maintenance > Configuration > Delete



Для удаления файла с конфигурацией из коммутатора нажмите кнопку «Delete Configuration File»

Внимание

- ✓ Качественное заземление является обязательным условием подключения.

11. Технические характеристики*

Модель	SW-80402-IL(port 90W,360W)
Общее кол-во портов	6
Кол-во портов FE+PoE	-
Кол-во портов FE	-
Кол-во портов GE+PoE	4
Кол-во портов GE (не Combo порты)	-
Кол-во портов Combo GE (RJ45+SFP)	-
Кол-во портов SFP (не Combo порты)	2 GE (100/1000Мбит/с)
Мощность PoE на порт (макс.)	90 Вт
Суммарная мощность PoE всех портов (макс.)	360 Вт
Стандарты PoE	IEEE 802.3af/at/bt
Метод подачи PoE	Метод A+B 1, 2, 4, 5(+), 3, 6, 7, 8(-)
Топологии подключения	звезда каскад кольцо
Буфер пакетов	4.1 МБ
Таблицы MAC-адресов	8 К
Пропускная способность коммутационной матрицы (Switching fabric)	12 Гбит/с
Скорость обслуживания пакетов (Forwarding rate)	1000 Мбит/с – 1488,000 пакетов/с 100 Мбит/с - 148,800 пакетов/с 10 Мбит/с- 14,880 пакетов/с
Поддержка Jumbo frame	9 КБ
Размер flash памяти	128 МБ

Модель	SW-80402-IL(port 90W,360W)
Размер SDRAM	1 Гб
Стандарты и протоколы	• IEEE 802.3 – 10BaseT • IEEE 802.3u – 100BaseTX • IEEE 802.3ab – 1000BaseT • IEEE 802.3z 1000 BaseSX/LX • IEEE 802.3af Power over Ethernet • IEEE 802.3at Power over Ethernet • IEEE 802.3bt Power over Ethernet • IEEE 802.3x – Flow Control • IEEE 802.1Q – VLAN • IEEE 802.1p – Class of Service • IEEE 802.1D – Spanning Tree • IEEE 802.1w – Rapid Spanning Tree • IEEE 802.1s – Multiple Spanning Tree • IEEE 802.3ad – Link Aggregation Control Protocol (LACP) • IEEE 802.1AB – LLDP (Link Layer Discovery Protocol) • IEEE 802.1X – Access Control
Функции уровня 2	• IEEE 802.1D (STP) • IEEE 802.1w (RSTP) • IEEE 802.1s (MSTP) • VLAN / VLAN Group 4K • Tagged Based • Port-based • Voice VLAN • Link Aggregation IEEE 802.3ad with LACP • IGMP Snooping v1/v2/v3 • IGMP Static Multicast Addresses • Storm Control
Качество обслуживания (QoS)	• 8 очередей / порт
Безопасность	• Management System User Name/Password Protection • IEEE 802.1x Port-based Access Control • HTTP & SSL (Secure Web) • SSH v2.0 (Secured Telnet Session)

Модель	SW-80402-IL(port 90W,360W)
Управление	• Управление через Web-интерфейс • CLI • Telnet • SSH v1/v2 • SNMP
Индикаторы	V1 (1-й БП), V2 (2-й БП), SYS (работа коммутатора), Link (установка соединения), PoE, 5F, 6F (активность SFP портов)
Грозозащита	6 kV
Питание	DC 48-57V
Энергопотребление	<15 Вт (без PoE) <375 Вт (с PoE)
Охлаждение	Конвекционное (без вентилятора)
Класс защиты	IP30
Размеры (ШхВхГ) (мм)	47x145x112
Вес (кг)	0,6
Способ монтажа	На DIN рейку
Рабочая температура	-40...+75 °C
Наработка на отказ MTBF (ч)	50000
Дополнительно	-

* Производитель имеет право изменять технические характеристики изделия и комплектацию без предварительного уведомления.

12. Гарантия

Гарантия на все оборудование OSNOVO – 7 лет (84 месяца) с даты продажи, за исключением аккумуляторных батарей, гарантийный срок - 12 месяцев.

В течение гарантийного срока выполняется бесплатный ремонт, включая запчасти, или замена изделий при невозможности их ремонта.

Подробная информация об условиях гарантийного обслуживания находится на сайте www.osnovo.ru