OSNOVO
cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Промышленные управляемые L2+ коммутаторы
Gigabit Ethernet на 10 и 12 портов

SW-70802/IL

SW-70804/IL

Прежде чем приступать к эксплуатации изделия,
внимательно прочтите настоящее руководство

Оглавление

1. Назначение 5

2. Комплектация* 6

3. Особенности оборудования 6

4. Внешний вид и описание элементов 6

4.1 Внешний вид 6

4.2 Описание элементов коммутаторов 7

5. Схема подключения 11

6. Проверка работоспособности системы 12

7. Подготовка перед управлением коммутатором через WEB-интерфейс 13**

8. Управление через WEB интерфейс 15

8.1 Основные сведения 15

8.2 Главное меню WEB интерфейса 16

8.3 Network Admin (Настройка сетевых параметров и администрирование) 17

8.3.1 IP Configuration (Настройка IP адреса) 17

8.3.2 SNTP Configuration (Настройка протокола времени SNTP) 18

8.3.3 SNMP Configuration (Настройка протокола управления SNMP) 19

8.3.4 System Log Configuration (Настройка системного журнала) 21

8.4 Port Configure (Конфигурирование портов) 22

8.4.1 Port Configuration (Настройка портов) 22

8.4.2 Link aggregation (Агрегация каналов)..... 23
8.4.3 Port Mirroring (Зеркалирование портов)..... 26
8.4.4. Thermal Protection Configuration (Температурная защита)..... 27
8.5 Advanced Configure (Расширенные настройки) 28
8.5.1 VLAN (Настройка VLAN)..... 28
8.5.2 Port Isolation (Изоляция портов) 32
8.5.3 STP (Протокол связующего дерева)..... 33
8.5.4 MAC Address Table (Таблица MAC адресов) 36
8.5.5 IGMP Snooping 37
8.5.6 ERPS (Протокол ERPS) 40
8.5.7 LLDP (Настройка протокола LLDP)..... 43
8.5.8 Loop Protection (Защита от сетевых петель)..... 44
8.6 QoS (Приоритезация трафика)..... 45
8.6.1 QoS Port Classification (Классификация портов с помощью QoS) 46
8.6.2 Port Policing (Функция ограничения скорости на портах)..... 47
8.6.3 Storm Control Configuration (Настройка защиты от сетевого шторма) 48
8.7 Security Configure (Настройки безопасности)..... 49
8.7.1 Password (Пароль)..... 49
8.7.2 802.1X 49
8.7.3 DHCP Snooping (Защита от атак с использованием DHCP)... 51
8.7.4 IP&MAC Source Guard 53

8.7.5 ARP Inspection (Проверка ARP пакетов) 55
8.7.6 ACL (Правила контроля доступа) 58
8.8 Diagnostics (Инструменты диагностики и мониторинга) 61
8.8.1 Ping Test (Тестирование соединия с помощью PING) 61
8.8.2 Cable Diagnostics (Проверка кабеля) 63
8.8.3 CPU Load (Загрузка CPU коммутатора) 63
8.9 Maintenance (Обслуживание) 64
8.9.1 Restart Device (Перезагрузка коммутатора) 64
8.9.2 Factory Defaults (Возврат к заводским настройкам) 64
8.9.3 Firmware Upgrade (Обновление прошивки) 65
8.9.4 Firmware Select (Выбор текущей прошивки коммутатора) 65
8.9.5 Configuration (Текущая конфигурация) 66
9. Технические характеристики* 69
10. Гарантия 71

1. Назначение

Промышленные управляемые L2+ коммутаторы Gigabit Ethernet SW-70802/IL и SW-70804/IL на 10 и 12 портов соответственно предназначены для объединения сетевых устройств в пределах одного или нескольких узлов компьютерной сети. Коммутаторы способны работать в условиях использования в промышленных неотапливаемых помещениях.

Коммутаторы оснащены 8 основными медными портами Gigabit Ethernet (10/100/1000Base-T), а также SFP слотами для связи с помощью оптоволоконного кабеля:

– 2мя Gigabit Ethernet (1000Base-X) SFP слотами – для модели SW-70802/IL;

– 4мя Gigabit Ethernet (1000Base-X) SFP слотами – для модели SW-70804/IL;

В качестве SFP-модулей (приобретаются) рекомендуется использовать модули с подходящими скоростными характеристиками – 1 Гбит/с.

Коммутаторы SW-70802/IL и SW-70804/IL поддерживают автоматическое определение MDI/MDIX (Auto Negotiation) на всех медных портах.

Коммутаторы распознают тип подключенного сетевого устройства и при необходимости меняют контакты передачи данных, что позволяет использовать кабели, обжатые любым способом (кроссовые и прямые).

Коммутаторы гибко настраиваются через WEB-интерфейс и имеют множество функций L2+ уровня, таких как VLAN, IGMP snooping, QoS и др.

Кроме того, в коммутаторах предусмотрен порт RJ-45 (Console) для управления через интерфейс RS-232.

Коммутаторы SW-70802/IL и SW-70804/IL могут быть с успехом использованы в самых различных сферах применения. В первую очередь, коммутаторы как нельзя лучше подойдут для организации системы видеонаблюдения с возможностью диагностики и мониторинга в торговом центре, на предприятии, на производстве.

2. Комплектация*

1. Промышленный коммутатор – 1 шт;
2. Крепление на DIN-рейку – 1шт;
3. Клеммная колодка – 1шт;
4. Руководство по эксплуатации – 1шт.

3. Особенности оборудования

- Увеличенное количество SFP слотов (4 шт) для SW-70804/IL;
- Промышленное исполнение с креплением на DIN рейку и расширенным диапазоном рабочих температур;
- Возможность работы в сети с топологией «кольцо»;
- Гибкость настройки через WEB, поддержка функций L2+, простота и надежность в эксплуатации.

4. Внешний вид и описание элементов

4.1 Внешний вид

Рис.1 Коммутаторы SW-70802/IL, SW-70804/IL, внешний вид

4.2 Описание элементов коммутаторов

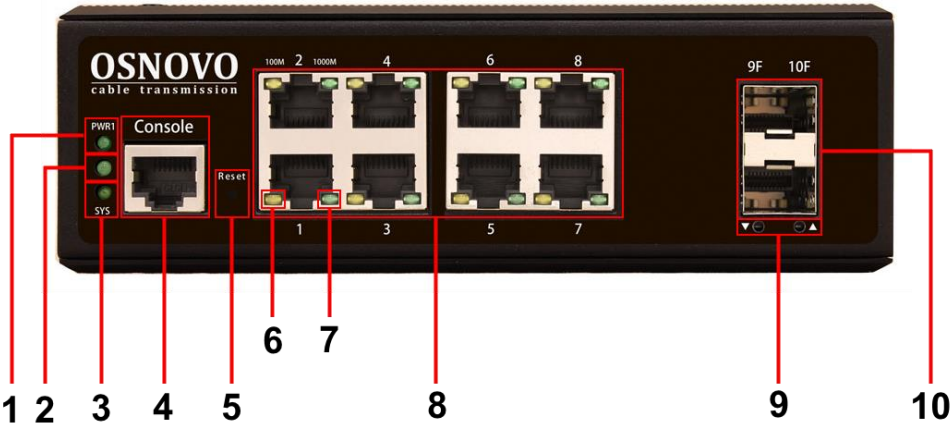


Рис. 3 Коммутатор SW-70802/IL, разъемы и индикаторы на передней панели

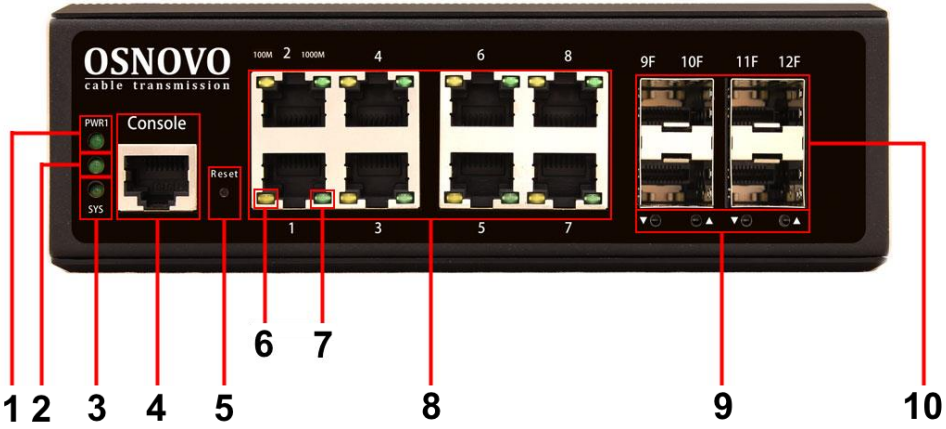


Рис. 4 Коммутатор SW-70804/IL, разъемы и индикаторы на передней панели

Таб. 1 Назначение разъемов и индикаторов на передней панели коммутаторов SW-70802/IL и SW-70804/IL

№ п/п	Обозначение	Назначение
1	PWR 1	LED индикатор подключения основного блока питания. Горит – БП подключен, питание подается. Не горит – питание не подается. Проверьте подключение БП к клеммной колодке коммутатора.
2	-	LED индикатор подключения резервного блока питания. Горит – БП подключен, питание подается. Не горит – питание не подается. Проверьте подключение БП к клеммной колодке коммутатора.
3	SYS	LED индикатор ошибки. Мигает – коммутатор функционирует в штатном режиме; Не горит – ошибка. Проверьте подключение БП.
4	Console	Разъем RJ-45 для подключения коммутатора через RS 232. Используется для загрузки прошивки в коммутатор аварийным способом
5	Reset	Микрокнопка для сброса коммутатора до заводских настроек.
6	100M	LED индикатор скорости 100Мбит/с Горит – подключено устройство на скорости 100Мбит/с Не горит – подключено устройство на скорости 1000Мбит/с или устройство не подключено
7	1000M	LED индикатор скорости 1000Мбит/с Горит – подключено устройство на скорости 1000Мбит/с Не горит – подключено устройство на скорости 100Мбит/с или устройство не подключено

№ п/п	Обозначение	Назначение
8	1-8	Разъемы RJ-45 с 1 по 8й для подключения для подключения сетевых устройств на скорости 10/100/1000 Мбит/с
9		Для SW-70802/IL LED индикатор подключения к SFP слотам Горит/мигает ▼ соединение установлено, идет обмен данных (SFP слот 9F) Горит/мигает ▲ соединение установлено, идет передача данных (SFP слот 10F)
		Для SW-70804/IL LED индикатор подключения к SFP слотам Горит/мигает ▼ соединение установлено, идет обмен данных (SFP слоты 9F 11F) Горит/мигает ▲ соединение установлено, идет передача данных (SFP слоты 10F 12F)
10	9F 10F	Для SW-70802/IL SFP слоты (2 шт) Предназначены для подключения коммутатора к сети или другому устройству по оптоволоконному кабелю (SFP) с использованием SFP модулей (приобретаются отдельно). Скорость – 1000Мбит/с.
	9F 10F 11F 12F	Для SW-70804/IL SFP слоты (4 шт) Предназначены для подключения коммутатора к сети или другому устройству по оптоволоконному кабелю (SFP) с использованием SFP модулей (приобретаются отдельно). Скорость – 1000Мбит/с.

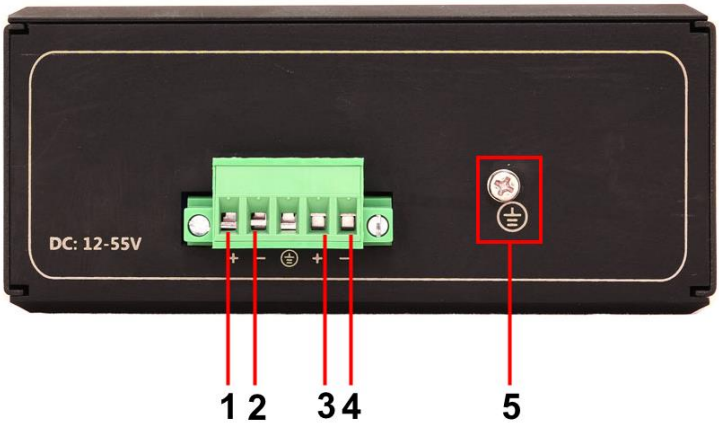


Рис. 5 Коммутаторы SW-70802/IL, SW-70804/IL, разъемы на боковой панели

Таб. 2 Назначение разъемов на боковой панели коммутаторов SW-70802/IL и SW-70804/IL

№ п/п	Обозначение	Назначение
1	+	Часть клеммной колодки для подключения контакта «+» основного блока питания* с напряжением DC 12-55V
2	-	Часть клеммной колодки для подключения контакта «-» основного блока питания* с напряжением DC 12-55V
3	+	Часть клеммной колодки для подключения контакта «+» основного блока питания* с напряжением DC 12-55V
4	-	Часть клеммной колодки для подключения контакта «-» резервного блока питания* с напряжением DC 12-55V
5	⏚	Винтовая клемма для заземления корпуса коммутатора.

*Блок питания не входит в комплект поставки. Приобретается отдельно.

5. Схема подключения

Рис.6 Типовая схема подключения коммутатора на примере SW-70804/IL

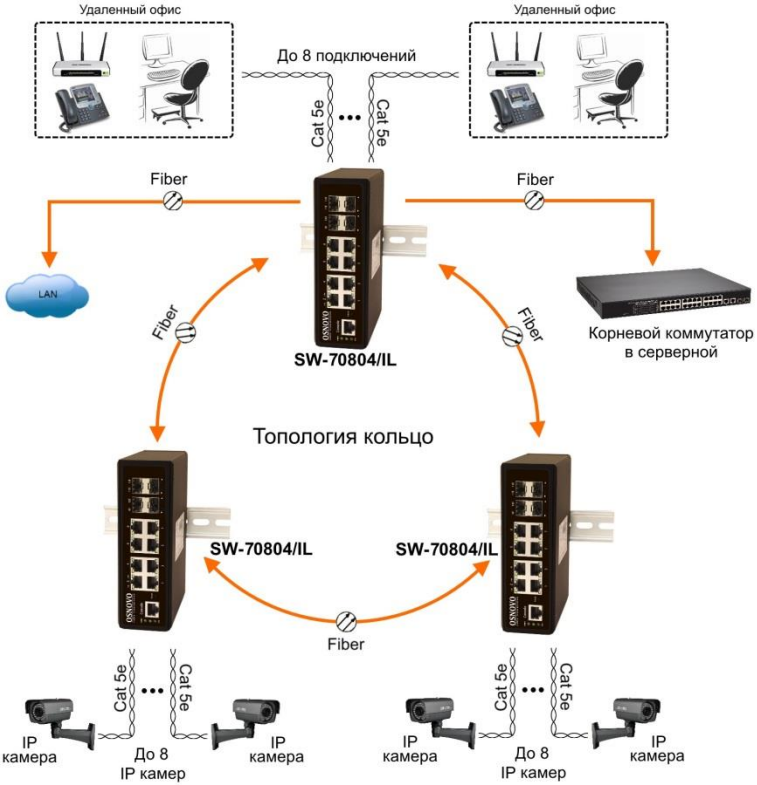


Рис.7 Типовая схема подключения коммутатора в топологии «кольцо» на примере SW-70804/IL

6. Проверка работоспособности системы

После подключения кабелей к разъёмам и подачи питания на коммутатор можно убедиться в его работоспособности.

Подключите коммутатор между двумя ПК с известными IP-адресами, располагающимися в одной подсети, например, 192.168.1.1 и 192.168.1.2.

На первом компьютере (192.168.1.2) запустите командную строку (выполните команду cmd) и в появившемся окне введите команду:

ping 192.168.1.1

Если все подключено правильно, на экране монитора отобразится ответ от второго компьютера (Рис. 8) Это свидетельствует об исправности коммутатора.

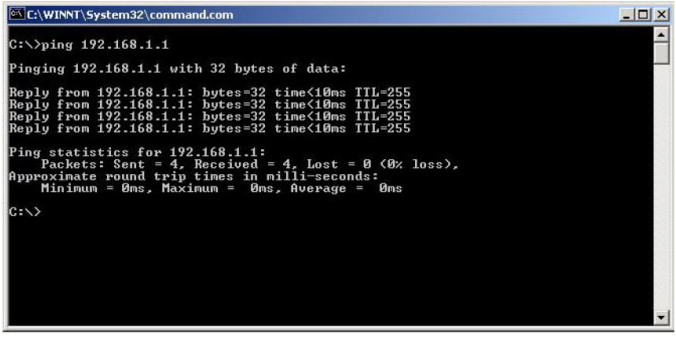


Рис.8 Данные, отображающиеся на экране монитора, после использования команды Ping.

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;
- о неисправности коммутатора;
- о помехах в линии.

Примечание:

Причины потери в оптической линии могут быть вызваны:

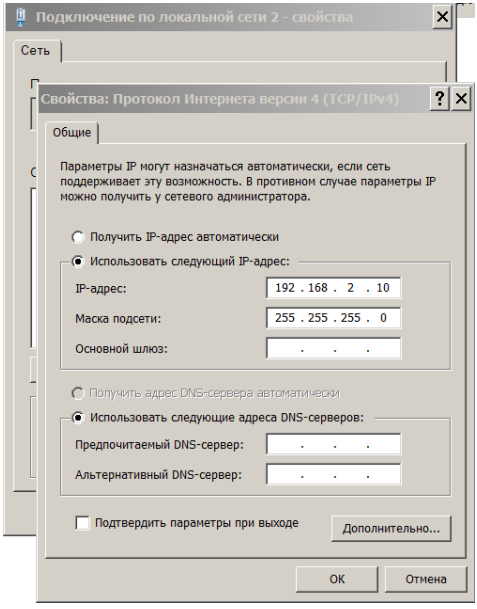
- неисправностью SFP-модулей
- изгибами кабеля
- большим количеством узлов сварки
- неисправностью или неоднородностью оптоволокна.

7. Подготовка перед управлением коммутатором через WEB-интерфейс**

Web-интерфейс позволяет гибко настраивать и отслеживать состояние коммутатора, используя браузер (Google Chrome, Opera, IE и тд) из любой точки в сети.

Прежде, чем приступить к настройке коммутатора через Web-интерфейс, необходимо убедиться, что ваш ПК и коммутатор находятся в одной сети. Чтобы правильно сконфигурировать ваш ПК используйте следующую пошаговую инструкцию:

1. Убедитесь, что сетевая карта в вашем ПК установлена, работает и поддерживает TCP/IP протокол.
2. Подключите между собой коммутатор и ваш ПК, используя патч-корд RJ-45
3. По умолчанию IP-адрес коммутатора: **192.168.2.1.** Коммутатор и ваш ПК должны находиться в одной подсети. Измените IP адрес вашего ПК на 192.168.2.X, где X-число от 2 до 254. Пожалуйста, убедитесь, что IP-адрес, который вы назначаете вашему ПК, не совпадал с IP-адресом коммутатора.



4. Запустите Web-браузер (IE, Firefox, Chrome) на вашем ПК
5. Введите в адресную строку **192.168.2.1** (IP-адрес коммутатора) и нажмите Enter на клавиатуре.
6. Появится форма аутентификации. По умолчанию

логин: **admin**

пароль: **system**

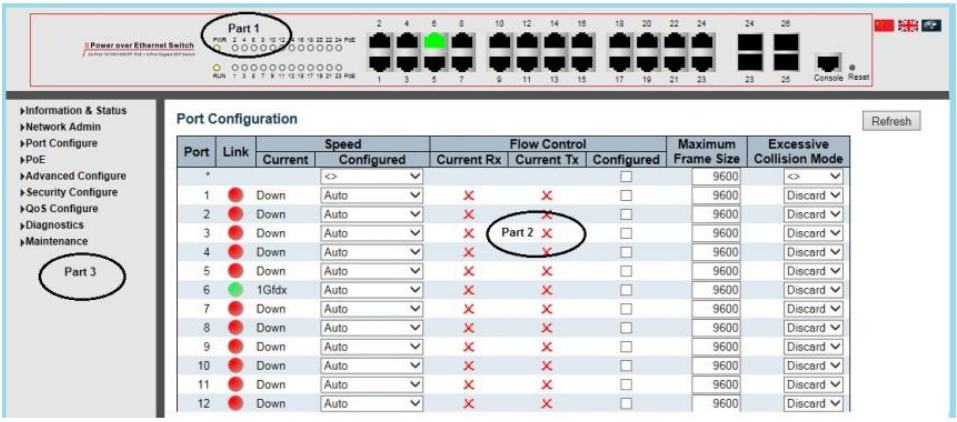
В дальнейшем пароль и логин можно поменять через WEB интерфейс коммутатора.

7. После корректного ввода имени пользователя (логин) и пароля появится главное окно WEB интерфейса коммутатора

8. Управление через WEB интерфейс.

8.1 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

8.2 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 8:

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.

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

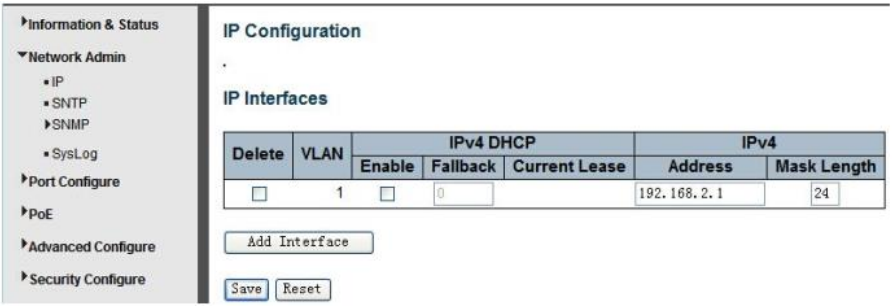
настройкам, обновление прошивки, загрузка и сохранение текущей конфигурации, перезагрузка коммутатора) в данном пункте главного меню WEB интерфейса.

8.3 Network Admin (Настройка сетевых параметров и администрирование)

8.3.1 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*



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.

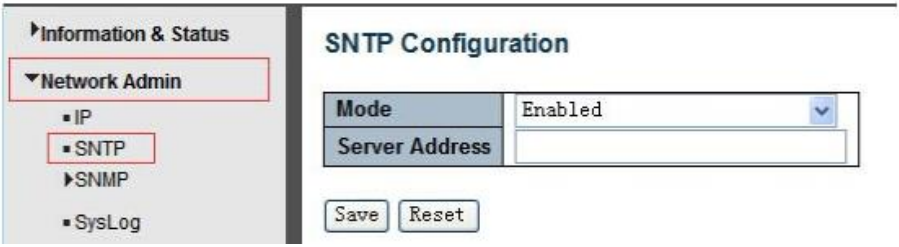
Нажмите Add Interface, чтобы задать новые настройки для VLAN и IP адреса. Нажмите Save, чтобы сохранить настройки.

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.

8.3.2 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.

8.3.3 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. Ккоммутатор 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

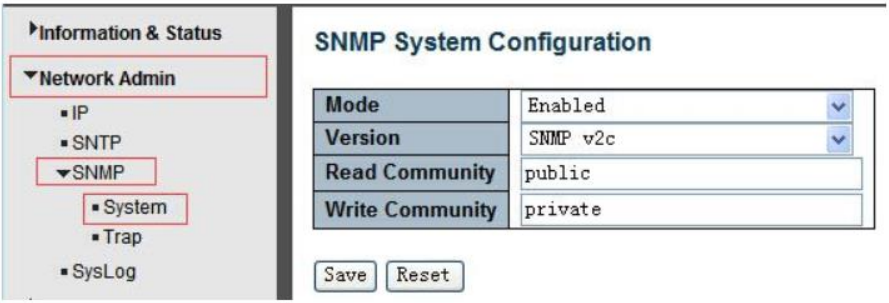
Это коллекция управляемых объектов, находящихся в виртуальном хранилище информации. Коллекции связанных управляемых объектов определены в определенных модулях MIB. Коммутатор использует стандартный модуль управления информацией MIB-II. Таким образом, значение объекта MIB может быть прочитано

любым программным обеспечением, управляемым через SNMP протокол.

8.3.3.1 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

8.3.3.2 SNMP Trap Configuration (Настройка SNMP Trap)

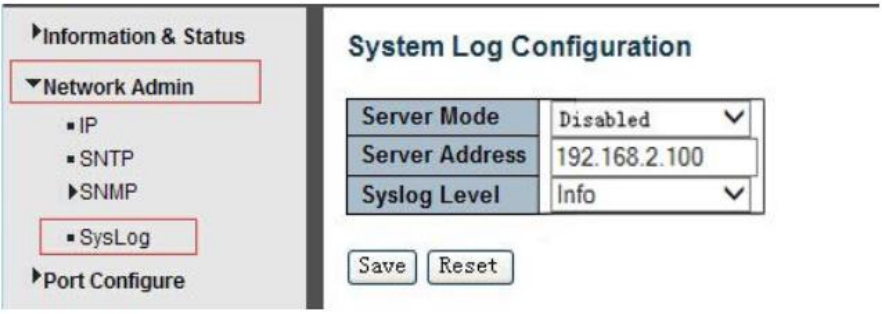
Вы можете включить или выключить данную функцию и настроить ее в следующем разделе

Network Admin>SNMP>Trap

8.3.4 System Log Configuration (Настройка системного журнала)

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

Network Admin > Syslog



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

8.4 Port Configure (Конфигурирование портов)

8.4.1 Port Configuration (Настройка портов)

Данный раздел WEB интерфейса содержит перечень настроек для портов коммутатора.

Port Configure>Ports

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.

8.4.2 Link aggregation (Агрегация каналов)

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

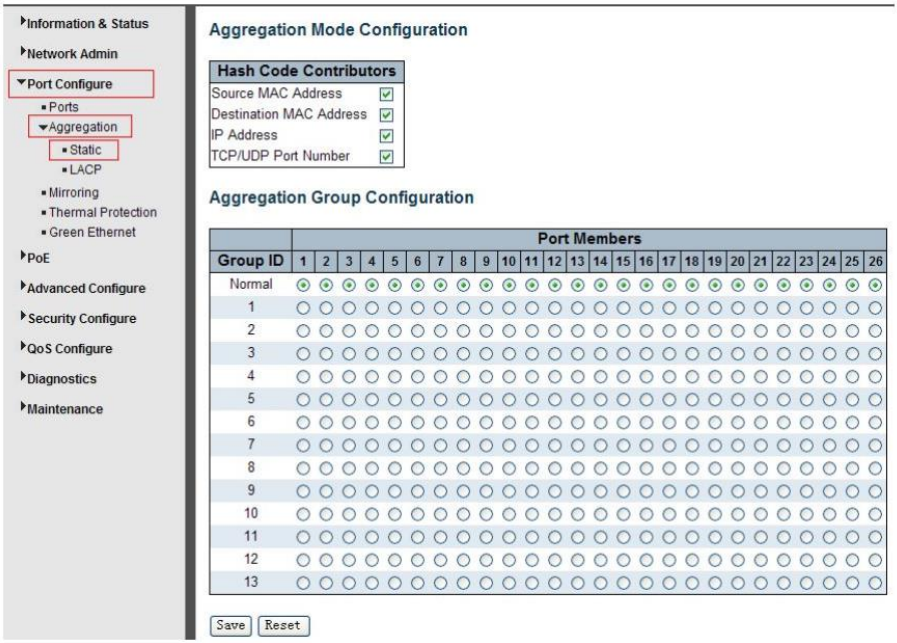
Коммутатор поддерживает до 13 групп агрегации каналов. От 2 до 8 портов в виде единого логического порта.

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.

8.4.2.1 Static Aggregation (Статическая Агрегация)

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

Port Configure > Aggregation > Static



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.

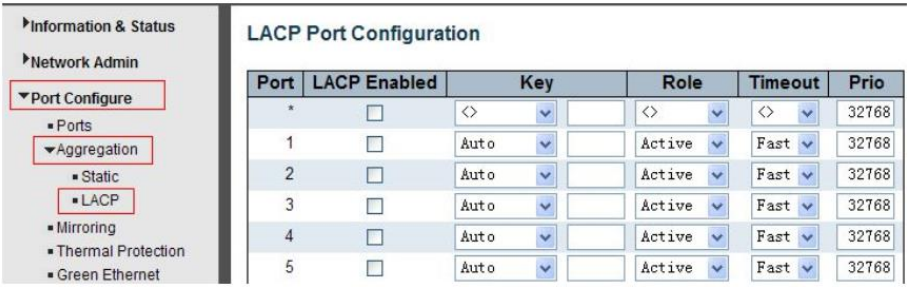
8.4.2.2 LACP Aggregation (Агрегация на основе LACP)

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



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.

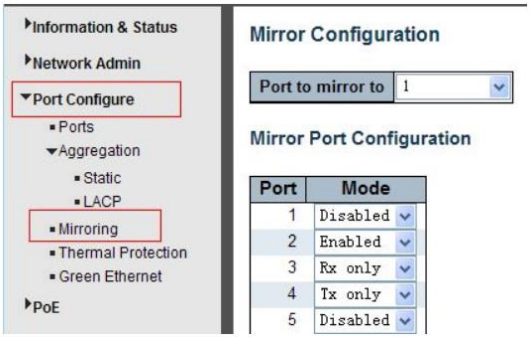
Нажмите Save, чтобы сохранить настройки.

8.4.3 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



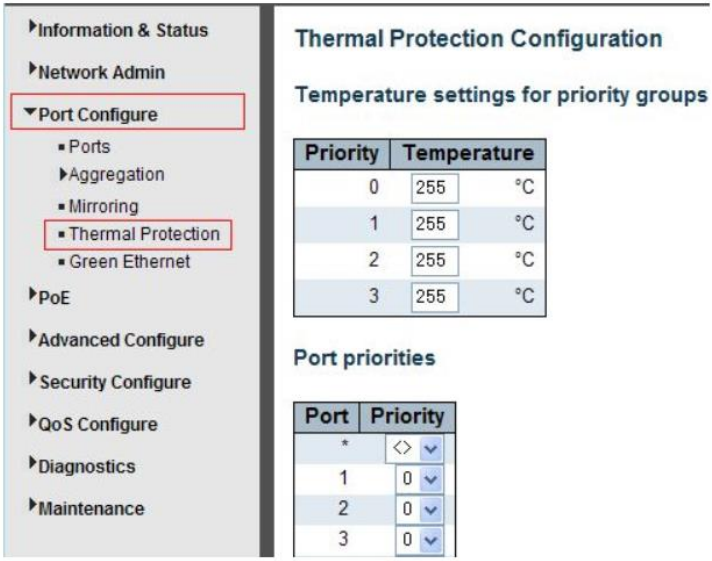
Port mirror to	Пакеты с портов, для которых включено зеркалирование rx или tx будут доступны на этом порте. Disabled – отключает зеркалирование
Mode	Выбор режима зеркалирования для порта источника. Rx only – пакеты, полученные на этом порте будут отправлены за порт-зеркало (mirror port). Исходящие пакеты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

8.4.4. 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



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 С

8.5 Advanced Configure (Расширенные настройки)

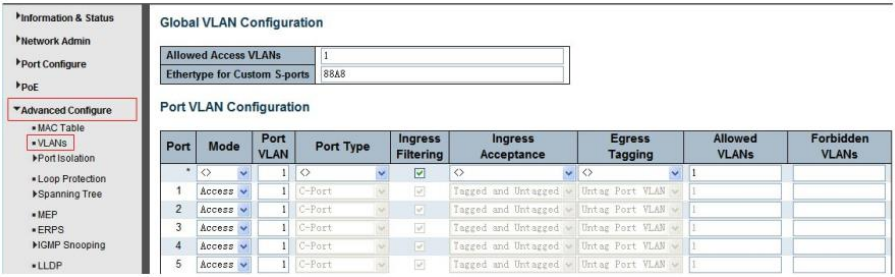
8.5.1 VLAN (Настройка VLAN)

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



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. Access. 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. Trunk. 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. Hybrid. 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. Unaware. 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. C-port. 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. S-port. 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. S-Custom-Port. 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. Tagged and Untagged. Все типы пакетов с меткой или без будут приниматься. Tagged only. Только помеченные пакеты будут приниматься на входе. Пакеты без метки будут отброшены. Untagged only. 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 Untag Port VLAN. Пакеты относящиеся к Port VLAN будут передаваться без метки. Остальные пакеты получат соответствующую метку. Tag All. Все пакеты, относящиеся к Port VLAN или нет будут передаваться с меткой. Untag All. 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.

8.5.2 Port Isolation (Изоляция портов)

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

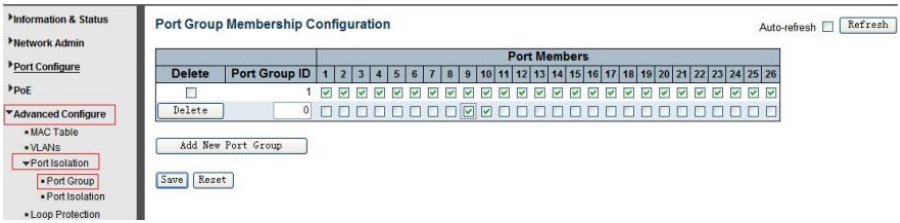
8.5.2.1 Port Group (Группа портов)

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



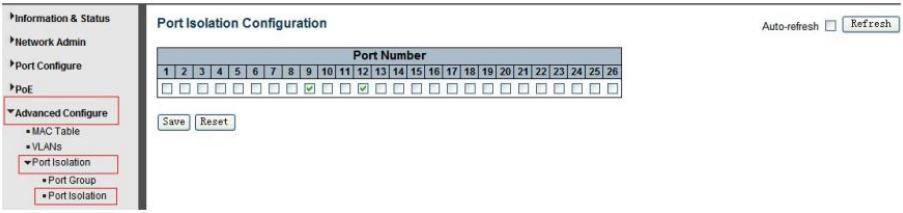
Port members	Отметьте порты, которые будут принадлежать одной группе.

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

8.5.2.2 Port Isolation (Изоляция портов)

Настройка изоляции портов находится в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > Port isolation > Port Isolation



Port number	Отметьте порты, которые будут изолированы.

Нажмите Save, чтобы сохранить настройки.

8.5.3 STP (Протокол связующего дерева)

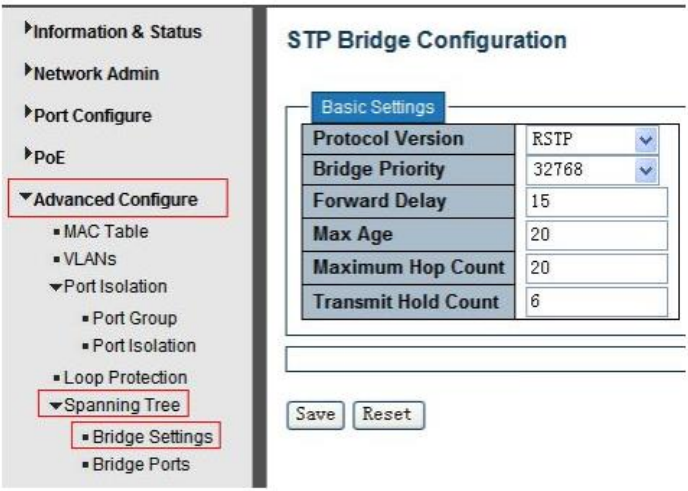
Spaning Tree Protocol (STP) – или протокол связующего дерева используется для обнаружения и исправления сетевых петель. Он обеспечивает запасные соединения между коммутаторами, мостами и маршрутизаторами.

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.

8.5.3.1 STP Bridge Settings (Настройки протокола STP)

Настройки протокола STP находятся в следующем разделе WEB интерфейса коммутатора:

Advanced Configure > Spanning Tree > Bridge Settings



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.

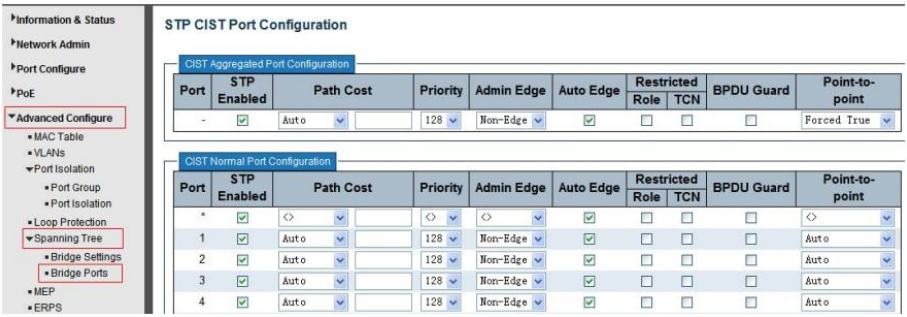
Transmit Hold Count (1-10)	Количество BPDU пакетов, которые корневой порт (bridge port) может отправлять за 1 секунду. Если необходимо, может быть организована задержка перед отправкой следующего BPDU пакета. Доступные значения от 1 до 10 BPDU пакетов в секунду. Значение по умолчанию – 6.

Нажмите Save, чтобы сохранить настройки.

8.5.3.2 STP Bridge Port (Выбор bridge порта)

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

Advanced Configure > Spanning Tree > Bridge Ports



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

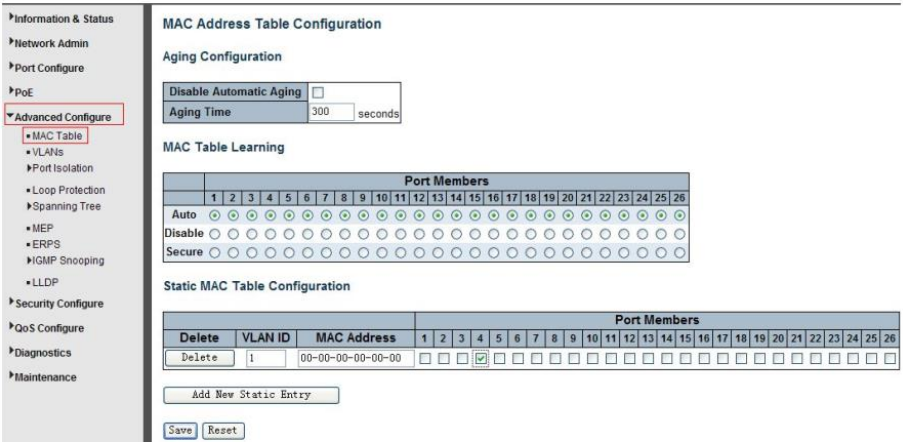
Priority	Поле определяет приоритет порта.
Auto Edge	Отметьте, чтобы превратить порт в Auto Edge
Restricted Role	Отметьте, чтобы превратить порт в Restricted Role
Restricted TCN	Отметьте, чтобы превратить порт в Restricted TCN
BPDU Guide	Отметьте, чтобы активировать BPDU Guide. Когда порт получает BPDU 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.

8.5.4 MAC Address Table (Таблица MAC адресов)

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

Advanced Configure > MAC Table



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 зпоминает 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.

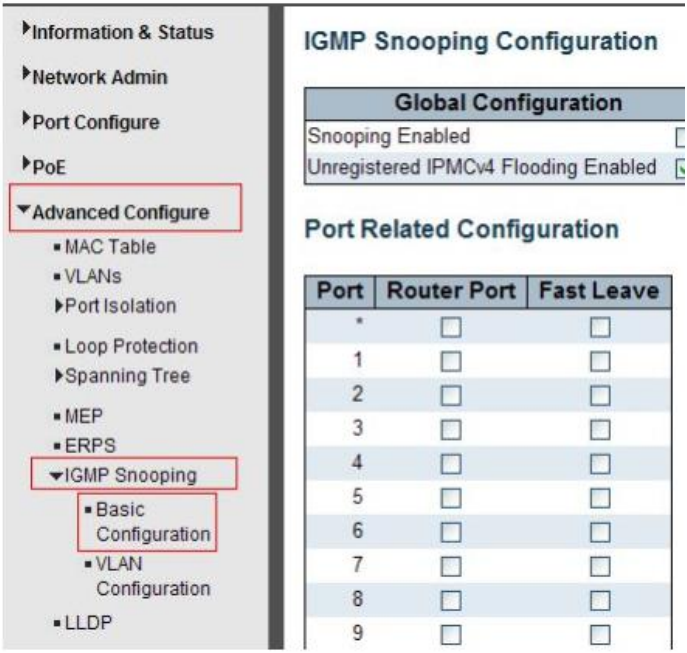
8.5.5 IGMP Snooping

Internet Group Management Protocol (IGMP) – позволяет хостами маршрутизаторам обмениваться информацией о multicast группах. 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.

8.5.5.1 Basic Information

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

Advanced Configure > IGMP Snooping > Basic Configuration



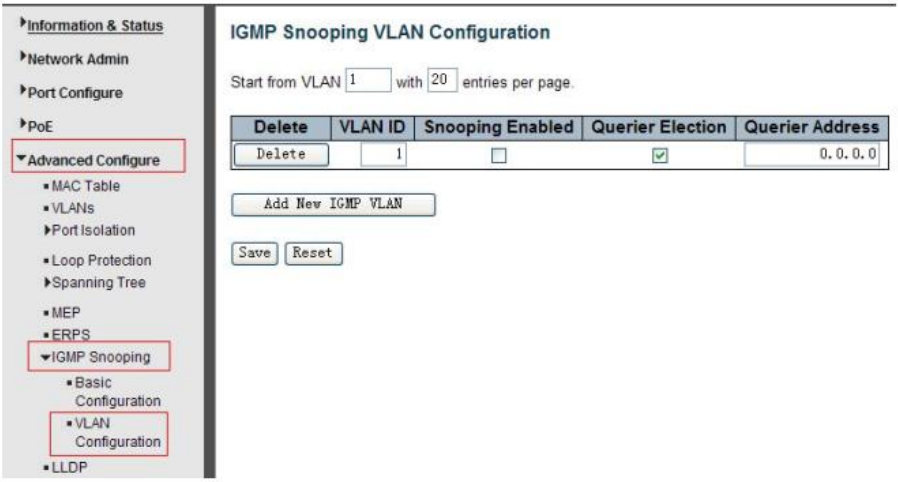
Snooping Enabled	Вкл/выкл функции IGMP Snooping. Значение по умолчанию – отключено (disabled)
Unregistred IPMCv4 Flooding Enabled	Отметьте чекбокс, чтобы включить функцию Unregistred IPMCv4 Flooding.
Router Port	Поле определяет, какие порты будут отмечены, как router порты. Router порт в коммутаторе 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.

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

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

Advanced Configure > IGMP Snooping > VLAN Configuration



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.

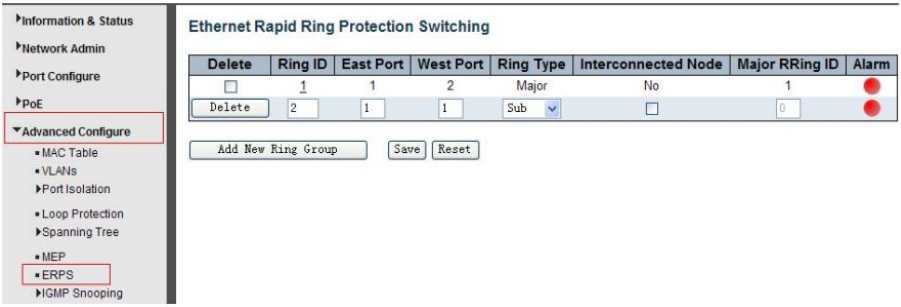
8.5.6 ERPS (Протокол ERPS)

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

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

Раздел с настройками ERPS находится по адресу:

Advanced Configure > ERPS

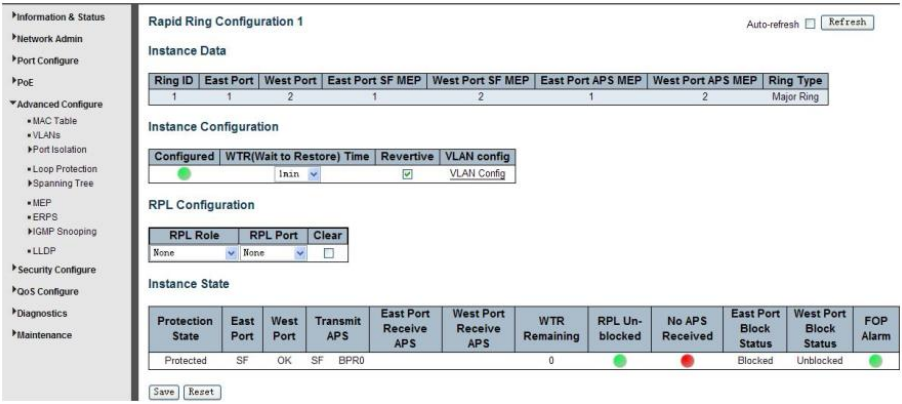


Ring ID	Идентификатор ERPS Ring
East Port	Номер порта, который участвует в Ring Protection
West Port	Номер другого порта, который участвует в Ring Protection
Ring Type	Доступен выбор Major Ring – основное кольцо Sub Ring – вспомогательное кольцо По умолчанию тип кольца – Major Ring.

Intercorrected Node	В топологии «мультикольцо», Intercorrected 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:



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:

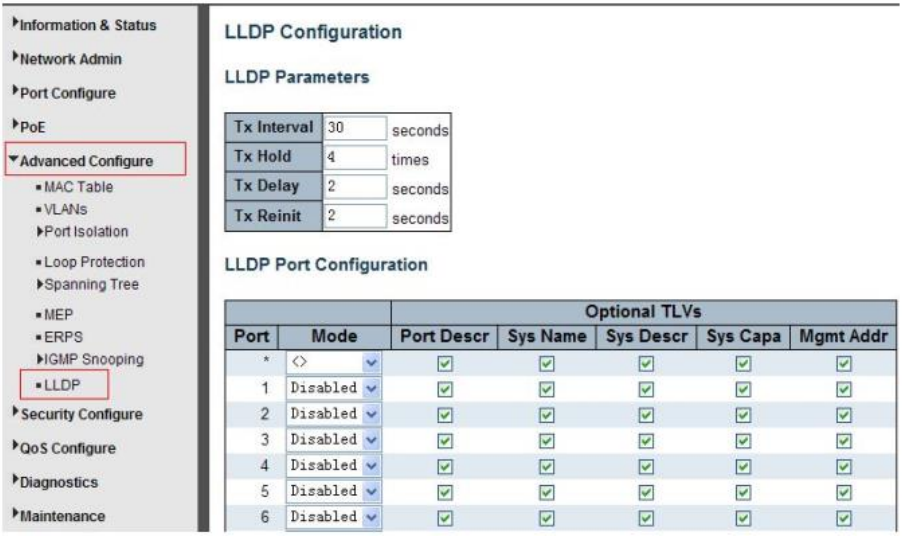
Нажмите Add New Entry, чтобы добавить новую запись.
Нажмите Save, чтобы сохранить настройки.

8.5.7 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



LLDP Parameters	В данном поле есть возможность настроить текущие LLDP настройки для порта: TX interval Tx Hold Tx Delay Tx Remit

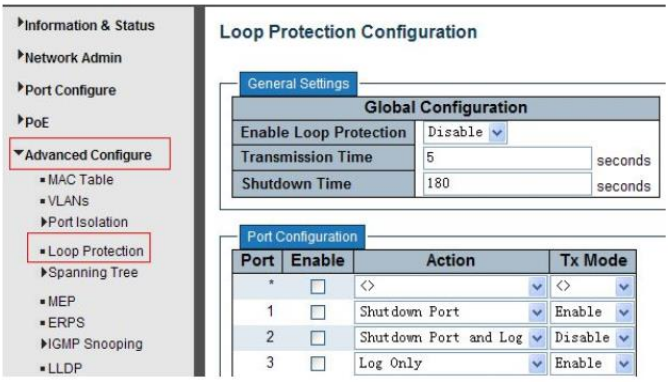
Mode	Выбор LLDP сообщений для режима отправки и приема. Tx Only Rx Only Enabled Disabled
Optional TLVs	Поле отвечающее за настройку информации, которая включена в TLV поле публикуемых сообщений. Port Descr Sys Name Sys Descr Sys Capa Mgmt Addr

Нажмите Save, чтобы сохранить настройки.

8.5.8 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



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 Режима передачи Tx

Нажмите Save, чтобы сохранить настройки.

8.6 QoS (Приоритезация трафика)

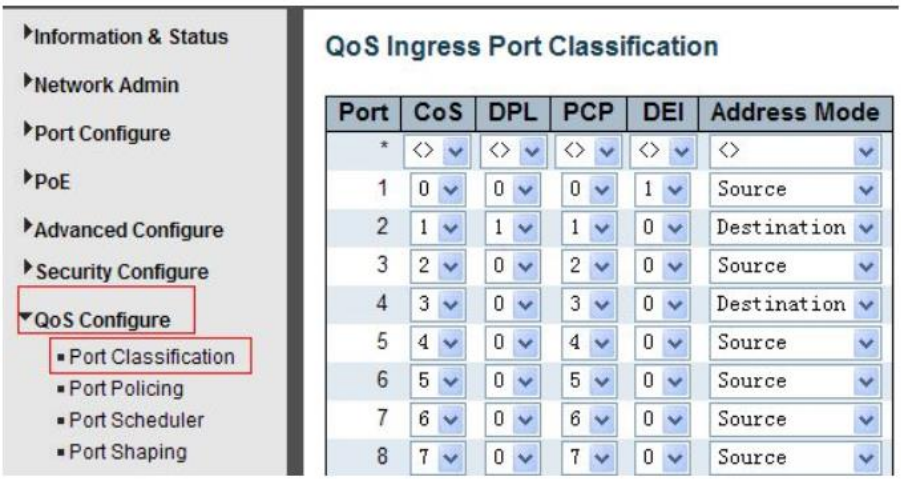
Quality of Service (QoS) – технология предоставления различным классам трафика различных приоритетов в обслуживании.

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.

8.6.1 QoS Port Classification (Классификация портов с помощью QoS)

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

QoS Configure > Port Classification



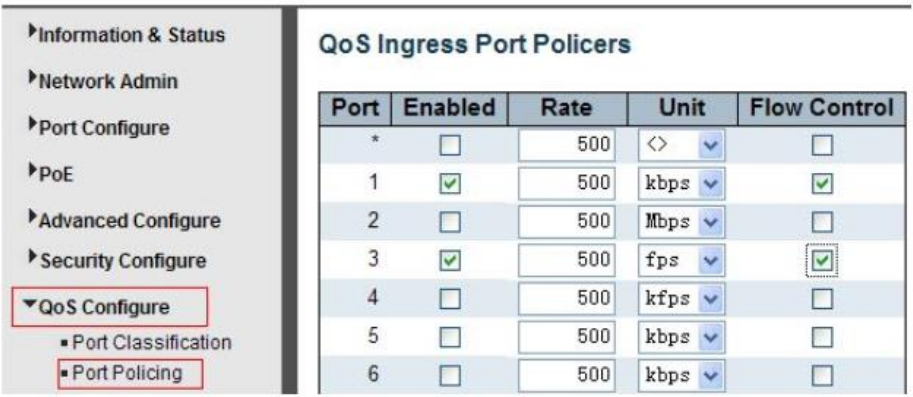
CoS	Поле отвечает класс обслуживания. Диапазон от 0 до 7, где 0 (самый низкий приоритет), а 7 (самый высокий приоритет). *Примечание: По умолчанию значение CoS изменяется динамически.*
DPL	Поле отвечает за Drop Precedence Level
PCP	Поле отвечает за значение PCP. Все пакеты классифицируются на основе 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.

8.6.2 Port Policing (Функция ограничения скорости на портах)

Данная функция находится в следующем разделе WEB интерфейса коммутатора:

QoS Configure > Port Policing



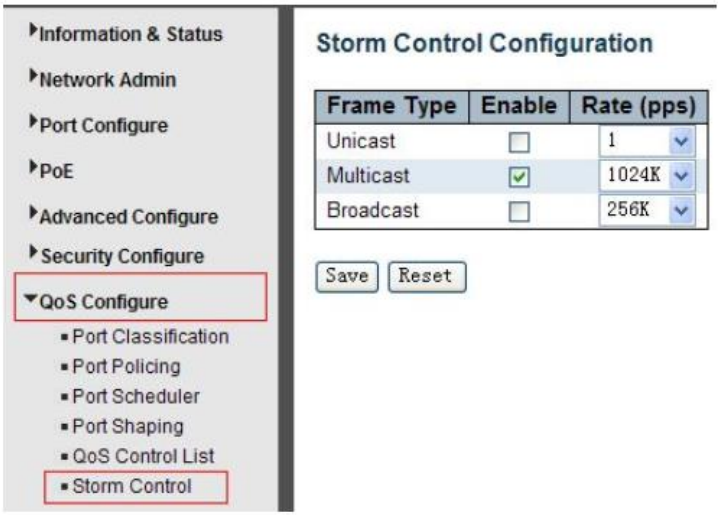
Enabled	Отметьте чекбокс, чтобы активировать функцию Port Policing для порта
Rate	Значение по умолчанию 500. Диапазон возможных значений 100-1000000, если в поле Unit выбрано kbps (Кбит/с) или fps (пакетов в сек) и 1-3300, если в поле Unit выбрано mbps (Мбит/с) или kfps (тысяч пакетов/сек)
Unit	Значение 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.

8.6.3 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.

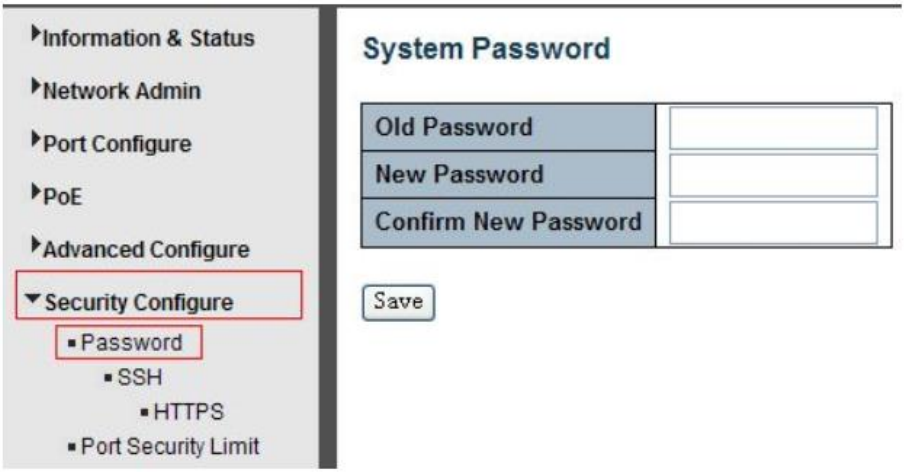
Нажмите Save, чтобы сохранить настройки.

8.7 Security Configure (Настройки безопасности)

8.7.1 Password (Пароль)

Пароль системы можно поменять в данном разделе WEB интерфейса коммутатора:

Security Configure > Password



Нажмите Save, чтобы сохранить настройки.

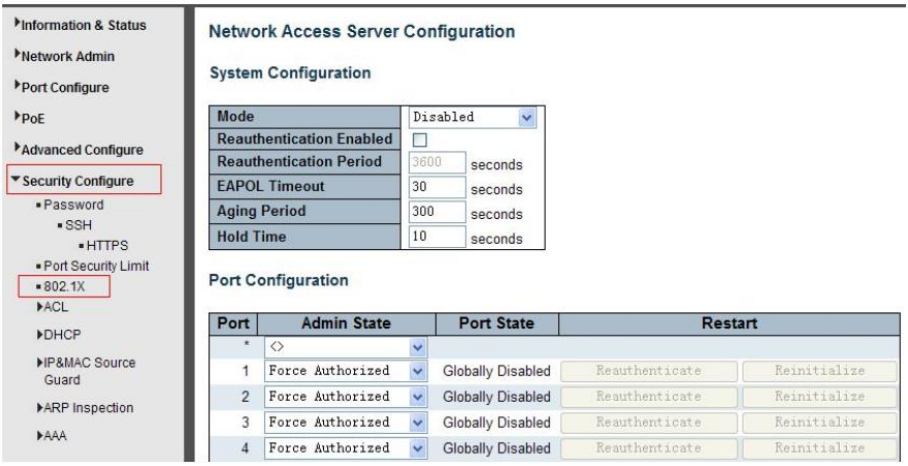
8.7.2 802.1X

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



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.

8.7.3 DHCP Snooping (Защита от атак с использованием DHCP)

8.7.3.1 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):

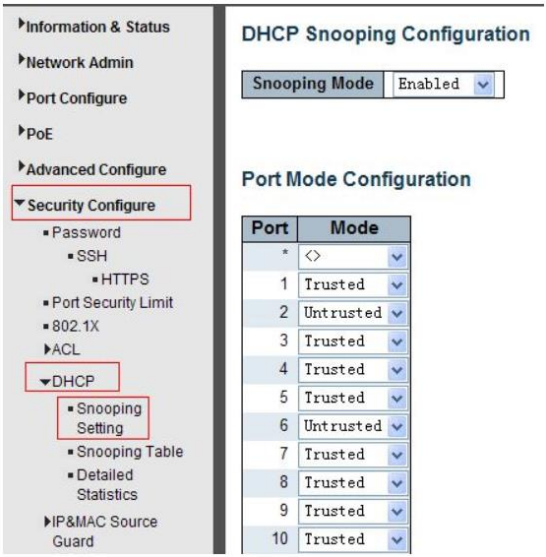
- ✓ Ненадёжные (Untrusted) — порты, к которым подключены клиенты. DHCP-ответы, приходящие с этих портов отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database).

- ✓ Доверенные (Trusted) — порты коммутатора, к которым подключен другой коммутатор или DHCP-сервер. DHCP-пакеты, полученные с доверенных портов не отбрасываются.

8.7.3.2 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.

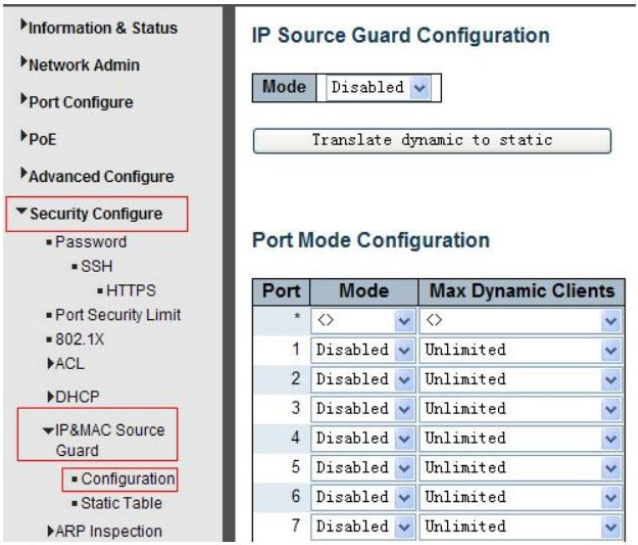
8.7.4 IP&MAC Source Guard

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.

8.7.4.1 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.

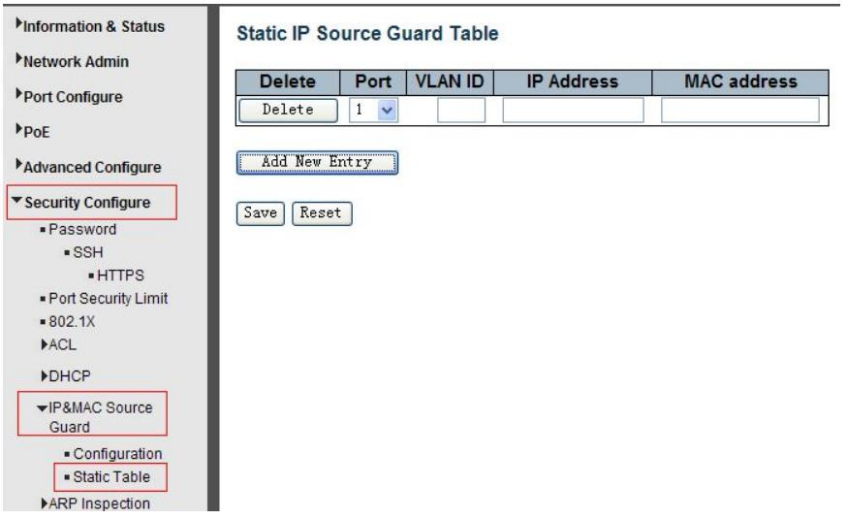
Max Dynamic Clients	Нажмите на выпадающее меню, чтобы выбрать максимальное количество динамических клиентов. Доступные значения: Unlimited, 0, 1, 2.

Нажмите Save, чтобы сохранить настройки.

8.7.4.2 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



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.

8.7.5 ARP Inspection (Проверка ARP пакетов)

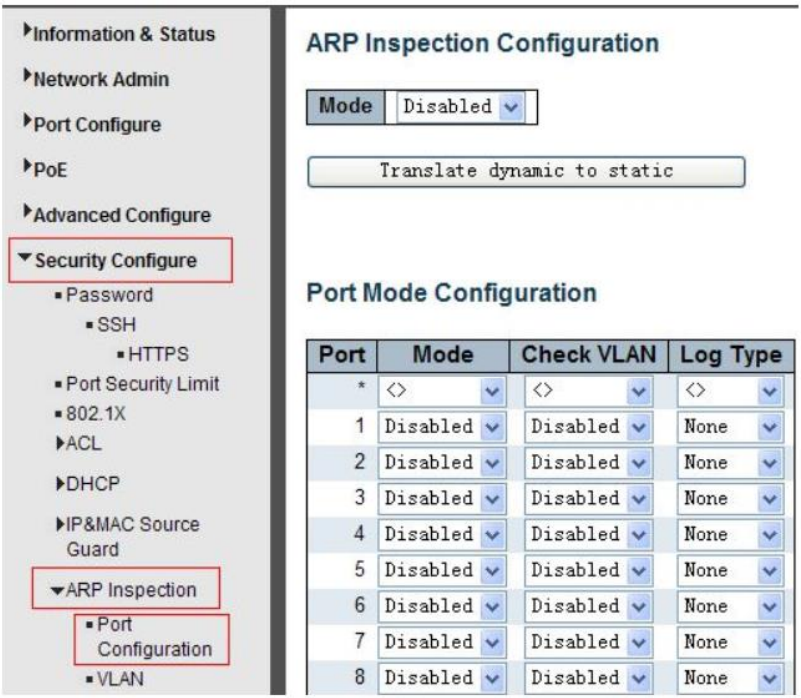
Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Например, атаки ARP-spoofing, позволяющей перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена.

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

8.7.5.1 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



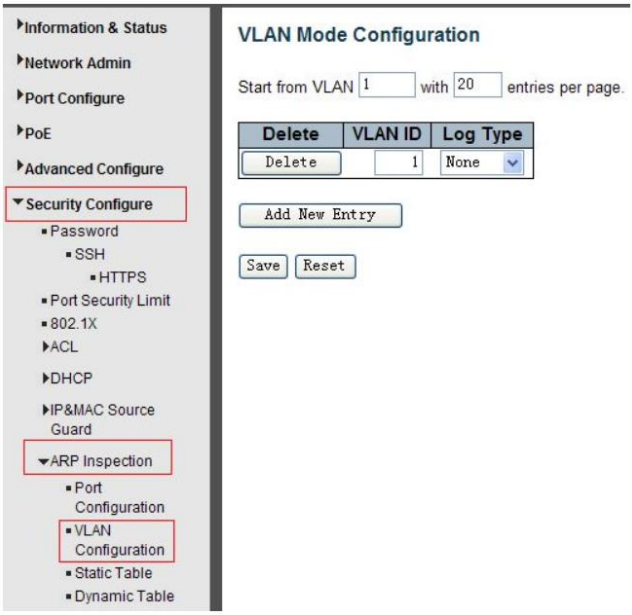
Global Mode	Нажмите на выпадающее меню, чтобы вкл/выкл ARP Inspection глобально.
Port Mode	Нажмите на выпадающее меню, чтобы вкл/выкл ARP Inspection для портов.
Check VLAN	Если необходимо включить ARP Inspection для VLAN, активируйте (enable) функцию в выпадающем меню «Check VLAN». Значение по умолчанию – 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.

8.7.5.2 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



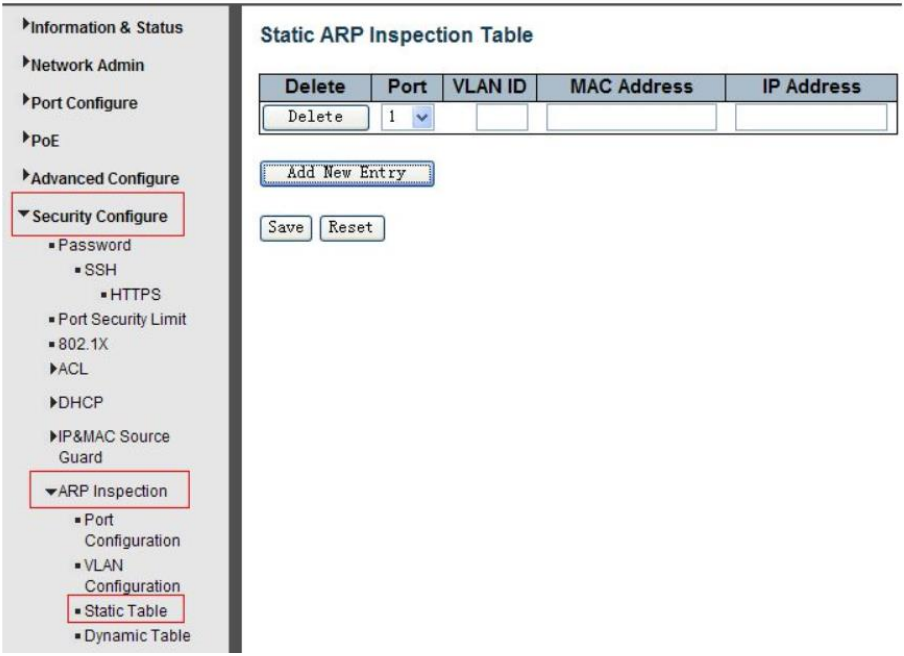
VLAN ID	Отображает VLAN ID для текущей VLAN
Log Type	None – журнал ARP Inspection не ведется. Deny – журнал ведется для заблокированных записей. Permit – журнал ведется для разрешенных записей. ALL – журнал ведется для всех типов записей.

Нажмите Save, чтобы сохранить настройки.

8.7.5.3 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



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.

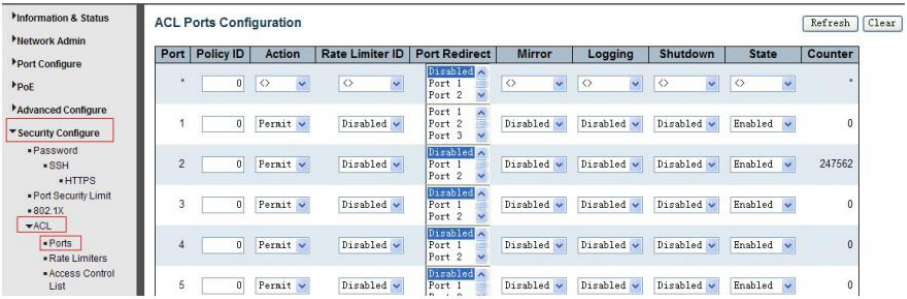
8.7.6 ACL (Правила контроля доступа)

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).

8.7.6.1 ACL Port Configure (Настройка ACL для портов)

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

Security Configure > ACL > Ports



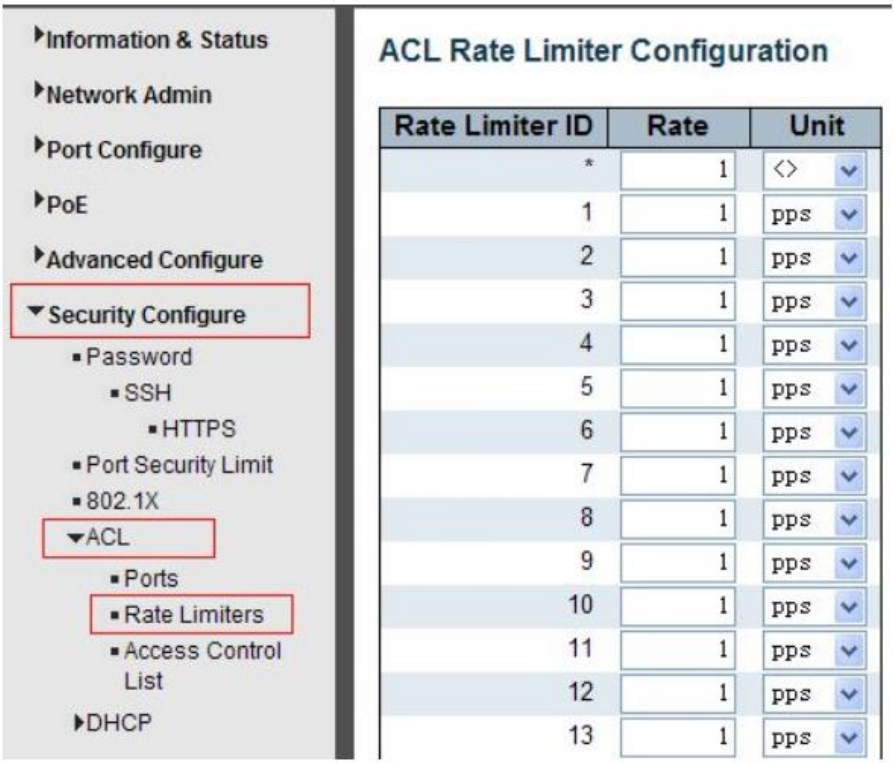
Action	Permit – разрешает выбранному порту пропускать данные Deny – запрещает выбранному порту пропускать данные
Rate Limiter ID	Ограничитель пропускной способности портов. Настройки находятся в соответствующем разделе.
Port Redirect	Выбор порта, пакеты с которого будут перенаправлены. Значение по умолчанию – 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. *Примечание: данная функция работает, только если размер пакета меньше 1518 (без VLAN тэгов)*
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.

8.7.6.2 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

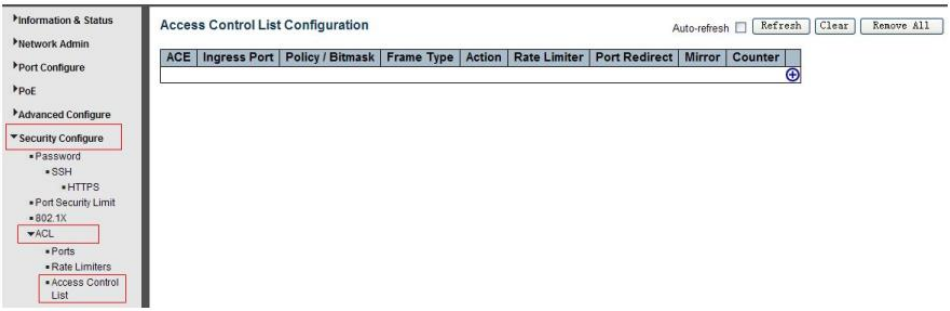


Нажмите Save, чтобы сохранить настройки.

8.7.6.3 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 «+»

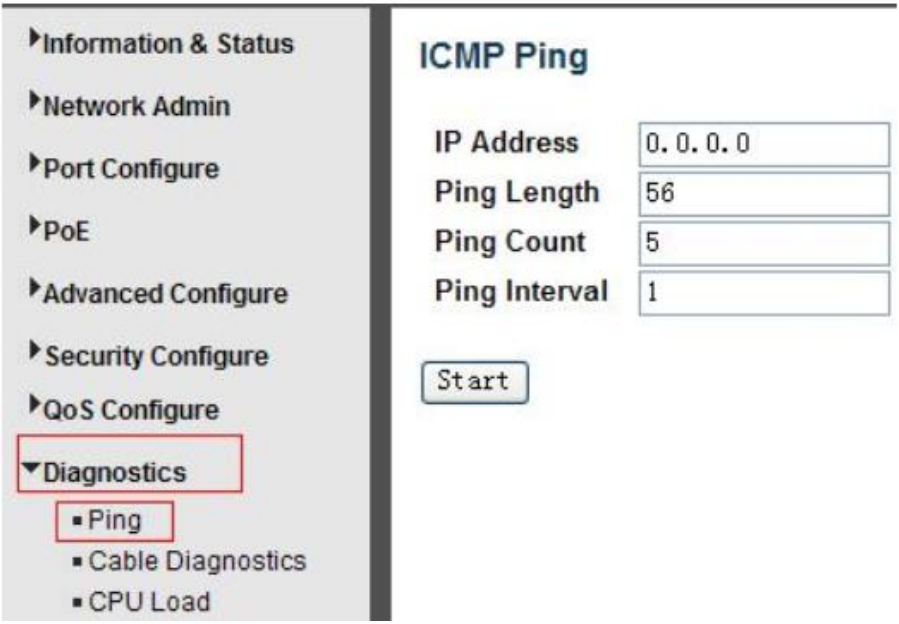
8.8 Diagnostics (Инструменты диагностики и мониторинга)

8.8.1 Ping Test (Тестирование соединия 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



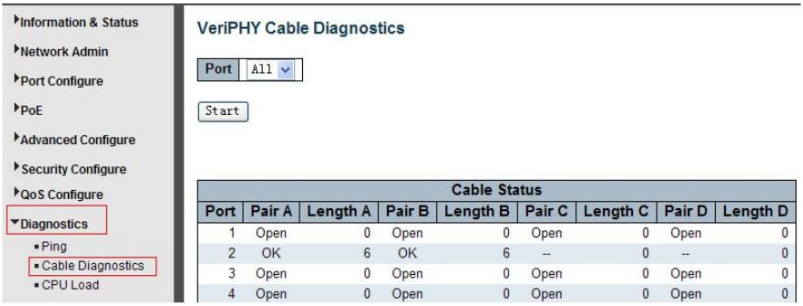
IP Address	IP адрес удаленного адресата, который необходимо проверить
Ping Length	Число от 1 до 1452. Значение по умолчанию – 56
Ping Count	Количество отправляемых PING запросов. От 1 до 60.
Ping Interval	Интервал между отправкой PING запросов.

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

8.8.2 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



Нажмите кнопку «Start», чтобы приступить к диагностике.

8.8.3 CPU Load (Загрузка CPU коммутатора)

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

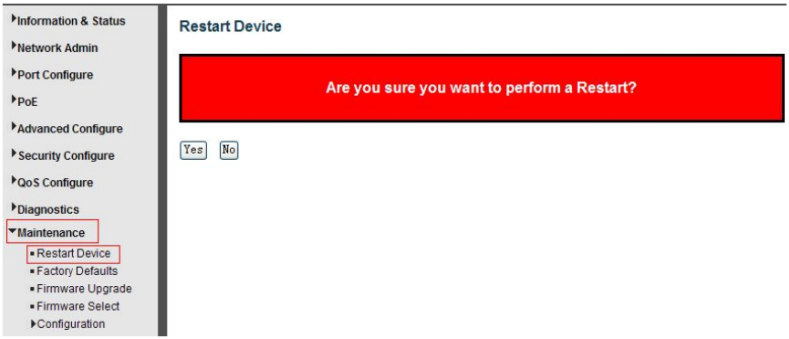
Diagnostics > CPU Load

8.9 Maintenance (Обслуживание)

8.9.1 Restart Device (Перезагрузка коммутатора)

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

Maintenance > Restart Device



Yes – перезагрузка коммутатора

8.9.2 Factory Defaults (Возврат к заводским настройкам)

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

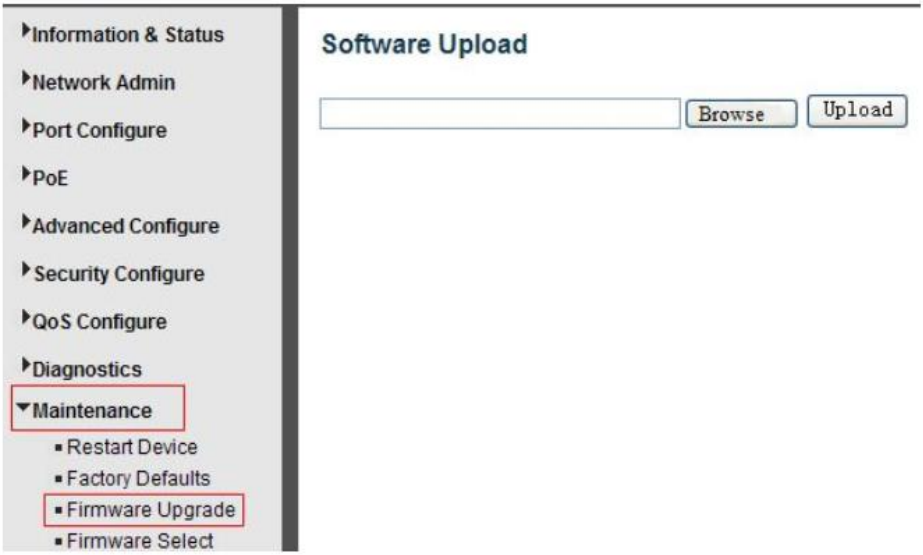
Maintenance > Factory Defaults

Yes – сброс настроек коммутатора к заводским.

8.9.3 Firmware Upgrade (Обновление прошивки)

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

Maintenance > Firmware Upgrade



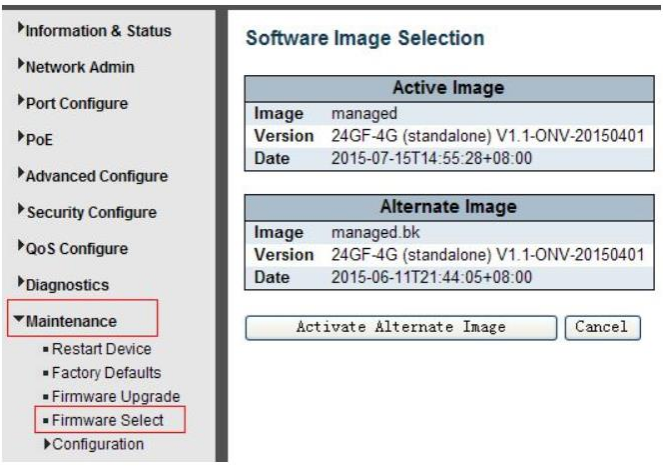
Нажмите Browse, выберите файл с прошивкой. Нажмите Upload, чтобы загрузить прошивку в коммутатор.

8.9.4 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»

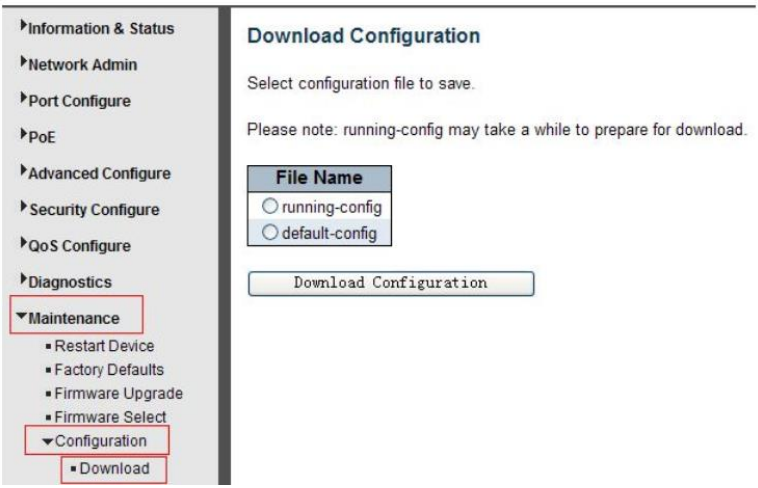


8.9.5 Configuration (Текущая конфигурация)

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

8.9.5.1 Download (Сохранение файла с текущей конфигурацией коммутатора)

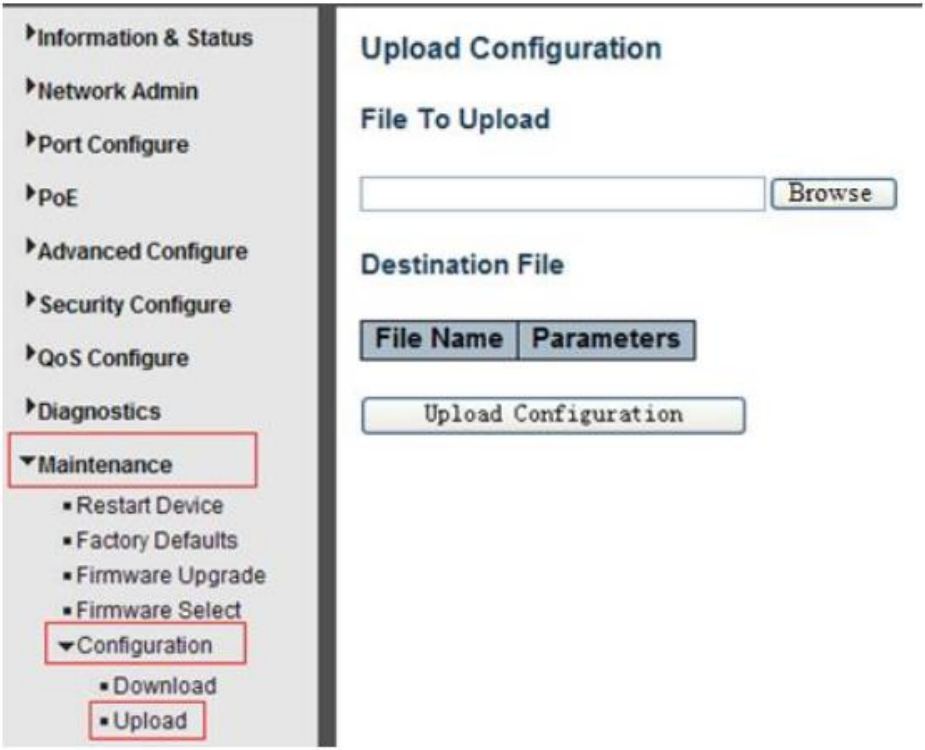
Maintenance > Configuration > Download



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

8.9.5.2 Upload Configuration (Загрузка файла с конфигурацией)

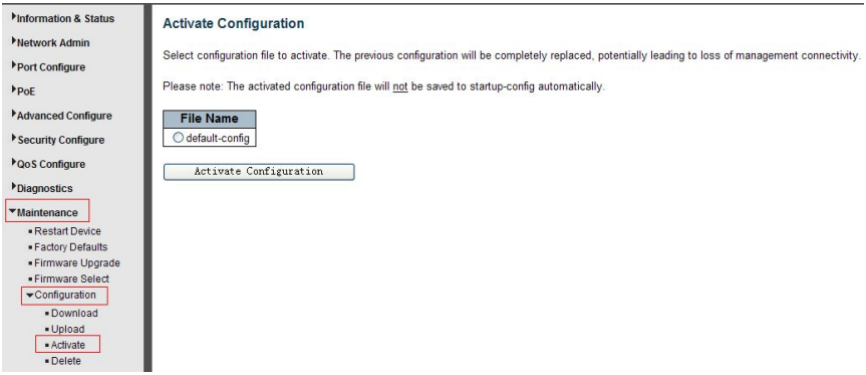
Maintenance > Configuration > Upload



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

8.9.5.3 Activate Configuration (Активация файла с конфигурацией)

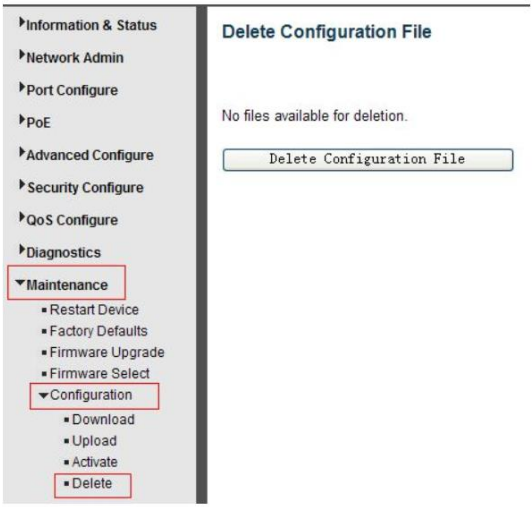
Maintenance > Configuration > Activate



Для активации нажмите кнопку «Activate Configuration»

8.9.5.4 Delete Configuration File (Удаление файла с кофигурацией)

Maintenance > Configuration > Delete



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

9. Технические характеристики*

Модель	SW-70802/IL	SW-70804/IL
Общее кол-во портов	10	12
Кол-во портов FE	-	
Кол-во портов FE	-	
Кол-во портов GE	8	
Кол-во портов GE (не Combo порты)	-	
Кол-во портов Combo GE (RJ45+SFP)	-	
Кол-во портов SFP (не Combo порты)	2 x 1000 Мбит/с	4 x 1000 Мбит/с
Встроенные оптические порты	-	
Топологии подключения	Звезда, каскад, кольцо	
Буфер пакетов	4 МБ	
Таблицы MAC-адресов	8 К	
Пропускная способность коммутационной матрицы (Switching fabric)	20 Гбит/с	24 Гбит/с
Скорость обслуживания пакетов (Forwarding rate)	1000Mbps port – 1,488,000 пакетов/с 100Mbps port - 148,800 пакетов/с	
Поддержка jumbo frame	9 КБ	
Стандарты и протоколы	• IEEE 802.3 – 10BaseT • IEEE 802.3u – 100BaseTX • IEEE 802.3ab – 1000BaseT • IEEE 802.3z 1000 BaseSX/LX • 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	

Модель	**SW-70802/IL**	**SW-70804/IL**
	• 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	
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)	
Управление	• Управление через Web-интерфейс • CLI • Telnet • SNMP	
Индикаторы	• PWR1, • PWR2, • SYS, • Link • SFP Link	
Реле аварийной сигнализации	-	
Питание	DC 12-55V	

Модель	**SW-70802/IL**	**SW-70804/IL**
Энергопотребление	<15Вт	
Встроенная грозозащита	6 kV	
Охлаждение	Конвекционное (без вентилятора)	
Класс защиты	IP40	
Размеры (ШхВхГ) (мм)	53.5x165x123	
Способ монтажа	на DIN-рейку	
Рабочая температура	-40…+75°C	
Дополнительно	-	

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

10. Гарантия

Гарантия на все оборудование OSNOVO – 60 месяцев 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.