OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Промышленный управляемый (L2+) PoE коммутатор Gigabit Ethernet на 12 портов

SW-80822/ILR



Прежде чем приступать к эксплуатации изделия, внимательно прочтите настоящее руководство

www.osnovo.ru

Содержание

1. Назначение 7
2. Комплектация* 8
3. Особенности оборудования 9
4. Внешний вид и описание элементов 10
4.1 Внешний вид 10
4.2 Описание разъемов и индикаторов коммутатора 11
5. Подключение и монтаж 16
5.1 Схемы подключения 16
5.2 Подключение датчика температуры и влажности 17
5.3 Подключение блоков питания 18
5.4 Подключение системы оповещения 19
5.5 Монтаж на DIN рейку, стену 20
6. Проверка работоспособности системы 22
7. Подготовка перед управлением коммутатором через WEB. 23
8. Подготовка перед управлением коммутатором через порт CONSOLE 26
9. Подготовка перед управлением коммутатором через Telnet/SSH 28
10. Управление через WEB-интерфейс, основные элементы 30
10.1 Структура дерева навигации по группам 30
10.2 Описание кнопок WEB интерфейса 30
10.3 Сообщения об ошибке 31
10.4 Поля для ввода информации или значений 31
10.5 Поля со значениями текущего статуса 32
11. Описание основных групп и элементов WEB интерфейса коммутатора 33
11.1 Главная страница WEB интерфейса 33
11.2 Мониторинг датчиков (Industrial Switch Monitoring) 33
11.3 Конфигурация системы (System Configuration) 37

11.3.1 Общая информация (Basic Information) 37
11.3.2 Serial information (Информация о RS 232/485 порте для управления коммутатором) 38
11.3.3 User Management (Информация о пользователях) 39
11.3.4 Safe management (управление безопасностью) 40
11.3.5 SNTP Configuration (Настройка протокола синхронизации времени) 41
11.3.6 Jumbo Frame Configuration (Выбор размера для Jumbo пакетов) 42
11.3.7 Current Configuration (Просмотр текущей конфигурации) 43
11.3.8 Configuration file (Стартовая конфигурация, сохранение файла с настройками) 44
11.3.9 File Upload (Загрузка файла с настройками в коммутатор) 45
11.3.10 System reset (Перезагрузка коммутатора) 46
11.4 Port configuration (Конфигурирование портов) 47
11.4.1 Common configuration (Базовая конфигурация портов) 47
11.4.2 Port statistics (Статистика работы портов) 48
11.4.3 Flow Control (управление потоком для портов) 49
11.4.4 Broadcast storm control (управление защитой от Broadcast storm) 50
11.4.5 Port Rate Limit (Ограничение пропускной способности на портах) 51
11.4.6 Protected Port (Защита портов) 52
11.4.7 Learn limit (Ограничение максимального количества MAC для работы) 53
11.4.8 Port trunking (Конфигурирование trunk'ов) 54
11.4.9 Mirror (Зеркалирование портов) 55
11.4.10 DDM Information (Информация о подключённых SFP модулях) 56
11.5 MAC binding (привязка MAC адреса) 56

11.5.1 MAC binding configuration (Настройка привязки MAC адресов) 56
11.5.2 MAC Auto Bind (Автоматическая привязка MAC адресов) 57
11.6 MAC Filter (фильтр MAC адресов) 58
11.6.1 MAC Filter Configuration (Настройка фильтра MAC адресов) .. 58
11.6.2 MAC Auto Filter (Автоматический фильтр MAC адресов) 59
11.7 VLAN Configuration (Настройка VLAN) 60
11.7.1 VLAN Information (информация о VLAN) 60
11.7.2 Static VLAN Configuration (Настройка VLAN) 61
11.7.3 VLAN Port Configuration (Конфигурация портов VLAN) 62
11.8 SNMP Configuration (Настройка SNMP протокола управления) 63
11.8.1 Community Name (Общие настройки для SNMP) 63
11.8.2 TRAP Target (Настройка TRAP уведомлений) 64
11.9 ACL Configuration (Настройка Access Control List) 65
11.9.1 Standard IP (Настройка ACL для IP) 65
11.9.2 Extended IP (Расширенная настройка ACL правил для IP) 66
11.9.3 MAC IP (Настройка ACL правил с помощью MAC) 66
11.9.4 MAC ARP (Настройка ACL правил для ARP с помощью MAC адресов) 67
11.9.5 ACL Information (Набор действующих ACL правил) 68
11.9.6 ACL reference configuration (Настройка ACL правил) 68
11.10 QoS Configuration (Настройка предоставления трафика с разным приоритетом) 69
11.10.1 QoS Apply (Настройка приоритетов трафика для портов) 69
11.10.2 QoS Schedule (Настройка расписания применения QoS) 70
11.11 IP Basic Configuration (Базовая настройка IP) 71
11.11.1 IP Address Configuration (Настройка IP адреса коммутатора) 71
11.11.2 ARP Configuration and Display (Настройка протокола ARP и отображение таблицы ARP) 72

11.11.3 Host Static Route Configuration (Настройка таблицы Static маршрутизации) 73
11.12 AAA Configuration (настройка системы аутентификации авторизации и учета событий) 74
11.12.1 Tacacs+ Configuration (настройка Radius системы AAA) 74
11.12.2 Radius Configuration (настройка Radius системы AAA) 75
11.12.3 802.1x Configuration (Настройка параметров системы авторизации и аутентификации по стандарту 802.1x) 76
11.12.4 802.1x Port Configuration (Настройка портов для системы авторизации и аутентификации по стандарту 802.1x) 78
11.12.5 802.1x User Authentication Information (Информация о всех процессах аутентификации по стандарту 802.1x) 79
11.13 MSTP Configuration (Настройка работы протокола MSTP) 79
11.13.1 MSTP Configuration (Основные настройки MSTP) 79
11.13.2 Port Configuration (настройка MSTP на портах) 81
11.13.3 Port Information (Общая информация о конфигурации MSTP) 82
11.14 IGMP Snooping Configuration (Настройка отслеживания IGMP трафика) 83
11.14.1 IGMP Snooping Configuration (Настройки функции IGMP snooping) 83
11.14.2 Multicast Group Information (Общая информация о IGMP) 84
11.15 GMRP Configuration (Настройка работы протокола GMRP) 84
11.15.1 GMRP Global Configuration (Глобальные настройки GMRP) 84
11.15.2 GMRP Ports Configuration (Настройка GMRP на портах) 85
11.15.3 GMRP State machine (Общая информация о GMRP) 86
11.16 EAPS Configuration (Настройка работы протокола EAPS) 87
11.16.1 EAPS Configuration (Основные настройки работы протокола EAPS) 87
11.16.2 EAPS information (Сводная информация о работе протокола EAPS) 88

11.17 RMON Configuration (Настройка работы протокола RMON) 88
11.17.1 Statistics Configuration (Настройка групп статистики для RMON) 88
11.17.2 History Configuration (Настройка групп предыстории для RMON) 89
11.17.3 Alarm Configuration (Настройка групп аварийных сигналов для RMON) 90
11.17.4 Event Configuration (Настройка групп событий для RMON) .. 91
11.18 Cluster configuration (Настройка кластера) 92
11.18.1 NDP Configuration (Настройка работы протокола NDP) 92
11.18.2 NTDP Configuration (Настройка работы протокола NTDP) 93
11.18.3 Cluster Configuration (Настройка кластера) 94
11.19 ERPS Configuration (Настройка ERPS) 96
11.19.1 ERPS Configuration (Настройка протокола ERPS) 96
11.19.2 ERPS Information (Информация о работе ERPS) 97
11.20 Log management (Управление записью логов) 98
11.21 PoE Power Control (Управление параметрами PoE) 99
11.21.1 POE Port Configuration (Настройка параметров PoE для портов) 99
11.21.2 POE Policy Configuration (Настройка подачи PoE по расписанию) 100
11.21.3 PD Query Configuration (Настройка функции автоопределения зависших PoE устройств) 101
12. Изменение IP адреса коммутатора 104
13. Технические характеристики* 104
14. Гарантия 107
Приложение А……..108

1. Назначение

Промышленный управляемый (L2+) PoE коммутатор Gigabit Ethernet на 12 портов SW-80822/ILR предназначен для объединения, сетевых устройств, передачи данных и питания (PoE) к ним.

Коммутатор спроектирован для успешной эксплуатации в промышленных системах. Подходит для установки в уличные станции OSNOVO.

Отличительная черта данной модели – возможность удаленного мониторинга таких показателей, как:

- ✓ температура на внешнем датчике;
- ✓ влажность на внешнем датчике;
- ✓ напряжение питания на основном и резервном блоках питания.

В модели SW-80822/ILR применяются высоконадежные комплектующие и элементная база с расширенным диапазоном рабочих температур, рассчитанная на эксплуатацию в неотапливаемых помещениях. Конструкция коммутатора позволяет осуществлять монтаж на DIN рейку.

Промышленный коммутатор (далее по тексту - коммутатор) оснащен 8 портами Gigabit Ethernet (10/100/1000Base-T) с поддержкой PoE (Power Over Ethernet) к каждому из которых можно подключать сетевые устройства с помощью кабеля витой пары. Порты соответствуют стандартам PoE IEEE 802.3af/at/bt и автоматически определяют подключаемые к ним устройства. Максимальная мощность PoE на порт для 1 и 2 порта составляет 90 Вт, для остальных портов – 30 Вт. Общая выходная мощность (PoE бюджет) находится на уровне 360 Вт.

В коммутаторе SW-80822/ILR помимо основных портов предусмотрены 2 Gigabit Ethernet Uplink порта (RJ-45) и 2 SFP Gigabit Ethernet порта, которые позволяют подключать коммутатор к общей сети медным и оптоволоконным кабелем. Для подключения коммутатора оптоволоконным кабелем требуются SFP модули (не входят в комплект поставки). Рекомендуется использовать промышленные SFP модули с расширенным температурным диапазоном.

Все медные порты (RJ-45) коммутатора поддерживают автоматическое определение MDI/MDIX (Auto Negotiation) на всех портах. Коммутатор распознает тип подключенного сетевого устройства и при

необходимости меняют контакты передачи данных, что позволяет использовать кабели, обжатые любым способом (кроссовые и прямые).

Также, в устройстве реализована грозозащита портов, а также защита от статического электричества (ESD).

Питание коммутатора осуществляется от блоков питания с широким диапазоном выходного напряжения DC 48-57V (DC 36-57V, без PoE). Предусмотрено резервирование питания за счет подключения второго блока питания. Рекомендуется использовать промышленные БП с расширенным температурным диапазоном. Максимальная потребляемая мощность находится на уровне 385 Вт.

Коммутатор имеет возможность гибкой настройки параметров через WEB-интерфейс и имеют множество функций L2+ уровня, таких как VLAN, IGMP snooping, QoS и др.

Кроме того коммутатор поддерживает работу в кольцевой топологии (Ring) с высокой отказоустойчивостью благодаря поддержке протоколов ERPS и EAPS. Данный режим можно задействовать с помощью кнопки на корпусе и через WEB интерфейс.

Предусмотрен режим передачи данных на 250м со скоростью 10 Мбит/с (требуется выставить скорость портов в WEB интерфейсе)

В коммутаторе реализована функция PD Querry (WatchDog) – автоматическое определение и перезапуск зависших PoE устройств

2. Комплектация*

1. Коммутатор SW-80822/ILR – 1шт;
2. Клеммная колодка 6pin – 1шт;
3. Датчик температуры и влажности – 1шт;
4. Комплект креплений – 1шт;
5. Руководство по эксплуатации – 1шт;
6. Паспорт – 1шт;
7. Упаковка – 1шт

3. Особенности оборудования

- ✓ Возможность удаленного мониторинга таких показателей, как:
  - Температура на внешнем датчике;
  - Влажность на внешнем датчике;
  - Напряжение питания на основном и резервном блоках питания.
- 8 GE PoE портов, 2 GE Uplink порта и 2 GE SFP Uplink порта обеспечивают гибкость подключения;
- Мощность PoE до 90Вт (1, 2 порты). Поддержка стандартов PoE IEEE 802.3 af/at/bt;
- Коммутатор предназначен для организации сети в условиях эксплуатации в промышленных неотапливаемых помещениях;
- Подходит для установки в уличные станции OSNOVO;
- Расширенный диапазон рабочих температур: -40… +80 °C;
- Встроенная грозозащита и ESD защита медных портов;
- Расширенный диапазон входного напряжения: DC12-57V;
- Управление через WEB интерфейс;
- Поддержка функций L2 (VLAN,QOS,LACP,LLDP,IGMP snooping);
- Поддержка кольцевой топологии подключения (ERPS, EAPS, STP, RSTP).
- Режим передачи данных на 250м (10 Мбит/с).

4. Внешний вид и описание элементов

4.1 Внешний вид



Рис. 1 Коммутатор SW-80822/ILR, внешний вид



Рис. 2 Датчик температуры и влажности

4.2 Описание разъемов и индикаторов коммутатора

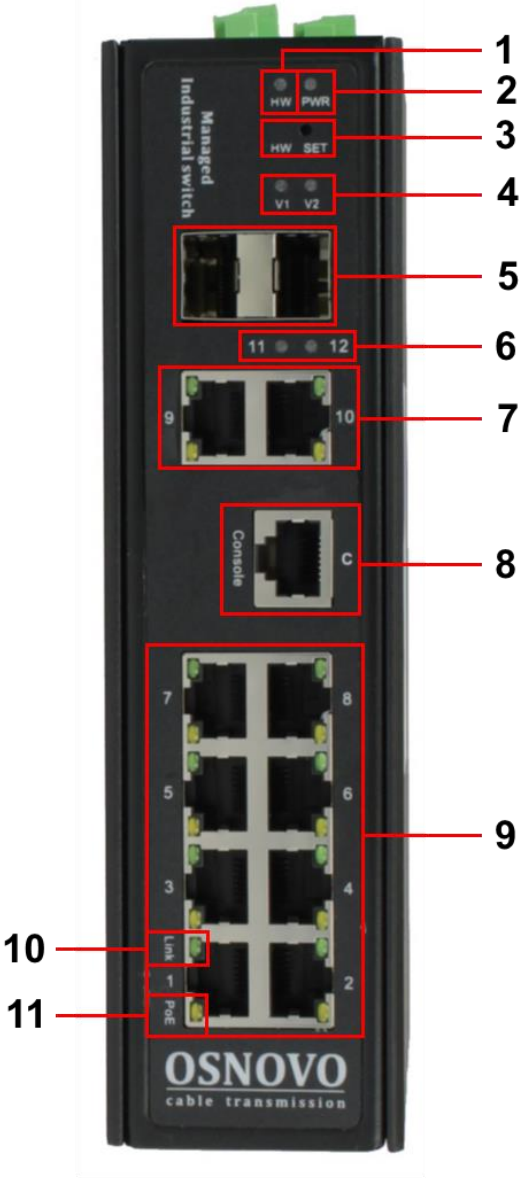


Рис.3 Коммутатор SW-80822/ILR, разъемы, кнопки и индикаторы на передней панели

Таб. 1 Коммутатор SW-80822/ILR, назначение разъемов кнопок и индикаторов на передней панели

№ п/п	Обозначение	Назначение
1	HW	LED индикатор режима работы коммутатора «Кольцо». Горит зеленым – коммутатор работает по топологии «кольцо». Кольцо сформировано. Не горит – режим «кольцо» отключен.
2	PWR	LED-индикатор работы коммутатора Горит зеленым в течение 30 сек – коммутатор загружается Горит зеленым более 30 сек – коммутатор не смог загрузиться (системная ошибка) Не горит – коммутатор не исправен или нет питания Мигает зеленым 1 раз / сек – коммутатор работает в штатном режиме.
3	HW SET	Кнопка для активации режима работы коммутатора по кольцевой топологии
4	V1 V2	V1. LED-индикатор подключения основного БП (DC 12-57V) Горит зеленым – питание подается. Не горит – питание на входе отсутствует. Мигает с частотой 1/4 сек – питание на входе либо ниже либо выше требуемого. Мигает с частотой 1 сек – питание в резерве V2. LED-индикатор подключения резервного БП (DC 12-57V) Горит зеленым – питание подается. Не горит – питание на входе отсутствует. Мигает с частотой 1/4 сек – питание на входе либо ниже либо выше требуемого. Мигает с частотой 1 сек – питание в резерве

№ п/п	Обозначение	Назначение
5	11, 12	SFP порты Используются для подключения коммутатора к другим сетевым устройствам с помощью оптоволоконного кабеля и SFP модулей (не входят в комплект поставки)
6	11, 12	LED индикаторы активности SFP портов Горит, мигает зеленым – установлено соединение по оптике. Идет передача данных Не горит – проверьте подключение SFP модулей и качество подключения оптоволоконного кабеля
7	9-10	Разъемы RJ-45 Предназначены для подключения коммутатора к другим сетевым устройствам с помощью медного кабеля витой пары. Желтый LED индикатор горит – скорость передачи данных 1 Гбит/с. Не горит – скорость передачи данных 10/100 Мбит/с Зеленый LED индикатор горит – установлено соединение, идет передача данных. Не горит – соединение не установлено, проверьте подключение кабеля витой пары.
8	Console C	Разъем RJ-45. Предназначен для управления коммутатором через RS-232 (конфигурирование, обновление прошивки и тд. посредством CLI команд)
9	1 2 3 4 5 6 7 8	Разъемы RJ-45 с 1 по 8й Предназначены для подключения сетевых устройств (в том числе с PoE) на скорости 10/100/1000 Мбит/с 1,2 порты обеспечивают до 90Вт PoE 802.3bt 3-8 порты обеспечивают 30Вт PoE 802.3af/at

№ п/п	Обозначение	Назначение
10	Link	LED индикатор сетевой активности портов 1-8 Горит/мигает зеленым – соединение с портом установлено. Идет передача данных Не горит – нет соединения. Проверьте подключение сетевого кабеля, проверьте работоспособность подключаемого к порту устройства
11	PoE	LED индикатор PoE для портов 1-8 Горит желтым – подключено PoE устройство, PoE подается Не горит – подключено устройство без поддержки PoE

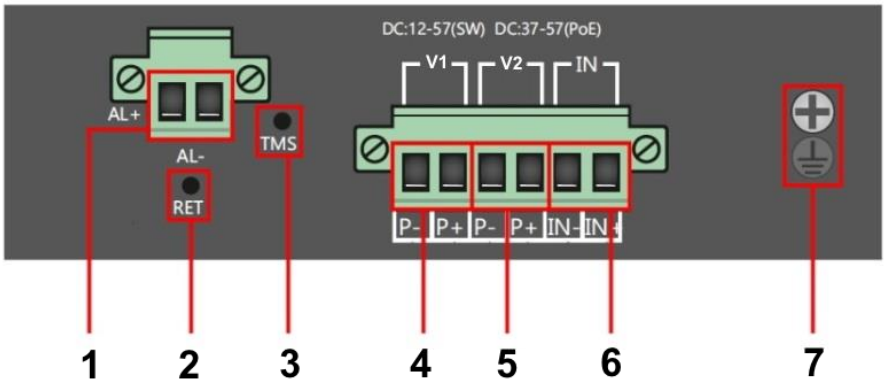


Рис.4 Коммутатор SW-80822/ILR, разъемы на верхней панели

Таб. 2 Коммутатор SW-80822/ILR, назначение разъемов на верхней панели

№ п/п	Обозначение	Назначение
1	AL+ AL-	Клеммная колодка 2-pin выхода Alarm (реле типа «сухой контакт» стр. 36).
2	RET	Кнопка для сброса коммутатора к заводским настройкам
3	TMS	Разъем TRS 3.5mm Предназначен для подключения комплектного датчика температуры и влажности по интерфейсу 1-Wire
4	V1 P- P+	Часть общей 6-pin клеммной колодки. Используется для подключения основного блока питания с напряжением DC 12-57V P- используется для подключения минусового проводника от БП P+ используется для подключения плюсового проводника от БП
5	V2 P- P+	Часть общей 6-pin клеммной колодки. Используется для подключения резервного блока питания с напряжением DC 48-57V (DC 12-36V без PoE) P- используется для подключения минусового проводника от БП P+ используется для подключения плюсового проводника от БП
6	IN IN- IN+	Часть общей 6-pin клеммной колодки. Используется для подключения контролируемого напряжения.
7		Винтовая клемма Предназначена для заземления корпуса коммутатора.

5. Подключение и монтаж

5.1 Схемы подключения

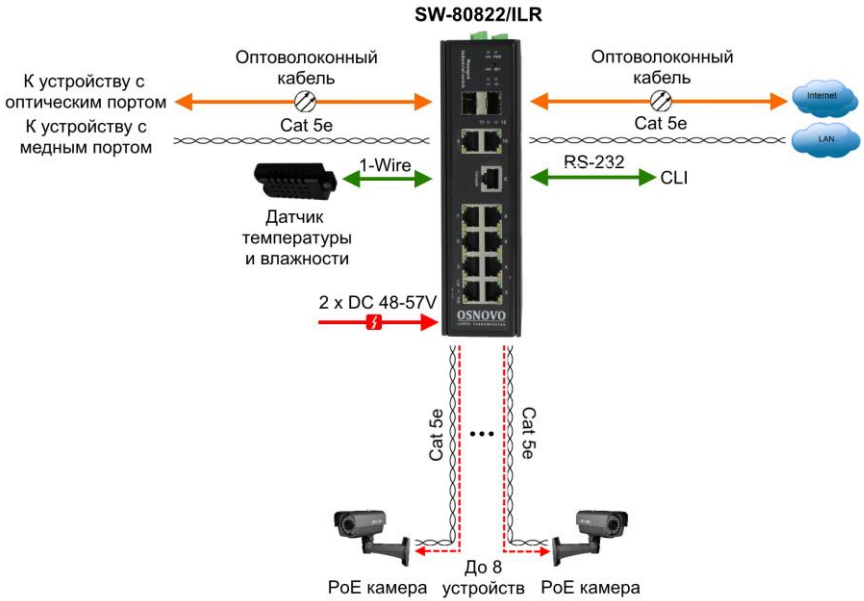


Рис. 5 Типовая схема подключения коммутатора SW-80822/ILR

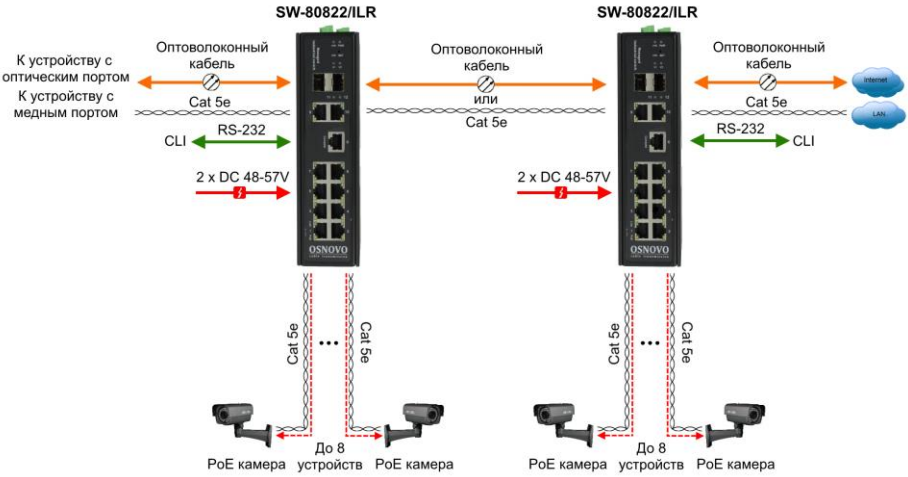


Рис. 6 Схема каскадного подключения коммутатора SW-80822/ILR

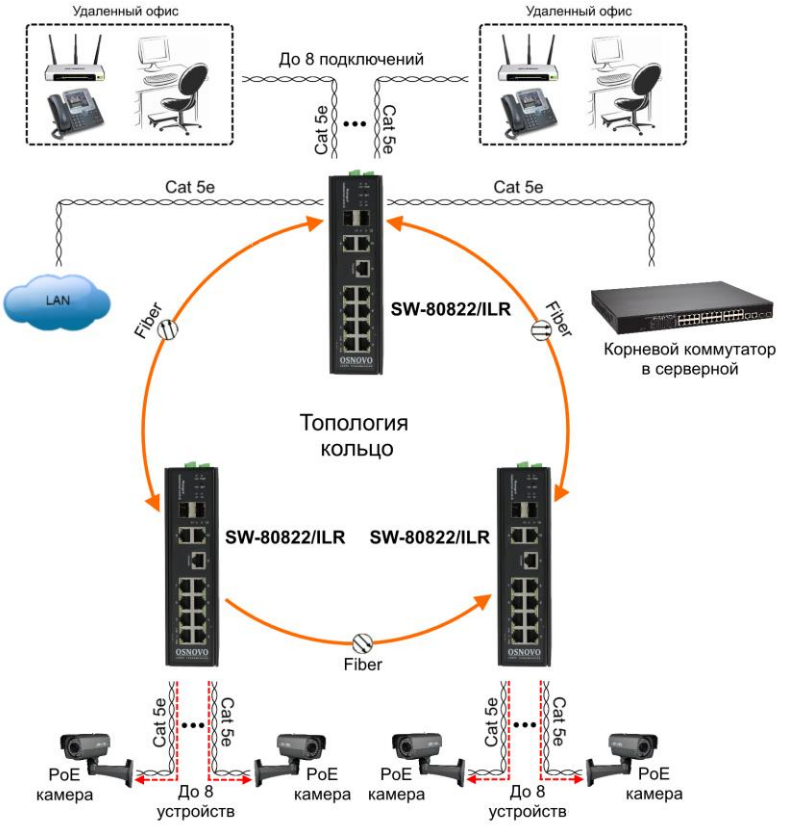


Рис. 7 Схема кольцевого подключения коммутатора SW-80822/ILR

5.2 Подключение датчика температуры и влажности

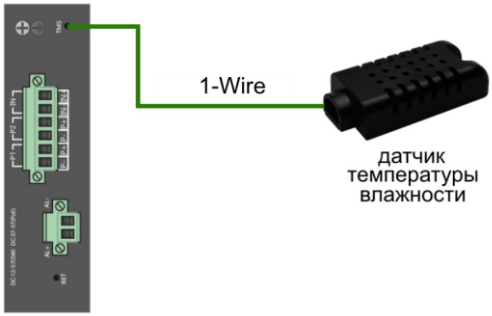


Рис.8 Схема подключения внешнего датчика температуры и влажности

Внешний датчик предназначен для передачи данных о температуре (°C) и влажности (%) окружающей среды. В качестве интерфейса используется цифровой интерфейс на основе протокола 1-Wire. Подключается датчик комплектным кабелем к разъему TRS 3.5mm (miniJack) на коммутаторе (рис. 8).

Для контроля значений температуры и влажности используется соответствующая страница WEB интерфейса (рис. 9). Подробная информация о мониторинге параметров находится в разделе 11.2 «Мониторинг датчиков (Industrial Switch Monitoring)» полной документации на сайте.

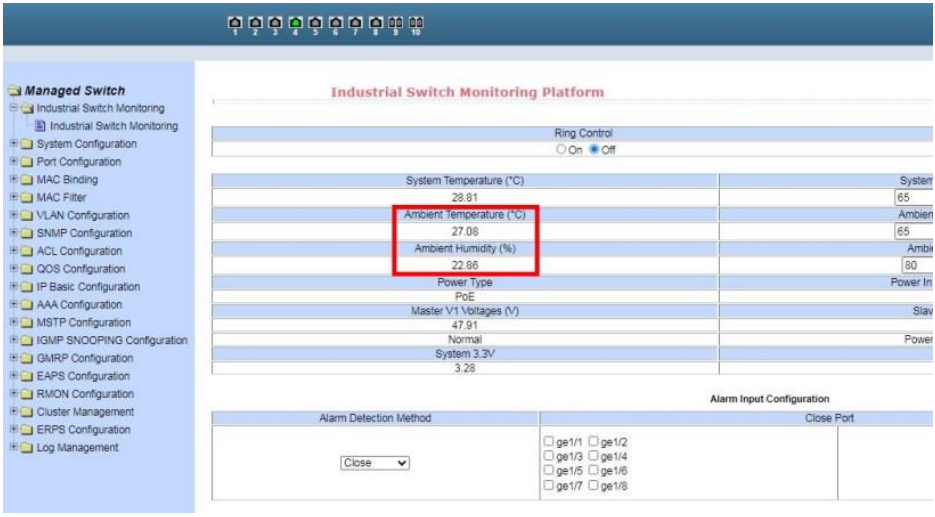


Рис.9 Контроль параметров температуры и влажности окружающей среды через Web-интерфейс коммутатора

5.3 Подключение блоков питания

Коммутатор поддерживает подключение до 2х источников питания – основного и резервного с широким диапазоном выходного напряжения DC 12-57V.

Для активной функции PoE выходное напряжение блоков питания должно находиться в диапазоне DC 48-57V. Мощность БП должна быть не ниже 380-385 Вт. Блоки питания не входят в комплект поставки.

Соблюдайте полярность при подключении!

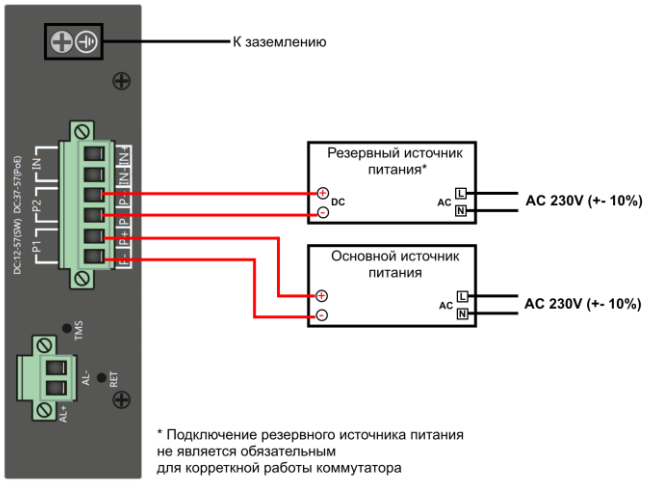


Рис. 10 Подключение блоков питания к коммутатору SW-80822/ILR

5.4 Подключение системы оповещения

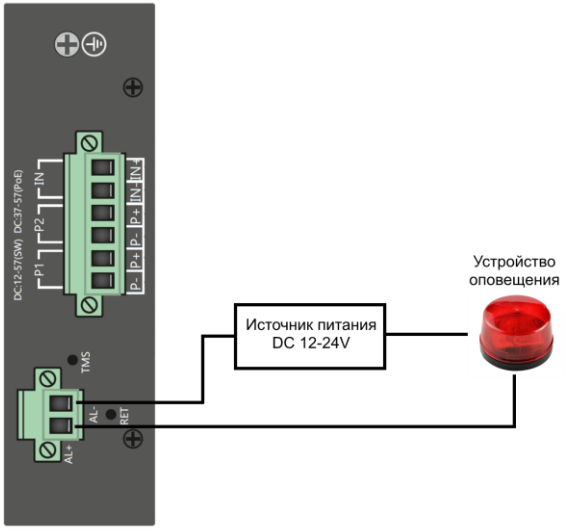


Рис. 11 Подключение устройства оповещения к коммутатору

Максимальная мощность подключаемого устройства оповещения – 24 Вт. Напряжение питания DC <24V.

5.5 Монтаж на DIN рейку, стену

Для монтажа коммутатора на DIN рейку предусмотрено специальное крепление. Порядок монтажа показан ниже на рис. 12

- Наденьте крепление-защелку на DIN рейку (1);
- Нажатием на верхнюю часть коммутатора произведите монтаж коммутатора на DIN рейку до характерного щелчка (2);
- Правильное положение крепления-защелки (3) коммутатора на DIN рейке показано на рис 12

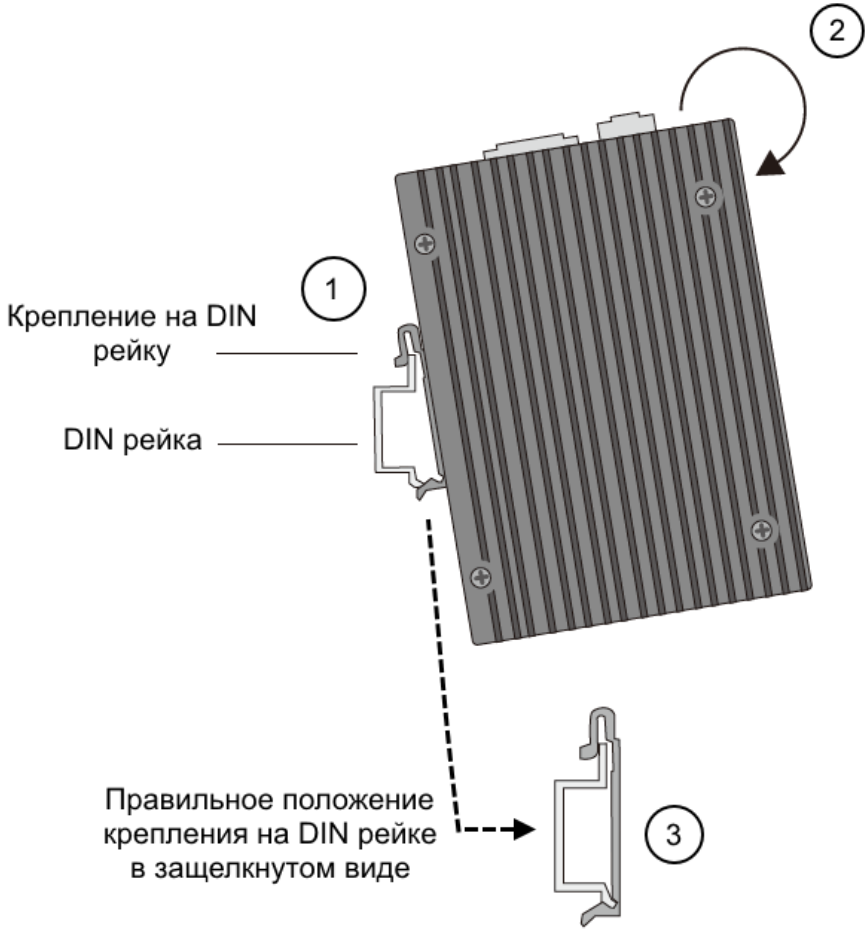


Рис. 12 Порядок монтажа коммутатора на DIN рейку

Для монтажа коммутатора на стену также предусмотрено специальное крепление. Порядок монтажа показан ниже на рис. 13

- Закрепите винтами крепления на стену на задней панели коммутатора (1). Крепление – защелку на DIN рейку следует демонтировать с корпуса;
- Установите коммутатор в месте предполагаемой эксплуатации на стене и закрепите с помощью саморезов (2);

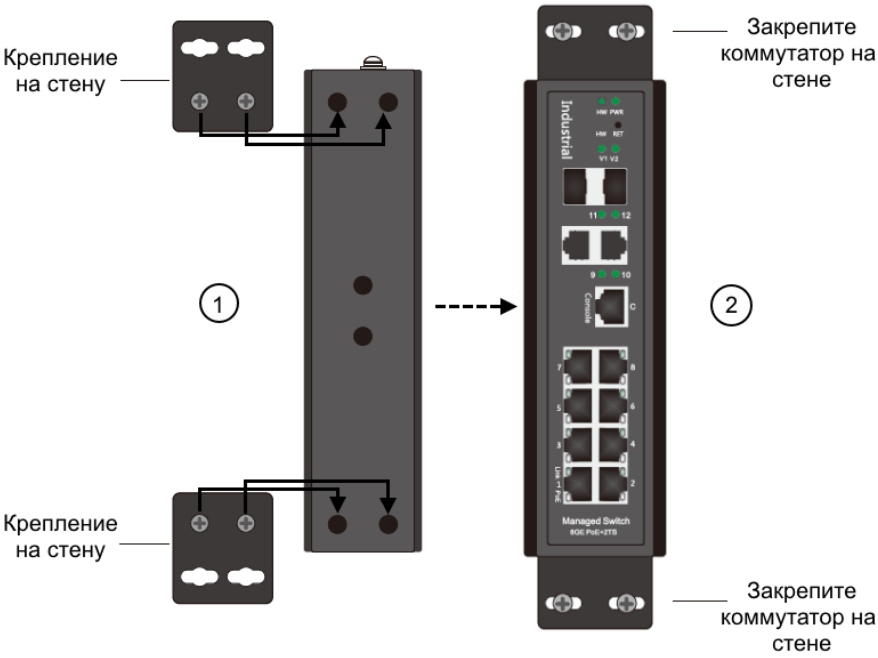


Рис. 13 Порядок монтажа коммутатора на стену

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, 192.168.1.1 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. Это свидетельствует об исправности коммутатора.

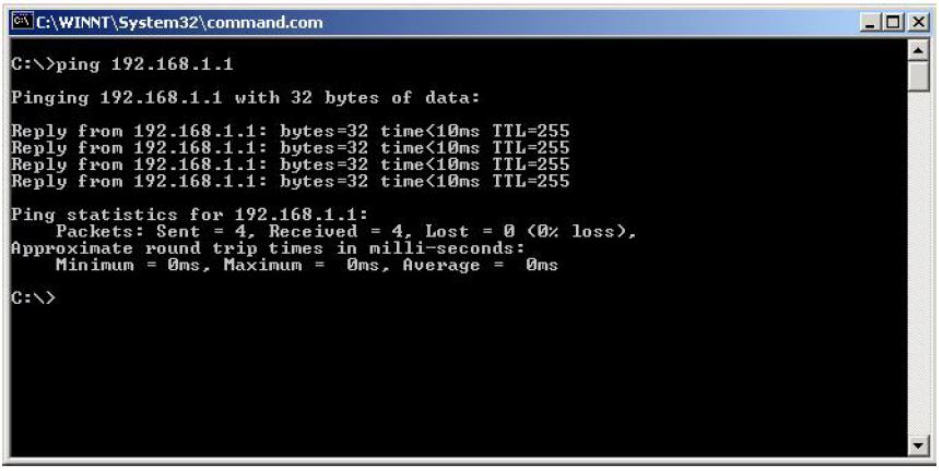


Рис.14 Данные, отображающиеся на экране монитора, после использования команды Ping.

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.

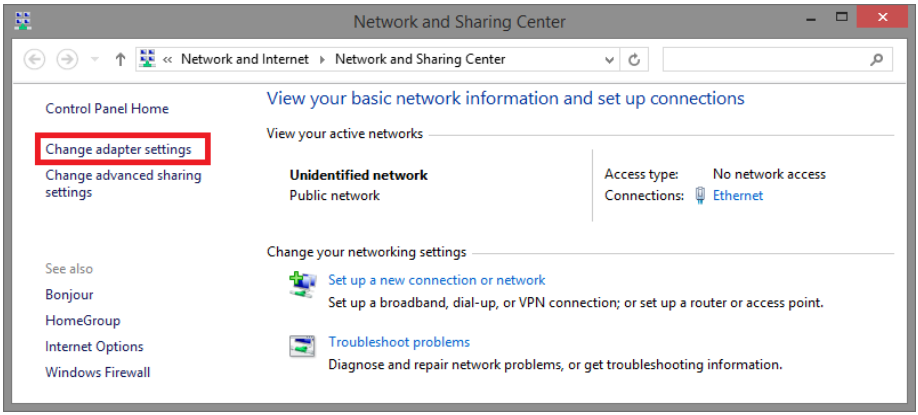
Кроме того, подобные потери могут быть вызваны:

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

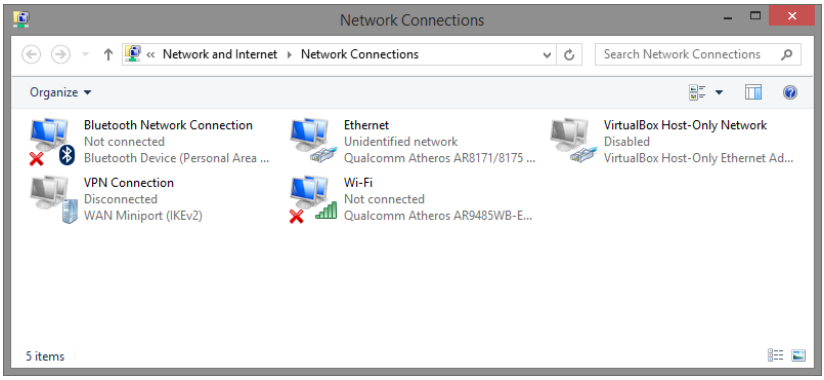
7. Подготовка перед управлением коммутатором через WEB.

Здесь будет показана детальная настройка сети для ПК под управлением Windows 8 (похожий интерфейс у Windows 10, Windows 7 и Windows Vista).

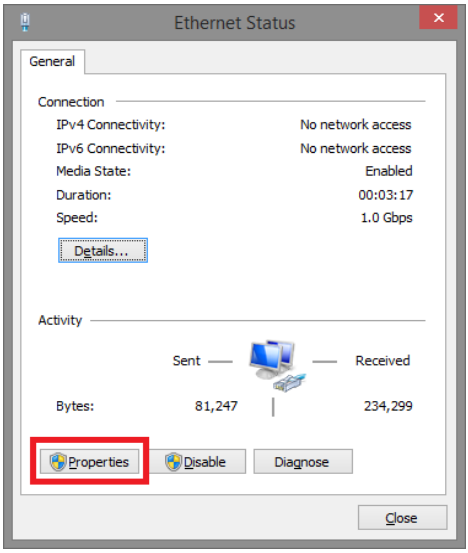
1. Откройте «Центр управления сетями и общим доступом» (Network and Sharing in Control Panel) и нажмите «Изменение параметров адаптера» (Change adapter setting) как на рисунке ниже.



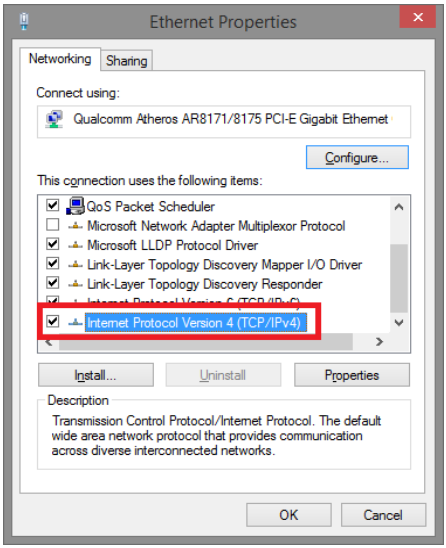
2. В появившемся окне «Сетевые подключения» (Network Connections) отображены все сетевые подключения, доступные вашему ПК. Сделайте двойной клик на подключении, которое вы используете для сети Ethernet



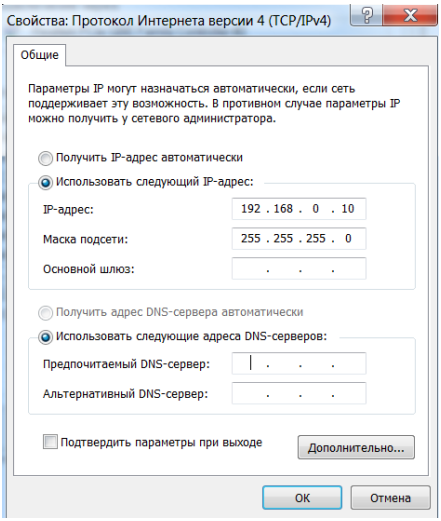
3. В появившемся окне «Состояние - Подключение по локальной сети» (Ethernet Status) нажмите кнопку «Свойства» (Properties) как показано ниже.



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

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

По умолчанию:

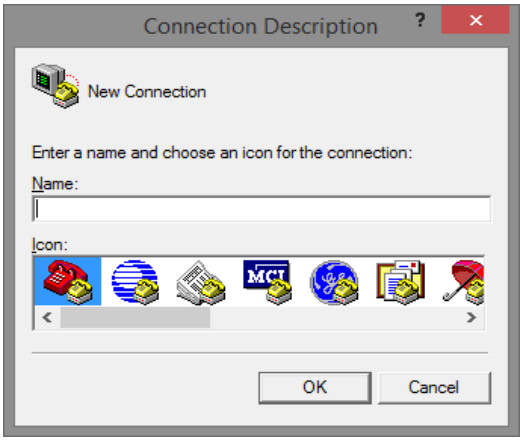
- ✓ Login: **admin**
- ✓ Password: **admin**

8. Подготовка перед управлением коммутатором через порт CONSOLE

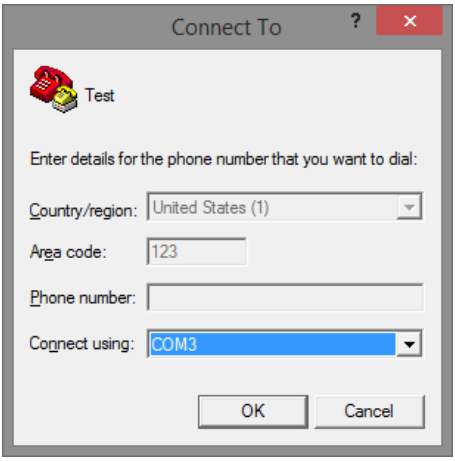
Управление коммутатором через COM-порт (RS-232) может потребоваться, если по каким-либо причинам управление через WEB-недоступно.

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.

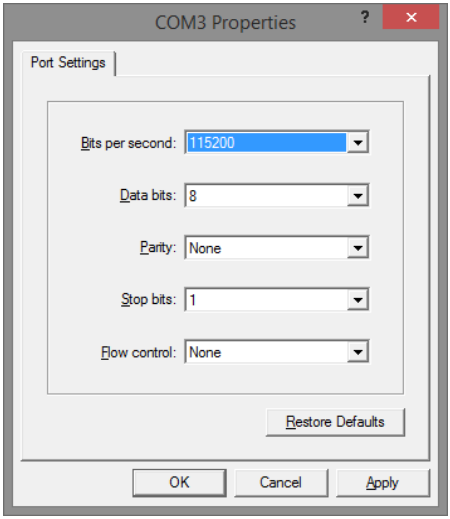


4. Выберите COM-порт, к которому подключен коммутатор.



5. Настройте COM-порт следующим образом:

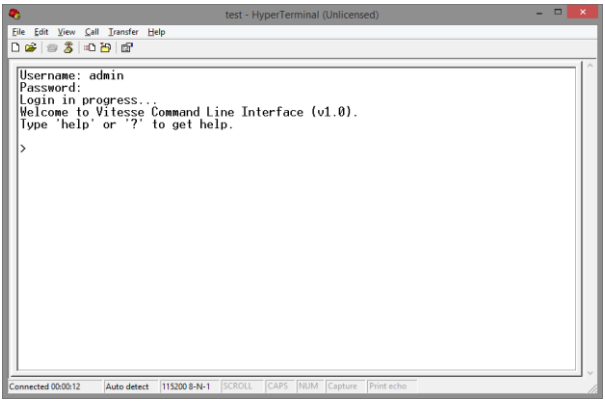
- ✓ Скорость передачи данных (Baud Rate) – 115200;
- ✓ Биты данных (Data bits) – 8;
- ✓ Четность (Parity) – нет;
- ✓ Стоп биты (Stop bits) – 1;
- ✓ Управление потоком (flow control) – нет.



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

По умолчанию:

- ✓ Login: **admin**
- ✓ Password: **admin**



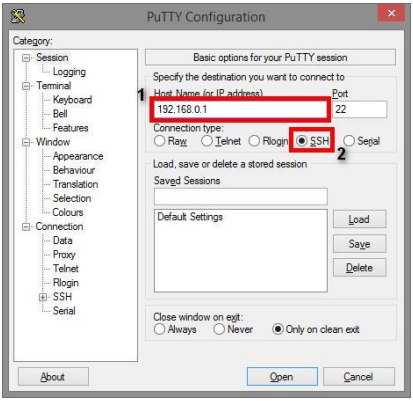
9. Подготовка перед управлением коммутатором через Telnet/SSH

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.

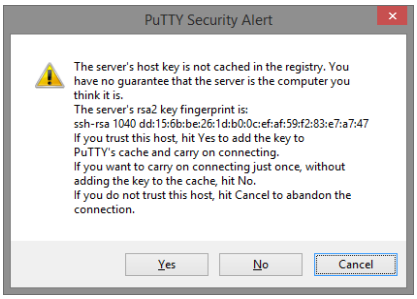
Чтобы получить доступ к CLI коммутатора через Telnet/SSH, ваш ПК и коммутатор должны находиться в одной сети. Подробнее, как это сделать рассматривалось в разделе инструкции «Подготовка перед управлением коммутатором через WEB-интерфейс».

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 **192.168.0.1**
2. Выберите тип подключения (Connection type) – SSH.



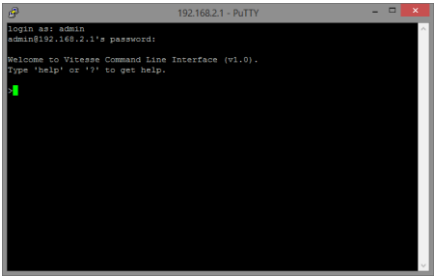
3. Если вы подключаетесь к коммутатору через SSH впервые, вы увидите окно PuTTY Security Alert. Нажмите Yes (Да) для продолжения.



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

По умолчанию:

- ✓ Login: **admin**
- ✓ Password: **admin**



10. Управление через WEB-интерфейс, основные элементы

10.1 Структура дерева навигации по группам

Весь web-интерфейс визуально разделен на 19 групп:



10.2 Описание кнопок WEB интерфейса

Большинство кнопок для изменения тех или иных настроек коммутатора через WEB интерфейс чаще всего выполняют одну и ту же роль. В таблице ниже дано общее описание функций, которые выполняют те или иные кнопки.

Кнопка	Назначение
Refresh (Обновить)	Обновляет значение всех текстовых полей на странице
Apply (Принять/подтвердить)	Числовое значение будет обновлено в памяти. Поскольку проверка ошибок выполняется на стороне коммутатора, проверка ошибки будет выполнена только после того, как пользователь выберет эту кнопку.

Кнопка	Назначение
Delete (Удалить)	Удаляет текущее значение
Help (Помощь/справка)	Открывает страницу справки, для каждого случая существует индивидуальная страница справки.

10.3 Сообщения об ошибке

Если произошла ошибка при обработке запроса от пользователя к серверу (коммутатору), то появится диалоговое окно с конкретным описанием ошибки.



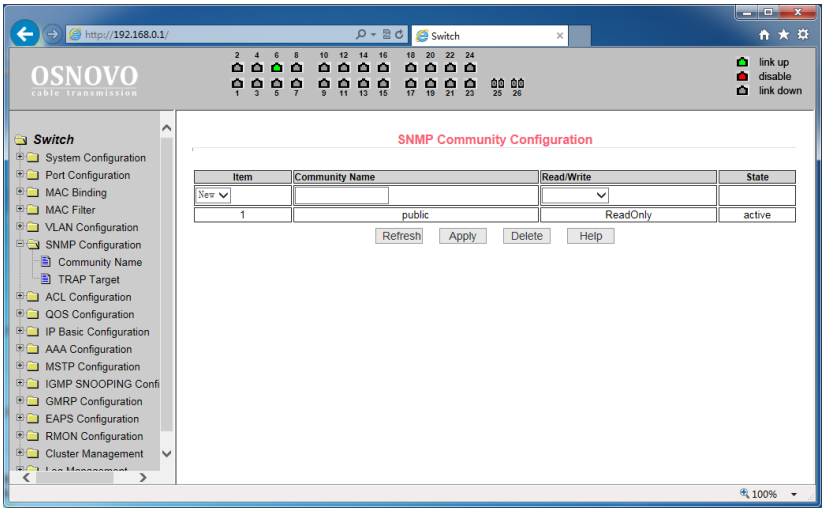
10.4 Поля для ввода информации или значений

Некоторые страницы WEB интерфейса коммутатора содержат поля для ввода той или иной информации или значений. С помощью этих полей можно получить доступ к различным строкам в таблице (см. рисунок ниже).

Если понадобится добавить новую строку необходимо выбрать из выпадающего списка NEW (новая) и подтвердить кнопкой Apply (принять).

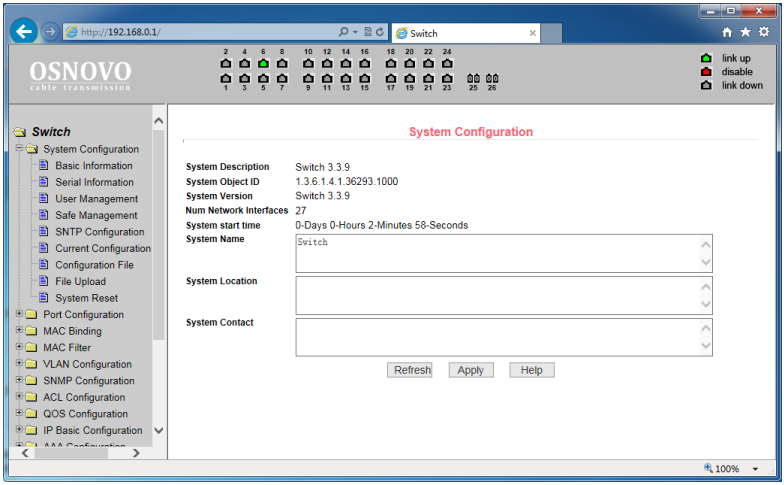
Если необходимо изменить уже существующую строку необходимо выбрать из выпадающего списка соответствующий номер строки, затем отредактировать должным образом и подтвердить изменения кнопкой Apply (принять).

Для удаления строки из таблицы выберите из выпадающего списка номер строки для удаления, а затем нажмите кнопку Delete (удалить).



10.5 Поля со значениями текущего статуса

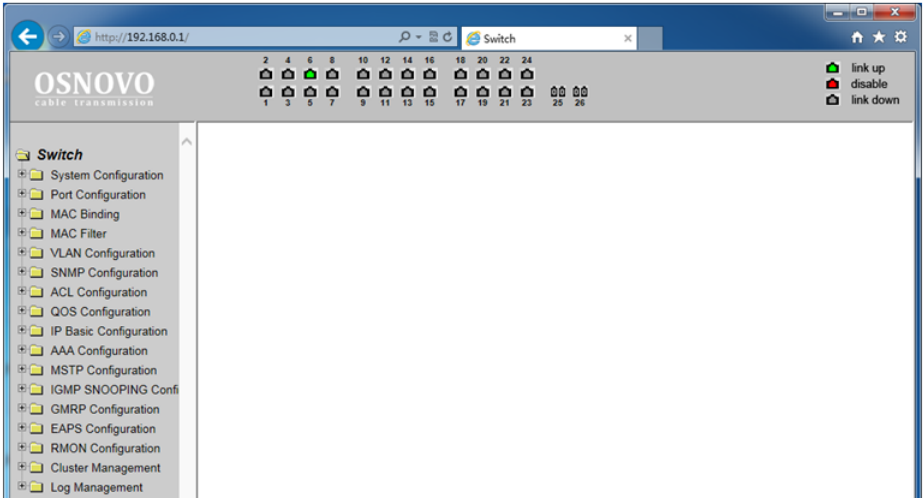
На некоторых страницах WEB интерфейса существуют поля, где отображен текущий статус (см. рисунок ниже). Такие поля предназначены только для чтения и не могут быть изменены.



11. Описание основных групп и элементов WEB интерфейса коммутатора

11.1 Главная страница WEB интерфейса

После того, как были введены корректные данные для входа (логин и пароль), коммутатор отобразит главную страницу WEB интерфейса управления (см. рисунок ниже)



11.2 Мониторинг датчиков (Industrial Switch Monitoring)



На данной странице WEB интерфейса коммутатора находятся данные с датчиков температуры, влажности и тд.

Кроме того, здесь также представлена возможность настройки сценариев реагирования портов коммутатора на различные события.

- ✓ **Ring Control** – при активации (on) позволяет отслеживать обнаружение кольцевой топологии в сети.
- ✓ **System Temperature** – поле отображает текущую температуру на центральном чипе коммутатора.
- ✓ **System Temperature Uppe**r – значение температуры из диапазона на центральном чипе коммутатора, при превышении которого подается сигнал (если настроен) на выход ALARM коммутатора.
- ✓ **System Temperature Lower** – отрицательное значение температуры из диапазона на центральном чипе коммутатора, при понижении которого подается сигнал (если настроен) на выход ALARM коммутатора.
- ✓ **Ambient Temperature** – поле отображает текущую температуру на внешнем подключаемом к коммутатору датчике.
- ✓ **Ambient Temperature Upper** – значение температуры из диапазона на внешнем подключаемом к коммутатору датчике, при превышении которого подается сигнал (если настроен) на выход ALARM коммутатора.
- ✓ **Ambient Temperature Lower** – отрицательное значение температуры из диапазона на внешнем подключаемом к коммутатору датчике, при понижении которого подается сигнал (если настроен) на выход ALARM коммутатора.
- ✓ **Ambient Humidity** – поле отображает текущую влажность на внешнем подключаемом к коммутатору датчике.
- ✓ **Ambient Humidity Upper** – значение влажности из диапазона на внешнем подключаемом к коммутатору датчике, при превышении которого подается сигнал (если настроен) на выход ALARM коммутатора.

- ✓ **Power In (Master V1, Slave V2)** – поле отображает подключенные к коммутатору блоки питания. Основной – V1 и резервный – V2.
- ✓ **System Current (A)** – поле отображает ток в Амперах, потребляемый коммутатором
- ✓ **Master V1 Voltages (V)** – поле отображает значение напряжения в Вольтах на основном блоке питания.
- ✓ **Slave V2 Voltages (V)** – поле отображает значение напряжения в Вольтах на резервном блоке питания.
- ✓ **System Power (W)** – поле отображает текущую потребляемую коммутатором мощность в Ваттах.
- ✓ **System 3.3V** – поле отображает значение системного напряжения 3.3V на плате коммутатора
- ✓ **System 1.5V** – поле отображает значение системного напряжения 1.5V на плате коммутатора
- ✓ **System 1.2V** – поле отображает значение системного напряжения 1.2V на плате коммутатора

Раздел **Alarm Input Configuration** позволяет настраивать сценарий работы портов коммутатора при получении сигнала тревоги на входе *Alarm*.

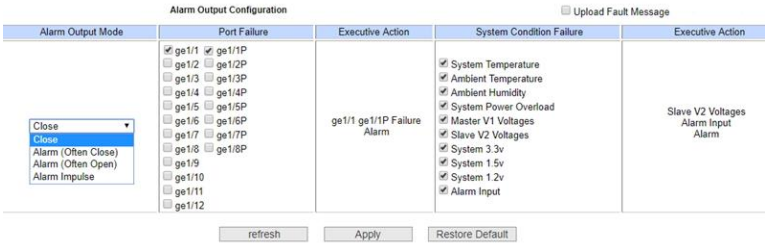
Alarm detection method – выбор порога срабатывания
- *OFF* - вход Alarm отключен
- *Low level alarm* – срабатывание при низком уровне напряжения на входе Alarm (low level < 5V)
- *High level alarm* - срабатывание при высоком уровне напряжения на входе Alarm (57V >high level >5V)



Close port / Reboot port – выбор сценария работы портов при получении сигнала тревоги, выбранные порты могут быть отключены. При

отключении сигнала тревоги выбранные порты могут быть автоматически включены или перезагружены.

Alarm Output Configuration – позволяет закрывать для трафика, перезагружать или отключать порты, замыкать/размыкать контакты релейного выхода Alarm в случае повышения температуры на основном чипе, на внешнем датчике, отклонения от нормы напряжения БП или отключения одного из БП.



Alarm Output Mode – Режим работы выхода Alarm (включение / отключение, другие режимы работы).

- *Close* – выход Alarm отключен
- *Normally closed* – при срабатывании «сухой контакт» замыкается
- *Normally open* – при срабатывании «сухой контакт» размыкается
- *Cycle alarm* – при срабатывании «сухой контакт» периодически замыкается

Port status Failure – позволяет контролировать состояние портов коммутатора. При возникновении сбоев в работе портов подается сигнал тревоги, при нормализации работы портов тревожный сигнал отключается.

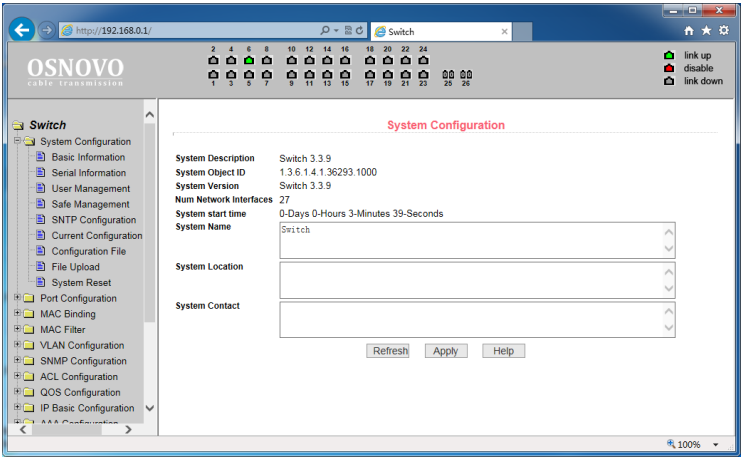
System Condition Failure - позволяет контролировать такие ошибки состояния системы как температура коммутатора, внешняя температура и влажность, параметры питания.

Для того чтобы обновить значения текущих параметров в используйте кнопку *Refresh*. Для подтверждения прочих настроек – кнопку *Apply*. Для возврата всех настроек на этой странице к исходным – кнопку *Restore Default*.

В Приложении А (в конце документа) рассмотрен пример использования входа Alarm Input коммутаторов серии ILS с внешним датчиком вскрытия.

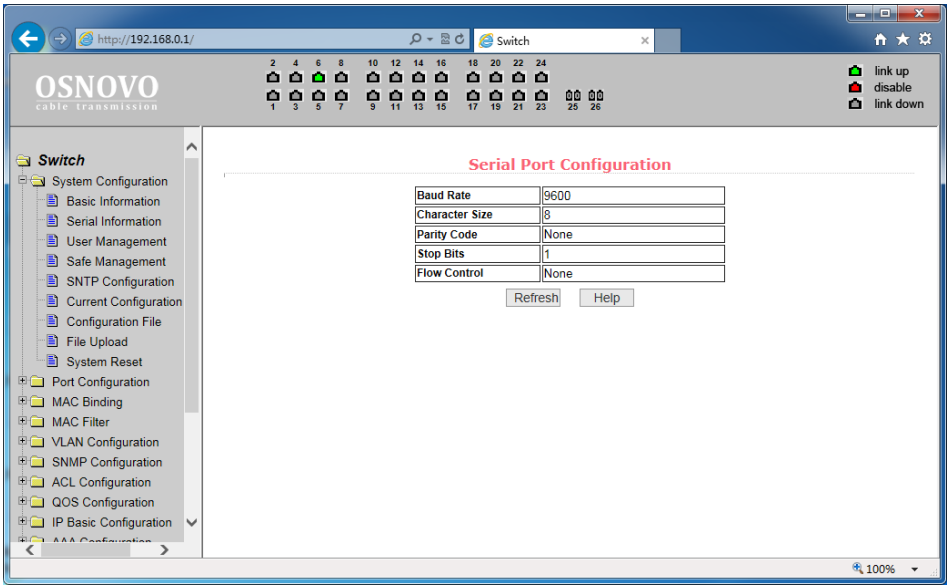
11.3 Конфигурация системы (System Configuration)

11.3.1 Общая информация (Basic Information)



- ✓ **System Description** (Описание системы) содержит общую информацию о системе;
- ✓ **System Object ID** (Идентификатор системы) отображает сетевой идентификатор системы;
- ✓ **System Version** (Версия прошивки) отображает текущую версию установленной на коммутатор прошивки;
- ✓ **Num network interfaces** (Количество портов в коммутаторе) отображает количество портов для соединения с сетью в коммутаторе;
- ✓ **System start time** (Время запуска системы) отображает сколько времени прошло с момента запуска коммутатора;
- ✓ **System name** (Имя коммутатора) отображает текущее имя коммутатора. Пользователь может изменять это значение;
- ✓ **System location** (Местоположение коммутатора) отображает физическое местоположение коммутатора. Задается пользователем;
- ✓ **System Contact** (Контактные данные) отображает владельца и контактные данные. Задается пользователем.

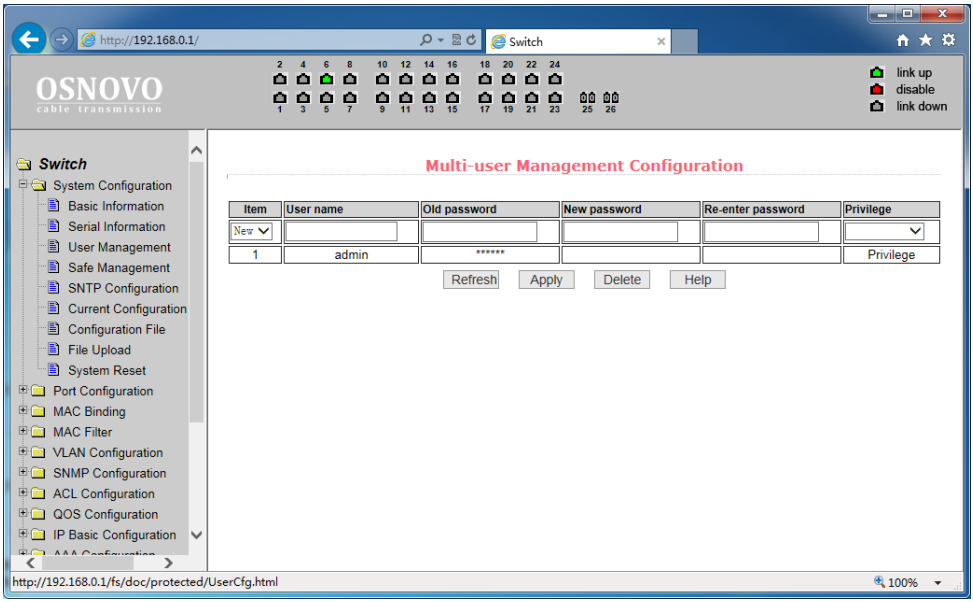
11.3.2 Serial information (Информация о RS 232/485 порте для управления коммутатором)



Данная страница WEB интерфейса содержит ряд параметров, которые необходимы для управления коммутатором через интерфейс RS232/485 используя порт CONSOLE. При управлении коммутатором через HyperTerminal убедитесь, что настройки соответствуют приведенным на этой странице значениям.

- ✓ **Baud rate** – скорость передачи данных
- ✓ **Character Size** – количество бит данных
- ✓ **Parity code –** четность
- ✓ **Stop bits –** стоповые биты
- ✓ **Flow control –** управление потоком

11.3.3 User Management (Информация о пользователях)



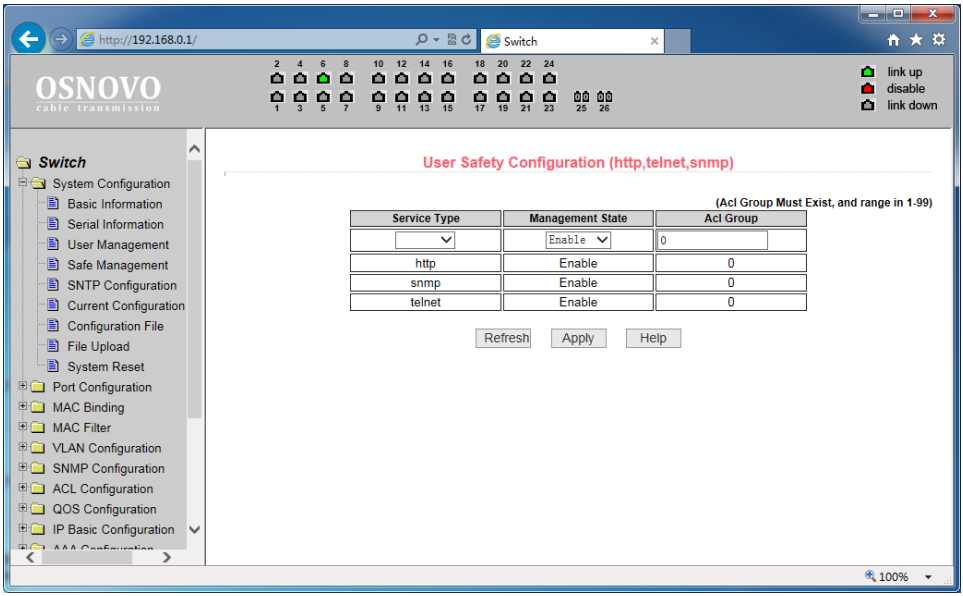
На этой странице можно задать новый пароль (new password) для текущего пользователя, изменить роль в управлении коммутатором (privilege) и тд.

Пароли чувствительны к регистру и могут содержать до 16 символов. Для смены пароля выбранного пользователя необходимо дважды ввести новый пароль в полях New Password и Re-enter Password. Для подтверждения нового пароля необходимо нажать кнопку Apply (Принять). После этого пользователю потребуется заново войти в WEB интерфейс, используя новый пароль.

С помощью настроек на этой странице пользователь может задать так называемый multi-user (многопользовательский) режим для управления коммутатором.

Для управления через Telnet и WEB для пользователя должен быть выбран многопользовательский режим.

11.3.4 Safe management (управление безопасностью)



На данной странице находятся настройки, позволяющие администратору гибко управлять доступом к управлению коммутатором (WEB, TELNET или SNMP) на основе ACL (лист управления доступом)

Есть возможность полностью отключить управление коммутатором для конкретного метода управления (WEB, TELNET или SNMP). По умолчанию управление с помощью каждого метода разрешено и ACL фильтрация не применяется.

Администратор может частично запретить управление коммутатором с помощью одного или нескольких методов, используя ACL фильтрацию.

Для применения ACL фильтрации для конкретного метода управления необходимо выбрать сам метод в списке service type, а затем выбрать ACL от 1 до 99. Главное условие – выбранный ACL должен быть создан заранее.

Обратите внимание, если администратор закроет возможность управлять коммутатором по WEB, эта страница с настройками перестанет быть доступна. Тогда можно воспользоваться другим методом управления, например через Telnet или SNMP.

11.3.5 SNTP Configuration (Настройка протокола синхронизации времени)



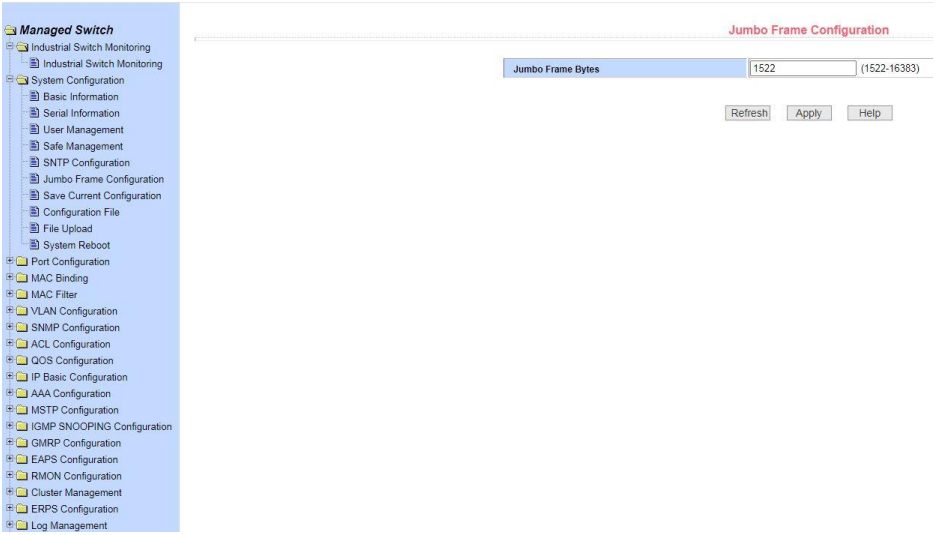
На данной странице WEB интерфейса представлены настройки для синхронизации времени коммутатора с одним из серверов с использованием протокола SNTP.

- ✓ **Server IP Address 1, Server IP Address 1, Server IP Address 1 –** поля для указания IP адресов серверов, с которыми будет проводится синхронизация.
- ✓ **Time Interval** – интервал синхронизации в сек. По умолчанию значение – 1800 сек.
- ✓ **Time Zone** – выбор часового пояса.

Refresh – обновить значения для обновляемых полей

Apply – принять настройки.

11.3.6 Jumbo Frame Configuration (Выбор размера для Jumbo пакетов)



На данной странице WEB интерфейса находится поле для указания размера обрабатываемых пакетов.

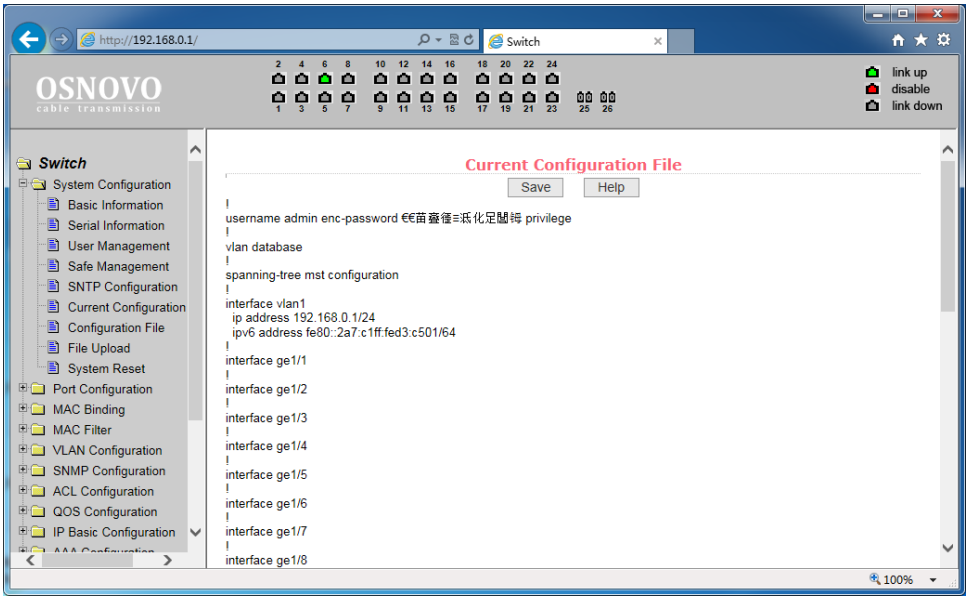
При работе с мультикаст трафиком (например, HDMI по Ethernet) рекомендуется выставлять значение не менее 10240 Байт.

- ✓ **Jumbo Frame Bytes** – поле в котором задается размер обрабатываемых пакетов. Доступные значение в диапазоне от 1522 до 16383 Байт. Значение по умолчанию – 1522.

Refresh – обновить значения для обновляемых полей

Apply – принять настройки.

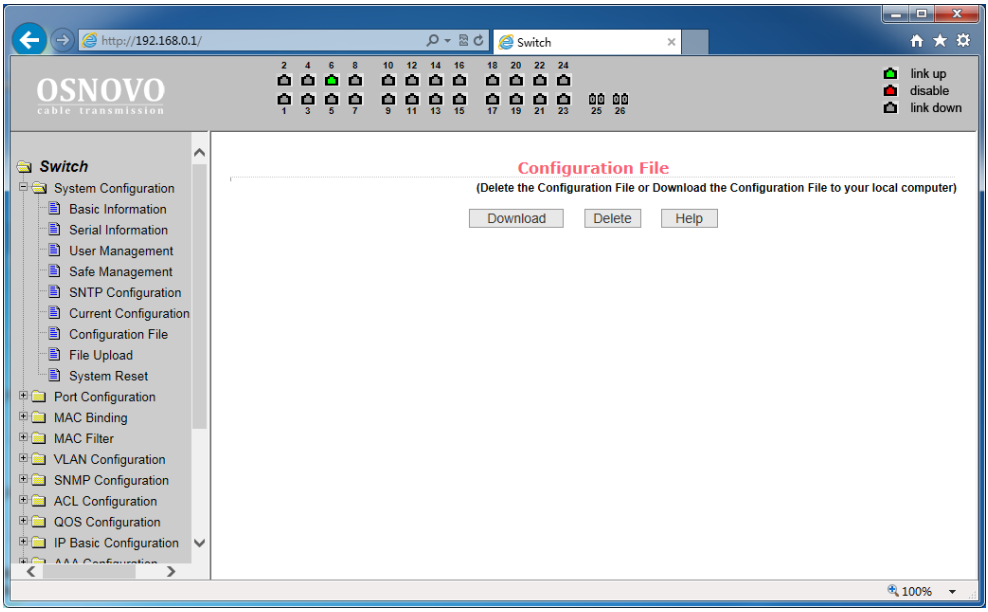
11.3.7 Current Configuration (Просмотр текущей конфигурации)



На этой странице можно просмотреть текущую конфигурацию коммутатора в виде текстовой информации. Кнопка Save (сохранить) позволит сохранить текущую конфигурацию коммутатора в память коммутатора.

Поскольку запись файла требует удаления/записи на FLASH память коммутатора, операция может занять определенное время.

11.3.8 Configuration file (Стартовая конфигурация, сохранение файла с настройками)

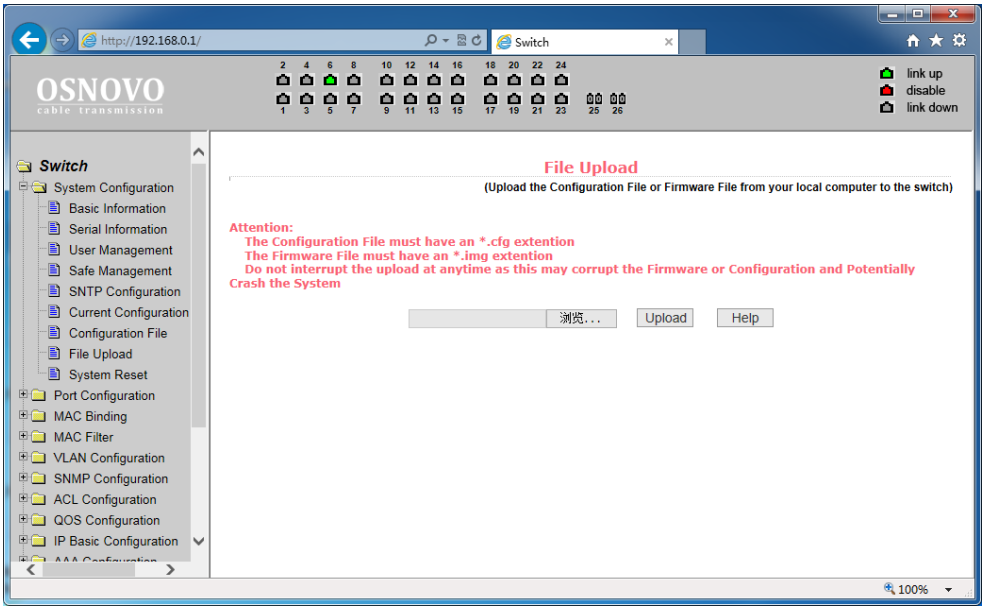


Стартовая конфигурация представляет собой файл, записанный во FLASH памяти коммутатора. Когда коммутатор запускается и не находит записанный ранее файл конфигурации во FLASH памяти, устройство использует файл с настройками по умолчанию (default).

Кнопка Delete (удалить) позволяет вызвать диалоговое окно, где будет предложено удалить текущий файл конфигурации из FLASH памяти. Если вы передумали это делать, нажмите кнопку Cancel (отмена).

Кнопка Download (скачивание) используется для скачивания конфигурационного файла на ПК из памяти коммутатора. В диалоговом окне выберите SAVE (сохранить), а затем путь к каталогу с файлами конфигурации. По умолчанию имя файла switch.cfg

11.3.9 File Upload (Загрузка файла с настройками в коммутатор)



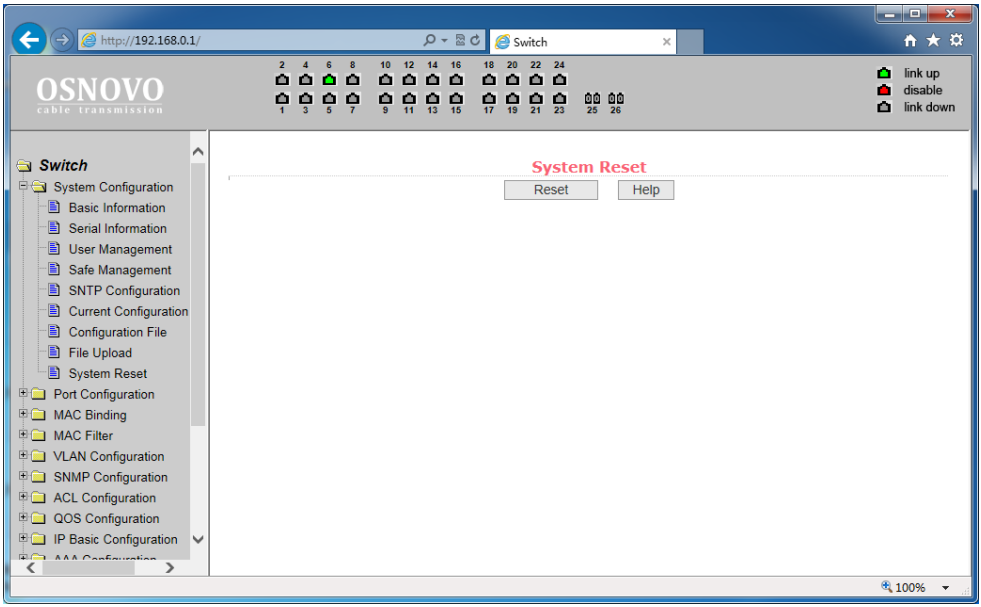
На этой странице представлена возможность для загрузки ранее созданных файлов конфигурации в память коммутатора.

Нажмите кнопку Path (путь), чтобы выбрать нужный файл с конфигурацией на ПК. Далее, после выбора необходимого файла нажмите кнопку Upload (загрузить). Файл должен иметь расширение .cfg

Если у вас есть образ диска с настройками, то вы можете загрузить его также. Образ должен иметь расширение файла .img

Во время загрузки файла конфигурации в память коммутатора не переходите на другие страницы WEB интерфейса, не перезагружайте и не отключайте коммутатор, иначе настройки будут записаны с ошибками, что может повлечь за собой сбои в работе коммутатора.

11.3.10 System reset (Перезагрузка коммутатора)



На данной странице WEB интерфейса может быть произведена перезагрузка коммутатора. Для этого нажмите кнопку Reset (перезагрузка). В появившемся диалоговом окне подтвердите свое действие кнопкой OK или отмените его с помощью кнопки Cancel (отмена).

11.4 Port configuration (Конфигурирование портов)

11.4.1 Common configuration (Базовая конфигурация портов)

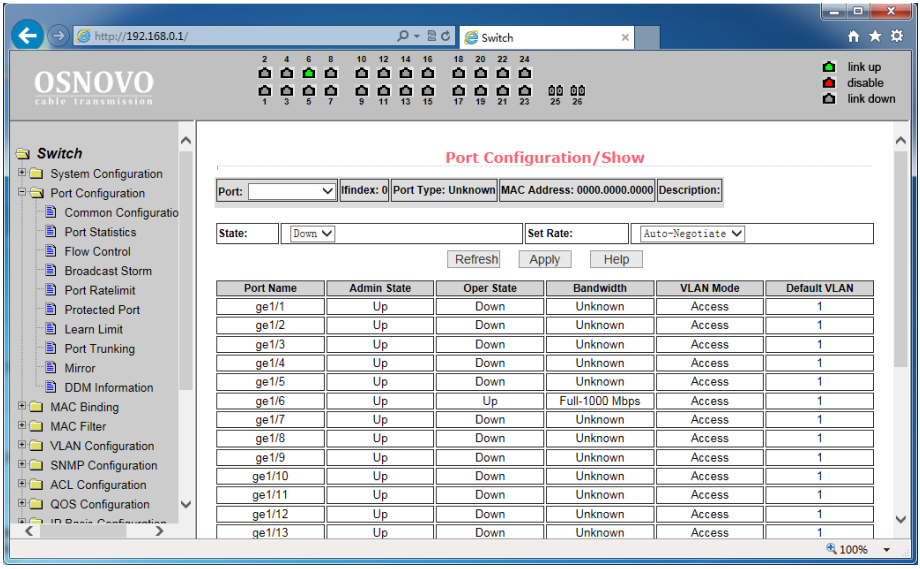
На этой страницы представлена информация по каждому из портов коммутатора. Пользователь может менять скорость, включать или отключать тот или иной порт, просматривать базовую информацию.

Для настройки конкретного порта необходимо выбрать его название из выпадающего списка. По умолчанию все порты включены (UP), чтобы выключить порт необходимо выбрать пункт DOWN (выключить) и применить изменения кнопкой Apply (принять).

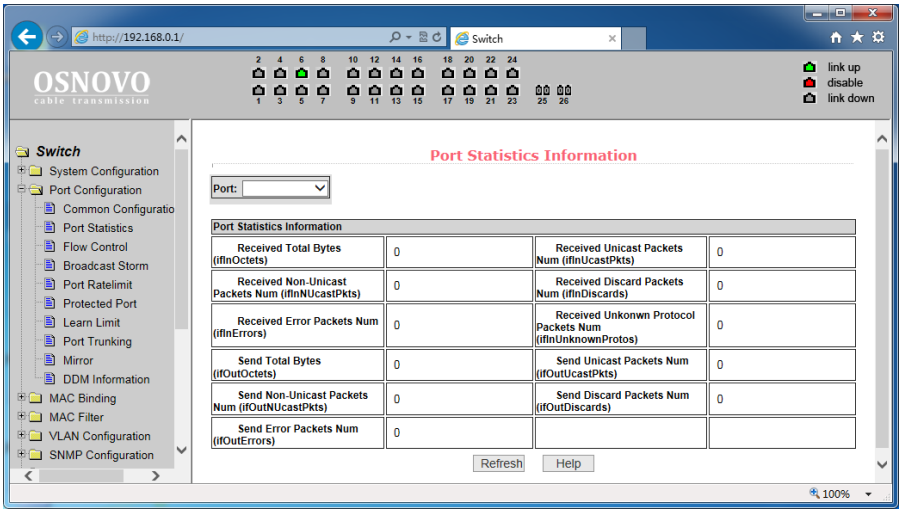
Таким же образом выбирается и значения скорости для выбранного порта. Если для какого-либо порта выбрать *Full-10 (Скорость передачи 10 Мбит/с, дуплекс),* то порт переключится в режим увеличения дальности передачи сигналов до 250м. Также порты матрицы способны автоматически переходить в этот режим при подключении к линии длиной 100-250м, обмен данными поддерживается только с Uplink портами.

Все изменения необходимо сохранять кнопкой Apply (принять).

Кнопка Refresh (обновить) обновит значения настроек для портов на данной странице.



11.4.2 Port statistics (Статистика работы портов)



На этой странице представлена сводная информация по работе портов. Для выбора конкретного порта воспользуйтесь выпадающем меню Port (порт). В таблице ниже отобразится вся доступная информация:

- Received Total Bytes (количество принятых байт);
- Received Non-Unicast Packets Num (количество принятых «не Unicast» пакетов);
- Received Error Packets Num (количество принятых пакетов с ошибкой);
- Send Total Bytes (количество отправленных байт);
- Send Non-Unicast Packets Num (количество отправленных «не Unicast» пакетов);
- Send Error Packets Num (количество отправленных с ошибкой пакетов);
- Received Unicast Packets Num (количество полученных Unicast пакетов);

- Received Discard Packets Num (количество «дропнутых» пакетов при получении);
- Received Unknown Protocol Packets Num (количество полученных пакетов с неизвестным протоколом передачи);
- Send Unicast Packets Num (количество отправленных Unicast пакетов);
- Send Discard Packets Num (количество отбрасываемых пакетов при отправке).

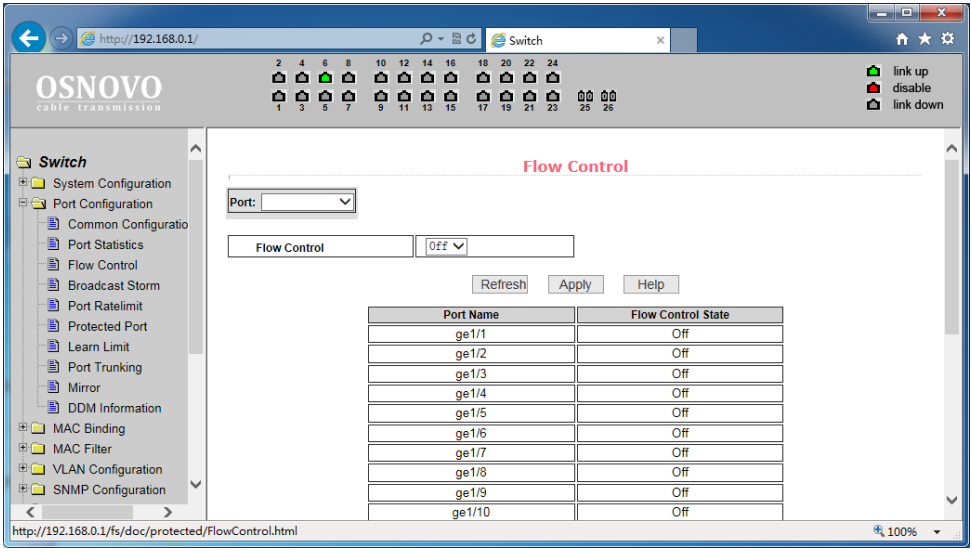
11.4.3 Flow Control (управление потоком для портов)

Данная страница позволяет настраивать функцию Flow Control (управление потоком) для конкретного порта.

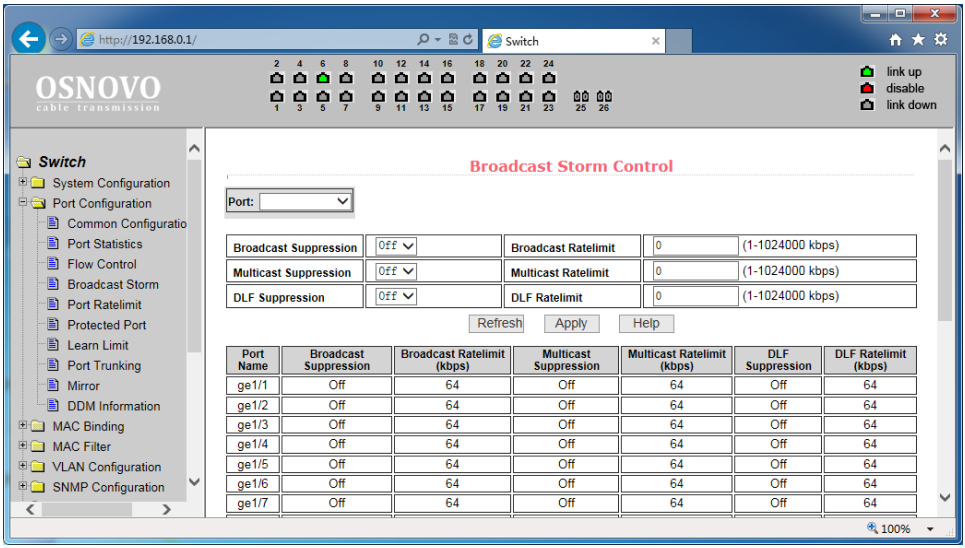
Чтобы включить или отключить Flow Control выберите конкретный порт из выпадающего меню, а затем состояние ON (вкл) или OFF (выкл.)

Данная настройка может выполняться для отправки и для получения пакетов.

Все изменения подтверждаются кнопкой Apply (принять).



11.4.4 Broadcast storm control (управление защитой от Broadcast storm)



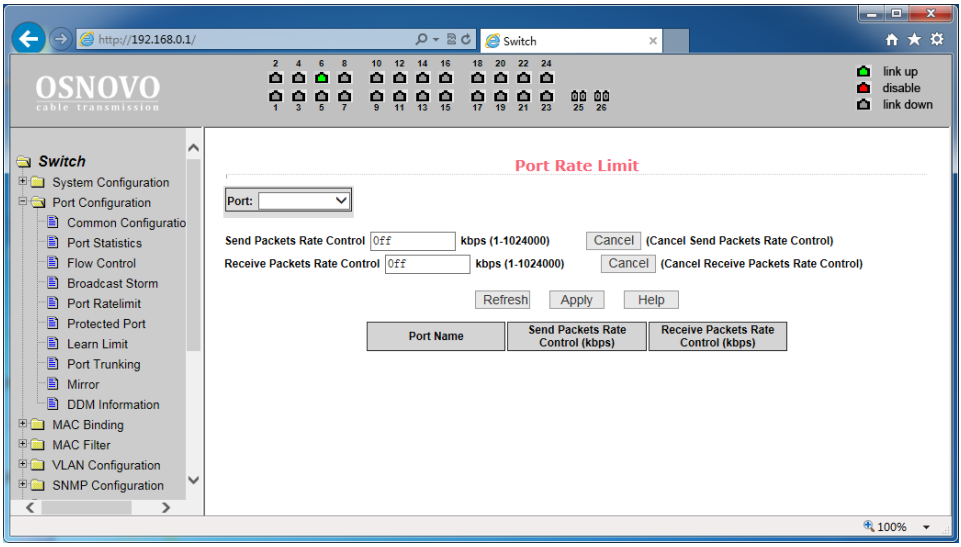
На данной странице находятся настройки, позволяющие включить или выключить защиту от влияния широковещательных (Multicast) пакетов и DLF пакетов на передаваемый/получаемый трафик.

В выпадающем списке PORT (порт) выберите необходимый порт, включите или выключите (ON или OFF) защиту для конкретного вида пакетов Broadcast, Multicast или DLF. Также можно задать скорость в Кбит/с для конкретного вида пакетов. DLF и Multicast скорости должны быть одинаковыми.

Refresh – обновить значения для обновляемых полей

Apply – принять настройки.

11.4.5 Port Rate Limit (Ограничение пропускной способности на портах)



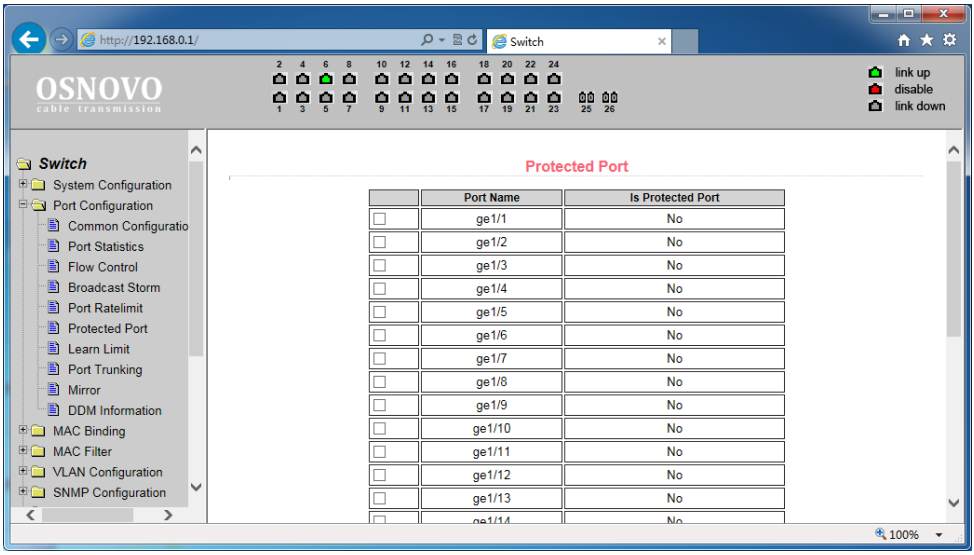
На данной странице можно гибко ограничивать скорость приема/передачи пакетов на выбранном порте. Для этого выберите порт в выпадающем списке PORT, а затем укажите значение в Кбит/с для скорости передачи данных (Send Packets Rate Control) и для скорости приема данных (Receive Packets Rate Control).

Для применения настроек нажмите кнопку Apply (принять).

Для отмены ограничения пропускной способности нажмите кнопку Cancel (отмена).

Refresh – обновить значения для обновляемых полей

11.4.6 Protected Port (Защита портов)



На данной странице можно выбрать порт, который будет изолирован от других.

Изолированный порт не может обмениваться данными с другими изолированными портами.

Изолированный порт может обмениваться данными только с неизолированным портом/портами.

Protected Port – изолировать порт

Unprotected Port – снять изоляцию порта

Refresh – обновить значения для обновляемых полей

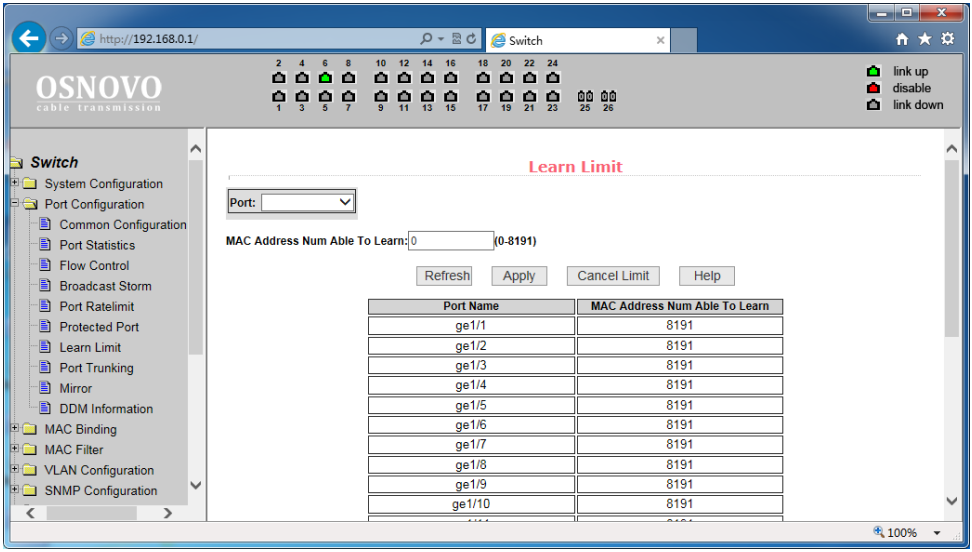
11.4.7 Learn limit (Ограничение максимального количества MAC для работы)

На данной странице WEB интерфейса представлена возможность управления максимальным количеством MAC адресов, с которыми способен работать порт. По умолчанию это значение равно 8191.

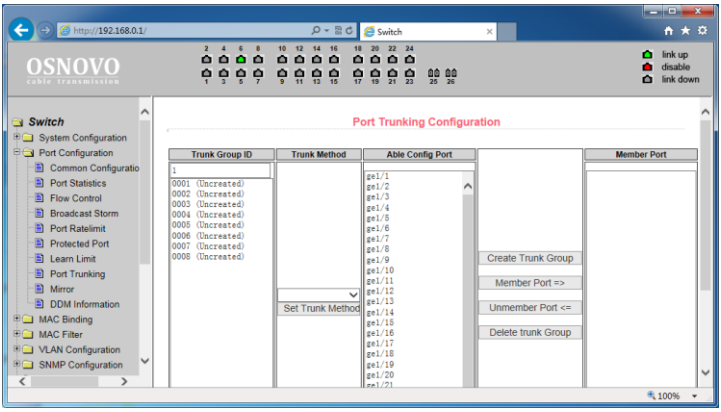
Для изменения этого значения выберите порт в выпадающем меню Port (порт), а затем в строке MAC Address Num Able to Learn (макс. количество MAC адресов) укажите свое значение.

Для применения настроек используйте кнопку Apply (принять),

Для отмены – Cancel Limit (отменить лимит).



11.4.8 Port trunking (Конфигурирование trunk'ов)



На данной странице представлены настройки для конфигурации Trunk портов.

Вы можете объединять их в группы (агрегирование), назначать ID для порта, менять способ выбора Trunk и тд.

Чтобы создать trunk для порта или изменить существующий необходимо выбрать ID от 1 до 3. Чтобы создать trunk группу выберите соответствующий идентификатор и нажмите кнопку Trunk ID Settings (настройка ID для trunk). Для настройки метода транкинга портов выберите из выпадающего списка необходимый и нажмите на кнопку Polymerization Settings.

Для удаления существующей группы trunk используйте кнопку Delete trunk group (удалить trunk группу).

В процессе настройки, по крайней мере один trunk должен быть установлен, чтобы Polymerization Settings вступили в силу. Выбранные методы создания Trunk'ов применяются ко всем группам.

Коммутатор позволяет использовать три метода создания trunk'ов:

- Метод, основанный на исходном MAC адресе;
- Метод, основанный на MAC адресе назначения;
- Метод, основанный как на исходном MAC, так и на MAC адресе назначения.

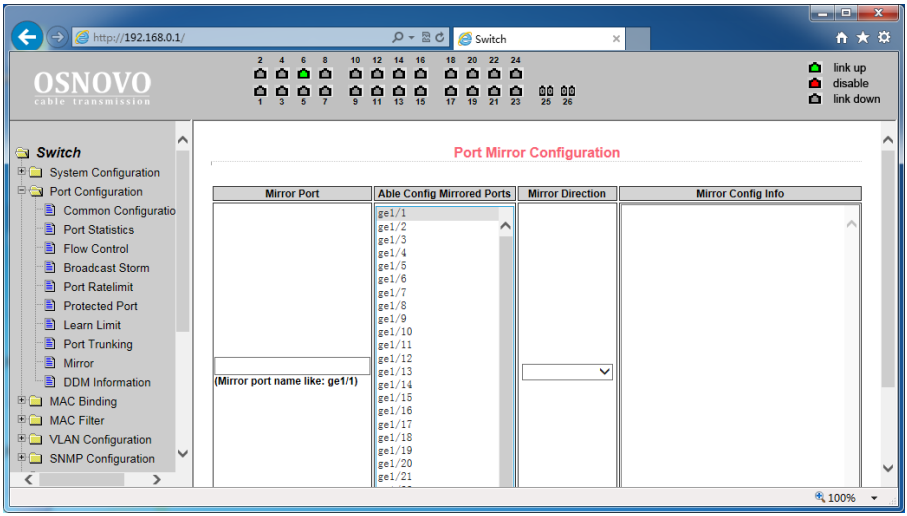
Коммутатор поддерживает максимум 3 группы trunk'ов. Trunk1 и Trunk2 не могут создавать trunk из гигабитных портов. Trunk3 может объединять максимум 2 гигабитных порта. Метод агрегирования общий для всех trunk'ов.

11.4.9 Mirror (Зеркалирование портов)

На данной странице представлены возможности для зеркалирования (mirroring) портов. Выбирается один порт (Mirror Port) который будет дублировать трафик других портов, указанных в настройках зеркалирования.

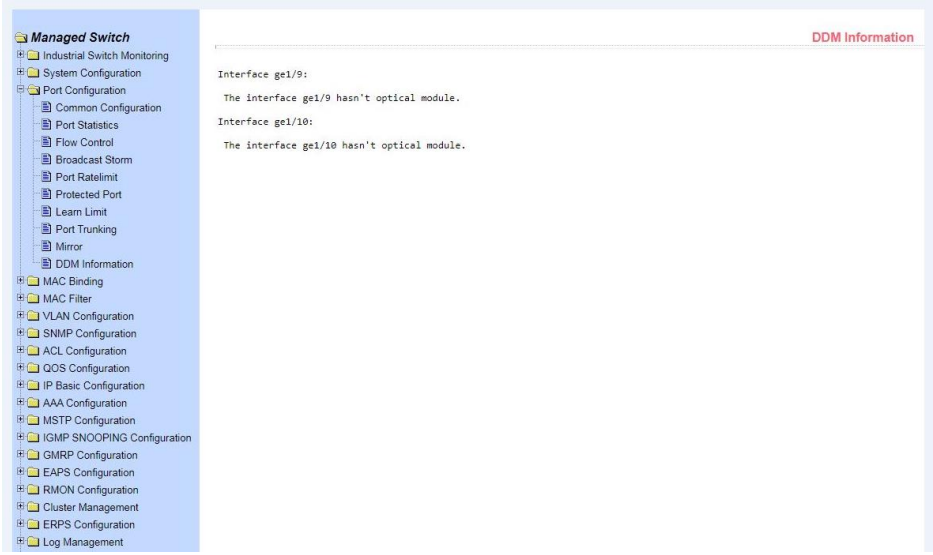
Выберите порт (порт-зеркало), который будет дублировать трафик других портов;

- Выберите порты, трафик которых будет дублироваться на порт-зеркало;
- Выберите, какие именно пакеты будут дублироваться на порт-зеркало в выпадающем меню Mirror Direction (RECEIVE – получаемые пакеты, TRANSMIT – отправляемые пакеты, BOTH – получаемые и отправляемые пакеты, NOT_RECEIVE – отменяет дублирование получаемых пакетов на порт-зеркало, NOT_TRANSMIT – отменяет дублирование отправляемых пакетов на порт-зеркало, NEITHER – отменяет дублирование каких либо пакетов на порт-зеркало);
- Результаты будут отображены в поле Mirror Config Info



11.4.10 DDM Information (Информация о подключённых SFP модулях)

На данной странице WEB интерфейса представлена диагностическая информация, которую можно получить от установленного модуля SFP, поддерживающего функцию DDM.

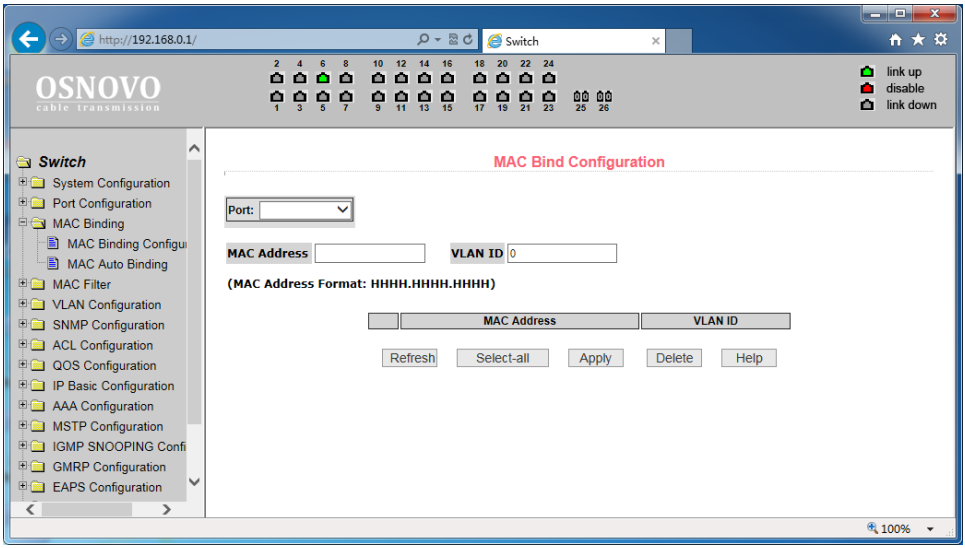


11.5 MAC binding (привязка MAC адреса)

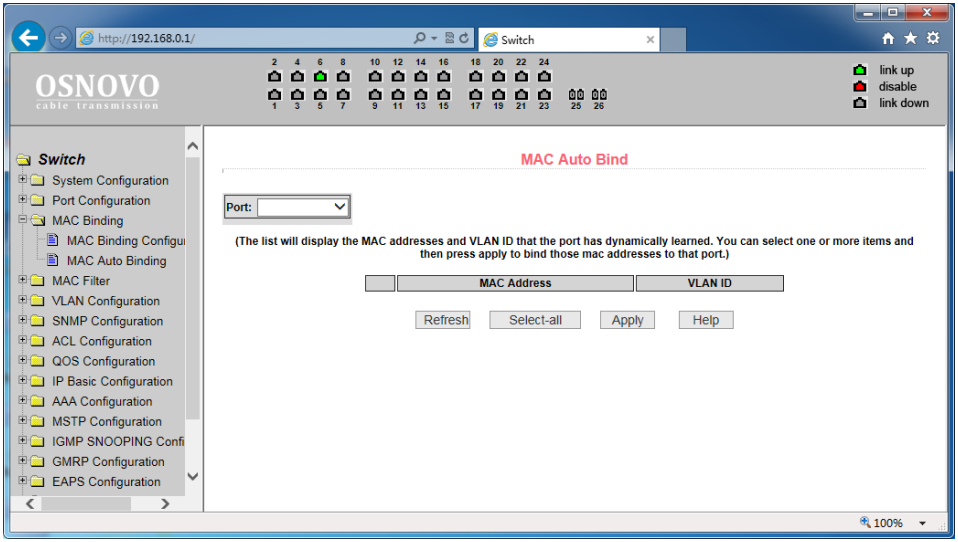
11.5.1 MAC binding configuration (Настройка привязки MAC адресов)

Данная страница предоставляет возможность привязки MAC адреса к порту (MAC Adress) или к VLAN (VLAN ID).

Все изменения на странице подтверждаются кнопкой Apply (Принять), если привязку необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все привязки, настроенные ранее.



11.5.2 MAC Auto Bind (Автоматическая привязка MAC адресов)



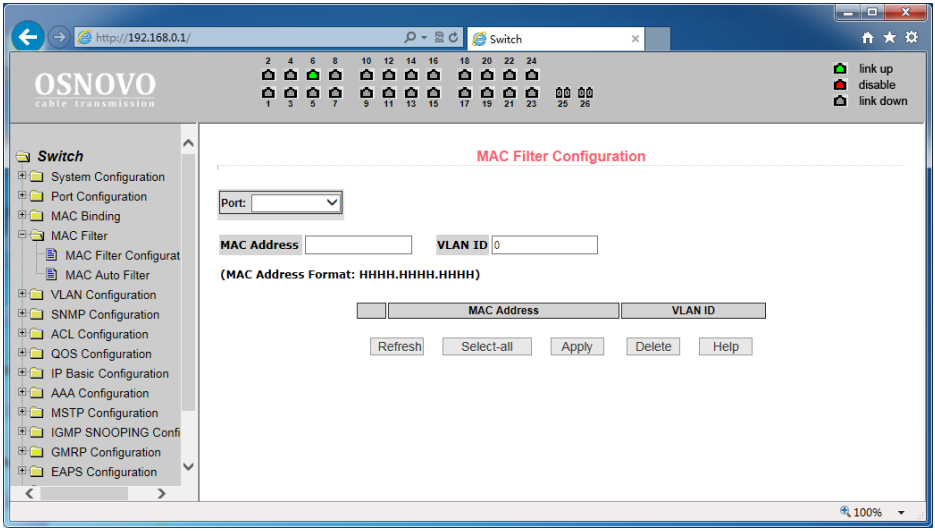
На данной странице находятся данные об автоматической привязке MAC адресов к портам. Показана динамическая привязка MAC

адресов к портам (MAC которые были занесены в таблицу MAC адресов коммутатора), а также к VLAN относящимся к этим портам. Вы можете выбрать одну из динамических привязок и конвертировать ее в постоянную привязку (static binding).

Все настройки на данной странице подтверждаются кнопкой Apply (принять), если запись необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все записи.

11.6 MAC Filter (фильтр MAC адресов)

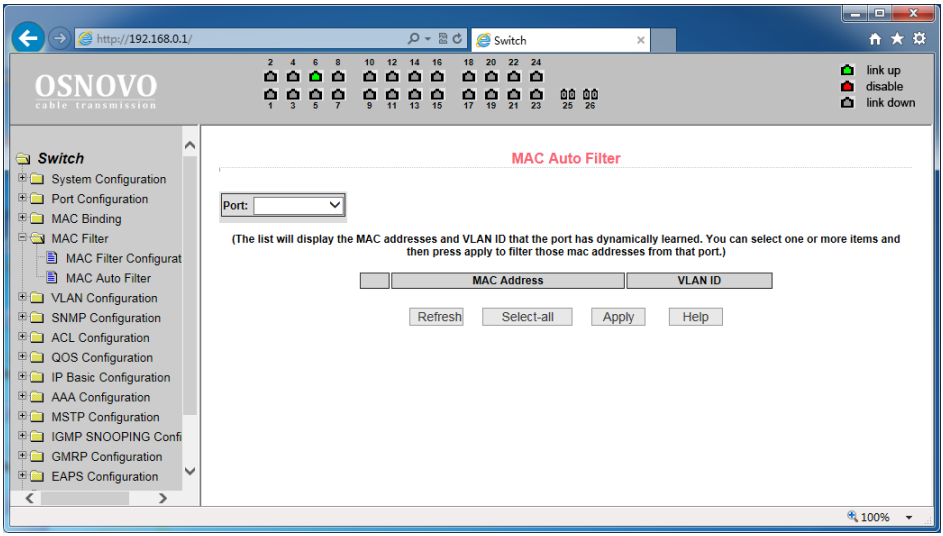
11.6.1 MAC Filter Configuration (Настройка фильтра MAC адресов)



Настройки на этой странице позволяют фильтрацию MAC адресов для портов. Записи с MAC адресами на этой странице используются для входа в фильтр MAC адресов, а VLAN ID используется для фильтрации MAC адреса соответствующей VLAN.

Все настройки на данной странице подтверждаются кнопкой Apply (принять), если запись необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все записи.

11.6.2 MAC Auto Filter (Автоматический фильтр MAC адресов)



Здесь представлены данные об автоматической конверсии MAC адресов.

Показана динамическая привязка MAC адресов к портам (MAC которые были занесены в таблицу MAC адресов коммутатора), а также к VLAN относящимся к этим портам.

Вы можете выбрать одну и привязок и конвертировать ее в постоянную привязку (static binding) для фильтра MAC адресов.

Все настройки на данной странице подтверждаются кнопкой Apply (принять), если запись необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все записи.

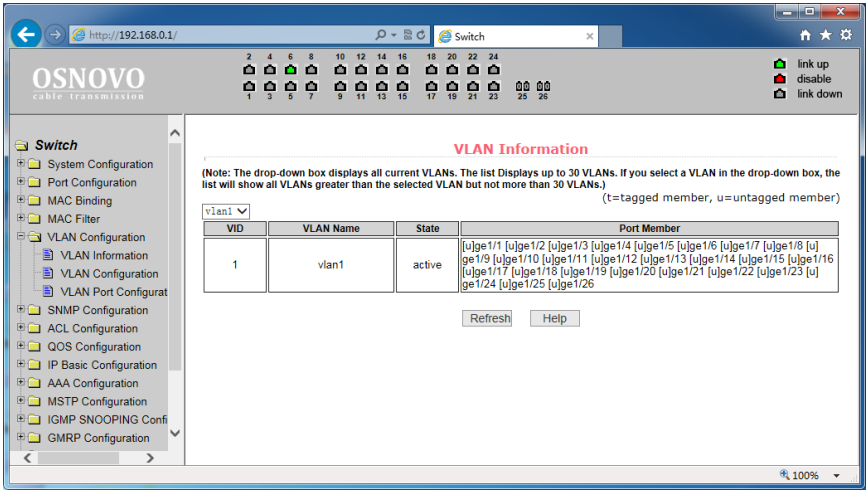
11.7 VLAN Configuration (Настройка VLAN)

11.7.1 VLAN Information (информация о VLAN)

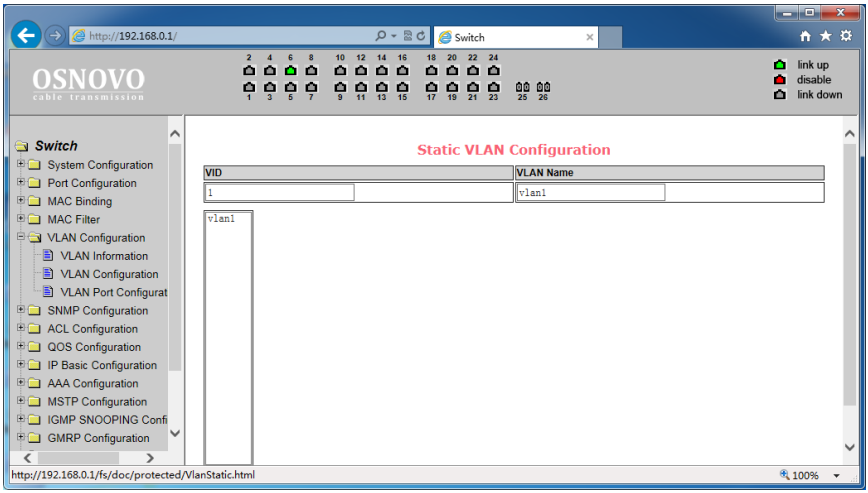
На этой странице представлена информация о существующих VLAN. Данные предоставлены только для чтения и не могут быть изменены.

Информация о текущей конфигурации VLAN выбирается в выпадающем меню в левом верхнем углу и включает в себя:

- ✓ VID (VLAN ID);
- ✓ VLAN Name (Имя VLAN);
- ✓ State (состояние активное или неактивное);
- ✓ Port member (порты – участники VLAN, могут включать в себя как тегированные порты (t) и нетегированные (u)).



11.7.2 Static VLAN Configuration (Настройка VLAN)



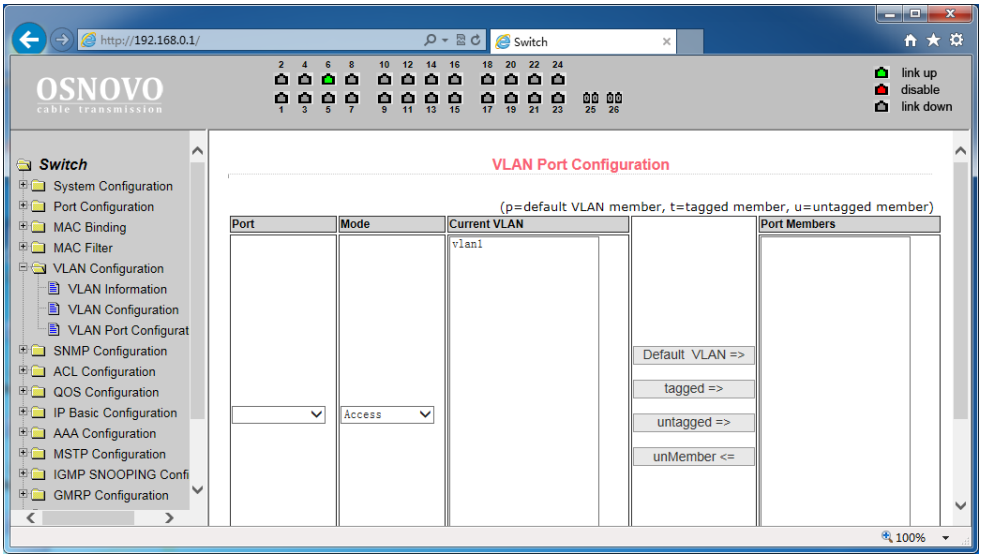
На этой странице вы можете создать VLAN. Для этого задайте VLAN ID в строке VID (от 2 до 4094, значение 1 зарезервировано системой).

Имя в строке VLAN Name задается автоматически и зависит от VLAN ID. Для подтверждения создания VLAN нажмите кнопку Apply (Принять).

В текстовом поле появится созданная VLAN (VLAN ID+ VLAN Name). VLAN1 нельзя изменить или удалить, данное имя зарезервировано системой.

Для удаления созданной ранее VLAN потребуется выбрать нужную запись из списка и далее нажать кнопку REMOVE (удалить). Запись из списка также будет удалена.

11.7.3 VLAN Port Configuration (Конфигурация портов VLAN)



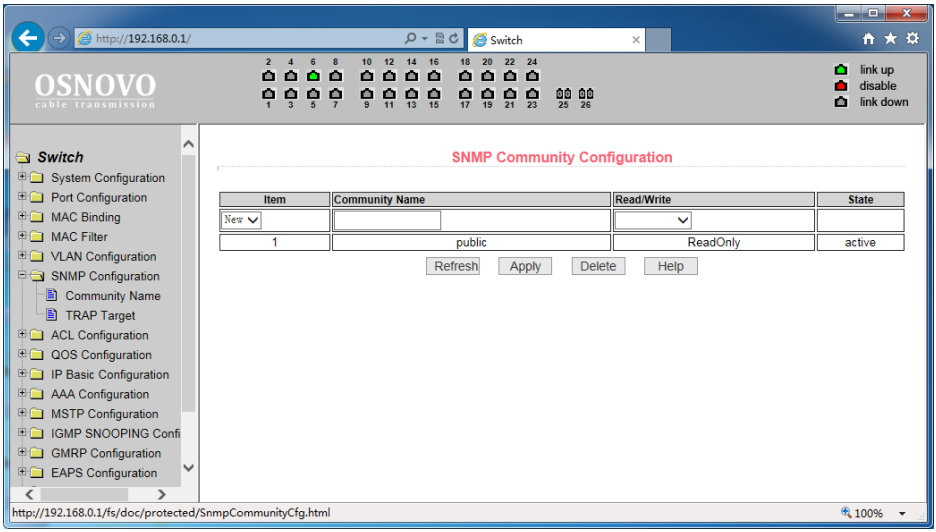
На этой странице представлены возможности по конфигурированию портов для VLAN, а также просмотру результатов.

Эта страница с настройками состоит из 8 частей:

- Port (Выбор порта);
- Mode (Режим, в котором порт будет работать в VLAN. Режим Access подразумевает, что порт будет помечен, как untagged (нетегированный) и являться членом VLAN1, Режим Hybrid подразумевает, что порт будет являться членом VLAN1 и будет помечен, как untagged (нетегированный). Режим TRUNK подразумевает, что порт будет являться членом VLAN1 и будет помечен, как tagged (тегированный));
- Current VLAN (имя VLAN. Позволяет выбрать одну или несколько VLAN, к которым будет относится выбранный порт);
- Port Members (порты – участники VLAN);
- Кнопки Default VLAN (добавить запись в VLAN по умолчанию), tagged => (добавить порт как тегированный), untagged => (добавить порт как нетегированный), unMember <= (удалить порт из поля Port Members)

11.8 SNMP Configuration (Настройка SNMP протокола управления)

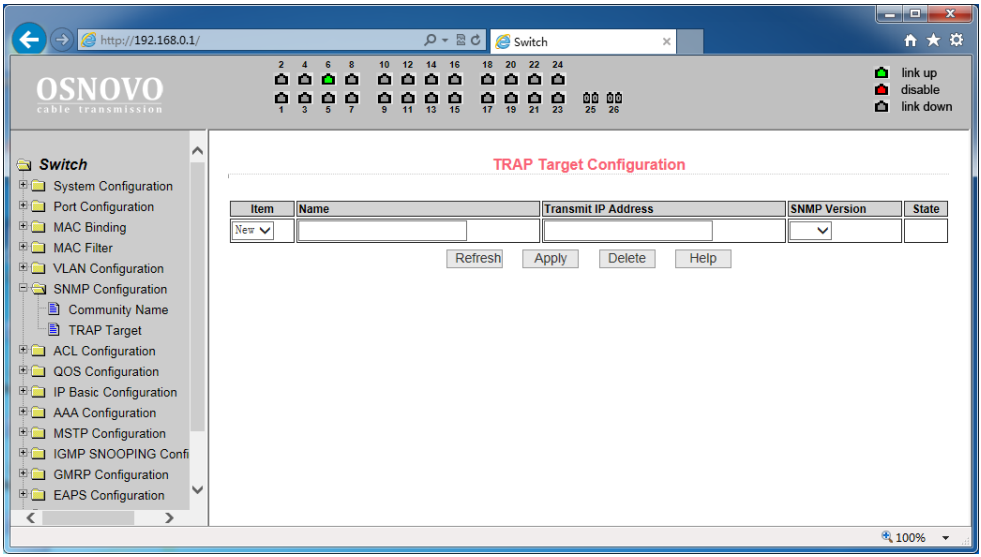
11.8.1 Community Name (Общие настройки для SNMP)



На этой странице представлены общие настройки для управления коммутатором через SNMP. По умолчанию в коммутаторе создана одна запись Public с правами только на чтение (ReadOnly).

Всего может быть создано 8 записей. Если предполагается управлять коммутатором через SNMP следует создать запись с правами на Чтение/Запись (Read/Write).

11.8.2 TRAP Target (Настройка TRAP уведомлений)



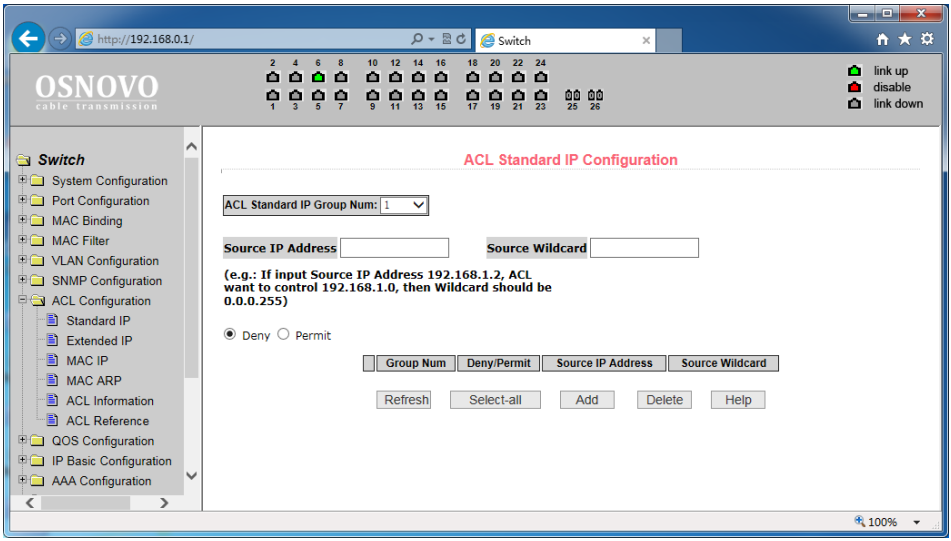
Настройки на данной странице позволяют сконфигурировать получение TRAP сообщений. Для этого необходимо:

- ✓ Выбрать в поле Name имя для получения TRAP сообщений;
- ✓ Выбрать IP адрес (Transmit IP Address), который будет использовать TRAP протокол;
- ✓ Выбрать версию SNMP (SNMP Version);

Когда все настройки будут произведены успешно в строке состояния (State) появится Active. Теперь коммутатор сможет пересылать TRAP сообщения на указанный IP адрес.

11.9 ACL Configuration (Настройка Access Control List)

11.9.1 Standard IP (Настройка ACL для IP)



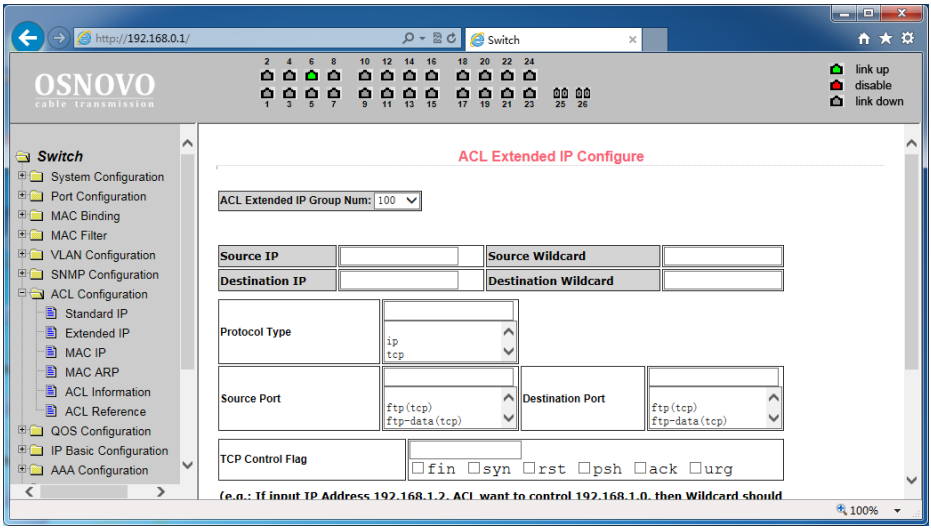
Здесь представлены настройки ACL для IP протокола. Пользователь может задать самостоятельно ACL базу с правилами для IP адресов. Стандартные правила контролируют перенаправление исходных IP пакетов.

Пользователь может настраивать правила, исходный IP адрес должен быть указан с маской, правило может совпадать с набором IP адресов. Каждое правило должно содержать параметр фильтрации: запретить (deny) или разрешить (allow).

Пользователь может создавать правило в группе, имя для правила автоматически задается. При удалении одного правила остальные правила не изменяются.

Для удаления всех правил сразу используйте кнопку Select all (выбрать все), а затем кнопку Delete (удалить).

11.9.2 Extended IP (Расширенная настройка ACL правил для IP)

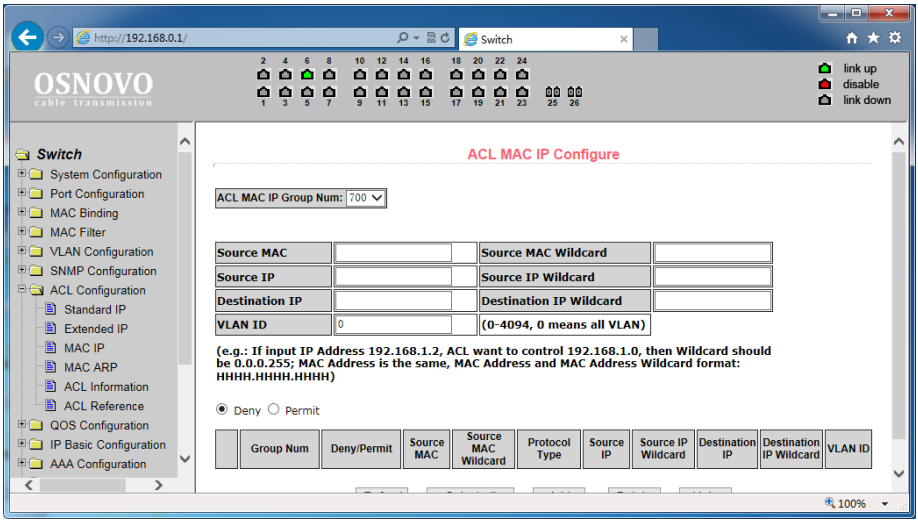


Здесь представлена возможность для создания ACL правил с расширенными настройками IP адресов. Контроль пересылки пакетов через исходный IP адрес, адрес назначения, тип протокола, служебный порт.

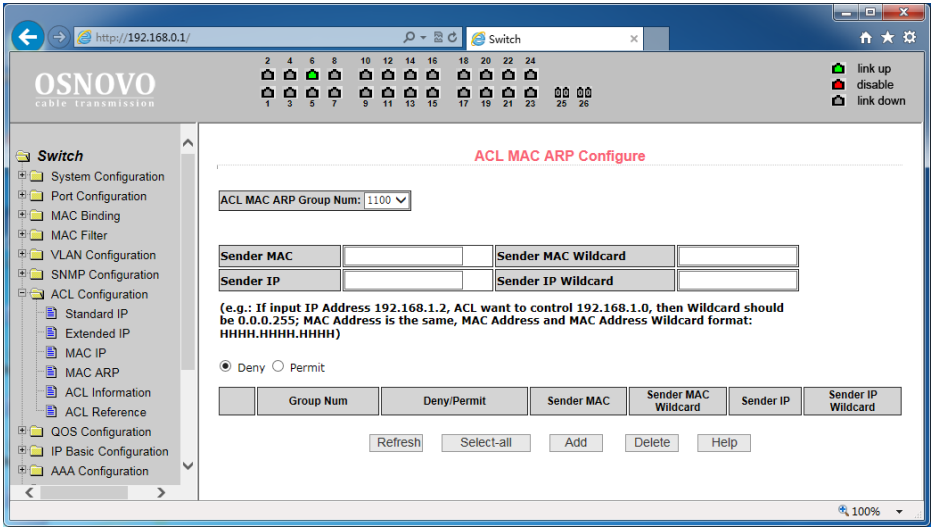
11.9.3 MAC IP (Настройка ACL правил с помощью MAC)

Здесь представлены настройки ACL правил для группы IP адресов, связанными с MAC адресами. Правила могут быть созданы на основе исходного IP адреса, исходного MAC адреса, а также IP адреса назначения.

Все настройки на данной странице подтверждаются кнопкой Apply (принять), если запись необходимо удалить используйте кнопку Delete (Удалить), кнопка Select all (выбрать все) позволит удалить сразу все записи.



11.9.4 MAC ARP (Настройка ACL правил для ARP с помощью MAC адресов)

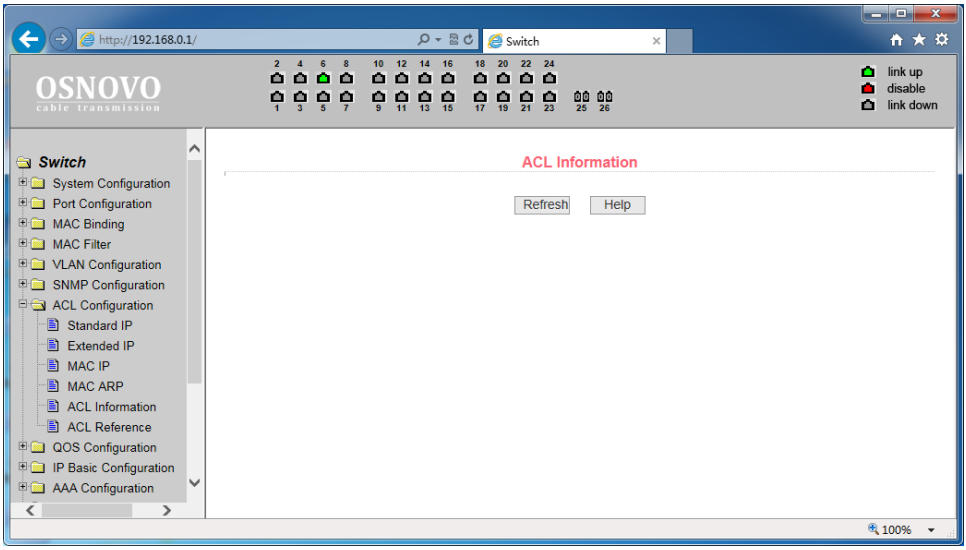


На этой странице представлены настройки ACL правил для ARP пакетов с помощью MAC адресов. Правила могут быть созданы на основе IP адреса отправителя, MAC адреса отправителя.

Все настройки на данной странице подтверждаются кнопкой Apply (принять), если запись необходимо удалить используйте кнопку Delete

(Удалить), кнопка Select all (выбрать все) позволит удалить сразу все записи.

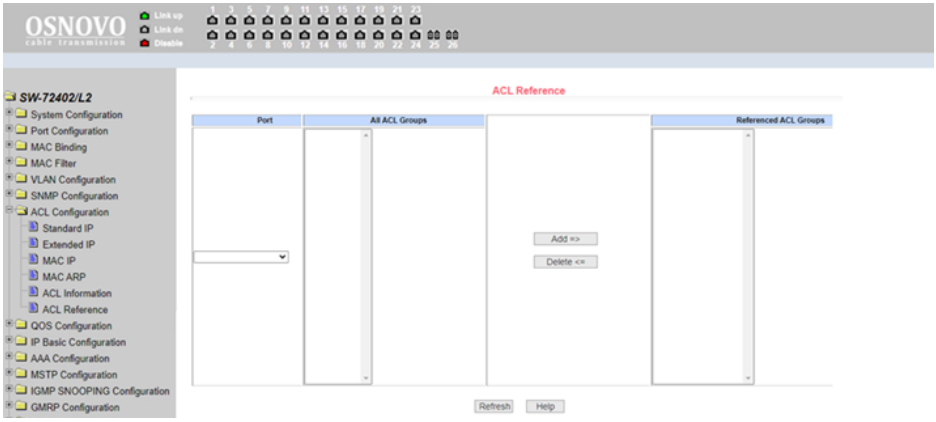
11.9.5 ACL Information (Набор действующих ACL правил)



На данной странице отображены действующие в текущий момент ACL правила.

Информация представлена только для чтения и может быть обновлена кнопкой Refresh (обновить).

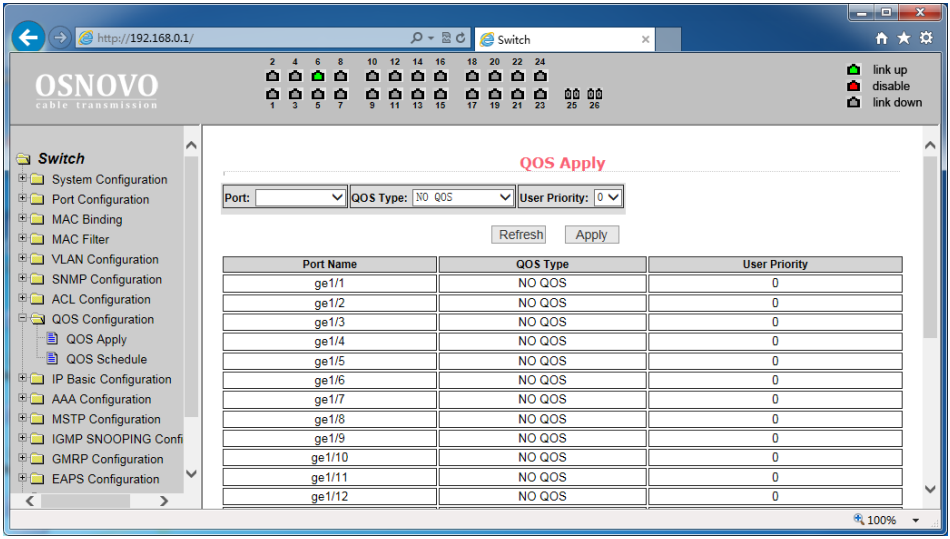
11.9.6 ACL reference configuration (Настройка ACL правил)



На этой странице представлены настройки ACL правил для фильтрации пакетов, получаемых портами. Выберите порт, выберите ALC группу из списка и нажмите *Add*=>. Для удаления выберите ALC группу из списка добавленных и нажмите *Delete*<=.

11.10 QoS Configuration (Настройка предоставления трафика с разным приоритетом)

11.10.1 QoS Apply (Настройка приоритетов трафика для портов)



На этой странице находятся основные настройки QoS. Вы можете выбрать порт в выпадающем меню PORT, затем QoS режим (QOS Type) для него (вкл/выкл) и приоритет трафика (User Priority).

По умолчанию QoS отключен на всех портах а приоритет трафика нулевой.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

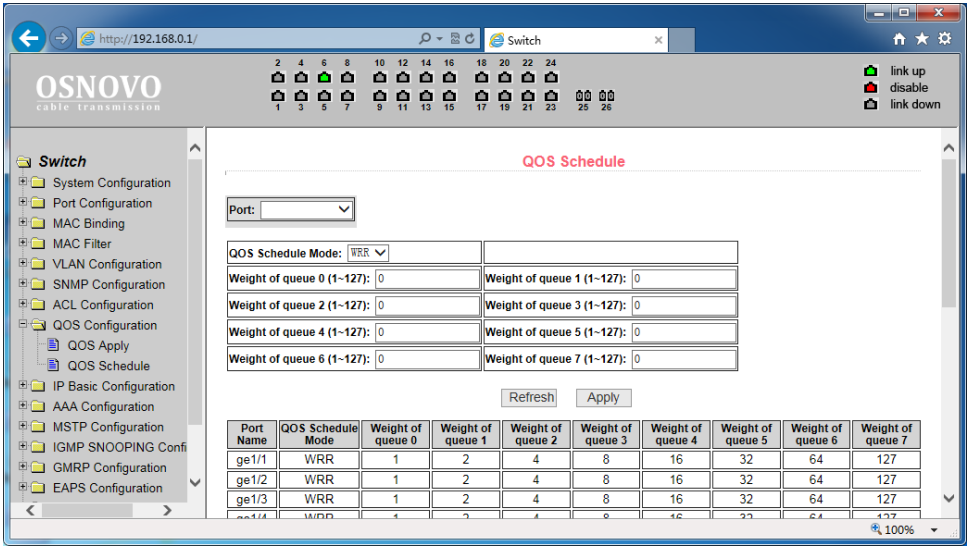
Чтобы обновить значения полей нажмите кнопку Refresh.

11.10.2 QoS Schedule (Настройка расписания применения QoS)

На этой странице WEB интерфейса представлены настройки позволяющие применять QoS приоритезацию трафика по расписанию.

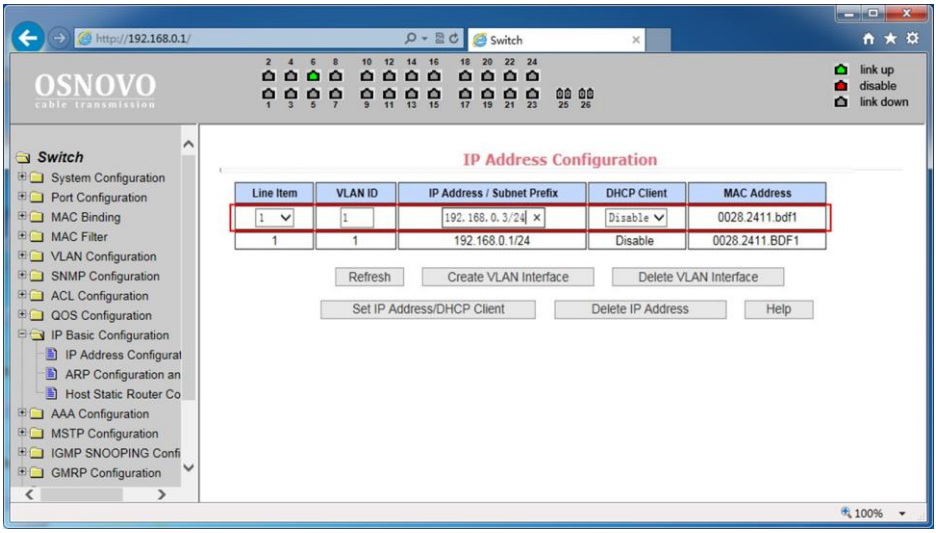
Все настройки на данной странице подтверждаются кнопкой Apply (принять).

Чтобы обновить значения полей нажмите кнопку Refresh.



11.11 IP Basic Configuration (Базовая настройка IP)

11.11.1 IP Address Configuration (Настройка IP адреса коммутатора)



Для изменения IP адреса:

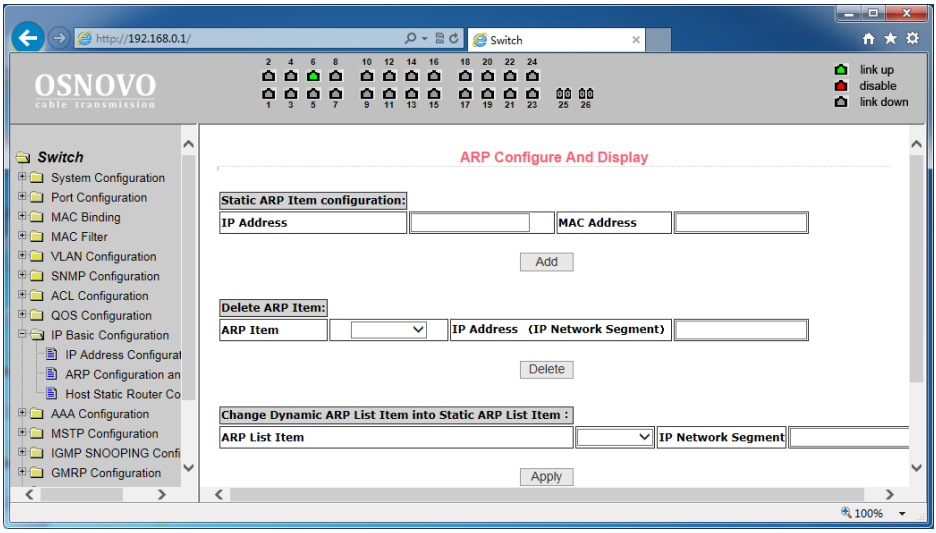
- установите *Line Item* «1», *DHCP Client* «Disable»;
- введите новый адрес в поле *IP Address/Subnet Prefix* (адрес должен быть уникальным и не должен повторяться);
- нажмите *Set IP Address/DHCP Client* (установить адрес), ***старый IP адрес автоматически перестанет действовать;***
- ***Выполните повторный вход в WEB интерфейс, используя новый IP адрес.***

Для сохранения нового IP адреса в энергонезависимой памяти коммутатора в разделе **11.3.7** Current Configuration (Просмотр текущей конфигурации) сохраните настройки, в противном случае при перезагрузке коммутатора будет установлен предыдущий IP адрес.

Также на этой странице находятся настройки VLAN интерфейса. Вы можете создать VLAN интерфейс, удалить его, изменить. Существующие VLAN интерфейсы могут быть настроены только если заданы остальные параметры такие как IP адрес, маска, и MAC адрес.

Коммутатор по умолчанию имеет VLAN1 интерфейс, который не может быть удален.

11.11.2 ARP Configuration and Display (Настройка протокола ARP и отображение таблицы ARP)



Страница настроек ARP предоставляет возможность отображать всю таблицу ARP коммутатора, менять Static ARP, удалять ARP, менять Dynamic ARP на Static ARP.

При настройке static ARP необходимо указать IP адрес и MAC адрес. MAC адрес должен быть типа unicast. После этого нажмите кнопку Add (добавить).

При удалении ARP вы можете выбрать, что именно удалить:

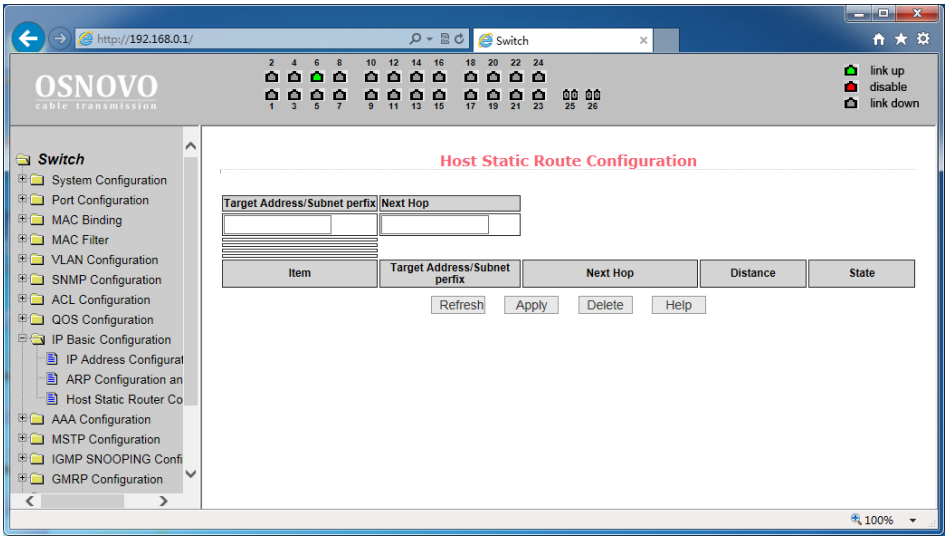
- ✓ Часть записи в ARP таблице коммутатора (для этого необходимо указать IP адрес или IP сегмента сети);
- ✓ Static ARP из таблицы;
- ✓ Dynamic ARP из таблицы.

Для подтверждения удаления используйте кнопку Delete (Удалить).

При переносе Dynamic ARP в Static ARP вы можете выбрать какой либо сегмент сети или все Dynamic ARP записи в таблице. Для первого случая следует указать IP адрес сегмента сети.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.11.3 Host Static Route Configuration (Настройка таблицы Static маршрутизации)

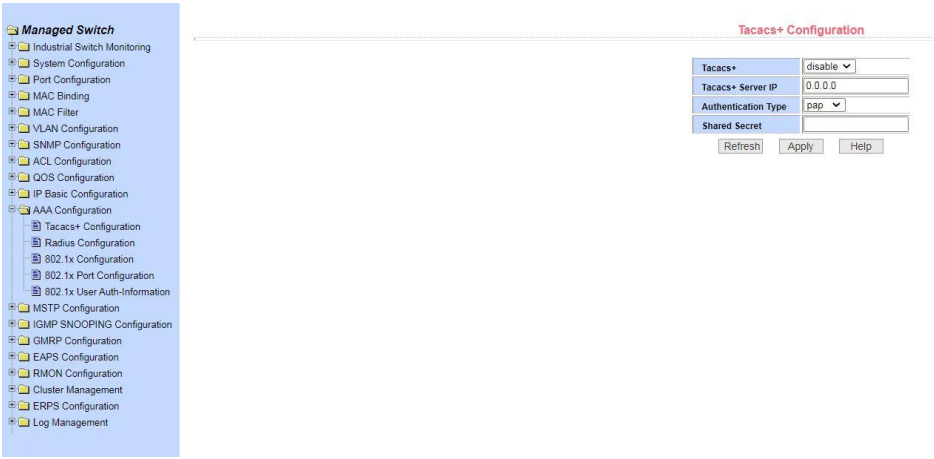


Вы можете добавлять и удалять записи в таблицу Static маршрутизации с помощью настроек на этой странице WEB-интерфейса. По умолчанию коммутатор не имеет каких-либо записей в таблице маршрутизации. Чтобы настроить маршрутизацию по умолчанию необходимо добавить 0.0.0.0 / 0 запись в таблицу.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.12 AAA Configuration (настройка системы аутентификации авторизации и учета событий)

11.12.1 Tacacs+ Configuration (настройка Radius системы AAA)



На этой странице WEB интерфейса представлены настройки TACACS + (Terminal Access Controller Access Control System plus) — сеансовый протокол, разработанного Cisco.

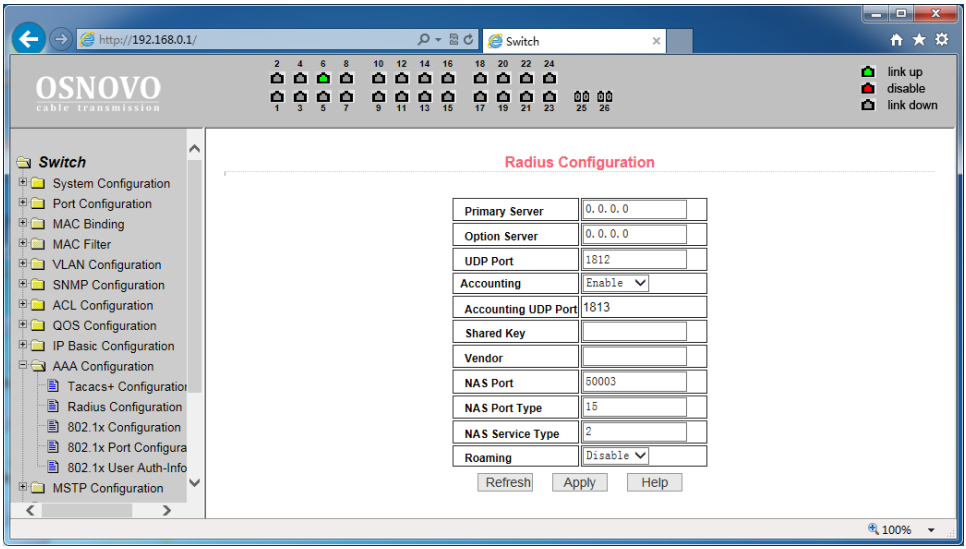
Улучшена безопасность протокола (шифрование), а также введено разделение функций аутентификации, авторизации и учёта, которые теперь можно использовать по отдельности.

- ✓ **Tacacs+** (disable/enable) – глобальное вкл/выкл протокола Tacacs+
- ✓ **Tacacs+ Server IP** – IP адрес сервера Tacacs+
- ✓ **Authentication Type** – типа аутентификации на сервере.
- ✓ **Shared Secret** – ключ для шифрования/дешифрования пакетов.

Refresh – обновить страницу.

Apply – сохранить настройки.

11.12.2 Radius Configuration (настройка Radius системы AAA)



На этой странице WEB интерфейса представлены настройки RADIUS (система использующая протокол для реализации аутентификации, авторизации и сбора сведений).

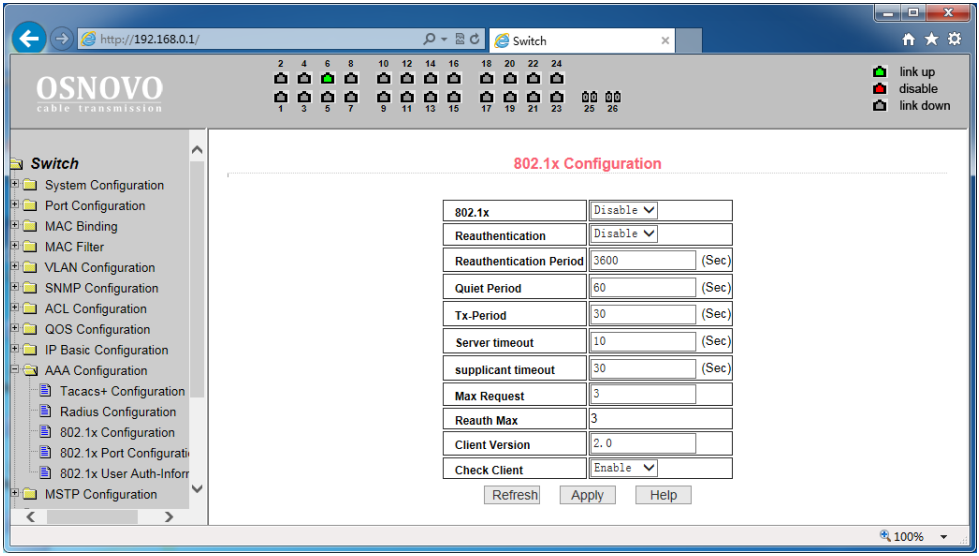
Для корректной работы системы RADIUS необходимо:

1) Быть уверенным, что IP адрес Radius сервера (Primary Server) задан прежде, чем выполнять аутентификацию и авторизацию;
2) Задать дополнительный IP адрес Radius сервера (Optional Server);
3) Указать UDP порт аутентификации (UDP Port). По умолчанию это значение равно 1812, обычно изменять это поле нет необходимости;
4) Указать следует ли выполнять аутентификацию и учет в целом в поле Accounting (значение Enable – вкл, Disable – откл.);
5) Указать порт выполнения учета (Accounting UDP Port). Значение по умолчанию 1813;

6) Ключ (Shared key) используется для установки общего пароля шифрования между коммутатором и Radius сервером. Убедитесь, что настройки аутентификации и учета (Accounting) имеют те же значения, что и на сервере Radius;
7) Информация о поставщике (vendor). Обычно, это поле не стоит изменять;
8) NAS Port, NAS port type, NAS type of service. Эти значения не меняются;
9) Roaming отвечает за включение/отключение функции Roaming протокола Radius.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.12.3 802.1x Configuration (Настройка параметров системы авторизации и аутентификации по стандарту 802.1x)



На этой странице WEB интерфейса представлены настройки системы аутентификации и авторизации на основе стандарта 802.1x:

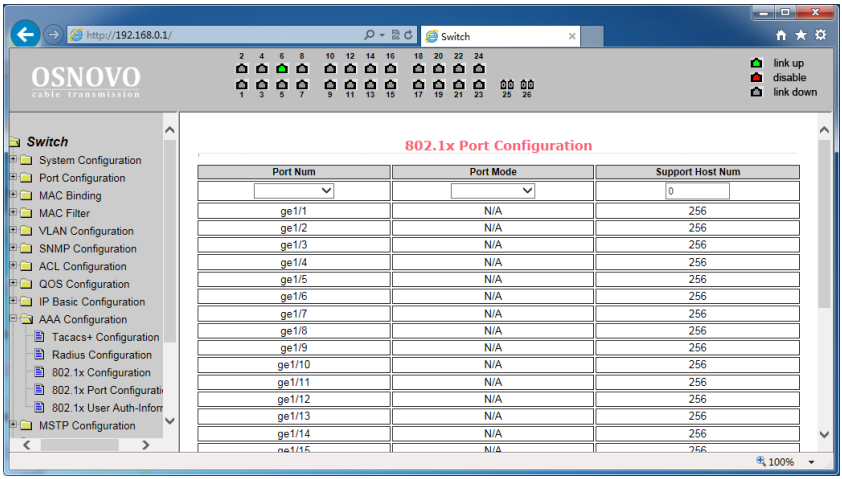
1) 802.1x – включает/выключает (Disable/Enable) применение аутентификации и авторизации по стандарту 802.1x;
2) Reauthentication – включает/выключает (Disable/Enable) повторную аутентификацию. По умолчанию отключено. Включение данной функции сделает аутентификацию пользователей более надежной, но незначительно увеличит сетевой трафик;
3) Reauthentication period – задается время в секундах для повторной аутентификации. Активно только при включенной функции Reauthentication;
4) Quiet Period – время в секундах, не требует изменения;
5) Tx-Period – не требует изменения;
6) Server timeout – не требует изменения;
7) Supplicant timeout – не требует изменения;
8) Max request users – не требует изменения;
9) Reauth Max – отображает максимальное количество повторных аутентификаций;
10) Client Version – отображает текущую версию клиента для удаленной авторизации и аутентификации через 802.1x;
11) Check Client – вкл/выкл проверки прохождения сертификата от клиента.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.12.4 802.1x Port Configuration (Настройка портов для системы авторизации и аутентификации по стандарту 802.1x)

С помощью этой страницы WEB интерфейса пользователь может изменить режим работы порта для работы системы авторизации и аутентификации по стандарту 802.1x. Порт может работать в 4х режимах:

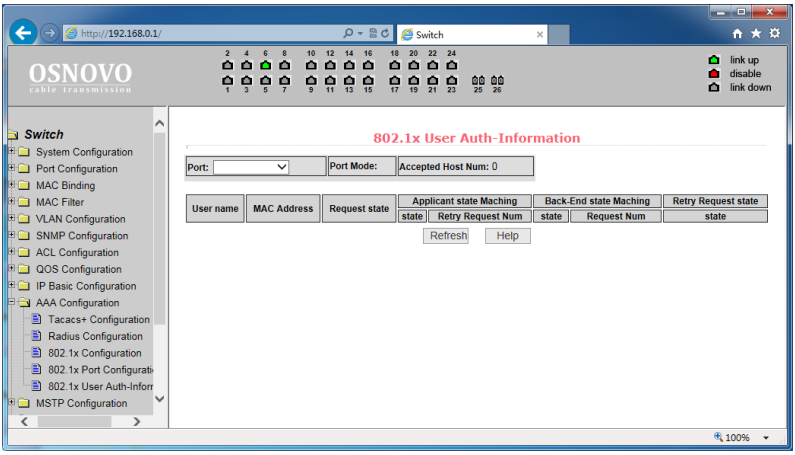
- ✓ N/A State (по умолчанию);
- ✓ Auto state (автоматически);
- ✓ Force-authorized (принудительная авторизация);
- ✓ Force-unauthorized (принудительный отказ от авторизации).



Если на порте требуется выполнять аутентификацию по стандарту 802.1x необходимо выставить режим Auto state. Если не требуется делать аутентификацию для доступа к сети следует выставить режим N/A. Остальные 2 режима редко используются в стандартных ситуациях.

Максимальное значение для пола Support Host Num – 100.

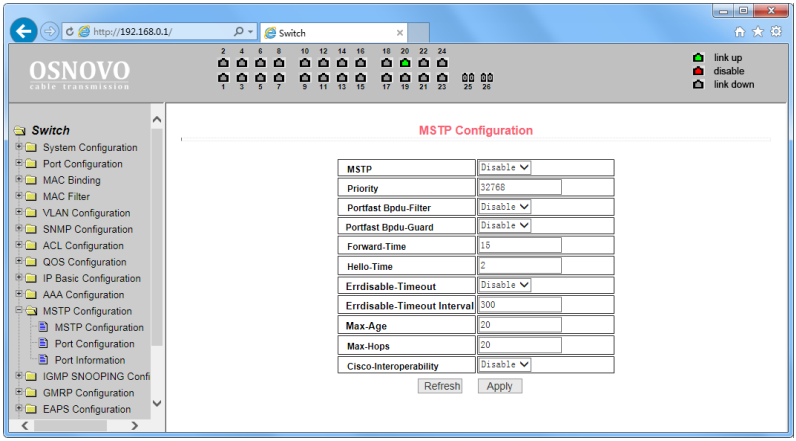
11.12.5 802.1x User Authentication Information (Информация о всех процессах аутентификации по стандарту 802.1x)



На этой странице представлены сведения обо всех процессах аутентификации на портах, настроенных для нее. Информация предоставлена только для чтения.

11.13 MSTP Configuration (Настройка работы протокола MSTP)

11.13.1 MSTP Configuration (Основные настройки MSTP)

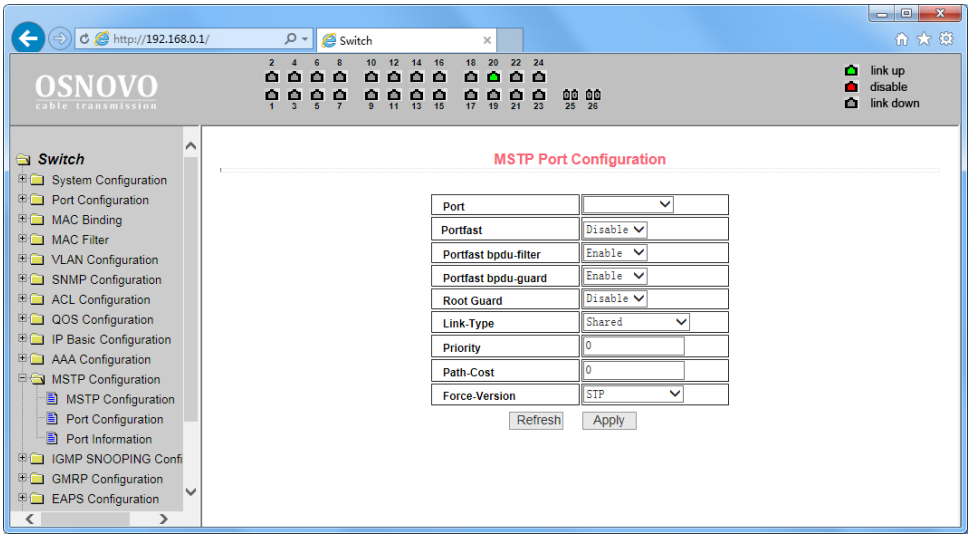


На данной странице WEB интерфейса представлены глобальные настройки протокола MSTP (Multiple Spanning Tree Protocol):

1) MSTP (Disable/Enable) – вкл/выкл поддержку протокола MSTP;
2) Priority – настройка приоритезации. Устройства с более низким приоритетом подходят больше для роли корневого моста(root bridge);
3) Portfast BPDU Filter (Disable/Enable) – вкл/выкл фильтрацию BPDU пакетов на порте;
4) Portfast BPDU Guard (Disable/Enable) – вкл/выкл функцию защиты BPDU пакетов;
5) Forward Time – настройка задержки пересылки пакетов;
6) Hello Time – настройка интервала отправки MSTP HELLO пакетов;
7) Errdisable Timeout (Enable/Disable) – вкл/выкл функции Errdisable. Если порт с включенным BPDU Guard получает пакеты BPDU запускается Errdisable таймер. По истечении заданного времени (Errdisable timeout) порт будет перезапущен;
8) Errdisable timeout – время после которого будет перезапущен порт получивший пакет BPDU;
9) Max Age – время в секундах в течение которого коммутатор ожидает информацию о конфигурации ST(spanning tree) прежде чем запустить процесс конфигурации заново;
10) Max Hops – количество переходов (хопов) до отбрасывания BPDU пакетов в домене;
11) CISCO Interoperability (Enable/Disable) – вкл/выкл совместимость с настройками STP CISCO.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.13.2 Port Configuration (настройка MSTP на портах)



1) На данной странице WEB интерфейса представлены настройки MSTP (Multiple Spanning Tree Protocol) для портов.
2) Port – выбор порта для настройки;
3) Portfast (Enable/Disable) – вкл/выкл состояния Portfast для выбранного ранее порта. В состоянии Portfast порт переходит из состояния блокировки в состояние пересылки(forward) пакетов минуя состояние обучения(learning) и прослушивания (listening);
4) Portfast BPDU filter (Enable/Disable) – вкл/выкл фильтрацию BPDU пакетов на выбранном порте;
5) Portfast BPDU GUARD (Enable/Disable) – вкл/выкл функцию защиты BPDU пакетов на выбранном порте;
6) Root Guard (Enable/Disable) – вкл/выкл функции защиты корневого моста (root bridge) от приема BPDU пакетов от устройств с более высоким приоритетом, чем мост;

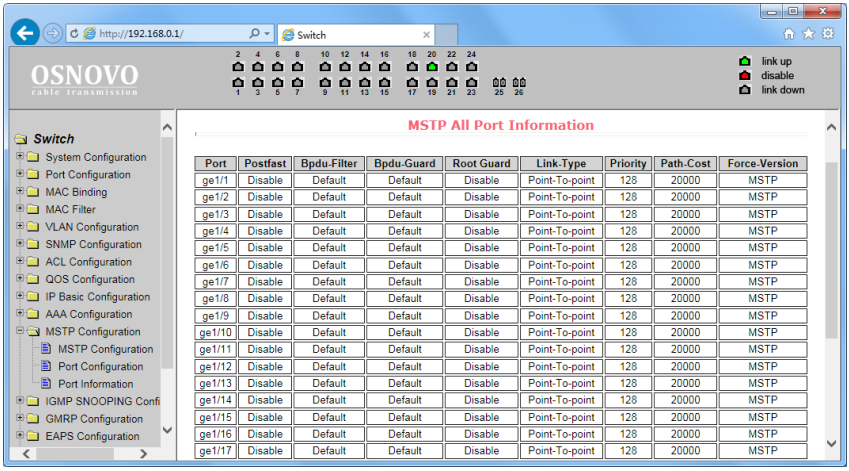
7) Link Type – настройка типа подключения. Point to Point (точка-точка) позволяет быстро менять состояние порта. Shared подключение не позволяет быстро менять состояние порта. Необходимо пройти 802.1D процедуры, чтобы определить статус порта;
8) Priority – настройка CIST приоритета, значение может быть только кратным 16 в диапазоне от 0-240. По умолчанию значение равно 128;
9) Path Cost – от 0 - 200000000. Более низкие значения обычно соответствуют root'ам;
10) Force Version – тип отправляемых пакетов.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.13.3 Port Information (Общая информация о конфигурации MSTP)

На данной странице WEB интерфейса представлена сводная информация о конфигурации MSTP.

Информация предоставлена только для чтения.



Port	Postfast	Bpdu-Filter	Bpdu-Guard	Root Guard	Link-Type	Priority	Path-Cost	Force-Version
ge1/1	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/2	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/3	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/4	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/5	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/6	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/7	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/8	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/9	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/10	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/11	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/12	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/13	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/14	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/15	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/16	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/17	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP

11.14 IGMP Snooping Configuration (Настройка отслеживания IGMP трафика)

11.14.1 IGMP Snooping Configuration (Настройки функции IGMP snooping)



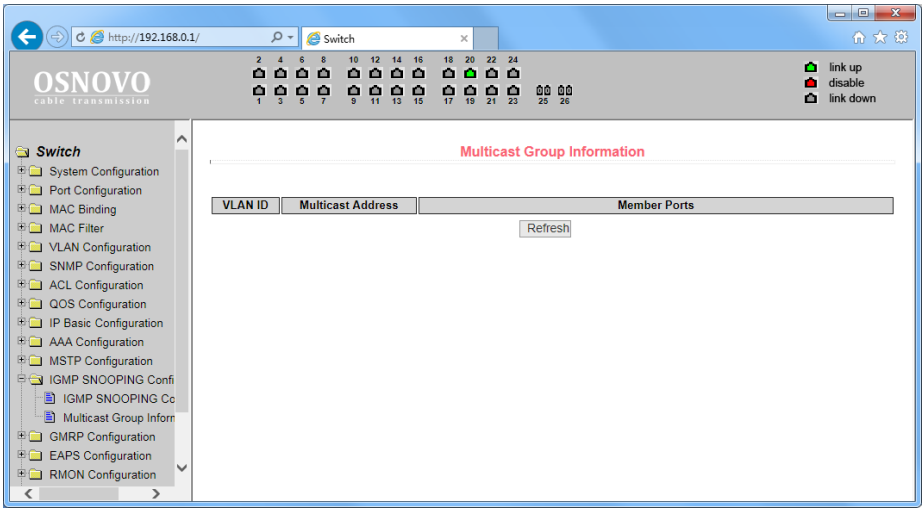
На данной странице WEB интерфейса вы можете глобально включить или выключить (Enable/Disable) функцию IGMP snooping (процесс отслеживания сетевого трафика IGMP, предотвращающий широковещательную (broadcast) ретрансляцию multicast трафика компьютерам-потребителям, которым не нужно его обрабатывать).

Включение данного протокола является обязательным при передаче трафика от большого количества передатчиков большому количеству приемников (HDMI по Ethernet). Рекомендуется также включить IGMP для VLAN

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

С помощью кнопки Refresh можно обновить значения полей.

11.14.2 Multicast Group Information (Общая информация о IGMP)



На данной странице WEB интерфейса представлена общая информация о Multicast группах созданных в процессе работы протокола IGMP.

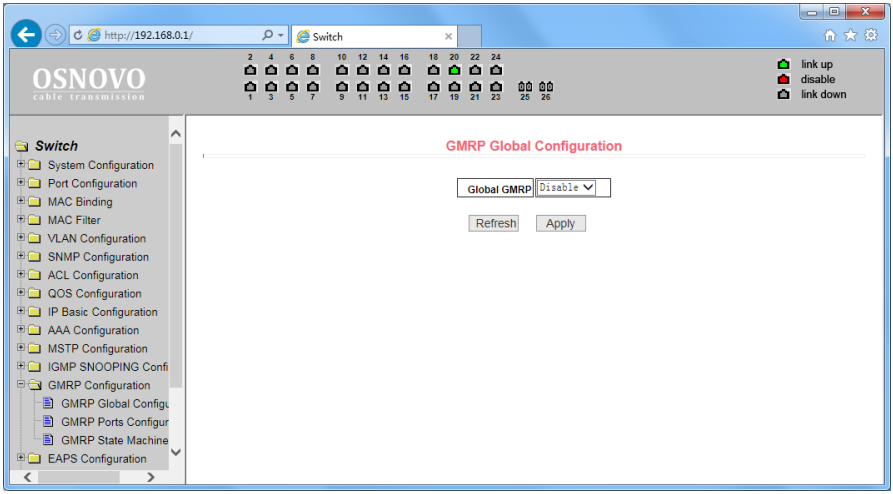
Информация предоставлена только для чтения и обновления (Refresh)

11.15 GMRP Configuration (Настройка работы протокола GMRP)

11.15.1 GMRP Global Configuration (Глобальные настройки GMRP)

На данной странице WEB интерфейса представлены глобальные настройки работы протокола GMRP (GARP Multicast Registration Protocol), предназначенного для упрощения распространения по сети информации о наличии определенной Multicast группы.

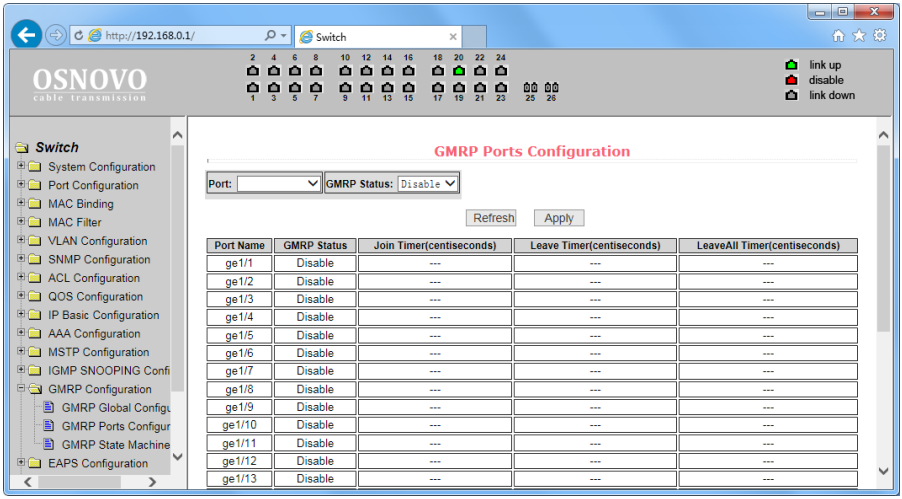
Включение/отключение поддержки GMRP осуществляется с помощью выбора Disable/Enable и последующего подтверждения кнопкой Apply (принять).



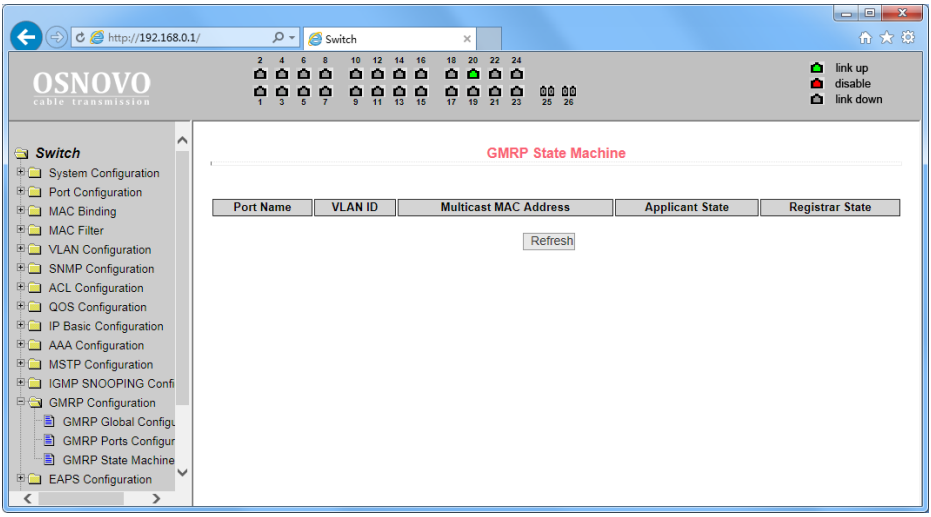
11.15.2 GMRP Ports Configuration (Настройка GMRP на портах)

На данной странице WEB интерфейса представлены настройки GMRP для отдельных портов. Порт выбирается в выпадающем меню Port, вкл/откл поддержки GMRP реализуется с помощью GMRP Status Disable/Enable.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).



11.15.3 GMRP State machine (Общая информация о GMRP)



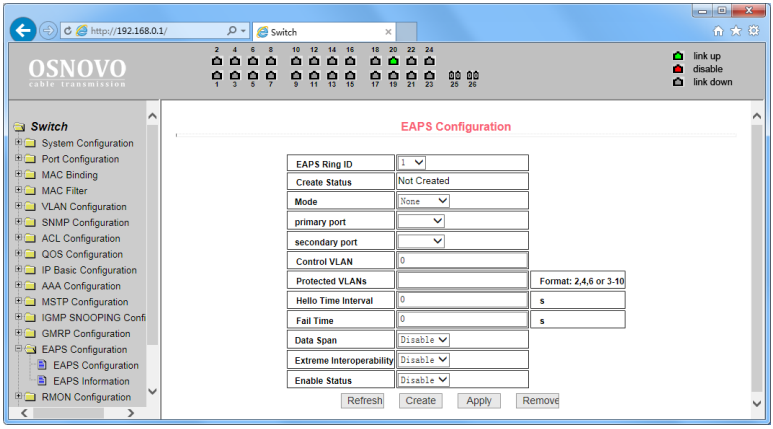
На данной странице WEB интерфейса находится сводная информация о работе протокола GMRP. Номер порта, VLAN ID, MAC адрес multicast группы и тд.

Информация предоставлена только для чтения.

Refresh – обновить содержание таблицы.

11.16 EAPS Configuration (Настройка работы протокола EAPS)

11.16.1 EAPS Configuration (Основные настройки работы протокола EAPS)

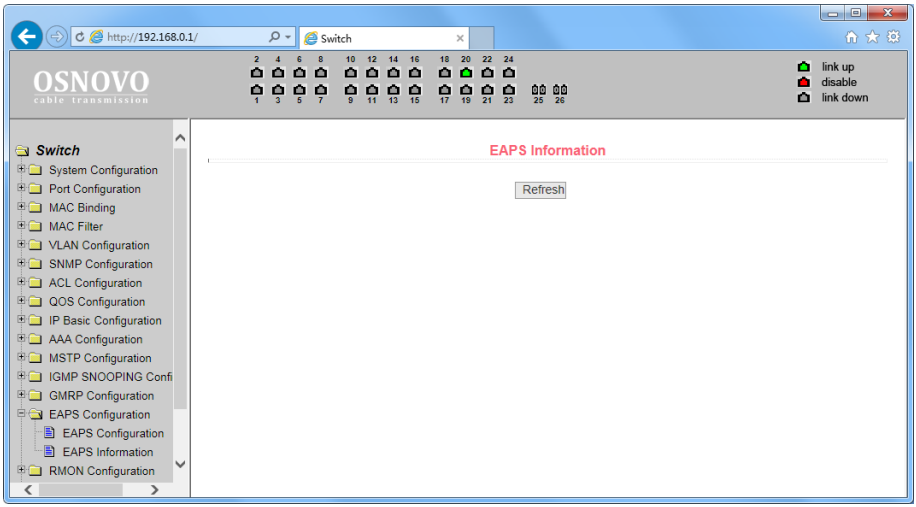


На данной странице WEB интерфейса представлены настройки протокола EAPS (Ethernet Automatic Protection Switching), предназначенного для защиты от петель в сети.

1) EAPS Ring ID – выбор ID для EAPS ring;
2) Mode – настройка режима работы рабочего узла для EAPS домена;
3) Primary Port – выбор ключевого порта для EAPS;
4) Secondary Port – выбор вторичного порта для EAPS;
5) Control VLAN – выбор VLAN ID для EAPS;
6) Protected VLANs – выбор одного или нескольких защищаемых VLAN в домене EAPS;
7) Hello Time Interval – настройка EAPS домена для периодической отправки пакетов HEALTH. Задаваемое значение в секундах должно быть меньше чем время до ошибки (fail time);
8) Fail Time – время до истечения срока действия в EAPS домене. Должно быть больше, чем Hello Time;
9) Extreme Interoperability (enable/disable) – вкл/выкл совместимость с extreme устройствами.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.16.2 EAPS information (Сводная информация о работе протокола EAPS)



На данной странице WEB интерфейса представлены общие сведения о работе протокола EAPS.

Информация представлена только для чтения и не может быть изменена с этой страницы.

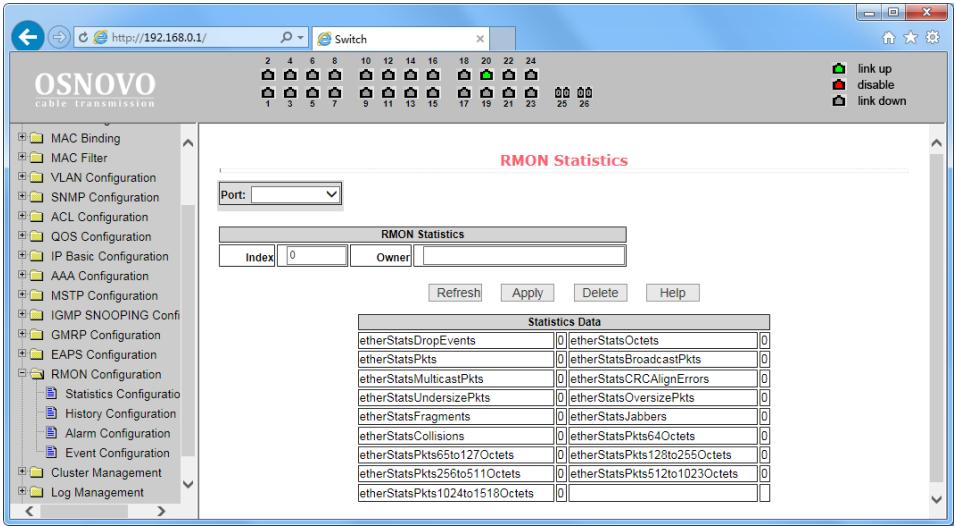
Refresh – обновить содержание страницы.

11.17 RMON Configuration (Настройка работы протокола RMON)

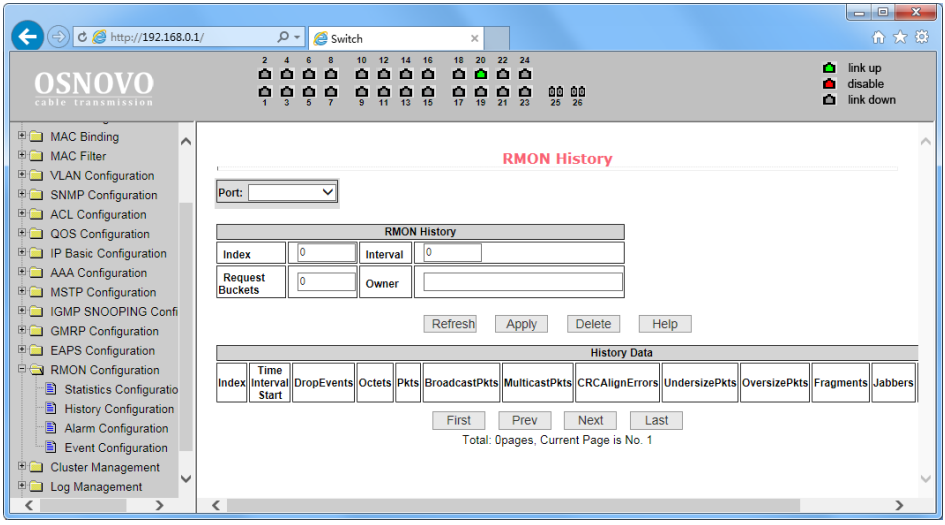
11.17.1 Statistics Configuration (Настройка групп статистики для RMON)

На данной странице WEB интерфейса представлены настройки групп статистики (Statistics) для работы RMON (дистанционный мониторинг сети).

Выберите порт из выпадающего списка Port, чтобы настроить группы данных статистики. Индекс 0 означает, что порт не сконфигурирован для RMON. Индекс может быть в пределах от 1-100. Заполнение поля Owner (владелец) не является обязательным.



11.17.2 History Configuration (Настройка групп предыстории для RMON)

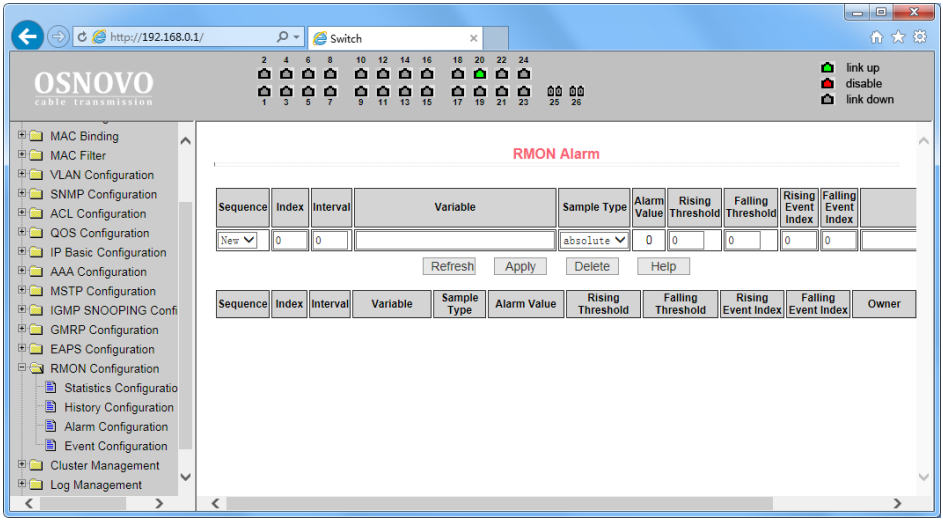


На данной странице WEB интерфейса представлены настройки групп предыстории (History) для работы RMON (дистанционный мониторинг сети).

Выберите порт из раскрывающегося списка Port для настройки. Если порт не сконфигурирован для RMON, в поле INDEX отобразится 0. Значение Index может быть в пределах от 1 до 100. Поле владельца (Owner) не обязательно к заполнению.

В поле Interval устанавливается время от 1-3600 в течение которого собираются данные. Bucket – это выделенное хранилище для сбора записей. Значение может быть от 1 – 100.

11.17.3 Alarm Configuration (Настройка групп аварийных сигналов для RMON)



На данной странице WEB интерфейса представлены настройки групп аварийных сигналов (Alarm) для работы RMON (дистанционный мониторинг сети).

Refresh – обновить таблицу.

Apply – сохранить настройки.

Delete – удалить запись из таблицы.

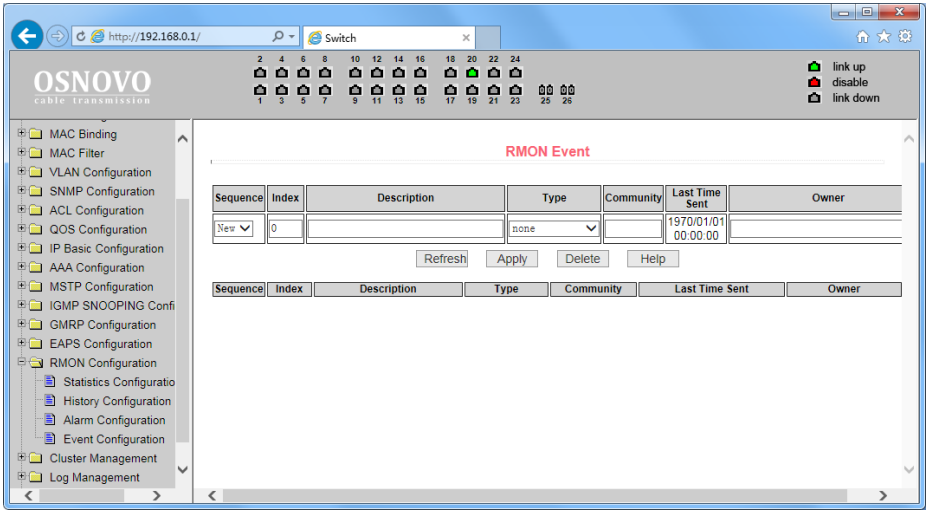
11.17.4 Event Configuration (Настройка групп событий для RMON)

На данной странице WEB интерфейса представлены настройки групп событий (Event) для работы RMON (дистанционный мониторинг сети).

Из выпадающего списка выберите группу событий, чтобы просмотреть или настроить ее. Нажмите (NEW), если хотите создать новую группу.

Диапазон возможных значений в поле Index 1-60. В поле Description (описание) задается текстовое описание группы событий. Тип событий может быть none (не реагировать), log (сохранить запись), snmp-trap, log and trap. Поле владельца (owner) заполнять не обязательно.

Поле Last time sent (последнее время отправки) доступно только для чтения и показывает, когда в последний раз событие было отправлено.



Refresh – обновить таблицу.

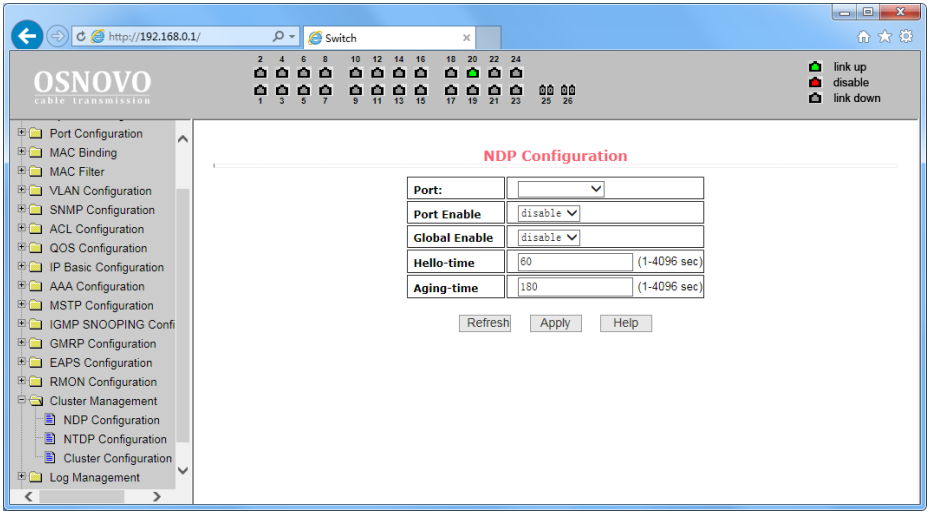
Apply – сохранить настройки.

Delete – удалить запись из таблицы.

11.18 Cluster configuration (Настройка кластера)

11.18.1 NDP Configuration (Настройка работы протокола NDP)

На данной странице WEB интерфейса представлены настройки работы протокола «обнаружения соседей» NDP (Neighbor Discovery Protocol). Данный протокол используется совместно с IPv6 и ответственен за обнаружение конфликта адресов, других узлов в кластере, поиск доступных DNS серверов и тд.



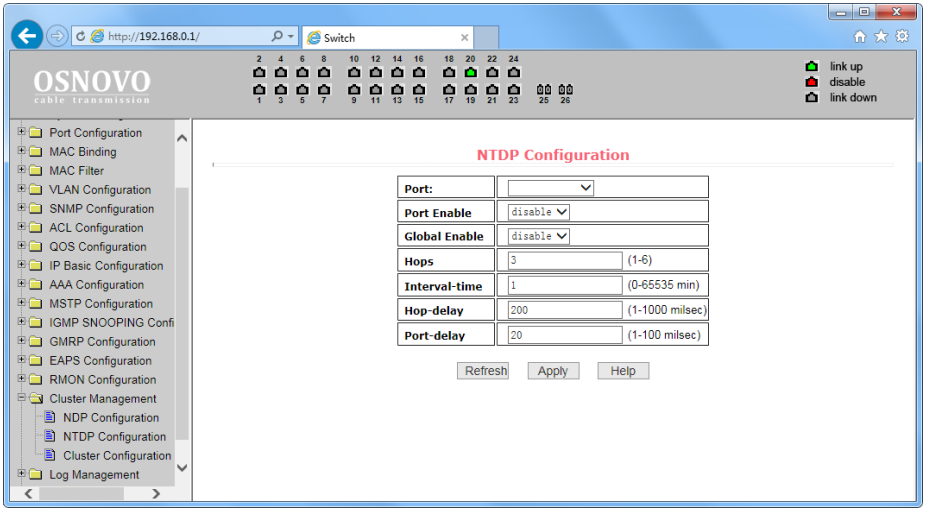
Доступны следующие настройки:

1) Port – выбор порта;
2) Port Enable (enable/disable) – вкл/выкл поддержки протокола NDP на выбранном порте;
3) Global Enable (enable/disable) – вкл/выкл глобальной поддержки протокола NDP;
4) Hello Time – интервал отправки NDP пакетов, 1-4096 сек, значение по умолчанию 60сек;
5) Aging time – интервал «старения» отправленных NDP пакетов не принятых удаленным устройством, 1-4096 сек, значение по умолчанию 180 сек.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.18.2 NTDP Configuration (Настройка работы протокола NTDP)

На данной странице WEB интерфейса представлены настройки работы протокола NTDP (Network Topology Discovery Protocol). Данный протокол используется для построения топологии в кластере.



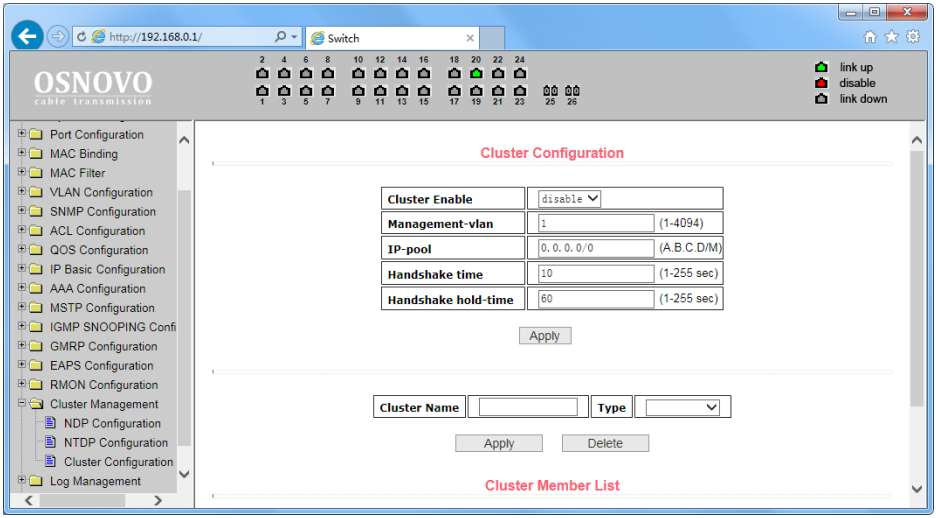
Доступны следующие настройки:

1) Port – выбор порта;
2) Port Enable (enable/disable) – вкл/выкл поддержки протокола NTDP на выбранном порте;
3) Global Enable (enable/disable) – вкл/выкл глобальной поддержки протокола NTDP;
4) Hops – доступный диапазон топологии 1-6. По умолчанию значение равно 3. Количество переходов (хопов) от самого удаленного устройства до устройства, которое контролирует всю топологию;
5) Interval Time – время сбора топологии в минутах. Значение по умолчанию 1;

6) Hop delay – допустимый интервал задержки между переходами. Доступные значения 1-1000мс. Значение по умолчанию 200мс;
7) Port delay – допустимый интервал задержки перед пересылкой пакетов на первый порт. Доступные значения 1-100мс. Значение по умолчанию 20мс.

Все настройки на данной странице подтверждаются кнопкой Apply (принять).

11.18.3 Cluster Configuration (Настройка кластера)



На данной странице WEB интерфейса представлены настройки для кластера.

Вы можете просмотреть и отредактировать таблицу с участниками кластера.

Возможные настройки включают в себя:

- ✓ Cluster enable (enable/disable) – вкл/выкл кластера;
- ✓ Management VLAN – диапазон доступных VLAN'ов от 1-4094. Значение по умолчанию 1;
- ✓ IP pool – диапазон (пул) IP адресов участников кластера. Доступный диапазон от 0.0.0.0 до 255.255.255.255. Допустимая длина маски 0 до 32;
- ✓ Handshake time – интервал отправки handshake пакетов. Допустимый диапазон значений 1-255. Значение по умолчанию 10;
- ✓ Handshake hold time – время «удерживания». Допустимый диапазон значений 1-255. Значение по умолчанию 60.

Чтобы настроить кластер вам необходимо выбрать имя кластера и выбрать соединение с кластером. Существуют ручные и автоматические методы соединения с кластером.

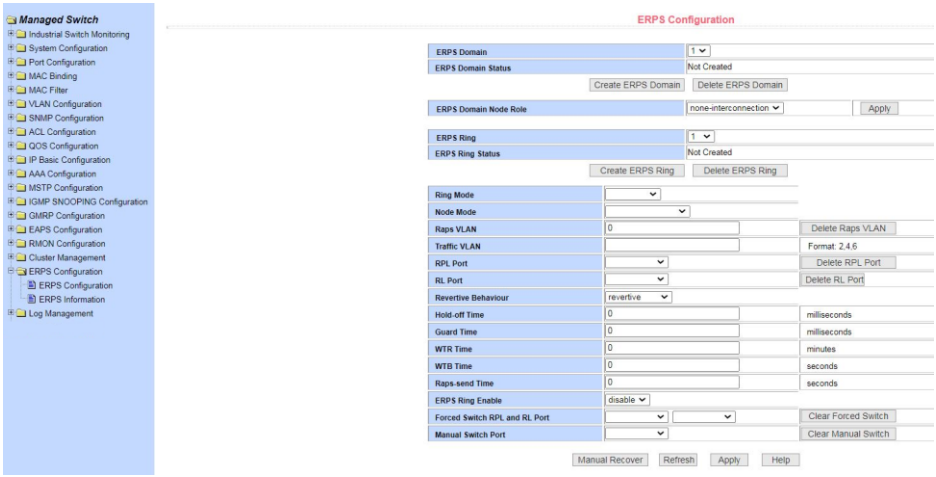
После подтверждения создания кластера вы можете автоматически переключится на ручной метод. Вы не можете в ручную переключится на автоматический метод. Ручной метод позволяет менять имя кластера.

После подтверждения создания кластера устройства – участники кластера и устройства-кандидаты могут быть просмотрены в таблице. Вы можете удалять участников кластера или добавлять устройства-кандидаты согласно списку ролей.

11.19 ERPS Configuration (Настройка ERPS)

11.19.1 ERPS Configuration (Настройка протокола ERPS)

На данной странице WEB интерфейса находятся настройки протокола ERPS – высокоэффективной альтернативе протокола STP (время восстановления линка 50мс). Данный сетевой протокол используется для исключения образования коллизий, при использовании кольцевой топологии подключения.



- ✓ Raps VLAN – VLAN ID, в которой будет передаваться служебный трафик ERPS
- ✓ Traffic VLAN – VLAN ID, которые необходимо защищать от петель и коллизий

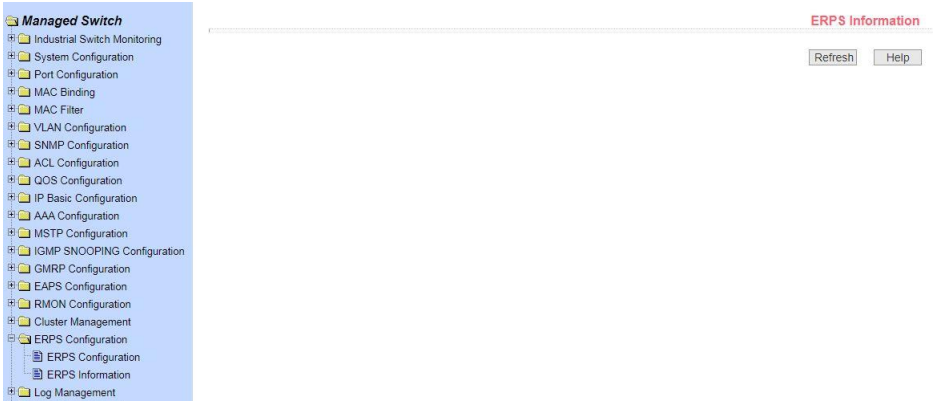
Refresh – обновить значения полей.

Apply – сохранить настройки.

11.19.2 ERPS Information (Информация о работе ERPS)

На данной странице WEB интерфейса находятся сводные данные о результате работы протокола ERPS.

Вся информация доступна только для чтения и может быть обновлена с помощью кнопки Refresh.

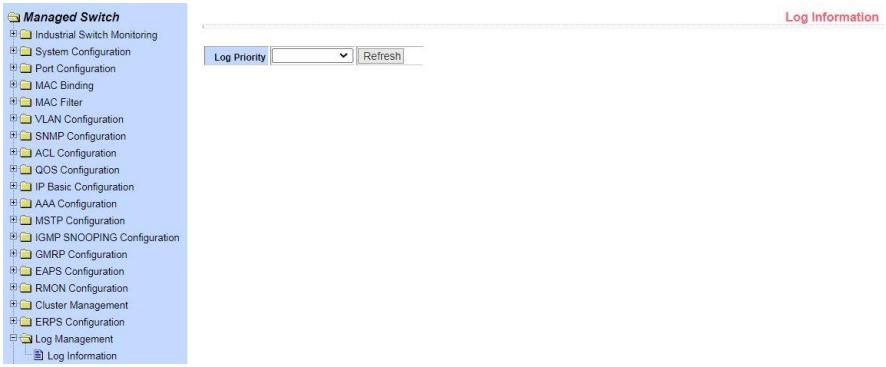


11.20 Log management (Управление записью логов)

На данной странице WEB интерфейса представлены настройки фильтра вывода записанных логов. В поле Log Priority могут быть следующие значения:

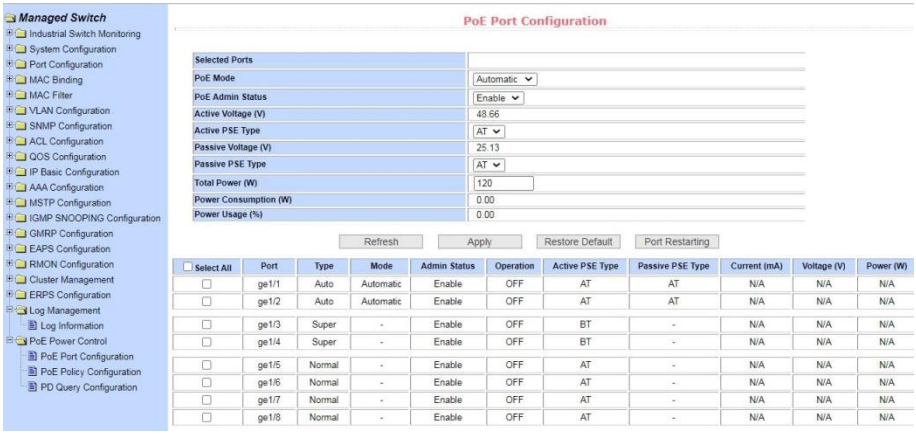
- ✓ Critical – выводить информацию, относящуюся только к критическому уровню важности;
- ✓ Debugging – выводить информацию для отладки;
- ✓ Informational – выводить информацию для отладки и общую информацию в логах;
- ✓ ALL – выводить всю информацию.

Чтобы применить фильтр логов нажмите кнопку Refresh (обновить)



11.21 PoE Power Control (Управление параметрами PoE)

11.21.1 POE Port Configuration (Настройка параметров PoE для портов)



На данной странице WEB интерфейса представлена конфигурация настроек подачи питания к подключенному к коммутатору оборудованию по технологии PoE. Для настройки доступны следующие параметры:

- ✓ PoE mode – выбор режима работы PoE для выбранного порта:
  - Automatic – автоматический режим;
  - Manual – ручной режим.
- ✓ PoE Admin Status – вкл/выкл функции PoE для выбранного порта (Enable / Disable);
- ✓ Active PSE type – выбор стандарта PoE (и ограничение максимальной мощности соответственно) для отмеченного порта:
  - AT – максимальная мощность PoE – 30 Вт;
  - AF – максимальная мощность PoE – 15.5 Вт;
  - BT – максимальная мощность PoE – 90 Вт.
- ✓ Total Power - суммарная мощность PoE. Поле для внесения информации о максимальной мощности используемого БП,

информация необходима для автоматического расчета текущей нагрузки PoE коммутатором. Установите значение равным мощности используемого БП;

Также на данной странице отражена информация о текущем состоянии PoE оборудования.

Имеется возможность обновить сведения (Refresh), подтвердить изменения (Apply), вернуть значения параметров к заводским настройкам (Restore Default), перезапустить порты (Port Restarting).

11.21.2 POE Policy Configuration (Настройка подачи PoE по расписанию)



На данной странице WEB интерфейса представлена конфигурация настроек подачи питания PoE к подключенному оборудованию по расписанию. Для настройки расписания доступны следующие параметры:

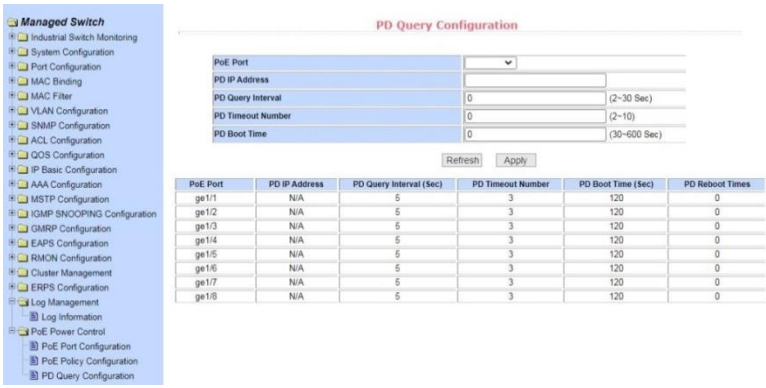
- ✓ PoE Port – выбор порта, для которого будет применяться расписание;
- ✓ Policy Status – вкл/выкл (enable/disable) применения расписания.
- ✓ Clock – выбор времени суток в часах от 00 до 24, в течение которого PoE будет активно на выбранном порте;

- ✓ Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday – выбор с помощью галок дней недели, когда будет применяться расписание

Для настройки расписания следует выбрать номер порта из выпадающего меню *PoE port*, активировать функцию Policy Status включения/отключения (enable/disable); Выбрать время в колонке Clock и день недели Monday…Sunday в соответствующей колонке.

Нажмите Apply для подтверждения, чтобы обновить информацию нажмите кнопку Refresh.

11.21.3 PD Query Configuration (Настройка функции автоопределения зависших PoE устройств)



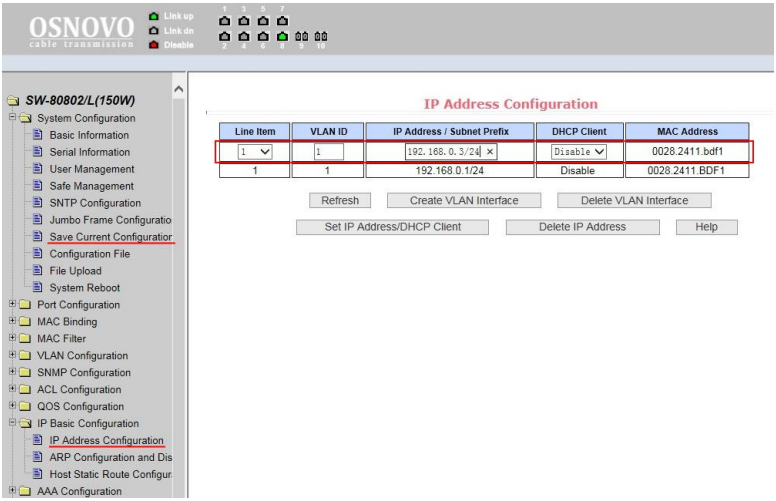
На данной странице WEB интерфейса представлена конфигурация PD Querry (PoE WatchDog) – функции автоматического определения и перезапуска зависших по какой-либо причине PoE устройств.

Для настройки доступны следующие параметры:

- ✓ PoE port – выбор номера порта (из выпадающего списка);
- ✓ PD IP address – IP адрес PoE подключенного оборудования;

- ✓ PD Query Interval – интервал отправки запросов к PoE оборудованию в пределах 2…30 сек (предустановленное время 5 сек);
- ✓ PD Timeout Number – количество запросов к PoE оборудованию, которое может оставаться без ответа в пределах 2…10 (предустановленное значение 3);
- ✓ PD Boot Time – максимальное время для перезагрузки PoE оборудования в пределах 30…600 сек (предустановленное время 120 сек).

12. Изменение IP адреса коммутатора



Для изменения IP адреса коммутатора:

- Выполните вход в WEB интерфейс коммутатора;
- Войдите в раздел меню IP Basic Configuration, пункт IP Address Configuration (Настройка IP адреса);
- установите *Line Item* «1», *DHCP Client* «Disable»;
- введите новый адрес в поле *IP Address/Subnet Prefix* (адрес должен быть уникальным и не должен повторяться);
- нажмите *Set IP Address/DHCP Client* (установить адрес), ***старый IP адрес автоматически перестанет действовать;***
- ***Выполните повторный вход в WEB интерфейс, используя новый IP адрес.***

Внимание!

Для сохранения нового IP адреса в энергонезависимой памяти коммутатора в разделе меню System Configuration, пункт Save Current Configuration (Просмотр текущей конфигурации) сохраните настройки, в противном случае при перезагрузке коммутатора будет установлен предыдущий IP адрес. Обратите внимание, что новые параметры, помимо самого IP адреса, должны содержать префикс маски подсети (значение в битах после символа "/". (Например: 192.168.0.1/24)

Внимание!

- ✓ Для обеспечения функционирования системы грозозащиты надежно заземлите корпус коммутатора;
- ✓ Соблюдайте полярность при подключении блоков питания к коммутатору;
- ✓ При обнаружении неисправности не разбирайте коммутатор и не ремонтируйте устройство самостоятельно.

13. Технические характеристики*

Модель	**SW-80822/ILR**
Общее кол-во портов	12
Кол-во портов FE+PoE	-
Кол-во портов FE	-
Кол-во портов GE+PoE	8
Кол-во портов GE (не Combo порты)	2
Кол-во портов Combo GE (RJ45+SFP)	-
Кол-во портов SFP (не Combo порты)	2
Встроенные оптические порты	-
Мощность PoE на порт (макс.)	1,2 порты – 90 Вт 3-8 порты – 30 Вт
Суммарная мощность (PoE бюджет), Вт	360 Вт
Стандарты PoE	IEEE 802.3af IEEE 802.3at IEEE 802.3bt
Метод и проводники для подачи PoE	1,2 порты – A+B (1,2,4,5+ 3,6,7,8-) 3-8 порты – A (1,2(+) 3,6(-))
Топологии подключения	звезда каскад кольцо

Модель	**SW-80822/ILR**
Буфер пакетов	4.1 МБ
Таблицы MAC-адресов	8 К
Пропускная способность коммутационной матрицы (Switching fabric)	128 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	16 КБ
Стандарты и протоколы Ethernet	• IEEE 802.3 – 10BaseT • IEEE 802.3u – 100BaseTX • IEEE 802.3ab – 1000BaseT • IEEE 802.3z – 1000Base-SX, 1000Base-LX • IEEE 802.3x – Flow Control • IEEE 802.1s, IEEE 802.1d, IEEE 802.1w – RSTP/MSTP(Rapid Spanning Tree Protocol) • EPPS ring network protocol • EAPS ring network protocol
Управление	• WEB interface; • CLI, Telnet, TFTIP, Console; • SNMP V1/V2/V3 management • RMONV1/V2 management; RMON management
Функции уровня 2	• VLAN • IGMP/MLD Snooping • DHCP Snooping • Internet Protocol Version 6 (IPv6) • Port Status, Statistics, Monitoring, Security, and Rate Limiting, Loop Detection, Port Mirroring
Качество обслуживания QoS	• CoS • ToS • Diffserv mapping • 802.1p port queue priority algorithm; • WRR, weighted priority rotation

Модель	**SW-80822/ILR**
	algorithm; • SP, WFQ priority scheduling modes
Безопасность	• User Name / Password Protection • MAC Based Authentication • User port+IP address+MAC address Support • ACL (Access control list)
Индикаторы	V1 (1-й БП), V2 (2-й БП), PWR (состояние коммутатора), Link/Speed (уст. соединения/скорость), Link/PoE, SFP Link, HW (кольцо)
Реле аварийной сигнализации	DC24V,1A(HO, H3)
Грозозащита	6 kV, 8/20us 8kV (ESD)
Питание**	DC 12-36V (без PoE) DC 48-57V (с PoE)
Энергопотребление	<25 Вт (без PoE) <385 Вт (с PoE)
Датчик температуры и влажности	• Температура (резистивный): -40…+80°C (± 0.5°C) • Влажность (емкостной): 0…99% (±3%) • Разъем – TRS 3.5mm • Интерфейс (цифровой): 1-Wire, питание (3.1-5.5V)
Охлаждение	Конвекционное (без вентилятора)
Класс защиты	IP40
Размеры (ШхВхГ) (мм)	50x188x130
Способ монтажа	На DIN рейку, на стену
Рабочая температура	-40...+80 °C
Вес	1300 г

Модель	**SW-80822/ILR**
Дополнительно	Дополнительные функции: • Передача информации о температуре и влажности окружающей среды с внешнего датчика; • Дальность передачи данных – 250м (10 Мбит/с); • PD Query – автоопределение и перезапуск зависших PoE устройств

* Производитель имеет право изменять технические характеристики изделия и комплектацию без предварительного уведомления.
**Блоки питания не входят в комплект поставки.

14. 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

Приложение А

Пример использования входа Alarm Input коммутаторов серии ILS с внешним датчиком вскрытия.

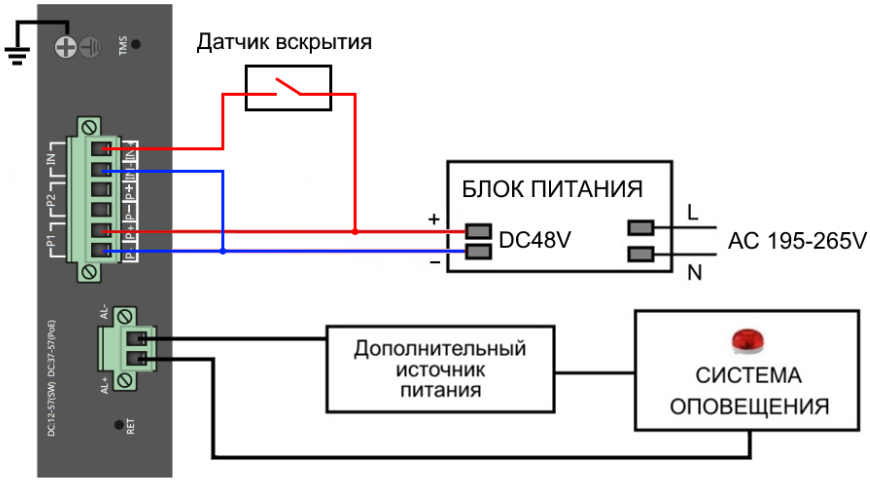
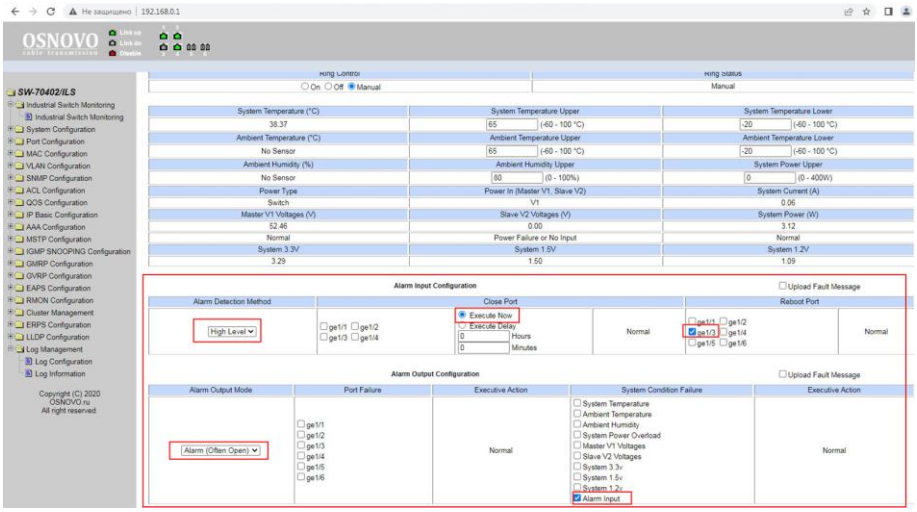


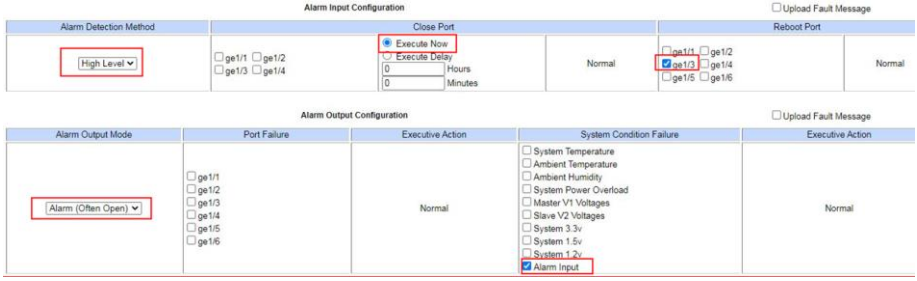
Схема подключения внешнего датчика вскрытия к входу Alarm Input коммутаторов серии ILS.

Датчик вскрытия для уличных станций OSNOVO серии OS и OSP позволяет организовать систему оповещения об открытии двери уличной станции. Датчик вскрытия представляет собой выключатель с нормально замкнутыми / разомкнутыми контактами. В зависимости от схемы подключения и типа используемых контактов датчика, требуется провести соответствующие настройки Alarm Input Configuration и Alarm Output Configuration в разделе **Мониторинг датчиков (Industrial Switch Monitoring)** WEB-интерфейса коммутатора.

Согласно приведенной выше схеме подключения, коммутатор питается от БП напряжением DC48V (клеммы P1). На вход IN клеммной колодки коммутатора подается напряжение с того же блока питания DC48V через датчик вскрытия с нормально разомкнутыми контактами (***Внимание!*** *Категорически запрещается подавать на клеммы IN напряжение более 56V)*. Для корректной работы оповещения по приведенной схеме должны быть сделаны следующие установки:



Раздел Мониторинг датчиков (Industrial Switch Monitoring) WEB-интерфейса коммутатора.



- **Alarm Input Configuration:** срабатывание (перезагрузка порта GE1/3, отмечен галкой) при подаче напряжения высокого уровня (установлено High Level, 5V < U <56V) на вход IN клеммной колодки.

- **Alarm Output Configuration:** замыкание контактов реле Al+ Al- выхода Alarm Output (установлено Often Open) при подаче сигнала высокого напряжения на вход IN клеммной колодки (установлено Alarm Input, отмечено галкой).

Таким образом, при замыкании контактов внешнего датчика вскрытия на клеммы IN колодки питания подается напряжение высокого уровня, происходит перезагрузка порта GE1/3 и замыкание контактов реле Al+ Al- выхода Alarm Output.