

OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Управляемый (L2+) коммутатор Gigabit
Ethernet на 52 порта

SW-74804/L



Прежде чем приступать к эксплуатации изделия,
внимательно прочтите настоящее руководство

www.osnovo.ru

Содержание

1. Назначение	5
2. Комплектация.....	5
3. Особенности оборудования	5
4. Внешний вид и описание элементов	6
4.1 Внешний вид	6
4.2 Описание разъемов, кнопок и индикаторов	6
5. Подключение.....	8
6. Проверка работоспособности системы	9
7. Подготовка перед управлением коммутатором через WEB.	11
8. Описание настроек и функций в WEB-интерфейсе коммутатора	14
8.1 Конфигурация системы (System Configuration).....	14
8.1.1 Basic Information (Общая информация).....	14
8.1.2 Serial Port Configuration (Настройка порта Console для управления)	15
8.1.3 User Management (Информация о пользователях)	16
8.1.4 Security Management Page (Управление безопасностью)	17
8.1.5 SNTP Configuration (Настройка протокола синхронизации времени)	18
8.1.6 Current Configuration File (Просмотр и сохранение текущей конфигурации в память коммутатора)	18
8.1.7 Configuration file (Стартовая конфигурация, сохранение файла с настройками) ..	19
8.1.8 File upload (Загрузка файла с конфигурацией)	20
8.1.9 System reboot (Перезагрузка коммутатора)	21
8.2 Port configuration (Настройка портов).....	21
8.2.1 Common Configuration (Общая настройка портов).....	21
8.2.2 Port statistics (Статистика работы портов).....	22
8.2.3 Flow Control (Управление потоком для портов)	24
8.2.4 Broadcast storm control (Настройка защиты от NetStorm)	24
8.2.5 Port rate limit (Ограничение пропускной способности на портах)	25
8.2.6 Protected Port (Защита портов)	26
8.2.7 Learn Limit (Ограничение максимального количества запоминаемых MAC адресов).....	26
8.2.8 Port Trunk Configuration (Конфигурирование trunk'ов)	27
8.2.9 Port mirroring configuration (Зеркалирование портов)	29

8.2.10 DDM information (Контроль параметров SFP модулей)	30
8. 2.11 Cable Diagnosis (Проверка кабеля).....	30
8.3 MAC binding (Привязка MAC адреса)	31
8.3.1 MAC binding configuration (Настройка привязки MAC адресов).....	31
8.3.2 MAC Auto Binding (Автоматическая привязка MAC адресов)	32
8.4 MAC filtering (Фильтрация MAC адресов).....	32
8.4.1 MAC Filter Configuration (Настройка фильтра MAC адресов)	32
8.4.2 MAC Auto Filter (Автоматический фильтр MAC адресов)	33
8.5 VLAN Configuration (Настройка VLAN)	34
8.5.1 VLAN information (Информация о VLAN)	34
8.5.2 Static VLAN Configuration (Настройка VLAN)	35
8.6 SNMP Configuration (Настройка протокола SNMP).....	36
8.6.1 SNMP Community Configuration (Общие настройки для SNMP)	36
8.6.2 TRAP Target Configuration (Настройка TRAP уведомлений)	37
8.7 ACL Configuration (Настройка Access Control List)	37
8.7.1 ACL Standard IP Configuration (Настройка ACL для IP).....	37
8.7.2 ACL Extended IP Configure (Расширенная настройка ACL правил для IP)	38
8.7.3 ACL MAC IP Configuration (Настройка ACL правил с помощью MAC).....	39
8.7.4 ACL MAC ARP Configure (Настройка ACL правил для ARP с помощью MAC адресов).....	39
8.7.5 ACL information (Информация о ACL).....	40
8.7.6 ACL reference configuration (Настройка ACL правил).....	41
8.8 QoS Configuration (Настройка предоставления трафика с разным приоритетом)	41
8.8.1 QoS Apply (Настройка приоритетов трафика для портов).....	41
8.8.2 QoS Schedule Configuration (Настройка расписания применения QoS).....	42
8.9 IP Basic Configuration (Базовая настройка IP).....	42
8.9.1 IP Address Configuration (Настройка IP адреса)	42
8.9.2 ARP configuration and display (Настройка протокола ARP и отображение таблицы ARP).....	43
8.9.3 Host Static Route Configuration (Настройка таблицы Static маршрутизации)	44
8.10 AAA Configuration (Настройка системы аутентификации авторизации и учета событий)	45
8.10.1 Tacacs+ configuration (Настройка протокола Tacacs+)	45
8.10.2 Radius Configuration (Настройка Radius системы AAA)	46

8.10.3 802.1x Configuration (Настройка параметров системы авторизации и аутентификации по стандарту 802.1x)	47
8.10.4 802.1x Port Configuration (Настройка портов для системы авторизации и аутентификации по стандарту 802.1x)	48
8.10.5 802.1x User Authentication Information (Информация о всех процессах аутентификации по стандарту 802.1x)	49
8.11 STP Configuration (Настройка протокола STP)	50
8.11.1 MSTP Configuration (Основные настройки MSTP).....	50
8.11.2 MSTP port configuration (Настройка MSTP на портах)	51
8.11.3 MSTP information (Общая информация о конфигурации MSTP)	53
8.12 IGMP snooping configuration (Настройка отслеживания IGMP трафика)	53
8.12.1 IGMP snooping configuration (Настройки функции IGMP snooping).....	53
8.12.2 Multicast Group Information (Общая информация о IGMP).....	54
8.13 GMRP Configuration (Настройка работы протокола GMRP)	54
8.13.1 GMRP Global Configuration (Глобальные настройки GMRP)	54
8.13.2 GMRP ports configuration (Настройка GMRP на портах)	55
8.13.3 GMRP State machine (Общая информация о GMRP)	56
8.14 EAPS Configuration (Настройка работы протокола EAPS)	56
8.14.1 EAPS Configuration (Основные настройки работы протокола EAPS).....	56
8.14.2 EAPS information (Сводная информация о работе протокола EAPS)	57
8.15 RMON configuration (Настройки дистанционного мониторинга сети).....	58
8.15.1 RMON statistics (Статистика дистанционного мониторинга сети)	58
8.15.2 RMON history (Журнал работы RMON).....	58
8.15.3 RMON alarm (Мониторинг тревожных событий).....	59
8.15.4 RMON event (Журнал событий)	60
8.16 Cluster configuration (Управление кластерами).....	61
8.16.1 NDP configuration (NDP конфигурация)	61
8.16.2 NTDP configuration (NTDP конфигурация)	62
8.16.3 Cluster configuration (Конфигурация кластеров).....	63
8.17 Log management (Управление журналами записей)	64
9. Изменение IP адреса коммутатора	65
10. Технические характеристики*	66
11. Гарантия.....	69

1. Назначение

Управляемый (L2+) коммутатор на 52 порта SW-74804/L предназначен для объединения сетевых устройств и передачи данных между ними.

Управляемый коммутатор (далее по тексту - коммутатор) оснащен 48 портами Gigabit Ethernet (10/100/1000Base-T), а также 4-мя Gigabit Ethernet SFP-слотами (1000Base-FX).

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

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

Коммутатор SW-74804/L рекомендуется использовать, если есть необходимость объединить большое количество сетевых устройств (IP-камеры, IP-телефоны и пр.) в одну сеть с единым управлением.

Кроме того коммутатор SW-74804/L может выступать в качестве коммутатора уровня ядра (корневого коммутатора) для локальной сети, основанной на большом количестве медных линий связи.

2. Комплектация

1. Коммутатор SW-74804/L – 1шт;
2. Кабель питания – 1шт;
3. Монтажный комплект для крепления в 19” стойку – 1шт;
4. Краткое руководство по эксплуатации – 1шт;
5. Упаковка – 1шт.

3. Особенности оборудования

- Большое количество основных портов – 48;
- Достаточное количество SFP слотов – 4;
- Гибкое управление через WEB интерфейс;
- Поддержка функций L2+ (VLAN,QOS,LACP,LLDP,IGMP snooping);

- Автоматический/ручной выбор режима увеличения дальности передачи сигналов до 250м. (Скорость передачи ограничена 10 Мбит/с).
- Активное интеллектуальное охлаждение.

4. Внешний вид и описание элементов

4.1 Внешний вид



Рис.1 Коммутатор SW-74804/L

4.2 Описание разъемов, кнопок и индикаторов

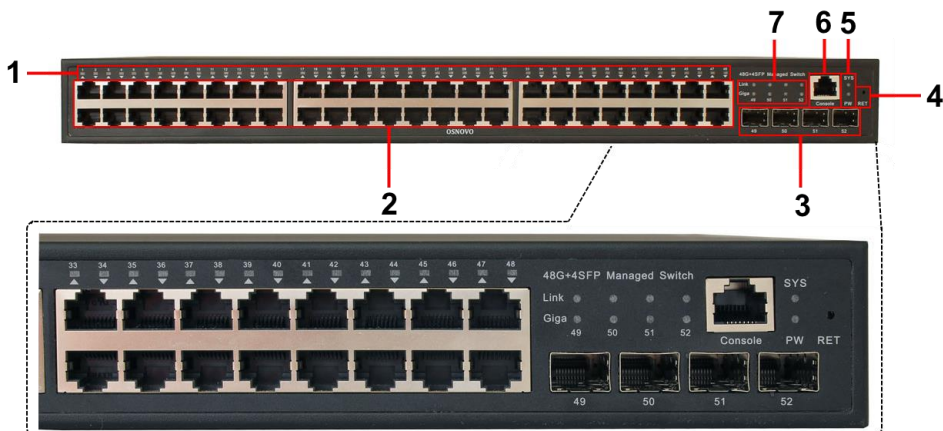


Рис.2 Коммутатор SW-74804/L , разъемы, кнопки и индикаторы

Таб. 1 Коммутатор SW-74804/L , назначение внутренних элементов

№ п/п	Обозначение	Назначение
1	1 – 48 	LED индикаторы сетевой активности и PoE на портах 1-48 <u>Горит/мигает зеленым</u> – установлено соединение.
2	1 – 48	Порты RJ-45 с 1 по 48. Предназначены для подключения сетевых устройств на скорости до 1 Гбит/с.
3	49 50 51 52	SFP слоты. Предназначены для подключения коммутатора к оптической линии связи на скорости 1Гбит/с используя SFP-модули 1,25 Гбит/с (приобретаются отдельно).
4	RET	Микрокнопка. Предназначена для сброса коммутатора к заводским настройкам. Необходимо продолжительное нажатие ~3 сек при включенном питании.
5	SYS PW	LED индикатор работы коммутатора. <u>Мигает</u> – работа в штатном режиме; <u>Горит</u> – аварийная ситуация (зависание коммутатора); <u>Быстро мигает</u> – идет загрузка прошивки. LED-индикатор подключения питания <u>Горит</u> – питание подается. <u>Не горит</u> – питание на входе отсутствует. Возможно, коммутатор не исправен.
6	Console	Разъем RJ-45. Предназначен для подключения коммутатора к COM порту. Позволяет загружать в коммутатор прошивку в случае аварийной ситуации

№ п/п	Обозначение	Назначение
7	Link Giga 49 50 51 52	LED индикаторы сетевой активности и скорости SFP слотов. <u>Link горит</u> – установлено соединение; <u>Giga горит</u> – скорость соединения 1 Гбит/с <u>Giga не горит</u> – скорость соединения 155 Мбит/с

5. Подключение

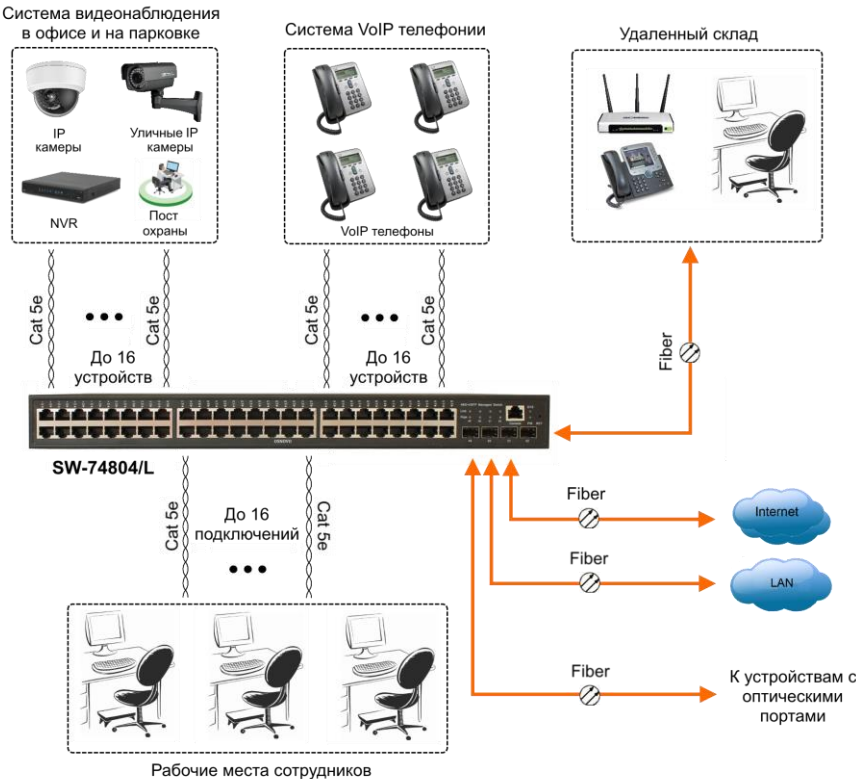


Рис. 3 Схема подключения коммутатора SW-74804/L на примере сети для большого разветвленного офиса

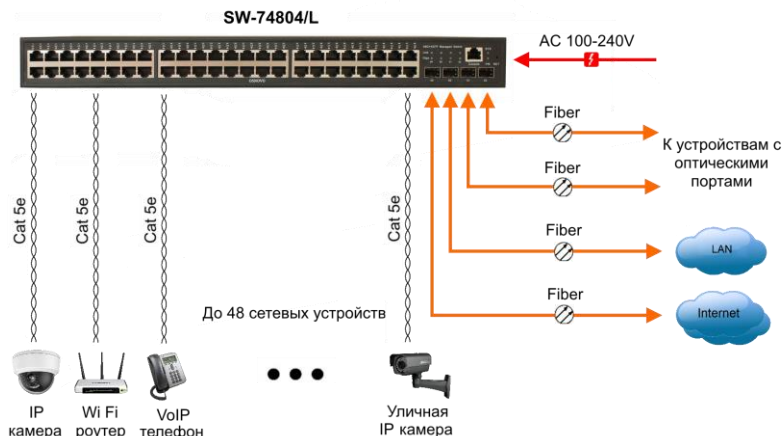


Рис. 4 Типовая схема подключения коммутатора SW-74804/L

6. Проверка работоспособности системы

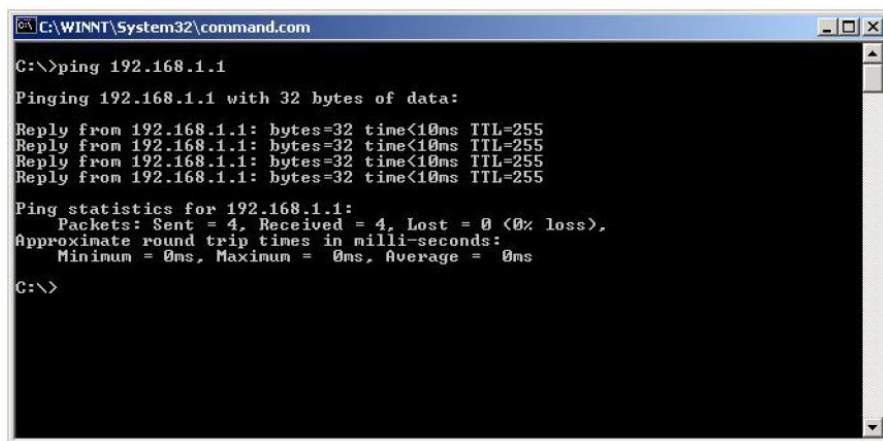
После подключения кабелей к разъёмам и подачи питания можно убедиться в работоспособности коммутатора.

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.

A screenshot of a Windows command prompt window. The title bar shows the path 'C:\WINNT\System32\command.com'. The command prompt shows the command 'C:\>ping 192.168.1.1' and its output. The output indicates a successful ping with 32 bytes of data, a time of less than 10ms, and a TTL of 255. It also shows ping statistics for 192.168.1.1: 4 packets sent, 4 received, 0% loss, and 0ms round trip times.

```
C:\WINNT\System32\command.com
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Если ответ ping не получен («Время запроса истекло»), то следует проверить соединительный кабель и IP-адреса компьютеров.

Если не все пакеты были приняты, это может свидетельствовать:

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

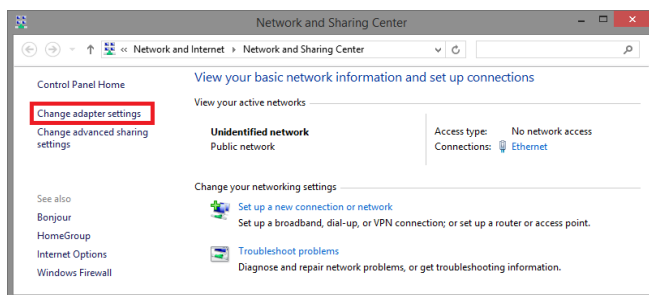
Примечание:

- Причины потери в оптической линии могут быть вызваны:
- неисправностью SFP-модулей;
- изгибами кабеля;
- большим количеством узлов сварки;
- неисправностью или неоднородностью оптоволоконка.

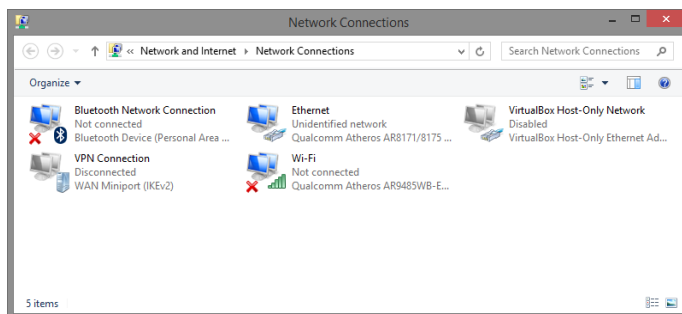
7. Подготовка перед управлением коммутатором через WEB.

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

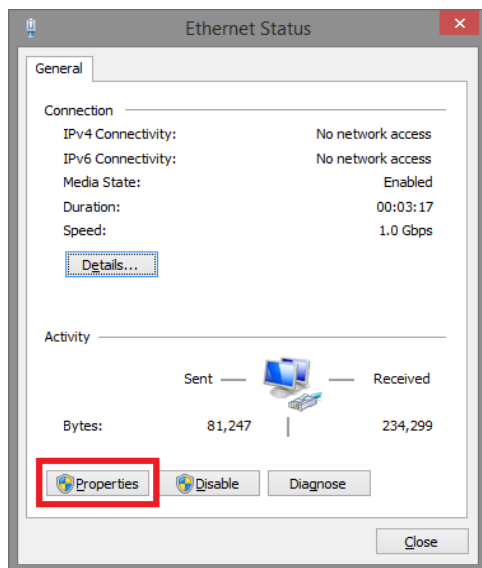
1. Откройте «Центр управления сетями и общим доступом» (Network and Sharing in Control Panel) и нажмите «Изменение параметров адаптера» (Change adapter setting) как на рисунке ниже.



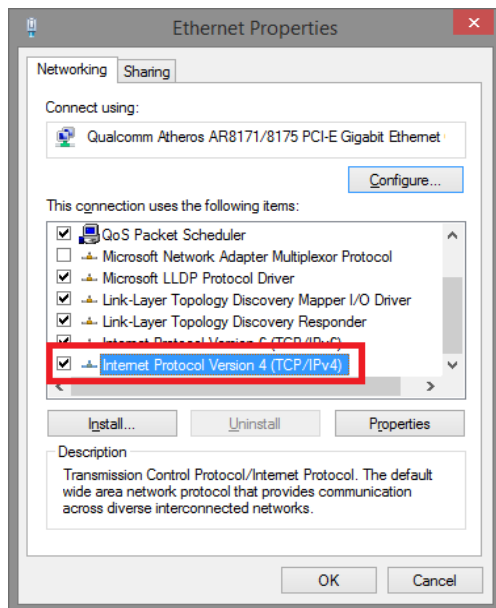
2. В появившемся окне «Сетевые подключения» (Network Connections) отображены все сетевые подключения, доступные вашему ПК. Сделайте двойной клик на подключении, которое вы используете для сети Ethernet



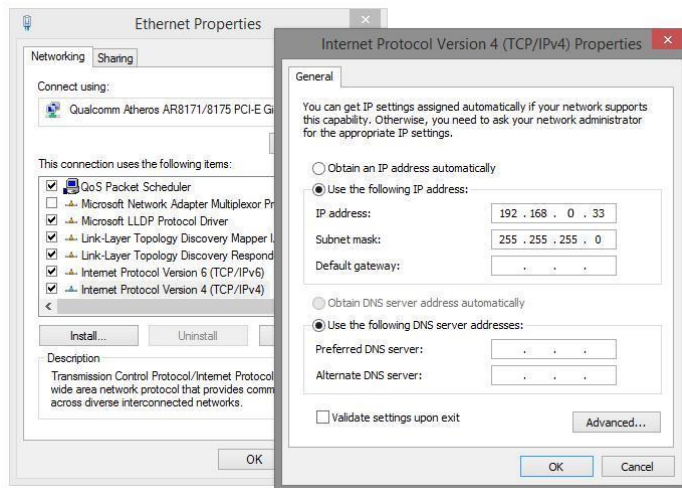
3. В появившемся окне «Состояние - Подключение по локальной сети» (Ethernet Status) нажмите кнопку «Свойства» (Properties) как показано ниже.



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

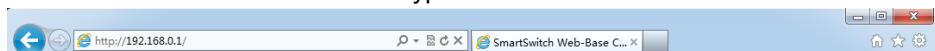


5. В появившемся окне «Протокол интернета версии IP V4 (TCP/IPv4)» сконфигурируйте IP адрес вашего ПК и маску подсети как показано ниже



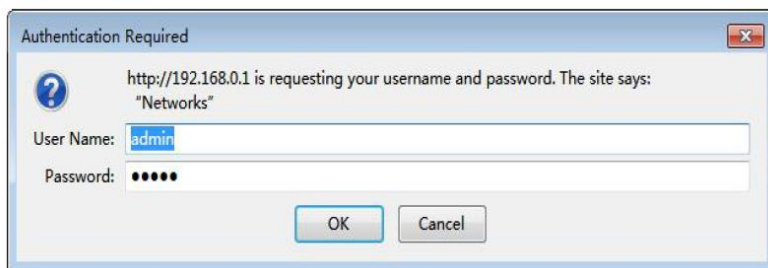
По умолчанию IP адрес коммутатора **192.168.0.1** Вы можете задать любой IP адрес в поле «IP адрес», в той же подсети что и IP адрес коммутатора. Нажмите кнопку ОК, чтобы сохранить и применить настройки.

6. Введите в адресную строку **192.168.0.1** (IP-адрес коммутатора) и нажмите Enter на клавиатуре.

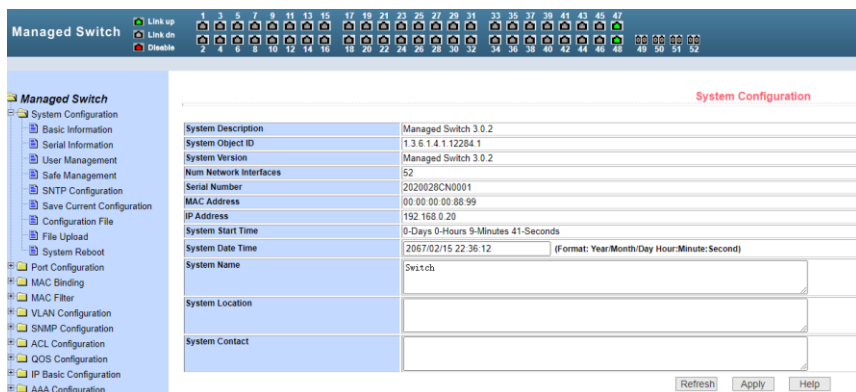


7. Появится форма аутентификации.

По умолчанию Login: **admin** Password: **admin**



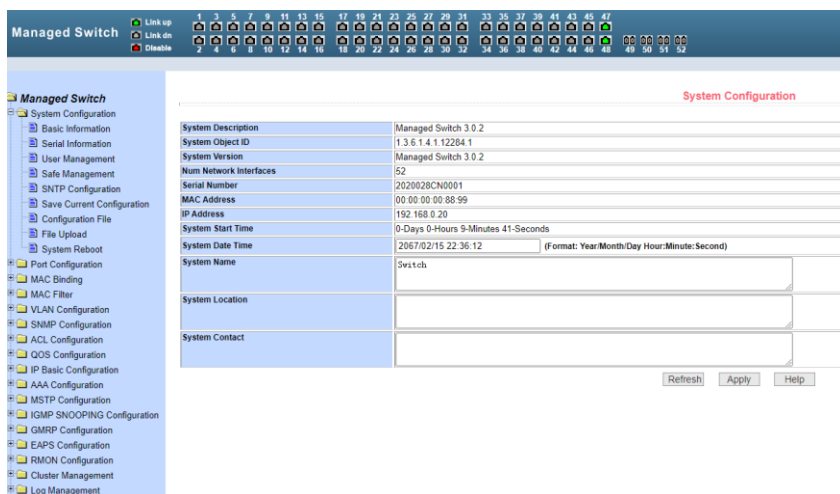
8. После корректного ввода имени пользователя(логин) и пароля появится главное окно WEB интерфейса коммутатора



8. Описание настроек и функций в WEB-интерфейсе коммутатора

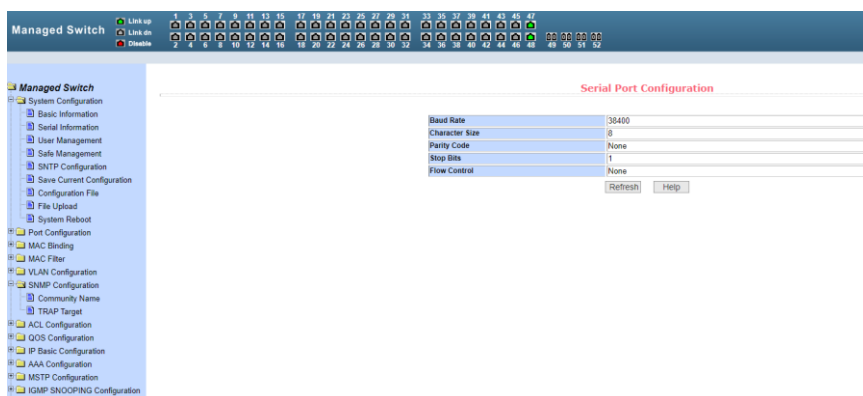
8.1 Конфигурация системы (System Configuration)

8.1.1 Basic Information (Общая информация)



- 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 всех портов для соединения с сетью;
- System start time (Время запуска системы) отображает сколько времени прошло с момента включения;
- System name (Имя коммутатора) отображает имя коммутатора. Пользователь может переименовать коммутатор;
- System location (Местоположение коммутатора) отображает физическое местоположение коммутатора. Задается пользователем;
- System Contact (Контактные данные) отображает имя владельца и его контактные данные. Задается пользователем.

8.1.2 Serial Port Configuration (Настройка порта Console для управления)



Данная страница WEB-интерфейса отображает параметры управления коммутатором через интерфейс RS232/485 (COM порт в ПК), используя его порт Console. При управлении коммутатором через HyperTerminal убедитесь, что настройки соответствуют приведенным на этой странице значениям.

- Baud rate (скорость передачи данных)
- Character Size (размер символов)
- Parity code (бит четности)
- Stop bits (стоповые биты)
- Flow control (управление потоком).

8.1.3 User Management (Информация о пользователях)

The screenshot displays the 'Multi-user Management Configuration' page. On the left is a navigation tree under 'Managed Switch' with categories like System Configuration, Basic Information, User Management, and Security Management. The main area contains a table for user management:

Item	User name	Old password	New password	Re-enter password	Privilege
New	admin				Privilege

Below the table are buttons: Refresh, Apply, Delete, and Help.

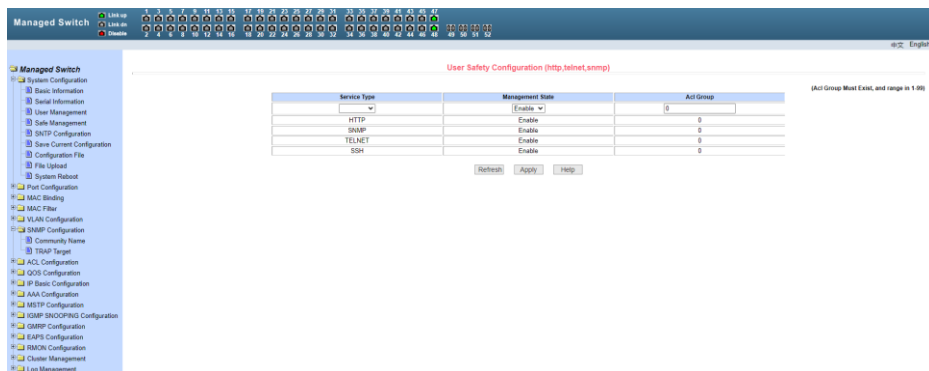
На данной странице WEB интерфейса можно изменить/задать новый пароль (new password) для текущего пользователя, изменить права доступа к управлению коммутатором (privilege) и др.

Пароли нужно вводить с учетом регистра. Они могут содержать до 16 символов. Для ввода пароля необходимо дважды ввести новый пароль в поле New Password и в Re-enter Password. Для того чтобы изменения вступили в силу, 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 многопользовательский режим управления коммутатором (*multi-user*).

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

8.1.4 Security Management Page (Управление безопасностью)



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

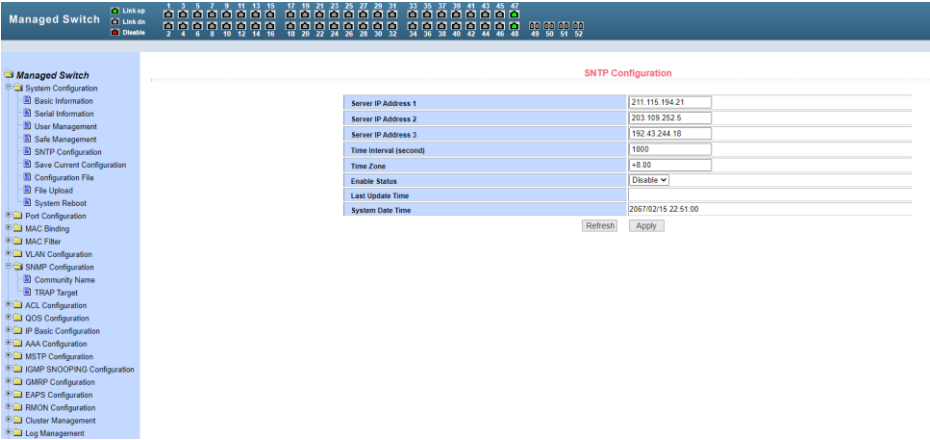
Есть возможность полностью отключить управление коммутатором для конкретного метода управления (WEB, TELNET или SNMP). По умолчанию управление с помощью каждого метода разрешено и ACL фильтрация не применяется.

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

При применении ACL фильтрации для каждого метода управления необходимо указать этот метод в списке *service type*, а затем выбрать ACL от 1 до 99. Главное условие – выбранный ACL должен быть создан заранее.

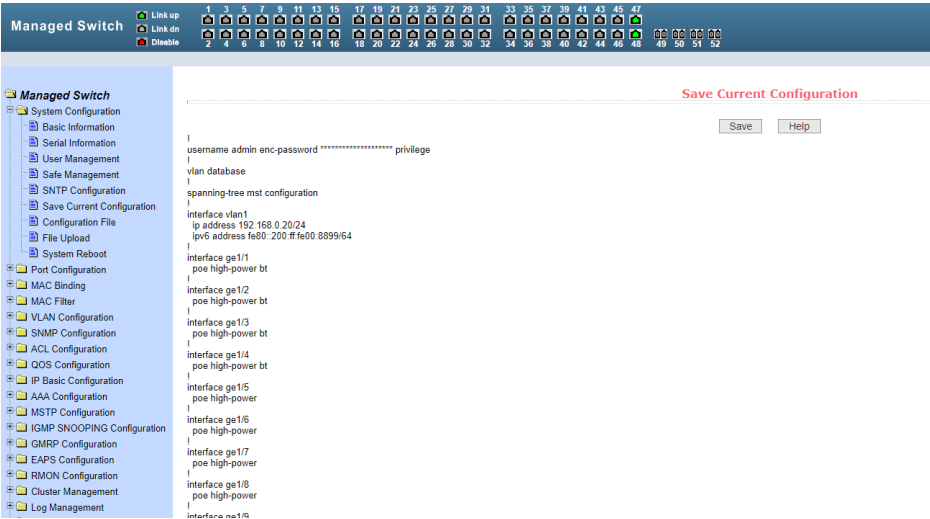
Обратите внимание, если администратор закроет возможность управлять коммутатором по WEB, эта страница с настройками перестанет быть доступна. Тогда можно воспользоваться другим методом управления, например через Telnet или SNMP.

8.1.5 SNTP Configuration (Настройка протокола синхронизации времени)



На этой странице находятся настройки SNTP (протокол синхронизации времени по компьютерной сети). После необходимых настроек необходимо нажать кнопку Apply (Принять).

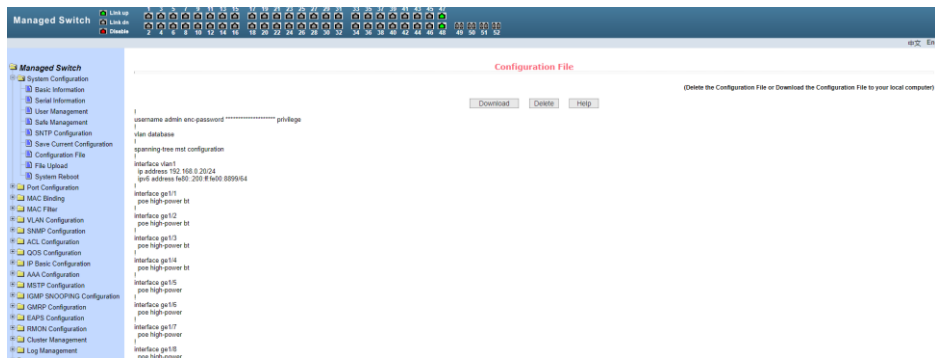
8.1.6 Current Configuration File (Просмотр и сохранение текущей конфигурации в память коммутатора)



На данной странице WEB интерфейса отображается текущая конфигурация коммутатора. Кнопка Save (сохранить) позволит сохранить текущую конфигурацию коммутатора в память коммутатора.

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

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

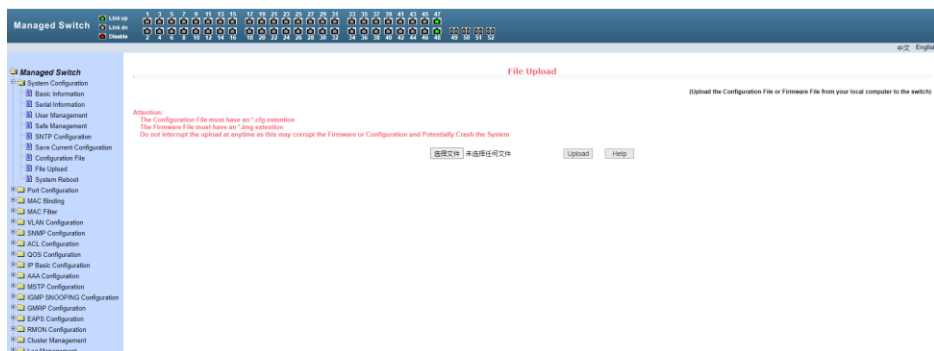


Стартовая конфигурация представляет собой файл, записанный во FLASH памяти коммутатора. Когда коммутатор запускается и не находит записанный ранее файл конфигурации во FLASH памяти, устройство использует файл с настройками по умолчанию (default).

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

8.1.8 File upload (Загрузка файла с конфигурацией)



На этой странице представляется доступ к загрузке ранее созданных файлов конфигурации в память коммутатора.

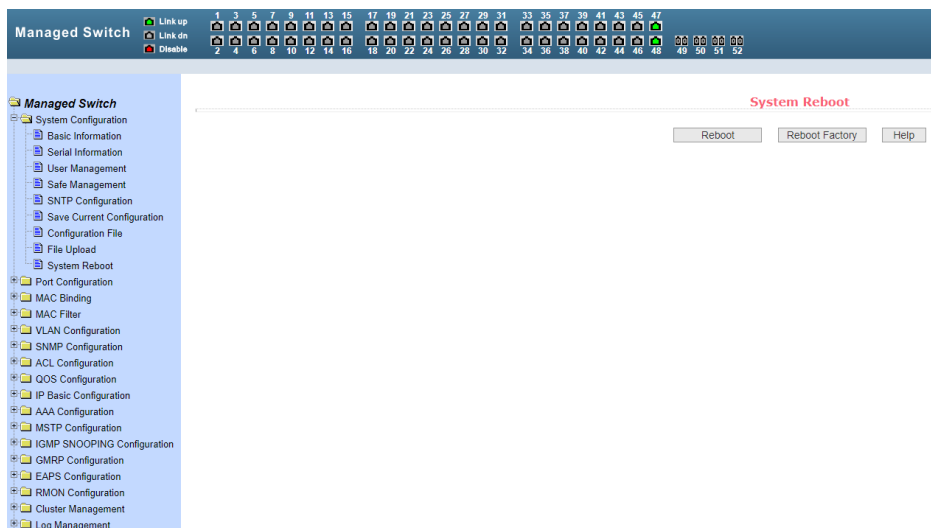
Нажмите кнопку Path (путь), чтобы выбрать нужный файл с конфигурацией на ПК. Затем нажмите кнопку Upload (загрузить). Файл должен иметь расширение: .cfg

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

Внимание

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

8.1.9 System reboot (Перезагрузка коммутатора)



На данной странице WEB интерфейса предоставляется доступ к перезагрузке коммутатора или загрузке заводских настроек.

Для этого нажмите кнопку Reboot (перезагрузка) или Reboot Factory (сброс к заводским настройкам). В появившемся диалоговом окне подтвердите свое действие кнопкой Ok или отмените его с помощью кнопки Cancel (отмена).

8.2 Port configuration (Настройка портов)

8.2.1 Common Configuration (Общая настройка портов)

На данной странице WEB интерфейса представлена информация о настройках по каждому порту коммутатора. Пользователь может менять скорость передачи данных, 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). Чтобы изменения вступили в силу, нажмите кнопку Apply (принять). Таким же образом выбирается 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.

После внесения изменений нажмите кнопку *Apply* (принять).

Нажатие кнопки *Refresh* (обновить) обновит значения настроек для портов до текущих.

Managed Switch

Link up

Link do

Disable

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

Port Common Configuration/Show

Selected Ports

Admin Status

Config Speed

Up

Auto-Negotiate

Refresh

Apply

Help

Select All	Port	Admin Status	Operate Status	Duplex/Flowcontrol	Config Speed	VLAN Mode	Default VLAN
☐	ge11	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge12	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge13	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge14	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge15	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge16	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge17	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge18	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge19	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge110	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge111	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge112	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge113	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge114	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge115	Up	Down	Unknown	Auto-Negotiate	Access	1
☐	ge116	Up	Down	Unknown	Auto-Negotiate	Access	1

8.2.2 Port statistics (Статистика работы портов)

Managed Switch

Link up

Link do

Disable

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

Port Statistics Information

Port:

Port Statistics Information

Received Total Bytes (RfInOctets)	0	Received Unicast Packets Num (RfInUcastPkts)	0
Received Non-Unicast Packets Num (RfInNucastPkts)	0	Received Discard Packets Num (RfInDiscards)	0
Received Error Packets Num (RfInErrors)	0	Received Unknown Protocol Packets Num (RfInUnknownProts)	0
Send Total Bytes (RfOutOctets)	0	Send Unicast Packets Num (RfOutUcastPkts)	0
Send Non-Unicast Packets Num (RfOutNucastPkts)	0	Send Discard Packets Num (RfOutDiscards)	0
Send Error Packets Num (RfOutErrors)	0		

Refresh

Help

На данной странице WEB интерфейса представлена накопленная информация по работе портов.

Для выбора конкретного порта воспользуйтесь выпадающим 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 «брошенных» 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).

8.2.3 Flow Control (Управление потоком для портов)

Данная страница WEB интерфейса 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).

Managed Switch

Link up

Link on

Disable

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

Managed Switch

System Configuration

Port Configuration

Common Configuration

Port Statistics

Flow Control

Broadcast Storm

Port RateLimit

Protected Port

Learn Limit

Port Tunneling

Mirror

DDM Information

MAC Binding

MAC Filter

VLAN Configuration

SNMP Configuration

ACL Configuration

QOS Configuration

IP Basic Configuration

AAA Configuration

MSTP Configuration

IGMP Snooping Configuration

GMP Configuration

EAPS Configuration

RMON Configuration

Cluster Management

Log Management

Flow Control

Port:

Flow Control

OFF

Refresh

Apply

Help

Port Name	Flow Control State
ge0/1	OFF
ge0/2	OFF
ge0/3	OFF
ge0/4	OFF
ge0/5	OFF
ge0/6	OFF
ge0/7	OFF
ge0/8	OFF
ge0/9	OFF
ge0/10	OFF
ge0/11	OFF
ge0/12	OFF
ge0/13	OFF
ge0/14	OFF
ge0/15	OFF
ge0/16	OFF
ge0/17	OFF
ge0/18	OFF
ge0/19	OFF
ge0/20	OFF

8.2.4 Broadcast storm control (Настройка защиты от NetStorm)

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

Managed Switch

Link up

Link on

Disable

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

Managed Switch

System Configuration

Port Configuration

Common Configuration

Port Statistics

Flow Control

Broadcast Storm

Port RateLimit

Protected Port

Learn Limit

Port Tunneling

Mirror

DDM Information

MAC Binding

MAC Filter

VLAN Configuration

SNMP Configuration

ACL Configuration

QOS Configuration

IP Basic Configuration

AAA Configuration

MSTP Configuration

IGMP Snooping Configuration

GMP Configuration

EAPS Configuration

RMON Configuration

Cluster Management

Log Management

Broadcast Storm Control

Port:

Broadcast Suppression

OFF

Broadcast RateLimit

0

(1-1024000 kbps)

Multicast Suppression

OFF

Multicast RateLimit

0

(1-1024000 kbps)

DLF Suppression

OFF

DLF RateLimit

0

(1-1024000 kbps)

Refresh

Apply

Help

Port Name	Broadcast Suppression	Broadcast RateLimit (kbps)	Multicast Suppression	Multicast RateLimit (kbps)	DLF Suppression	DLF RateLimit (kbps)
ge0/1	OFF	64	OFF	64	OFF	64
ge0/2	OFF	64	OFF	64	OFF	64
ge0/3	OFF	64	OFF	64	OFF	64
ge0/4	OFF	64	OFF	64	OFF	64
ge0/5	OFF	64	OFF	64	OFF	64
ge0/6	OFF	64	OFF	64	OFF	64
ge0/7	OFF	64	OFF	64	OFF	64
ge0/8	OFF	64	OFF	64	OFF	64
ge0/9	OFF	64	OFF	64	OFF	64
ge0/10	OFF	64	OFF	64	OFF	64
ge0/11	OFF	64	OFF	64	OFF	64
ge0/12	OFF	64	OFF	64	OFF	64
ge0/13	OFF	64	OFF	64	OFF	64
ge0/14	OFF	64	OFF	64	OFF	64
ge0/15	OFF	64	OFF	64	OFF	64
ge0/16	OFF	64	OFF	64	OFF	64
ge0/17	OFF	64	OFF	64	OFF	64
ge0/18	OFF	64	OFF	64	OFF	64
ge0/19	OFF	64	OFF	64	OFF	64
ge0/20	OFF	64	OFF	64	OFF	64

В выпадающем списке PORT (порт) выберите нужный порт, включите (ON) или выключите (OFF) защиту для конкретного вида пакетов *Broadcast*, *Multicast* или *DLF*.

Также можно задать скорость (Кбит/с) для конкретного вида пакетов. Значения скорости *DLF* и *Multicast* должны быть одинаковыми.

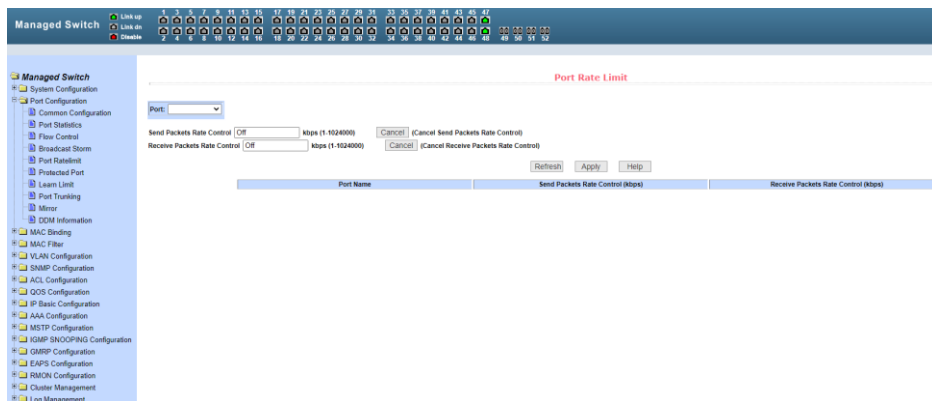
Все изменения подтверждаются кнопкой Apply (принять).

8.2.5 Port rate limit (Ограничение пропускной способности на портах)

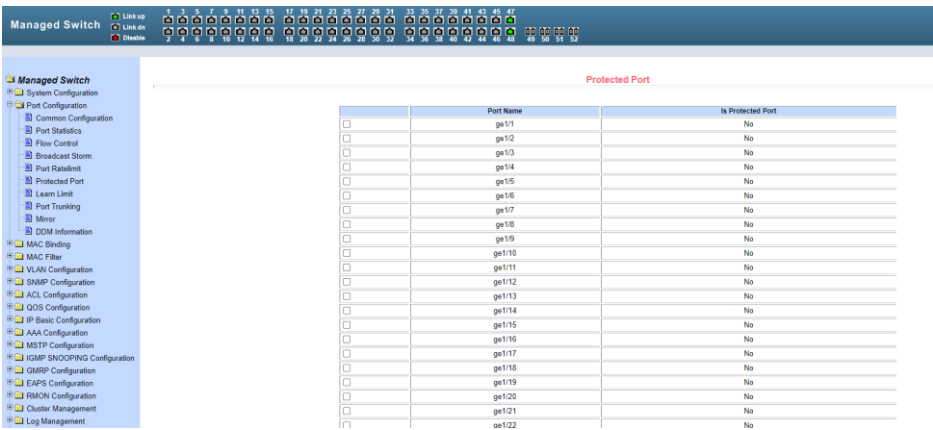
На данной странице можно гибко ограничивать скорость приема/передачи пакетов на выбранном порте. Для этого выберите порт в выпадающем списке PORT, укажите значение (Кбит/с) для скорости передачи данных (Send Packets Rate Control) и для скорости приема данных (Receive Packets Rate Control).

Для подтверждения выбранных настроек нажмите кнопку Apply (принять).

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



8.2.6 Protected Port (Защита портов)



На данной странице WEB интерфейса 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.

8.2.7 Learn Limit (Ограничение максимального количества запоминаемых MAC адресов)

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).

Learn Limit

Port:

MAC Address Num Able To Learn: (0-8191)

Port Name	MAC Address Num Able To Learn
ge1/1	8191
ge1/2	8191
ge1/3	8191
ge1/4	8191
ge1/5	8191
ge1/6	8191
ge1/7	8191
ge1/8	8191
ge1/9	8191
ge1/10	8191
ge1/11	8191
ge1/12	8191
ge1/13	8191
ge1/14	8191
ge1/15	8191
ge1/16	8191
ge1/17	8191
ge1/18	8191
ge1/19	8191
ge1/20	8191

8.2.8 Port Trunk Configuration (Конфигурирование trunk'ов)

На данной странице WEB интерфейса представлены настройки для конфигурации trunk портов.

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

Port Trunking Configuration

Trunk Group ID:

Trunk Method:

Member Port:

(Note: There must have at least one trunk group when you configure trunk method. All the trunks use the same trunk method. You can only delete or add a member port when a trunk already exists. Delete trunk groups when they have no member.)

Чтобы создать trunk для порта или изменить существующий, необходимо выбрать ID от 1 до 8.

Чтобы внести изменения или создать trunk-группу выберите соответствующий trunk group ID (от 1 до 8) из списка. Информация о trunk-группе будет отображена в поле member port.

Для создания trunk-группы выберите ID в trunk group ID и нажмите Create Trunk Group, в скобках появится соответствующая информация).

Для настройки метода транкинга портов выберите из выпадающего списка необходимый и нажмите на кнопку Set up aggregation method.

Чтобы добавить порт в trunk-группу выберите соответствующий порт из списка и нажмите Member Port =>. Для удаления порта из группы выберите соответствующий порт и нажмите Unmember port <=.

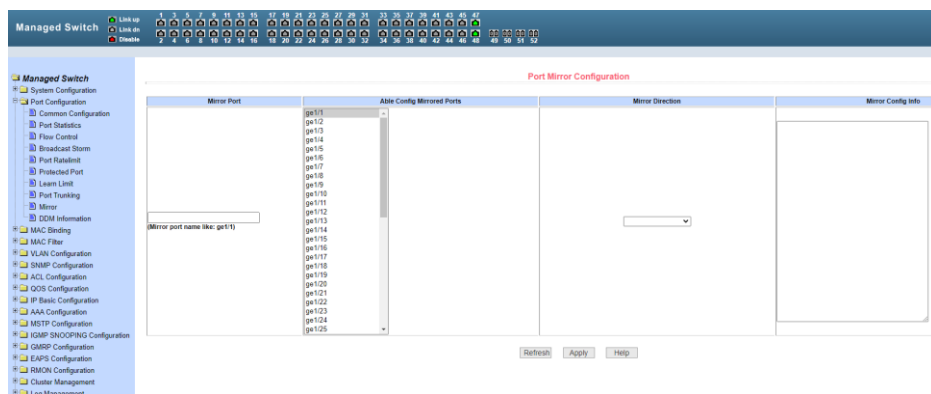
Для удаления существующей trunk-группы используйте кнопку Delete trunk group (удалить trunk-группу).

Коммутатор позволяет использовать шесть методов 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.
- Метод, основанный на исходном IP адресе;
- Метод, основанный на IP адресе назначения;
- Метод, основанный как на исходном IP, так и на IP адресе назначения.

Коммутатор поддерживает максимум 8 trunk-групп, до 8 портов в каждой группе. Trunk- группы могут использовать разные методы агрегирования.

8.2.9 Port mirroring configuration (Зеркалирование портов)



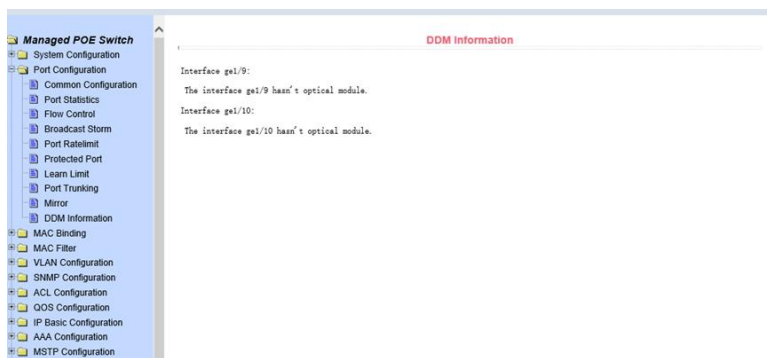
На данной странице WEB интерфейса доступны настройки зеркалирования (*mirroring*) портов. Выбирается один порт (*Mirror Port*), который будет дублировать трафик других портов, указанных в настройках зеркалирования.

- 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.

8.2.10 DDM information (Контроль параметров SFP модулей)

На данной странице WEB интерфейса представлена информация о таких параметрах работы SFP модулей как напряжение питания, температура модуля, ток смещения и мощность лазера, уровень принимаемого сигнала.

Данные параметры позволяют определить состояние линии в целом. *(Используемые SFP модули должны поддерживать эту функцию.)*



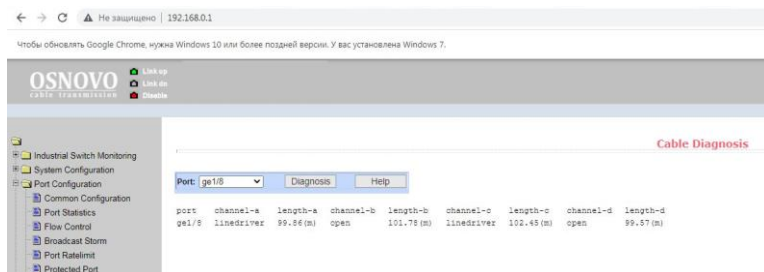
8. 2.11 Cable Diagnosis (Проверка кабеля)

Функция Cable Diagnosis (Проверка кабеля) доступна только для медных кабелей, совместимых со стандартом 10/100/1000BaseT. Инструмент позволяет определить длину кабеля (точность около 5%), его состояние. Максимальная длина проверяемого кабеля не более 100м (при попытке проверить более длинный кабель будет выводиться сообщение об ошибке в результатах тестирования). Тестирование проводится для каждой пары в кабеле в отдельности.

Open – означает, что ответная часть проверяемого кабеля не подключена куда-либо, при этом обжимка и целостность жил в порядке.

Linedriver – означает, что ответная часть проверяемого кабеля подключена к сетевому устройству, а обжимка и целостность жил в порядке.

Short – означает, что провода в выбранной паре закорочены.



Если по какой-либо причине функция Cable Diagnosis отсутствует в WEB интерфейсе коммутатора – обновите прошивку до последней доступной.

8.3 MAC binding (Привязка MAC адреса)

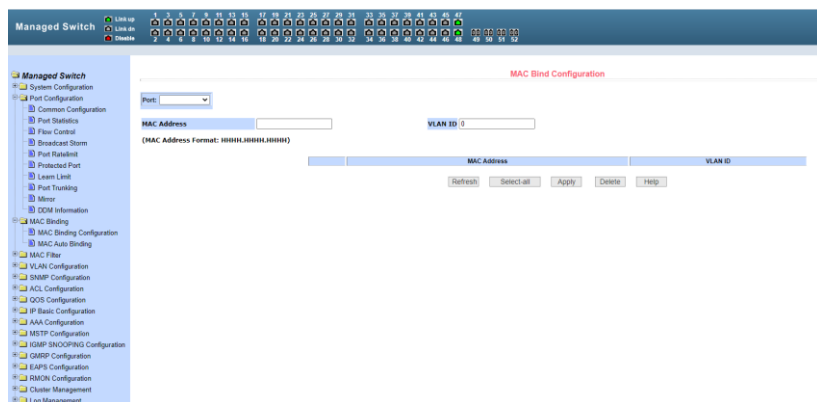
8.3.1 MAC binding configuration (Настройка привязки MAC адресов)

На данной странице WEB интерфейса находятся инструменты, позволяющие создать привязку MAC адреса к порту (MAC Address) или к VLAN (VLAN ID).

Все изменения на странице подтверждаются кнопкой Apply (Принять).

Если привязку необходимо удалить, используйте кнопку Delete (Удалить).

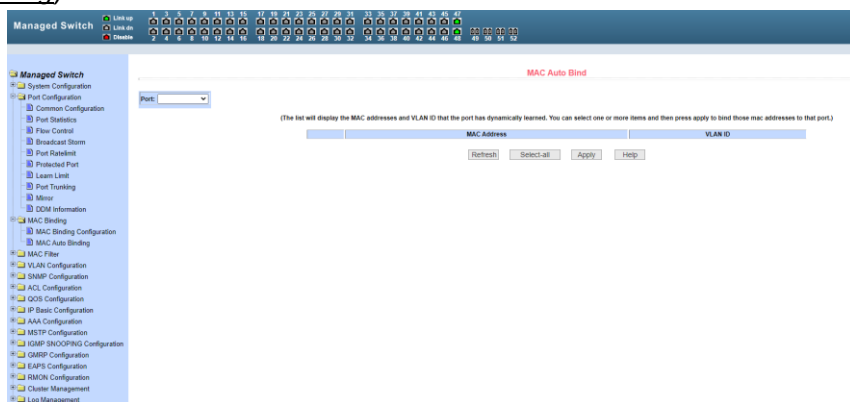
Кнопка Select all (выбрать все) позволит удалить сразу все привязки, настроенные ранее.



8.3.2 MAC Auto Binding (Автоматическая привязка MAC адресов)

На данной странице WEB интерфейса находятся сведения 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).



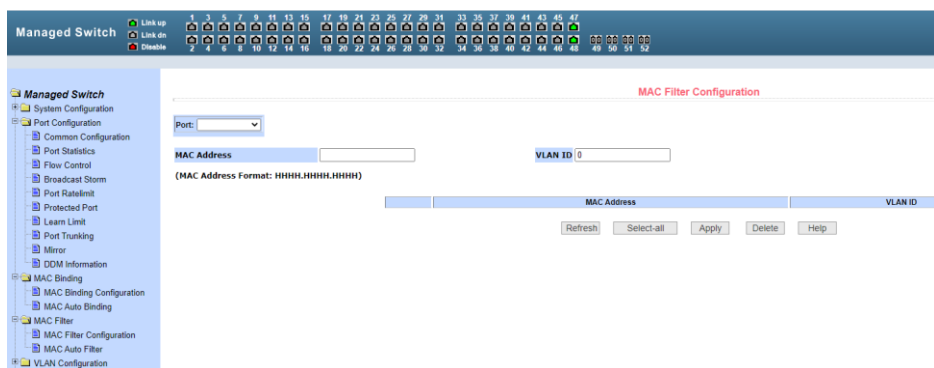
После окончания редактирования значений, нажмите кнопку Apply (Принять). Если запись необходимо удалить используйте кнопку Delete (Удалить). Кнопка Select all (Выбрать все) позволит удалить сразу все записи.

8.4 MAC filtering (Фильтрация MAC адресов)

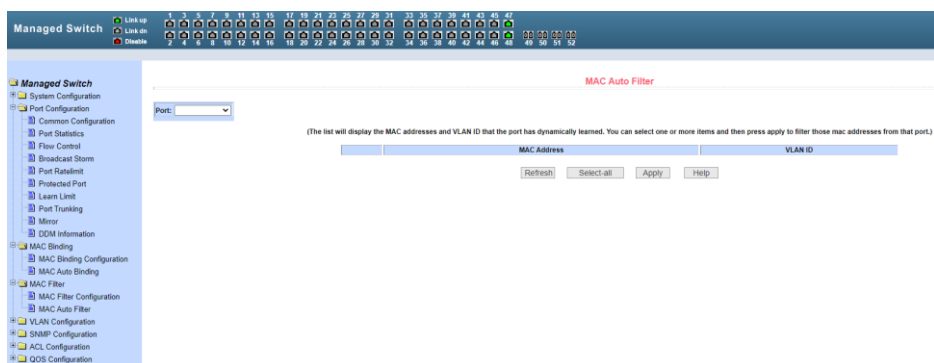
8.4.1 MAC Filter Configuration (Настройка фильтра MAC адресов)

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

Для того чтобы изменения вступили в силу нажмите кнопку Apply (Принять), если запись необходимо удалить, нажмите кнопку Delete (Удалить), кнопка Select all (Выбрать все) позволит удалить сразу все записи.



8.4.2 MAC Auto Filter (Автоматический фильтр MAC адресов)



На данной странице WEB интерфейса представлены данные об автоматической фильтрации 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 из 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.

8.5 VLAN Configuration (Настройка VLAN)

8.5.1 VLAN information (Информация о VLAN)

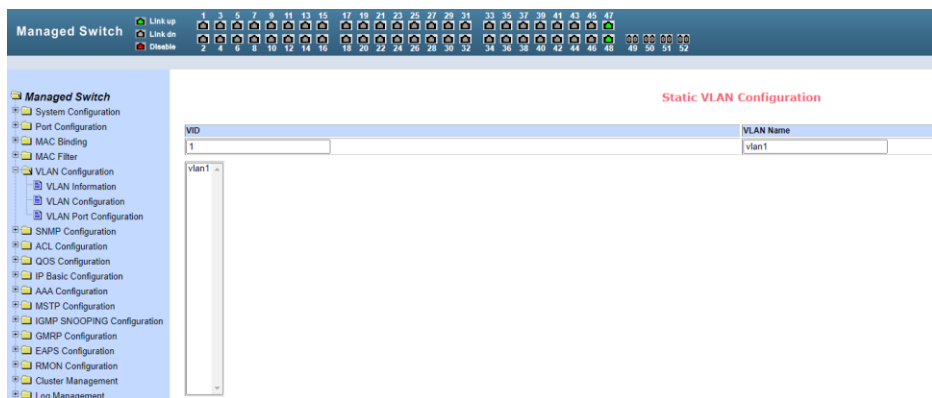
The screenshot shows the 'Managed Switch' web interface. On the left is a navigation menu with options like System Configuration, Port Configuration, MAC Binding, MAC Filter, VLAN Configuration (selected), SNMP Configuration, ACL Configuration, QoS Configuration, IP Basic Configuration, AAA Configuration, MSTP Configuration, IGMP Snooping Configuration, EAPS Configuration, RMON Configuration, Cluster Management, and Log Management. The main area is titled 'VLAN Information'. It includes a note: '(Note: The drop-down box displays all current VLANs. The list displays up to 1000 VLANs. If you select a VLAN in the drop-down box, the list will show all VLANs equal to or greater than the selected VLAN but not more than 1000 VLANs.)'. Below the note is a table with columns: VID, VLAN Name, State, and Port Member. A dropdown menu shows 'Vlan 1'. The table contains one entry: VID 1, VLAN Name vlan1, State active, and Port Member listing various ports like gige1/1, gige1/2, etc. Buttons for 'Refresh' and 'Help' are at the bottom right of the table.

VID	VLAN Name	State	Port Member
1	vlan1	active	gige1/1 gige1/2 gige1/3 gige1/4 gige1/5 gige1/6 gige1/7 gige1/8 gige1/9 gige1/10 gige1/11 gige1/12 gige1/13 gige1/14 gige1/15 gige1/16 gige1/17 gige1/18 gige1/19 gige1/20 gige1/21 gige1/22 gige1/23 gige1/24 gige1/25 gige1/26 gige1/27 gige1/28 gige1/29 gige1/30 gige1/31 gige1/32 gige1/33 gige1/34 gige1/35 gige1/36 gige1/37 gige1/38 gige1/39 gige1/40 gige1/41 gige1/42 gige1/43 gige1/44 gige1/45 gige1/46 gige1/47 gige1/48 gige1/49 gige1/50 gige1/51 gige1/52

На данной странице WEB интерфейса 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 не тегированные (u)).

8.5.2 Static VLAN Configuration (Настройка VLAN)



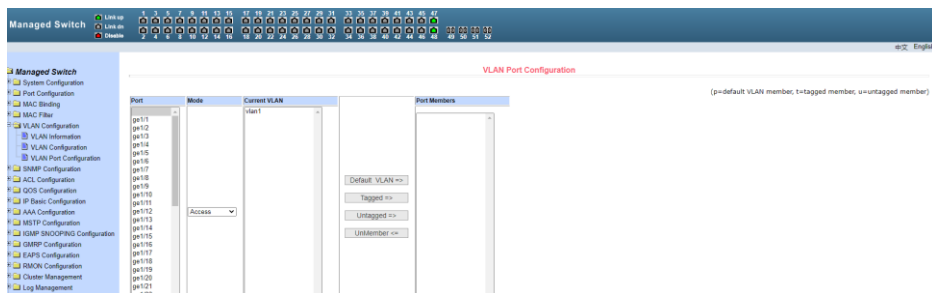
На этой странице можно создать VLAN. Для этого задайте VLAN ID в строке VID (от 2 до 4094, значение 1 - зарезервировано системой).

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 Delete (Удалить). Запись из списка также будет удалена.

8.5.3 VLAN Port Configuration (Конфигурация портов VLAN)

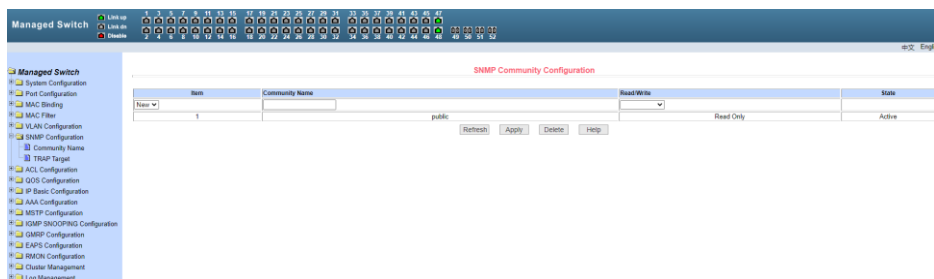


На этой странице представлены возможности по конфигурированию портов для VLAN, а также просмотру результатов. Эта страница с настройками состоит из 8 разделов:

- Port (Выбор порта);
- Mode (Режим, в котором порт будет работать в VLAN. Режим *Access* подразумевает, что порт будет помечен, как *untagged* (не тегированный) и являться членом VLAN1, Режим *Hybrid* подразумевает, что порт будет являться членом VLAN1 и будет помечен, как *untagged* (не тегированный). 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 относиться 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 не тегированный), *unMember* <= (удалить порт из поля *Port Members*).

8.6 SNMP Configuration (Настройка протокола SNMP)

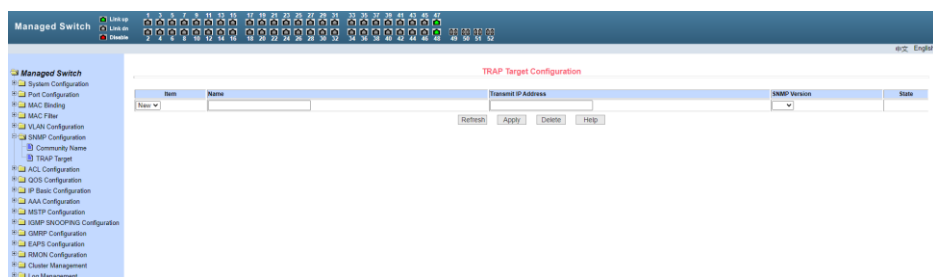
8.6.1 SNMP Community Configuration (Общие настройки для SNMP)



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

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

8.6.2 TRAP Target Configuration (Настройка TRAP уведомлений)



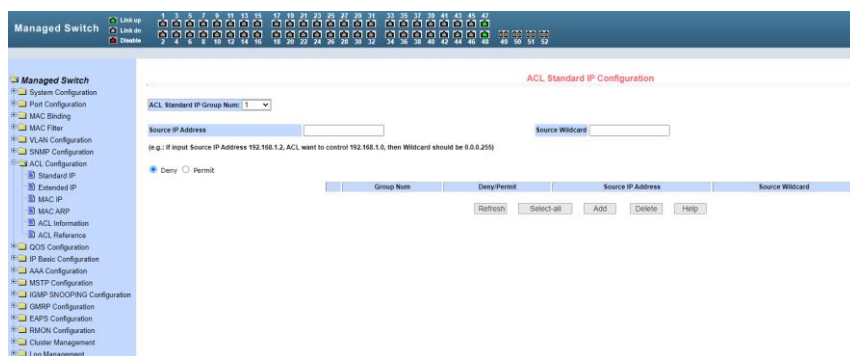
Настройки на данной странице WEB интерфейса позволяют сконфигурировать получение TRAP сообщений. Для этого необходимо:

- 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.

8.7 ACL Configuration (Настройка Access Control List)

8.7.1 ACL Standard IP Configuration (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).

8.7.2 ACL Extended IP Configure (Расширенная настройка ACL правил для IP)

Managed Switch

Link up
Link on
Disable

Managed Switch

- System Configuration
- Port Configuration
- MAC Binding
- MAC Filter
- VLAN Configuration
- SNMP Configuration
- ACL Configuration
 - Standard IP
 - Extended IP
 - MAC IP
 - MAC ARP
 - ACL Information
 - ACL Reference
- QoS Configuration
- IP Basic Configuration
- AAA Configuration
- MSTP Configuration
- IGMP SNOOPING Configuration
- DHCP Configuration
- RARP Configuration
- RMON Configuration
- Cluster Management
- Log Management

ACL Extended IP Group Name: 100

Source IP: Source Wildcard:

Destination IP: Destination Wildcard:

Protocol Type:

Source Port:

Destination Port:

TCP Control Flag: ☐ fin ☐ syn ☐ rst ☐ urg ☐ ack ☐ urg

☐ Deny ☐ Permit

Group Num	Deny/Permit	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol Type	Source Port	Destination Port	TCP Flag
-----------	-------------	-----------	-----------------	----------------	----------------------	---------------	-------------	------------------	----------

Refresh Select all Add Delete Help

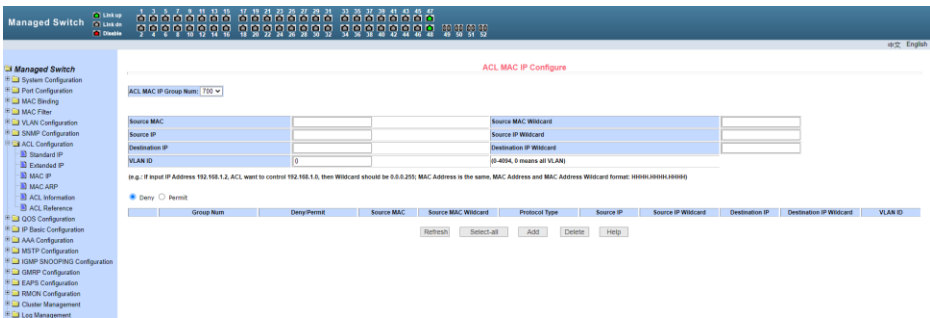
(e.g., If Host IP Address 192.168.1.2, ACL want to control 192.168.1.0, then Wildcard should be 0.0.0.255. The selected Protocol Type and Source Port is in one-to-one relationship, if the Protocol is udp, select the udp port; if the Protocol Type is not tcp or udp, the selected port is insignificant.)

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.

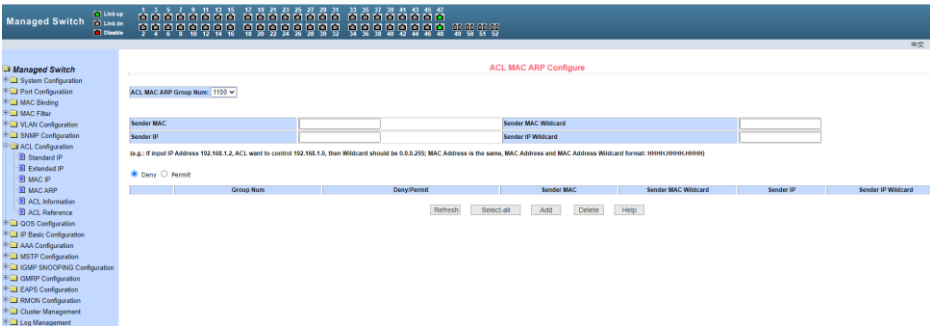
8.7.3 ACL MAC IP Configuration (Настройка ACL правил с помощью MAC)

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.



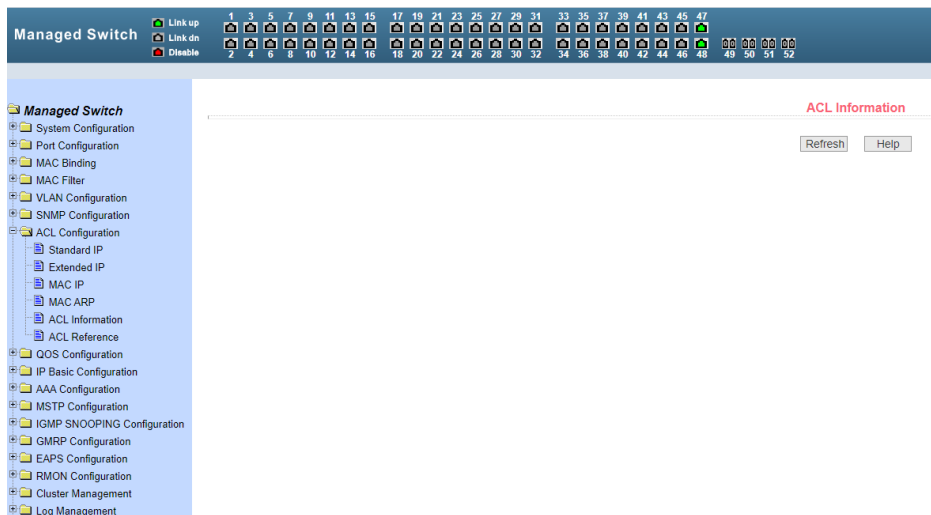
8.7.4 ACL MAC ARP Configure (Настройка ACL правил для ARP с помощью MAC адресов)



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.

8.7.5 ACL information (Информация о ACL)



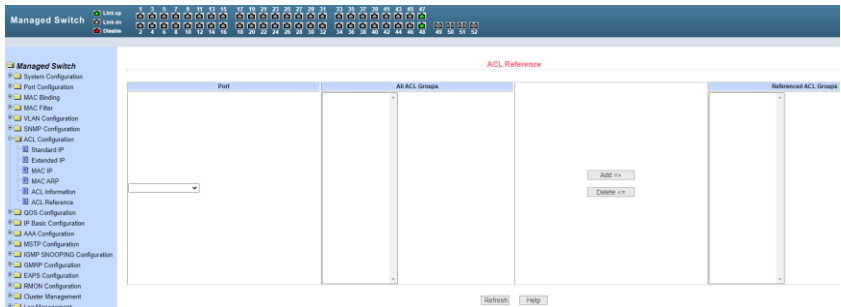
На данной странице отображены действующие в текущий момент ACL правила.

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

8.7.6 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 <=.



8.8 QoS Configuration (Настройка предоставления трафика с разным приоритетом)

8.8.1 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.

После внесения изменений в настройки, нажмите кнопку Apply (Принять).



8.8.2 QoS Schedule Configuration (Настройка расписания применения QoS)

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

После внесения изменений в настройки, нажмите кнопку Apply (Принять).

Port Name	QoS Schedule Mode	Weight of queue 1	Weight of queue 2	Weight of queue 3	Weight of queue 4	Weight of queue 5	Weight of queue 6	Weight of queue 7
ge1/1	WRR	1	2	4	8	16	32	64
ge1/2	WRR	1	2	4	8	16	32	64
ge1/3	WRR	1	2	4	8	16	32	64
ge1/4	WRR	1	2	4	8	16	32	64
ge1/5	WRR	1	2	4	8	16	32	64
ge1/6	WRR	1	2	4	8	16	32	64
ge1/7	WRR	1	2	4	8	16	32	64

8.9 IP Basic Configuration (Базовая настройка IP)

8.9.1 IP Address Configuration (Настройка IP адреса)

Line Item	VLAN ID	IP Address / Subnet Prefix	DHCP Client	MAC Address
1	1	192.168.0.3/24	Disable	0028.2411.bdf1

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 **8.1.6 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.

8.9.2 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).

Managed Switch

Link up

Link on

Disable

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

ARP Configure And Display

Static ARP Item configuration:

IP Address

MAC Address

Add

Delete ARP Item:

ARP Item

IP Address (IP Network Segment)

Delete

Change Dynamic ARP List Item into Static ARP List Item:

ARP List Item

IP Network Segment

Apply

IP Address	MAC Address	Type
192.168.0.1	0810 7919 1517	dynamic
192.168.0.13	00c1 a84a 4442	dynamic

43

»

»

»

SEC.RU

Короткий путь к информации

Скачано с sec.ru

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.

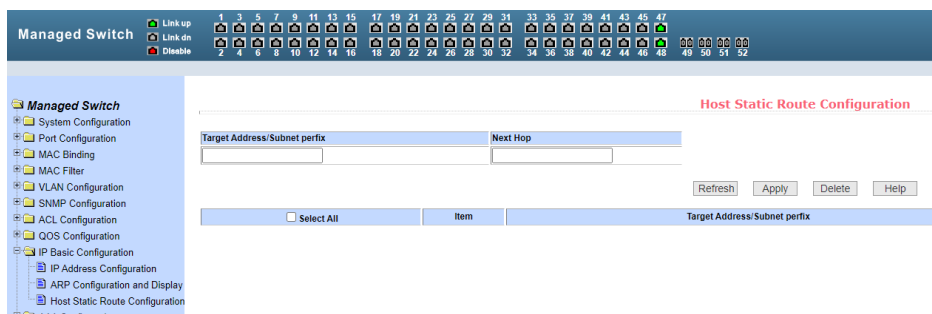
После внесения изменений в настройки нажми кнопку Apply (Принять).

8.9.3 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.

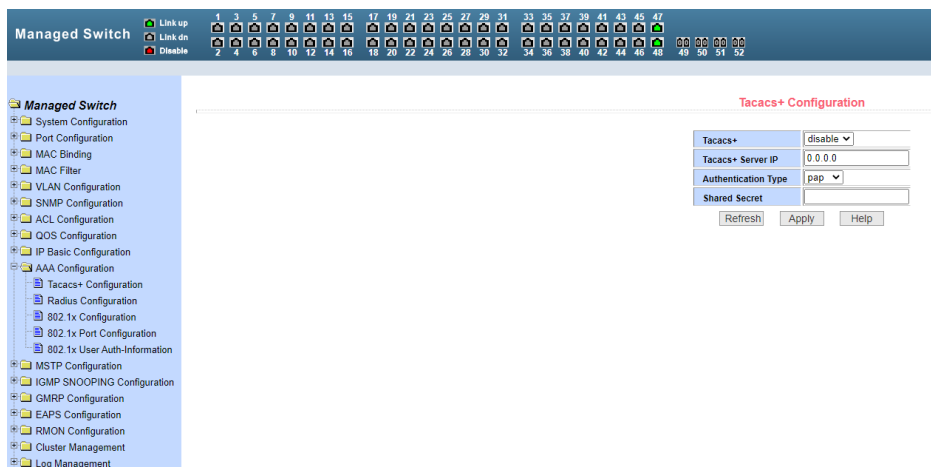
По умолчанию коммутатор не имеет каких либо записей в таблице маршрутизации. Чтобы настроить маршрутизацию по умолчанию необходимо добавить 0.0.0.0 / 0 запись в таблицу.

После внесения изменений в настройки, нажмите кнопку Apply (принять).



8.10 AAA Configuration (Настройка системы аутентификации авторизации и учета событий)

8.10.1 Tacacs+ configuration (Настройка протокола Tacacs+)



Страница настроек для использования протокола Tacacs+ предоставляет возможность пользователю включать и отключать Tacacs+, устанавливать Tacacs + server IP адрес, тип аутентификации и ключ группы пользователей.

Перед внесением изменений в установки, убедитесь, что функция Tacacs+ активирована.

Введите IP адрес Tacacs+ сервера. Выберите тип аутентификации (PAP или CHAP). Введите ключ группы пользователей в поле Shared Secret. Нажмите кнопку Apply (Принять).

8.10.2 Radius Configuration (Настройка Radius системы AAA)

Managed Switch

Link up
Link dn
Disable

1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
49 50 51 52

Managed Switch

- System Configuration
- Port Configuration
- MAC Binding
- MAC Filter
- VLAN Configuration
- SNMP Configuration
- ACL Configuration
- QoS Configuration
- IP Basic Configuration
- AAA Configuration
 - Tacacs+ Configuration
 - Radius Configuration
 - 802.1x Configuration
 - 802.1x Port Configuration
 - 802.1x User Auth-Information
- MSTP Configuration
- IGMP SNOOPING Configuration
- GMRP Configuration
- EAPS Configuration
- RMON Configuration
- Cluster Management
- Log Management

Radius Configuration

Primary Server	0.0.0.0
Option Server	0.0.0.0
UDP Port	1812
Accounting	Enable
Accounting UDP Port	1813
Shared Key	
Vendor	
NAS Port	50003
NAS Port Type	15
NAS Service Type	2
Roaming	Disable

Refresh Apply Help

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

Для корректной работы системы RADIUS необходимо:

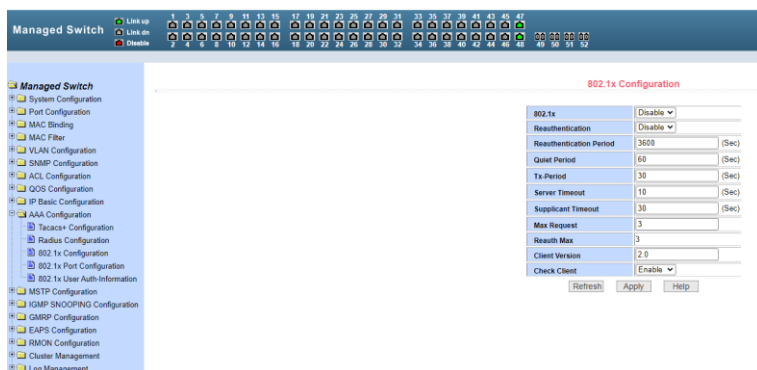
- Быть уверенным, что IP адрес Radius сервера (Primary Server) задан прежде, чем выполнять аутентификацию и авторизацию;
- Задать дополнительный IP адрес Radius сервера (Optional Server);
- Указать UDP порт аутентификации (UDP Port). По умолчанию это значение равно 1812, обычно изменять это поле нет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

- Информация о поставщике (*vendor*). Обычно, это поле не стоит изменять;
- *NAS Port*, *NAS port type*, *NAS type of service*. Эти значения не меняются;
- *Roaming* отвечает за включение/отключение функции Roaming протокола Radius.

После внесения изменений в настройки, нажмите кнопку *Apply* (принять).

8.10.3 802.1x 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:

- *802.1x* – включает/выключает (*Disable/Enable*) применение аутентификации и авторизации по стандарту 802.1x;
- *Reauthentication* – включает/выключает (*Disable/Enable*) повторную аутентификацию. По умолчанию отключено. Включение данной функции сделает аутентификацию пользователей более надежной, но незначительно увеличит сетевой трафик;

- Reauthentication period – задается время в секундах для повторной аутентификации. Активно только при включенной функции *Reauthentication*;
- Quiet Period – время в секундах, не требует изменения;
- Tx-Period – не требует изменения;
- Server timeout – не требует изменения;
- Supplicant timeout – не требует изменения;
- Max request users – не требует изменения;
- Reauth Max – отображает максимальное количество повторных аутентификаций;
- Client Version – отображает текущую версию клиента для удаленной авторизации и аутентификации через 802.1x;
- Check Client – вкл/выкл проверки прохождения сертификата от клиента.

После внесения изменений в настройки, нажмите кнопку Apply (принять).

8.10.4 802.1x Port Configuration (Настройка портов для системы авторизации и аутентификации по стандарту 802.1x)

The screenshot shows the configuration interface of a Managed Switch. On the left is a navigation tree with categories like System Configuration, Port Configuration, MAC Binding, VLAN Configuration, SNMP Configuration, ACL Configuration, QoS Configuration, IP Basic Configuration, AAA Configuration, and others. The main area displays the '802.1x Port Configuration' table.

Port Num	Port Mode	Support Host Num
ge1/1	N/A	256
ge1/2	N/A	256
ge1/3	N/A	256
ge1/4	N/A	256
ge1/5	N/A	256
ge1/6	N/A	256
ge1/7	N/A	256
ge1/8	N/A	256
ge1/9	N/A	256
ge1/10	N/A	256
ge1/11	N/A	256
ge1/12	N/A	256
ge1/13	N/A	256
ge1/14	N/A	256
ge1/15	N/A	256
ge1/16	N/A	256
ge1/17	N/A	256
ge1/18	N/A	256
ge1/19	N/A	256

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.

8.10.5 802.1x User Authentication Information (Информация о всех процессах аутентификации по стандарту 802.1x)

Managed Switch

Link up

Link on

Health

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

Managed Switch

System Configuration

Port Configuration

MAC Binding

MAC Filter

VLAN Configuration

SNMP Configuration

ACL Configuration

QoS Configuration

IP Basic Configuration

AAA Configuration

Tacacs+ Configuration

Radius Configuration

802.1x Configuration

802.1x Port Configuration

802.1x User Auth Information

MSTP Configuration

IGMP Snooping Configuration

GARP Configuration

EAPs Configuration

RAKON Configuration

Cluster Management

Log Management

802.1x User Auth-Information

Port: Port Mode: Accepted Host Num: 0

User name	MAC Address	Request State	State	Applicant State Machine	Back-End State Machine	Retry Request State
				Retry Request Num	Request Num	State
Refresh Help						

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

8.11 STP Configuration (Настройка протокола STP)

8.11.1 MSTP Configuration (Основные настройки MSTP)

MSTP Configuration	
MSTP	Disable
Priority	32768
Portfast Bpdu-Filter	Disable
Portfast Bpdu-Guard	Disable
Forward-Time	15
Hello-Time	2
Errdisable Timeout	Disable
Errdisable Timeout Interval	300
Max-Age	20
Max-Hops	20
Cisco-Interoperability	Disable

Refresh Apply

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

- MSTP (Disable/Enable) – вкл/выкл поддержку протокола MSTP;
- Priority – настройка приоритетизации. Устройства с более низким приоритетом подходят больше для роли корневого моста(root bridge);
- Portfast BPDU Filter (Disable/Enable) – вкл/выкл фильтрацию BPDU пакетов на порте;
- Portfast BPDU Guard (Disable/Enable) – вкл/выкл функцию защиты BPDU пакетов;
- Forward Time – настройка задержки пересылки пакетов;
- Hello Time – настройка интервала отправки MSTP HELLO пакетов;

- *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;
- *Errdisable timeout* – время после которого будет перезапущен порт получивший пакет BPDU;
- *Max Age* – время в секундах в течение которого коммутатор ожидает информацию о конфигурации ST(spanning tree) прежде чем запустить процесс конфигурации заново;
- *Max Hops* – количество переходов (хопов) до отбрасывания BPDU пакетов в домене;
- *CISCO Interoperability (Enable/Disable)* – вкл/выкл совместимость с настройками STP CISCO.

После внесения изменений в настройки, нажмите кнопку *Apply* (принять).

8.11.2 MSTP port configuration (Настройка MSTP на портах)

The screenshot displays the 'Managed Switch' configuration interface. On the left, a tree view shows the configuration hierarchy, with 'MSTP Configuration' expanded to 'Port Configuration'. The main panel is titled 'STP Port Configuration' and contains a table of settings for a selected port. The settings are as follows:

Port	Value
Portfast	Disable
Portfast bpdu-filter	Enable
Portfast bpdu-guard	Enable
Root Guard	Disable
Link Type	Shared
Priority	0
Path-Cost	0
Force-Version	STP

At the bottom of the configuration table, there are 'Refresh' and 'Apply' buttons.

На данной странице WEB интерфейса представлены настройки MSTP (*Multiple Spanning Tree Protocol*) для портов.

- *Port* – выбор порта для настройки;

- 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);
- Portfast BPDU filter (Enable/Disable) – вкл/выкл фильтрацию BPDU пакетов на выбранном порте;
- Portfast BPDU GUARD (Enable/Disable) – вкл/выкл функцию защиты BPDU пакетов на выбранном порте;
- Root Guard (Enable/Disable) – вкл/выкл функции защиты корневого моста (root bridge) от приема BPDU пакетов от устройств с более высоким приоритетом, чем мост;
- 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;
- Priority – настройка CIST приоритета, значение может быть только кратным 16 в диапазоне от 0-240. По умолчанию значение равно 128;
- Path Cost – от 0 – 200 000 000. Более низкие значения обычно соответствуют root'ам;
- Force Version – тип отправляемых пакетов.

После внесения изменений в настройки, нажмите кнопку Apply (принять).

8.11.3 MSTP information (Общая информация о конфигурации MSTP)

Managed Switch

Link up

Link down

Disable

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

STP All Port Information

Port	Portfast	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

На данной странице WEB интерфейса представлена сводная информация о конфигурации MSTP. Информация предоставлена только для чтения.

8.12 IGMP snooping configuration (Настройка отслеживания IGMP трафика)

8.12.1 IGMP snooping configuration (Настройки функции IGMP snooping)

Managed Switch

Link up

Link down

Disable

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

IGMP SNOOPING Configuration

IGMP SNOOPING

Disable

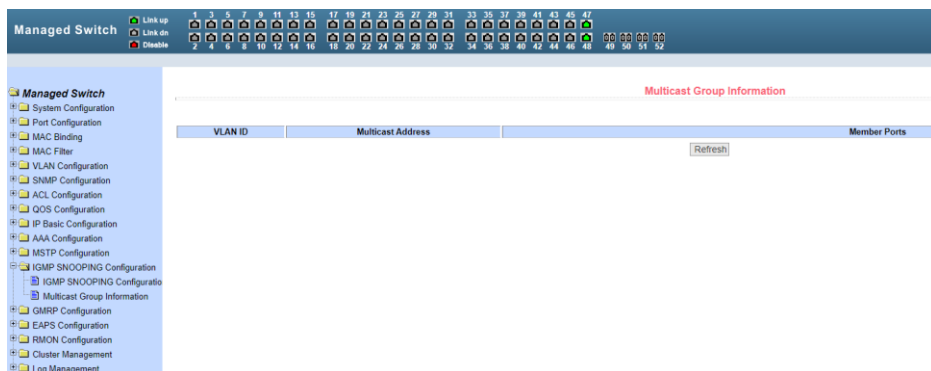
Refresh

Apply

На данной странице WEB интерфейса вы можете 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).

После внесения изменений в настройки, нажмите кнопку *Apply* (принять).

8.12.2 Multicast Group Information (Общая информация о IGMP)



На данной странице WEB интерфейса представлена общая информация о *Multicast* для всех VLAN'ов.

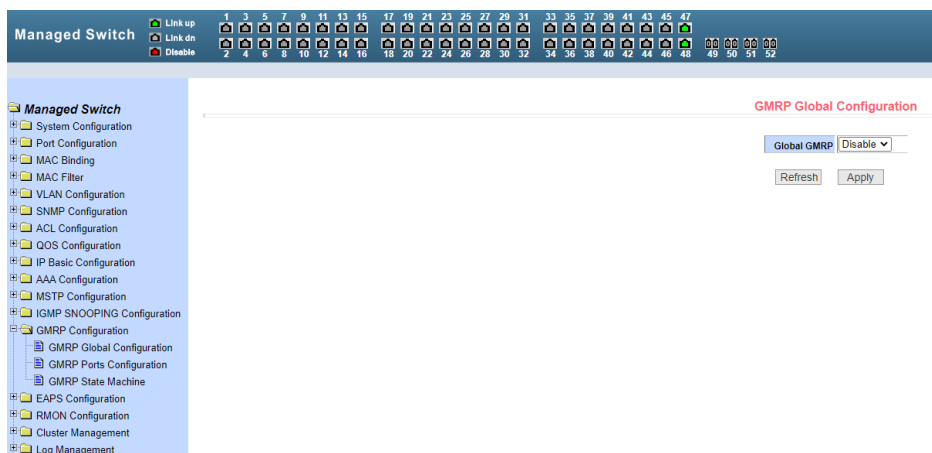
Информация предоставлена только для чтения.

8.13 GMRP Configuration (Настройка работы протокола GMRP)

8.13.1 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 (Вкл/Выкл) и последующего подтверждения кнопкой Apply (Принять).

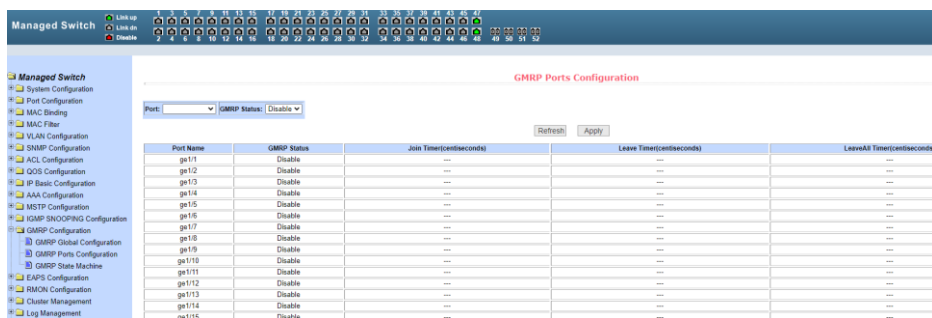


8.13.2 GMRP ports configuration (Настройка GMRP на портах)

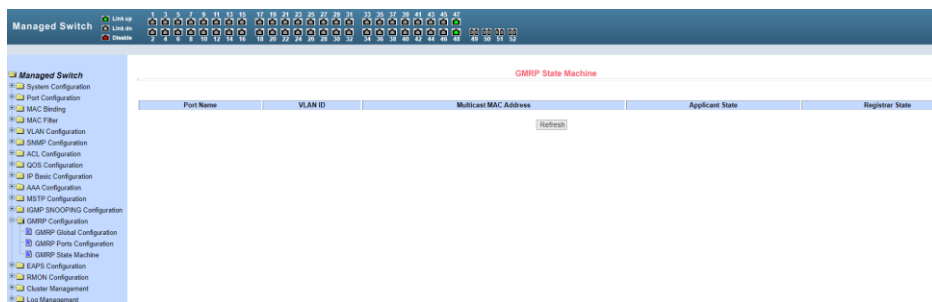
На данной странице WEB интерфейса представлены настройки GMRP для отдельных портов.

Порт выбирается в выпадающем меню Port, вкл/откл поддержки GMRP реализуется с помощью GMRP Status Disable/Enable.

После внесения изменений в настройки, нажмите кнопку Apply (принять).



8.13.3 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.

8.14 EAPS Configuration (Настройка работы протокола EAPS)

8.14.1 EAPS Configuration (Основные настройки работы протокола EAPS)

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

- EAPS Ring ID – выбор ID для EAPS ring;
- Mode – настройка режима работы рабочего узла для EAPS домена;
- Primary Port – выбор ключевого порта для EAPS;
- Secondary Port – выбор вторичного порта для EAPS;
- Control VLAN – выбор VLAN (2-4094) для EAPS;
- Protected VLANs – выбор одного или нескольких защищаемых VLAN в домене EAPS;

- Hello Time Interval – настройка EAPS домена для периодической отправки пакетов HEALTH. Задаваемое значение в секундах должно быть меньше чем время до ошибки (fail time);
- Fail Time – время до истечения срока действия в EAPS домене. Должно быть больше, чем Hello Time;
- Extreme Interoperability (enable/disable) – вкл/выкл совместимость с extreme устройствами.
- Enable status - Включение/отключение EAPS Ring.

После внесения изменений в настройки, нажмите кнопку Apply (принять).

The screenshot shows the 'Managed Switch' configuration interface. On the left is a navigation tree with 'EAPS Configuration' selected. The main area is titled 'EAPS Configuration' and contains the following settings:

EAPS Ring ID	1	
Create Status	Not Created	
Mode	None	
Primary Port		
Secondary Port		
Control VLAN	0	
Protected VLANs		Format: 2,4,6 or 3-10
Hello Time Interval	0	s
Fail Time	0	s
Data Span	Disable	
Extreme Interoperability	Disable	
Enable Status	Disable	

At the bottom of the configuration area are buttons: Refresh, Create, Apply, and Remove.

8.14.2 EAPS information (Сводная информация о работе протокола EAPS)

The screenshot shows the 'Managed Switch' configuration interface. On the left is a navigation tree with 'EAPS Configuration' selected. The main area is titled 'EAPS Information' and contains a 'Refresh' button.

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/

8.15 RMON configuration (Настройки дистанционного мониторинга сети)

8.15.1 RMON statistics (Статистика дистанционного мониторинга сети)

На данной странице WEB интерфейса представлены сведения о статистике работы портов.

Выберите порт из выпадающего списка, сформируйте группу статистики для этого порта. Корректное значение индекса: 1...100, поле OWNER опциональное.

Нажмите Apply для подтверждения. В таблице Statistics Data будет показана статистика работы порта.

Managed Switch

Link up
Link do
Status

Port:

Index: Owner:

Refresh Apply Delete Help

Statistics Data	
etherStatsDropEvents	0
etherStatsPkts	0
etherStatsMulticastPkts	0
etherStatsIndicastPkts	0
etherStatsFragments	0
etherStatsCollisions	0
etherStatsPkts127Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsOctets	0
etherStatsBroadcastPkts	0
etherStatsCRCAlignErrors	0
etherStatsOvercastPkts	0
etherStatsJabbers	0
etherStatsPkts64Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts512to1023Octets	0

8.15.2 RMON history (Журнал работы RMON)

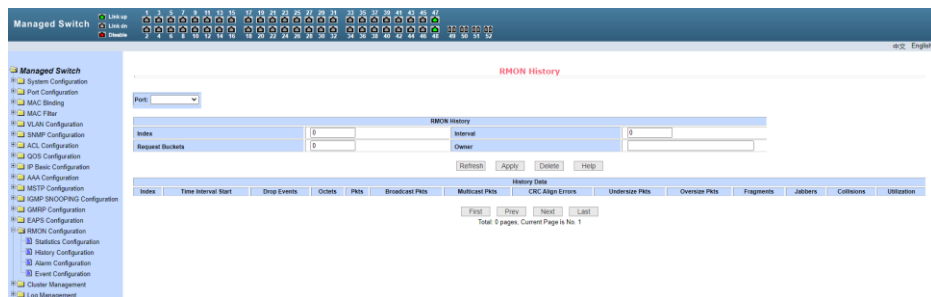
На данной странице WEB интерфейса возможно просматривать журнал работы портов.

Выберите порт из выпадающего списка для просмотра журнал работы этого порта. Корректное значение индекса: 1...100, поля Interval, Request Buckets и OWNER опциональные.

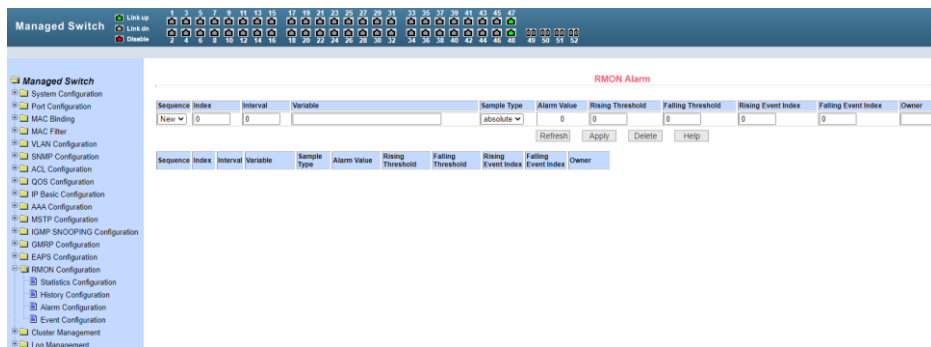
- Поле Interval показывает затраченное время на сбор данных в секундах (1...3600).
- Поле Request Buckets содержит количество сохраненных записей (1...100).

- В таблице Historical Data содержится остальная информация из журнала с момента формирования последней конфигурации.

Нажмите Apply для подтверждения. В таблице History Data будут показаны данные из журнала работы порта.



8.15.3 RMON alarm (Мониторинг тревожных событий)



На данной странице WEB интерфейса представлены настройки для создания тревожных групп и просмотра тревожных событий.

Выберите существующую группу из выпадающего списка для просмотра событий или внесения изменений в настройки. Для создания новой группы выберите New. Index должен находиться в пределах 1...60, Interval должен находиться в пределах 1...3600 (секунды).

8.15.4 RMON event (Журнал событий)

Managed Switch

Link up Link down Create

Managed Switch

- System Configuration
- Port Configuration
- MAC Binding
- MAC Filter
- VLAN Configuration
- SNMP Configuration
- ACL Configuration
- QoS Configuration
- IP Basic Configuration
- AAA Configuration
- MSTP Configuration
- RSPAN Configuration
- RSPAN Configuration
- EAP Configuration
- RMON Configuration
 - Statistics Configuration
 - History Configuration
 - Alarm Configuration
 - Event Configuration
- Cluster Management
- Log Management

RMON Event

Sequence	Index	Description	Type	Community	Last Time Sent	Owner
New	0		none		1970/01/01 00:00:00	

Refresh Apply Delete Help

На данной странице WEB интерфейса представлены настройки для просмотра и создания журнала событий.

Выберите существующую группу из выпадающего списка для просмотра событий или внесения изменений в настройки. Для создания новой группы выберите New.

- Index должен находиться в пределах 1...60,
- Description (описание) должно быть не более одной строки,
- Type (тип операции) должен быть выбран из: none (без операции), log, SNMP-trap или log-and-trap.
- Поле last send time (время отправки последнего события) только для чтения, поле owner не обязательно для заполнения.

Нажмите Apply для подтверждения.

8.16 Cluster configuration (Управление кластерами)

8.16.1 NDP configuration (NDP конфигурация)

На данной странице WEB интерфейса представлены настройки NDP. Настройки включают в себя выбор порта, NDP функцию порта, глобальную NDP функцию, интервал отправления пакетов NDP, время хранения NDP пакетов на принимающем оборудовании.

Выберите порт и включите функцию NDP. Одновременно должны быть включены NDP порта и глобальная NDP.

- Установите время хранения NDP пакетов на принимающем оборудовании в пределах 1...4096 секунд (предустановленное время 180 секунд).
- Установите интервал отправляемых NDP пакетов в пределах 1...4096 секунд (предустановленное время 60 секунд).
- Нажмите Apply для подтверждения.

Managed Switch

Link up Link dn Disable

1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
49 50 51 52

Managed Switch

- System Configuration
- Port Configuration
- MAC Binding
- MAC Filter
- VLAN Configuration
- SNMP Configuration
- ACL Configuration
- QOS Configuration
- IP Basic Configuration
- AAA Configuration
- MSTP Configuration
- IGMP SNOOPING Configuration
- GMRP Configuration
- EAPS Configuration
- RMON Configuration
- Cluster Management
 - NDP Configuration
 - NTDP Configuration
 - Cluster Configuration
- Log Management

NDP Configuration

Port:

Port Enable:

Global Enable:

Hello-time: (1-4096 sec)

Aging-time: (1-4096 sec)

Refresh Apply Help

8.16.2 NTDP configuration (NTDP конфигурация)

На данной странице WEB интерфейса представлены настройки NTDP. Настройки включают в себя выбор порта, NTDP функцию порта, глобальную NTDP функцию, topology collection range, topology collection time interval, время задержки отправления пакетов для первого порта, время задержки отправления пакетов для остальных портов.

Выберите порт и включите функцию NTDP. Одновременно должны быть включены NTDP порта и глобальная NTDP.

- Установите количество переходов в пределах 1...6, (предустановленное число переходов;
- Установите временной интервал в пределах 0...65535 минут (предустановленный интервал 1 минута).
- Установите время задержки отправляемых пакетов для первого порта Hop-delay в пределах 1...1000 мсек (предустановленное время 200 мсек).
- Установите время задержки отправления пакетов для остальных портов в пределах 1...100 мсек (предустановленное время 20 мсек).
- Нажмите Apply для подтверждения.

Managed Switch

Link up
Link dn
Disable

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52

Managed Switch

- System Configuration
- Port Configuration
- MAC Binding
- MAC Filter
- VLAN Configuration
- SNMP Configuration
- ACL Configuration
- QOS Configuration
- IP Basic Configuration
- AAA Configuration
- MSTP Configuration
- IGMP SNOOPING Configuration
- GMRP Configuration
- EAPs Configuration
- RMON Configuration
- Cluster Management
 - NDP Configuration
 - NTDP Configuration
 - Cluster Configuration
- Log Management

NTDP Configuration

Port:

Port Enable: ☐ enable ☒ disable

Global Enable: ☐ enable ☒ disable

Hops: (1-6)

Interval-time: (0-65535 min)

Hop-delay: (1-1000 msec)

Port-delay: (1-100 msec)

Refresh Apply Help

8.16.3 Cluster configuration (Конфигурация кластеров)

На данной странице WEB интерфейса представлены настройки конфигурации кластера. Настройки включают в себя включение/отключение кластера, настройки VLAN, пул адресов кластера, интервалы отправления handshake пакетов, имя кластера, путь включения в кластер, и удаление кластера.

- В поле management VLAN установите значение в пределах 1...4094 (предустановленное значение 1);
- Установите локальный IP адрес для устройств включенных в кластер (в диапазоне 0.0.0.0 - 255.255.255.255, длина маски 0 – 32);
- Установите интервал отправки handshake пакетов в пределах 1...255 секунд (предустановленное значение 10 секунд);
- Установите время удержания handshake пакетов в пределах 1...255 секунд (предустановленное значение 60 секунд).

Для создания кластера необходимо задать ему имя выбрать элементы кластера и путь для подключения к кластеру (в ручном и автоматическом режиме). После настройки кластера он может автоматически переходить в ручной режим.

Ручной режим позволяет изменять имя кластера. После формирования кластера имеется возможность просматривать элементы кластера и кандидатов на включение в кластер в таблице, добавлять новые элементы в кластер.

Нажмите Apply для подтверждения.

Managed Switch

Cluster Configuration

Cluster Enable:

Management-vlan: (1-4094)

IP pool: (A.B.C.D/M)

Handshake time: (1-255 sec)

Handshake hold time: (1-255 sec)

Apply

Cluster Name: Type:

Apply Delete

Cluster Member List

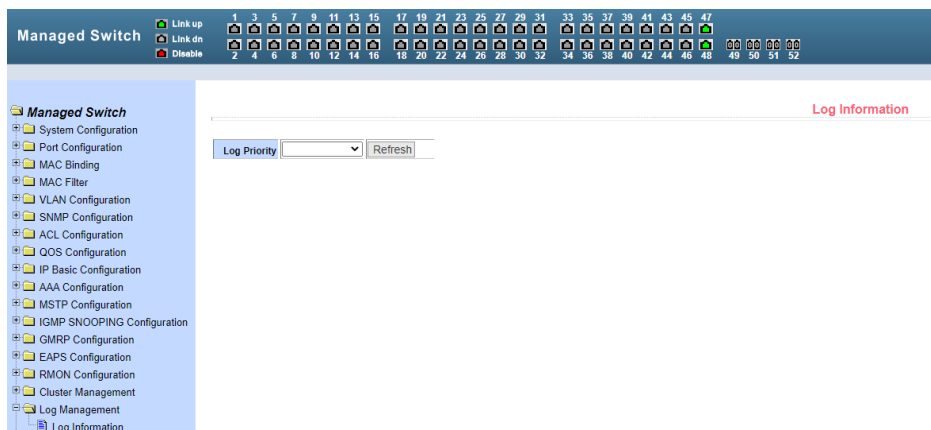
Serial	MAC	IP	Status
--------	-----	----	--------

8.17 Log management (Управление журналами записей)

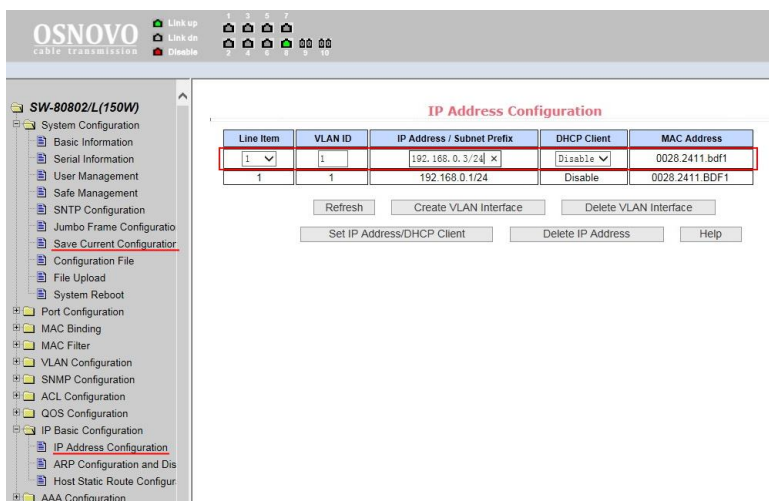
На данной странице WEB интерфейса представлены настройки фильтра вывода записей. В поле *Log Priority* могут быть следующие значения:

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

Чтобы применить фильтр записей нажмите кнопку *Refresh* (обновить).



9. 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 !

Качественное заземление является обязательным условием подключения.

10. Технические характеристики*

Модель	SW-74804/L
Общее кол-во портов	52
Кол-во портов FE+PoE	-
Кол-во портов FE	-
Кол-во портов GE+PoE	-
Кол-во портов GE (не Combo порты)	48
Кол-во портов Combo GE (RJ45+SFP)	-
Кол-во портов SFP (не Combo порты)	4 GE (1000Мбит/с)
Встроенные оптические порты	-
Топологии подключения	звезда каскад кольцо
Буфер пакетов	12 МБ
Таблицы MAC-адресов	16 К
Пропускная способность коммутационной матрицы (Switching fabric)	256 Гбит/с

Модель	SW-74804/L
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
Размер flash памяти	128 МБ
Стандарты и протоколы	• IEEE 802.3 – 10BaseT • IEEE 802.3u – 100BaseTX • IEEE 802.3ab – 1000BaseT • IEEE 802.3z – 1000 BaseSX/LX • IEEE 802.3x – Flow Control • IEEE 802.1q – VLAN • IEEE 802.1p – Class of Service • IEEE 802.1d – Spanning Tree • IEEE 802.1w – Rapid Spanning Tree • IEEE 802.1s – Multiple Spanning Tree • IEEE 802.3ad – Link Aggregation Control Protocol (LACP) • IEEE 802.1ab – LLDP (Link Layer Discovery Protocol) • IEEE 802.1c – Access Control
Функции уровня 2	• IEEE 802.1d (STP) • IEEE 802.1w (RSTP) • IEEE 802.1s (MSTP) • VLAN / VLAN Group 4K • Tagged Based • Port-based • Voice VLAN • Link Aggregation IEEE 802.3ad with LACP • IGMP Snooping v1/v2/v3 • IGMP Static Multicast Addresses • Storm Control
Качество обслуживания (QoS)	IEEE 802.1p CoS/ToS, WRR, WFQ

Модель	SW-74804/L
Безопасность	• Management System User Name/Password Protection • IEEE 802.1x Port-based Access Control • HTTP & SSL (Secure Web) • SSH v2.0 (Secured Telnet Session)
Управление	• Управление через Web-интерфейс • CLI • Telnet • SNMP
Индикаторы	PW (питание), SYS (работа коммутатора), Link (соединение есть/нет), Giga (100 или 1000 Мбит/с)
Грозозащита	3 kV
Питание	AC 100-240V
Энергопотребление	<30 Вт
Охлаждение	Активное (2 вентилятора с автоматическим изменением скорости вращения)
Способ монтажа	в 19" стойку, 1U
Рабочая температура	0...+55 °C
Вес (без упаковки), кг	4.7
Размеры (ШхВхГ) (мм)	440x45x360
Дополнительно	Режим увеличения дальности передачи сигналов до 250м. (Скорость передачи ограничена 10 Мбит/с).

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

11. 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

2

230329 (2)