OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Управляемый L3 коммутатор Gigabit Etherent с 10G портами на 16xGE SFP + 8xGE Combo (RJ45 + SFP) + 4x10G «SFP+» Uplink.

SW-32G4X-1L

Прежде чем приступать к эксплуатации изделия,
внимательно прочтите настоящее руководство

Содержание

1. Назначение

Управляемый (L3) коммутатор с 10G портами SW-32G4X-1L на 36 портов (16xGE SFP + 8xGE Combo (8xRJ45 + 8xSFP) + 4x10G «SFP+» Uplink) предназначен для объединения сетевых устройств, коммутаторов, передачи данных между ними.

В коммутаторе предусмотрен широкий набор портов:

- ✓ 16 основных SFP портов (1000Base-X) – обеспечивают скорость передачи данных до 1000 Мбит/с с помощью оптических (SC/LC) или медных (RJ-45) SFP модулей*.
- ✓ 8 Combo портов (8xRJ45 + 8xSFP) – предназначены для передачи данных по меди или оптике (SFP модули*) со скоростью до 1000 Мбит/с.
- ✓ 4 «SFP+» порта – работают на скорости 10G (10 Гбит/с) и способны без задержек передавать весь объем трафика на сервер или другое устройство с помощью оптических (SC/LC) или медных (RJ-45) «SFP+» модулей*.

Коммутатор имеет значительный запас по производительности благодаря универсальным интерфейсам и неблокируемой коммутационной матрице с пропускной способностью до 128 Гбит/с.

Коммутатор имеет возможность гибкой настройки параметров через WEB-интерфейс, имеют множество функций L2+ уровня (VLAN, IGMP snooping, Link aggregation и тд.) и L3 уровня (ARP, DHCP, Routing RIP V1/V2, OSPF V1/V2 и тд.)

Кроме того коммутатор поддерживают работу в кольцевой топологии (Ring) благодаря поддержке протоколов IEEE 802.1s (MSTP), IEEE 802.1w (RSTP), G.8032 (ERPS) и маршрутизации L3 (OSPF V1/V2).

Коммутатор выполнен в корпусе для установки в 19'' телекоммуникационную стойку или шкаф. Предусмотрено резервное питание от дополнительной электросети AC 230V.

В коммутаторе используется вентиляция по типу Front-to-Back и дополнительное активное охлаждение с помощью вентиляторов.

Коммутатор SW-32G4X-1L может быть использован на предприятиях малого, среднего и крупного бизнеса, в операторских сетях в качестве коммутатора уровня агрегации района или транспортного коммутатора.

*SFP и SFP+ модули приобретаются отдельно.

2. Комплектация**

1. Коммутатор – 1шт;
2. Крепление в 19” стойку – 1шт;
3. Кабель для подключения к сети AC230V – 2шт;
4. Краткое руководство по эксплуатации – 1шт;
5. Упаковка – 1шт.

3. Особенности оборудования

- ✓ Высокопроизводительные Uplink-порты 10G (4 x 10G «SFP+»);
- ✓ Универсальные интерфейсы – 16xGE SFP (1000Base-X) + 8xGE Combo (RJ45 + SFP);
- ✓ Поддержка функций L2 (VLAN, QOS, LACP, LLDP, IGMP snooping) и L3 (ARP, DHCP, Routing RIP V1/V2, OSPF V1/V2);
- ✓ Поддержка кольцевой топологии подключения (STP, RSTP, MSTP, ERPS);
- ✓ Возможность объединения в стек до 8 устройств;
- ✓ Резервное питание.

4. Внешний вид и описание элементов

4.1 Внешний вид и описание разъемов и индикаторов

Рис. 1 Коммутатор SW-32G4X-1L, внешний вид

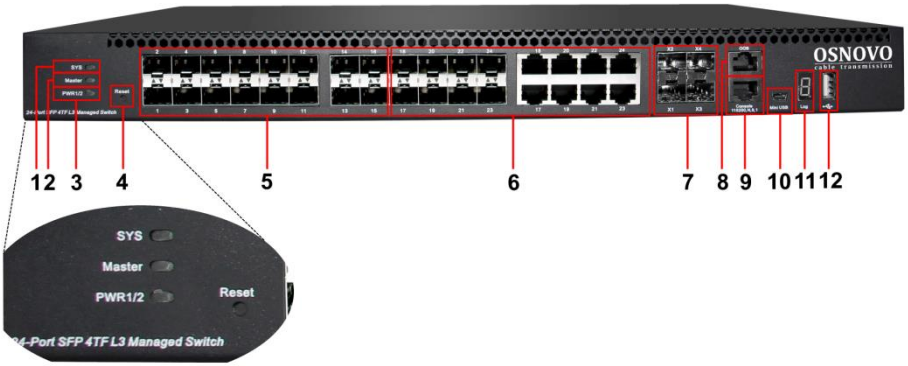


Рис.2 Коммутатор SW-32G4X-1L, разъемы, кнопки и индикаторы на передней панели

Таб. 1 Коммутатор SW-32G4X-1L, назначение разъемов, кнопок и индикаторов на передней панели

№ п/п	Обозначение	Назначение
1	SYS	LED индикатор работы системы Мигает – система работает корректно. Не горит – система работает в неправильном режиме. Прошивка коммутатора повреждена.

№ п/п	Обозначение	Назначение
2	Master	Индикатор режима работы устройства в стеке: Горит – ведущий (master) Не горит – ведомый (slave) или стекирование не используется.
3	PWR 1/2	LED индикатор питания подключения коммутатора к основой и резервной сети AC 230V Горит оранжевым – коммутатор подключен к основной и резервной сети AC 230V Горит зеленым – коммутатор подключен к основной сети AC 230V Горит красным – коммутатор подключен только к резервной сети AC 230V
4	Reset	Микрокнопка. Используется для сброса коммутатора к заводским настройкам.
5	1-16	SFP порты (1000Base-X) с 1 по 16. Используются для подключения к коммутатору сетевых устройств на скорости 1 Гбит/с с помощью SFP модулей.*
6	17-24	Combo порты SFP (SFP + RJ45) с 17 по 24. Используются для подключения сетевых устройств по меди (RJ-45 10/100/1000Base-T) или оптике (SFP порты 1000Base-X с помощью SFP модулей*) на скорости до 1 Гбит/с
7	X1 X2 X3 X4	«SFP+» Uplink порты. Используются для подключения коммутатора к оптическим линиям операторов связи, другим коммутаторам и маршрутизаторам на скорости 10 Гбит/с, используя SFP+ модули 10G*
8	OOB	Порт (out-of-band) RJ-45 (10/100/1000Base-T). Используются для удаленного управления коммутатором. Управление осуществляется по сети, раздельно с каналом передачи данных.

№ п/п	Обозначение	Назначение
9	Console 115200, N, 8, 1	Разъем RJ-45. Используется для управления коммутатором через RJ45-RS232 интерфейс с помощью CLI команд.
10	Mini USB	Разъем Mini USB. Используется для управления коммутатором через USB с помощью CLI команд
11	Log	Индикатор номера коммутатора в стеке. От 0 до 8
12		USB-A порт для подключения USB флеш накопителя. Используется для сохранения/загрузки файла с текущей конфигурацией, журналов работы коммутатора и тд.

* SFP и SFP+ модули приобретаются отдельно.

Рис. 3 Коммутатор SW-32G4X-1L, разъемы на задней панели

Таб. 2 Коммутатор SW-32G4X-1L, назначение разъемов

№ п/п	Обозначение	Назначение
1	1 AC 100-240V	Разъем для подключения коммутатора к сети AC 230V кабелем из комплекта поставки.
2		Винтовая клемма для подключения коммутатора к шине заземления.
3	2 AC 100-240V	Разъем для подключения коммутатора к резервной сети AC 230V кабелем из комплекта поставки.

5. Подключение

5.1 Схема подключения

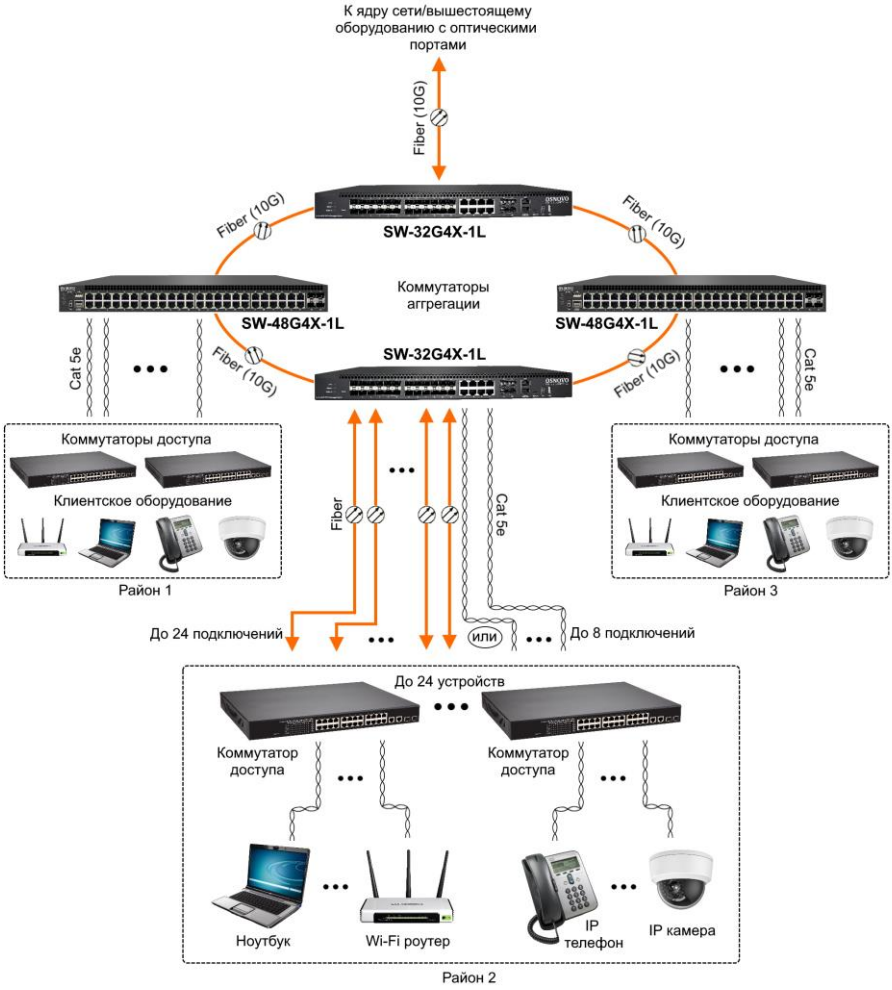


Рис. 4 Схема подключения коммутатора SW-32G4X-1L на примере построения сети оператора связи

5.2 Подключение питания

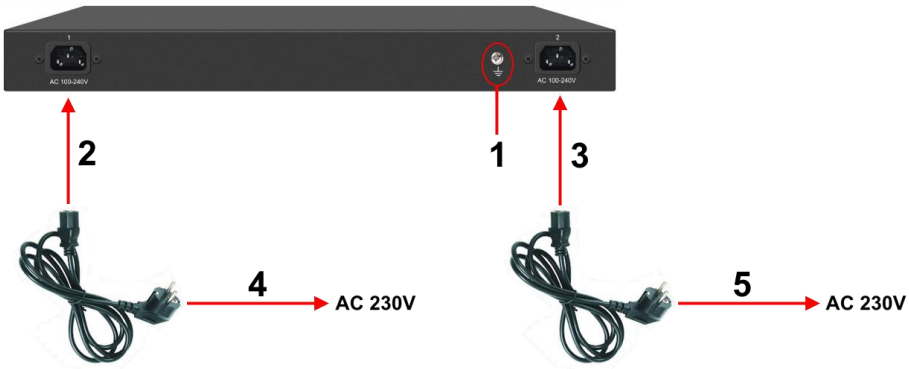


Рис. 5 Подключение коммутатора к сети AC 230V

Порядок подключения питания:

1) Подключите коммутатор к шине заземления внутри 19” шкафа/стойки (1);
2) Подключите комплектный шнур питания в соответствующий разъем на коммутаторе (2);
3) Подключите второй комплектный шнур питания в соответствующий разъем на коммутаторе (3)
4) Подключите вилки шнуров питания (4 и 5) к сети переменного тока AC 230V (могут быть 2 разных сети, чтобы обеспечивать резервирование).

Внимание!

Подключение резервного питания не является обязательным для работы коммутатора. Достаточно основного подключения к сети AC 230V. Об отсутствии резервного питания будет сообщать соответствующий LED индикатор на передней панели устройства (PWR 1/2).

6. Проверка работоспособности

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.

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:

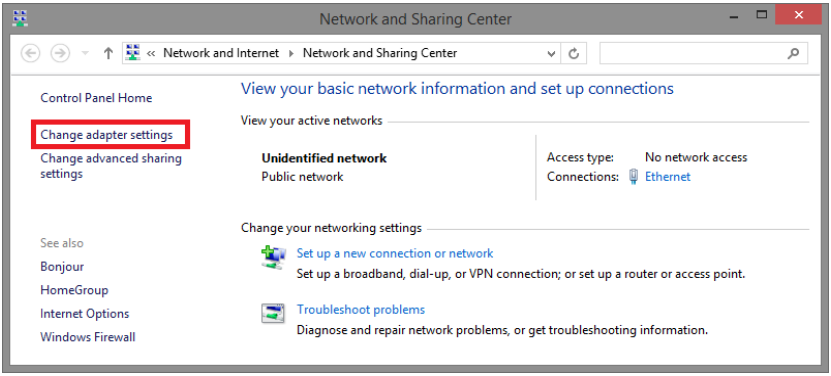
Причины потери в оптической линии могут быть вызваны:

- неисправностью SFP и/или SFP+ модулей (выбирайте модули с подходящей скоростью передачи данных);
- изгибами кабеля;
- большим количеством узлов сварки;
- неисправностью или неоднородностью оптоволокна.

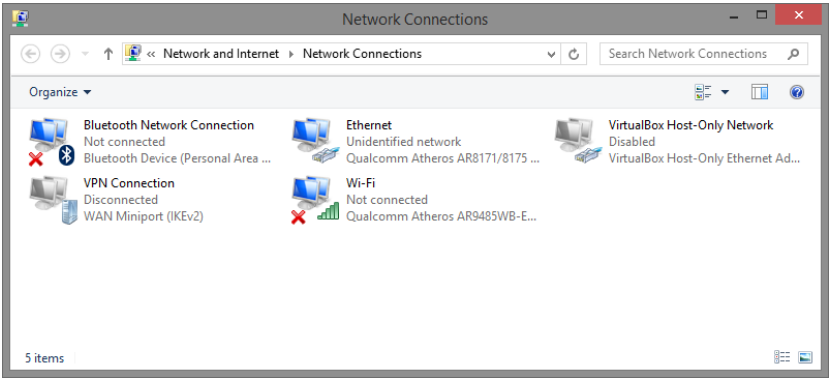
7. Подготовка перед управлением коммутатором через WEB.

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

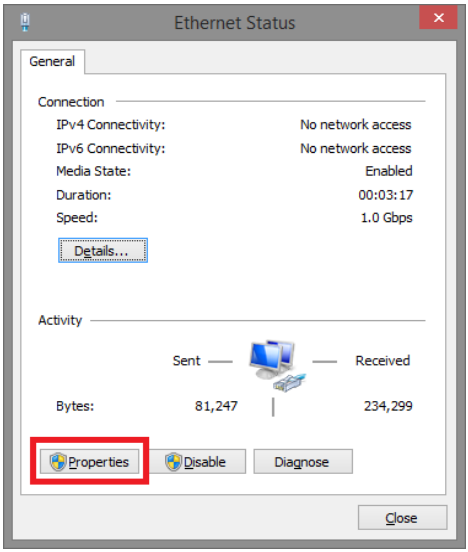
1. Откройте «Центр управления сетями и общим доступом» (Network and Sharing in Control Panel) и нажмите «Изменение параметров адаптера» (Change adapter setting) как на рисунке ниже.



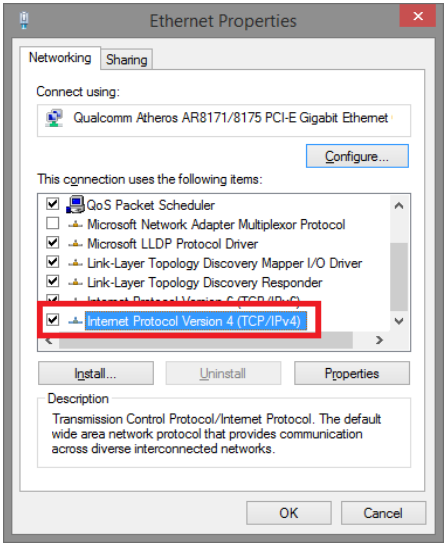
2. В появившемся окне «Сетевые подключения» (Network Connections) отображены все сетевые подключения, доступные вашему ПК. Сделайте двойной клик на подключении, которое вы используете для сети Ethernet



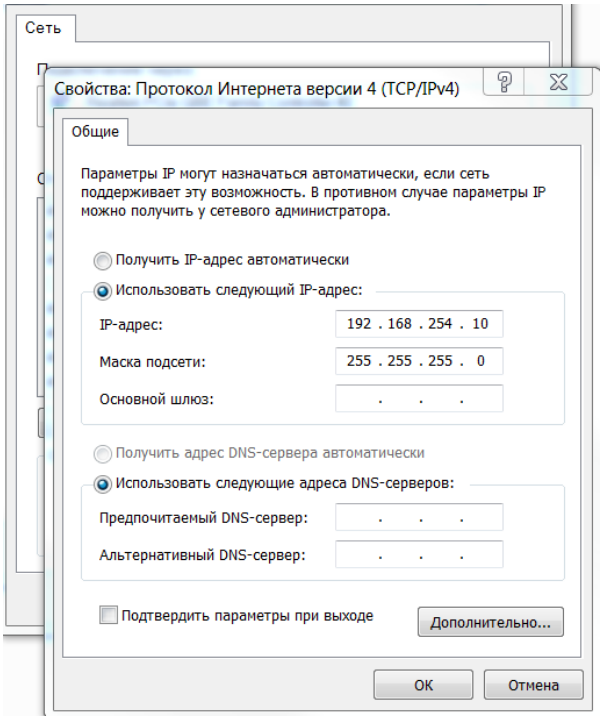
3. В появившемся окне «Состояние - Подключение по локальной сети» (Ethernet Status) нажмите кнопку «Свойства» (Properties) как показано ниже.



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

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

По умолчанию:

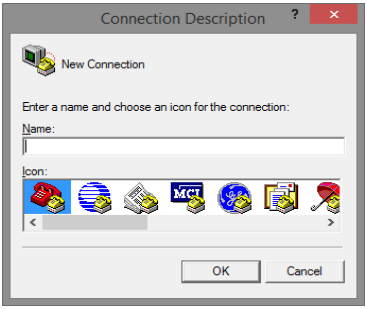
- ✓ Login: **admin**
- ✓ Password: **admin**

8. Подготовка перед управлением коммутатором через порт CONSOLE

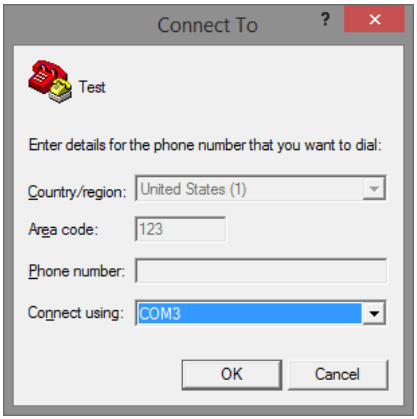
Управление коммутатором через COM-порт или USB (используется виртуальный COM порт) может потребоваться, если по каким-либо причинам управление через WEB-недоступно.

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.

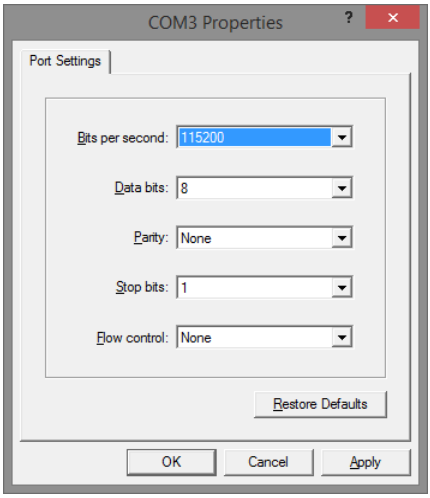


4. Выберите COM-порт, к которому подключен коммутатор.



5. Настройте COM-порт следующим образом:

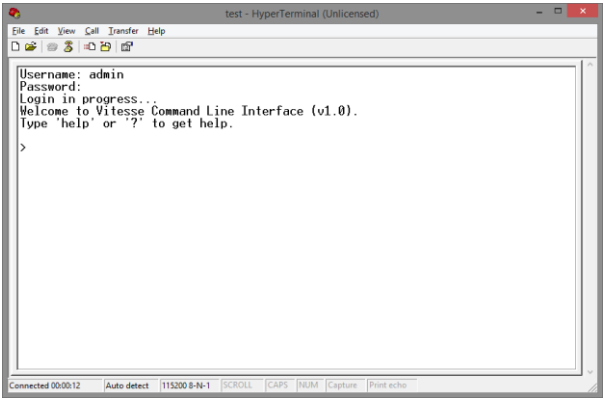
- ✓ Скорость передачи данных (Baud Rate) – 115200;
- ✓ Биты данных (Data bits) – 8;
- ✓ Четность (Parity) – нет;
- ✓ Стоп биты (Stop bits) – 1;
- ✓ Управление потоком (flow control) – нет.



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

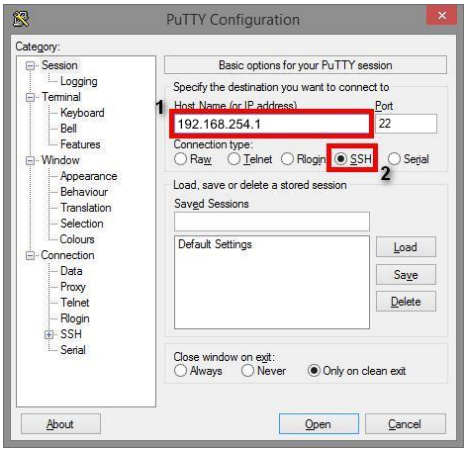
Протоколы Telnet и SSH предоставляют пользователю текстовый интерфейс командной строки для управления коммутатором (CLI). Но только SSH обеспечивает создание безопасного канала с полным шифрованием передаваемых данных.

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».

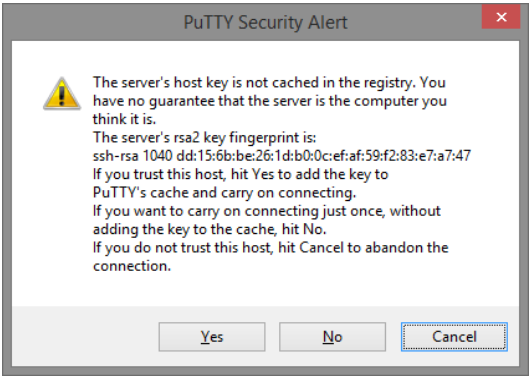
Telnet интерфейс встроен в командную строку CMD семейства операционных систем Microsoft Windows. SSH интерфейс доступен только с помощью программы эмулятора SSH терминала. Ниже показано, как получить доступ к CLI коммутатора через SSH с помощью программы PuTTY.

1. Зайдите в меню PuTTY Configuration. Введите IP адрес коммутатора в поле Имя хоста (Host Name) (или IP адрес). По умолчанию IP адрес коммутатора **192.168.254.1**

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



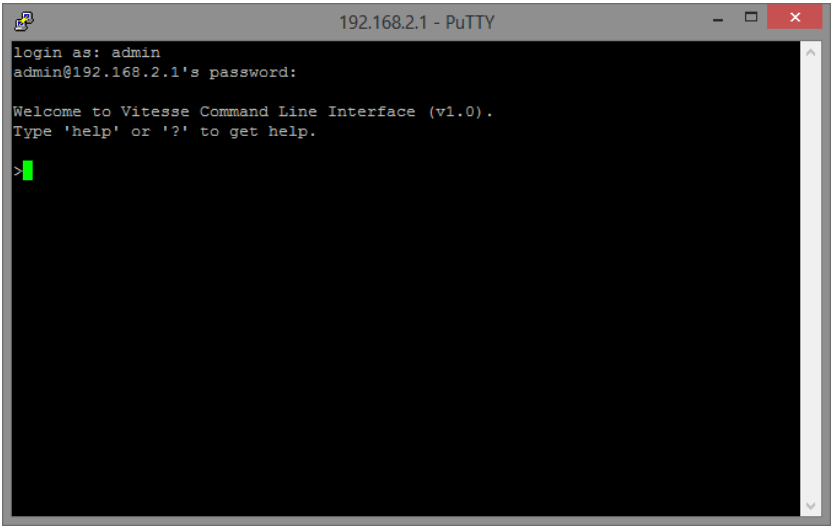
3. Если вы подключаетесь к коммутатору через SSH впервые, вы увидите окно PuTTY Security Alert. Нажмите Yes (Да) для продолжения.



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

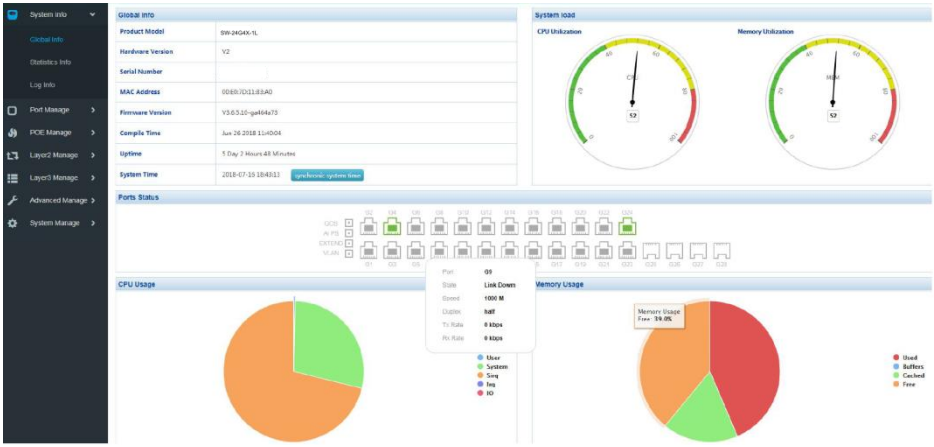
По умолчанию:

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



10. WEB интерфейс управления коммутатором

10.1 Общий вид WEB интерфейса



WEB интерфейс разделен на 7 групп настроек:

- ✓ System Info – журналы и тд., относящиеся к общим настройкам коммутатора;
- ✓ Port Manage – настройки, журналы и тд., относящиеся к портам коммутатора;
- ✓ POE Manage – настройки, журналы и тд., относящиеся к питанию PoE (Power Over Ethernet);
- ✓ Layer2 Manage – настройки, журналы и тд., относящиеся к функциям 2 уровня (Layer2);
- ✓ Layer3 Manage – настройки, журналы и тд., относящиеся к функциям 3 уровня (Layer3);
- ✓ Advanced Manage – дополнительные настройки коммутатора;
- ✓ System Manage – настройки системы, обновление прошивки и тд.

10.2 Системная информация (System Info)

10.2.1 Общая информация о системе (Global Info)

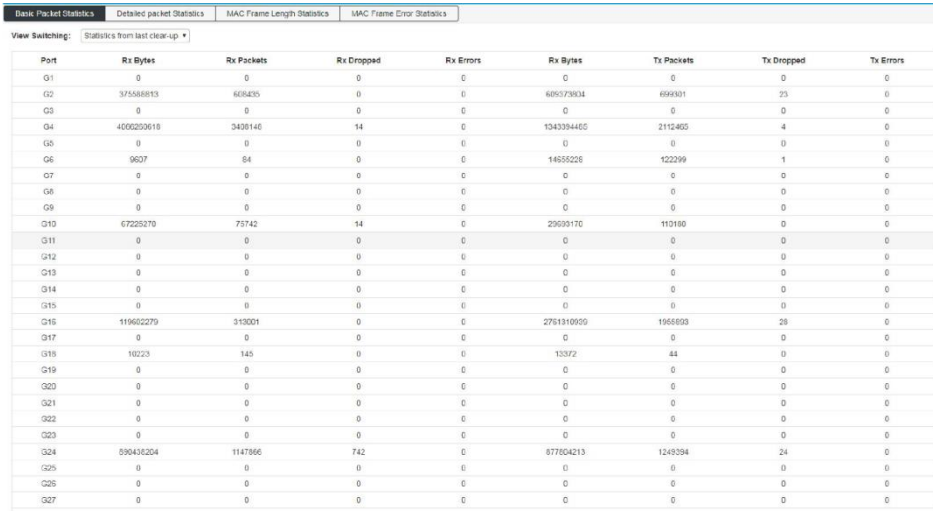
На данной странице WEB интерфейса представлена сводная информация о коммутаторе. Окно визуально разделено на несколько полей в которых содержится следующая информация:

- Global Info (Общая информация)

– Product Model – модель коммутатора;
– Hardware Version – версия исполнения;
– Serial Number – серийный номер устройства;
– MAC Address – MAC адрес устройства;
– Firmware Version – версия прошивки;
– Compile Time – дата создания прошивки;
– Uptime – общее время работы коммутатора со старта;
– System Time – системное время (предусмотрена кнопка для синхронизации с временем, установленным в ОС).

- System Load (Загрузка в % CPU и оперативной памяти коммутатора) – информация представлена в виде удобных диаграмм.
- Port Status (Информация о портах коммутатора) – вид передней панели коммутатора, на которой отображаются задействованные порты и кнопки. Дополнительные сведения (скорость, состояние и тд.) можно получить, нажав на соответствующий порт.
- CPU Usage (Диаграмма использования ресурсов CPU коммутатора)
- Memory Usage (Диаграмма использования памяти коммутатора)

10.2.2 Накопленная статистика работы (Statistic Info)


Basic Packet Statistics | Detailed packet Statistics | MAC Frame Length Statistics | MAC Frame Error Statistics

View Switching: Statistics from last clear-up

Port	Rx Bytes	Rx Packets	Rx Dropped	Rx Errors	Rx Bytes	Tx Packets	Tx Dropped	Tx Errors
G1	0	0	0	0	0	0	0	0
G2	375588813	608435	0	0	605373804	699301	23	0
G3	0	0	0	0	0	0	0	0
G4	4066250618	3408146	14	0	1343394466	2112465	4	0
G5	0	0	0	0	0	0	0	0
G6	9607	84	0	0	14656228	122299	1	0
G7	0	0	0	0	0	0	0	0
G8	0	0	0	0	0	0	0	0
G9	0	0	0	0	0	0	0	0
G10	67225270	75742	14	0	29939170	110180	0	0
G11	0	0	0	0	0	0	0	0
G12	0	0	0	0	0	0	0	0
G13	0	0	0	0	0	0	0	0
G14	0	0	0	0	0	0	0	0
G15	0	0	0	0	0	0	0	0
G16	119602279	313001	0	0	2761310939	1956693	28	0
G17	0	0	0	0	0	0	0	0
G18	10223	145	0	0	13372	44	0	0
G19	0	0	0	0	0	0	0	0
G20	0	0	0	0	0	0	0	0
G21	0	0	0	0	0	0	0	0
G22	0	0	0	0	0	0	0	0
G23	0	0	0	0	0	0	0	0
G24	590436204	1147866	742	0	877604213	1249394	24	0
G25	0	0	0	0	0	0	0	0
G26	0	0	0	0	0	0	0	0
G27	0	0	0	0	0	0	0	0

На данной странице WEB интерфейса коммутатора отображается информация по принятым/отправленным пакетам для каждого порта коммутатора (Basic Packet Statistics), а также:

- ✓ Port – номер порта коммутатора;
- ✓ Rx Bytes – количество принятой информации в байтах;

- ✓ Rx Packets – количество принятых пакетов;
- ✓ Rx Dropped – количество отброшенных пакетов при приеме;
- ✓ Rx Errors – количество ошибок при приеме;
- ✓ Tx Bytes – количество отправленной информации в байтах;
- ✓ Tx Packets – количество отправленных пакетов;
- ✓ Tx Dropped – количество отброшенных пакетов при передаче;
- ✓ Tx Errors – количество ошибок при передаче.

Также на данной странице WEB интерфейса содержится информация о:

- Detailed packet Statistics – таблица детальной статистики по принятым/отправленным пакетам;
- MAC Frame Length Statistics – таблица статистики по размеру пакетов;
- MAC Frame Error Statistics – таблица статистики ошибок для MAC пакетов.

10.2.3 Журналы событий (Log Info)

Данная страница WEB интерфейса коммутатора содержит журналы системных событий.

Коммутатор может записывать, классифицировать, управлять всей системной информацией. Журналы событий предоставляют значительную помощь для системного администратора при мониторинге состояния коммутатора и определении системных ошибок.

Журнал системных событий предоставляет 8 уровней информации:

Тип событий	Уровень	Описание
Emergencies (Чрезвычайные ситуации)	0	Система не доступна
Alerts (Оповещение)	1	События, которые требуют скорейшей реакции на них

Critical (Критические события)	2	Важные события
Errors (Ошибки)	3	Сообщения об ошибках
Warnings (Предупреждение)	4	Предупреждающие сообщения
Notification (Уведомления)	5	Стандартные, но важные сообщения
Informational (информационные сообщения)	6	Статистические сообщения, которые должны быть записаны в журнал
Debugging (отладочные сообщения)	7	Информационные сообщения, которые генерируются в процессе отладки

Журнал событий может быть выгружен на USB накопитель, подключенный к соответствующему порту.

10.2.3.1 Список журналов (Log List)

Журналы системных событий могут быть сохранены двумя различными способами: в буфер памяти и в файл на пзу.

Журналы, сохраненные в буфер памяти, стираются после перезагрузки коммутатора.

Журналы, сохраненные в файл на пзу, полностью доступны после перезагрузки коммутатора.

time	level	type	module	param	log
1970-01-01 08:17	5	Link	mono	G2	Interface[G2] state change to up.
1970-01-01 08:17	5	Link	mono	G2	Interface[G2] state change to down.
1970-01-01 08:01	5	Link	mono	G2	Interface[G2] state change to up.
1970-01-01 08:01	5	Enable	poe	G2	Interface[G2] poe power enable state change.
1970-01-01 08:01	5	Status	poe	G2	Interface[G2] poe power good state change.
1970-01-01 08:01	5	Connect	poe	G2	Interface[G2] poe disconnect.
1970-01-01 08:01	5	Enable	poe	G2	Interface[G2] poe power enable state change.
1970-01-01 08:01	5	Status	poe	G2	Interface[G2] poe power good state change.
1970-01-01 08:01	5	Link	mono	G2	Interface[G2] state change to down.
1970-01-01 08:00	5	Link	mono	G6	Interface[G6] state change to up.
1970-01-01 08:00	5	Link	mono	G2	Interface[G2] state change to up.
1970-01-01 08:00	5	Link	mono	G6	Interface[G6] state change to up.
1970-01-01 08:00	5	Link	mono	G2	Interface[G2] state change to up.
1970-01-01 08:00	5	Link	mono	G6	Interface[G6] state change to up.
1970-01-01 08:00	5	Link	mono	G2	Interface[G2] state change to up.

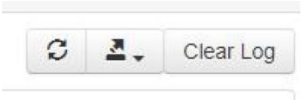
- Serial Number – серийный номер информации в журнале;
- Time – время появления информации в журнале. Время будет указано после синхронизации времени системы коммутатора с временем в ОС;
- Module Name – имя модуля, для которого отображается информация в журнале. Может быть выбран в выпадающем списке;
- Severity Level – уровень важности информации. Может быть выбран из выпадающего списка;
- Log information – содержимое информации в журнале событий.

Максимальное количество записей в журнале – 512.

10.2.3.2 Экспорт журналов событий (Log Save)

Экспорт (выгрузка) журналов позволяет выгружать журнал в виде текстового файла. Для этого необходимо перейти на соответствующую страницу WEB интерфейса:

System Settings >> Log Information >> Log Export



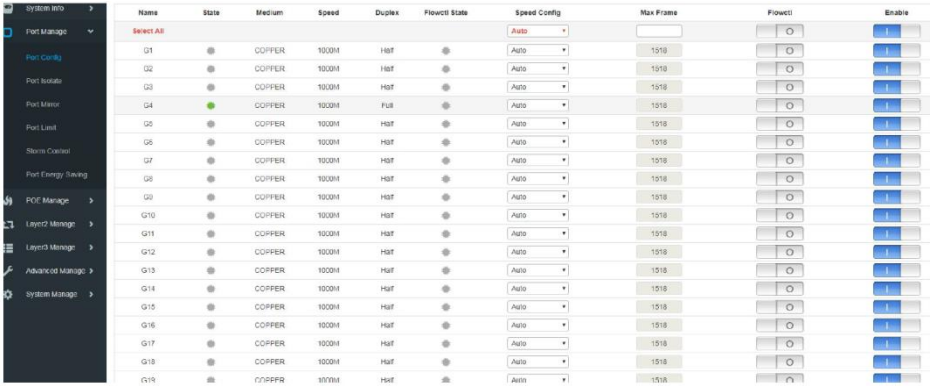
 Обновить списки журналов

 Выгрузка журналов в текстовый файл

Очистить текущий журнал

10.3 Управление портами (Port Managment)

10.3.1 Настройки портов (Port Configuration)

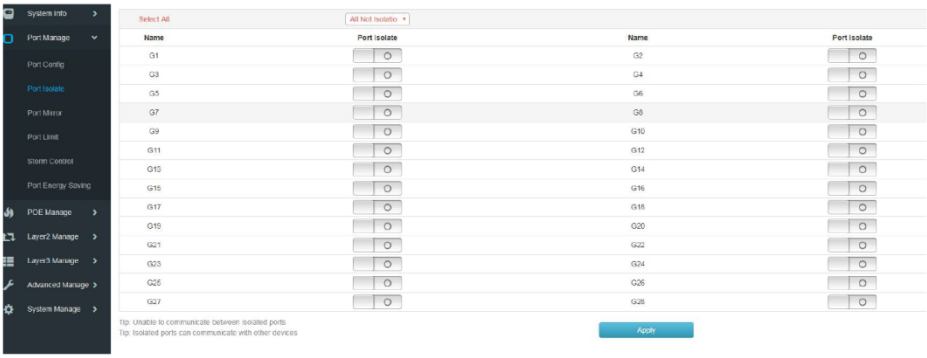


На данной странице WEB интерфейса можно сконфигурировать следующие параметры портов:

- State – цветовое отображение текущего состояния порта
  - Серый – порт не используется;
  - Оранжевый – порт работает на скорости 100 Мбит/с;
  - Зеленый – порт работает на скорости 1000 Мбит/с;
- Speed – скорость порта
- Duplex – режим работы порта
  - Half – полудуплекс;
  - Full – полный дуплекс;

- Rate Configuration – настройка скорости передачи данных для порта/портов.
    1) Скорость может быть установлена сразу для всех портов в самом верхнем выпадающем списке Select All (с красным цветом шрифта);
    2) Скорость может быть установлена для выбранного порта.
- Maximum frame length – максимальный размер обрабатываемых пакетов. Максимальный размер – 10Кбайт (Jumbo Frame).
    1) Размер обрабатываемых пакетов может быть установлен сразу для всех портов в самом верхнем поле Max Frame (красный цвет шрифта);
    2) Размер обрабатываемых пакетов может быть установлен для выбранного порта.
- Flow Control – контроль потока, по умолчанию отключено. Не рекомендуется включать эту функцию, если ваша сеть слишком нагружена.
- Enabled – вкл/выкл выбранного порта.

10.3.2 Изоляция портов (Port Isolation)

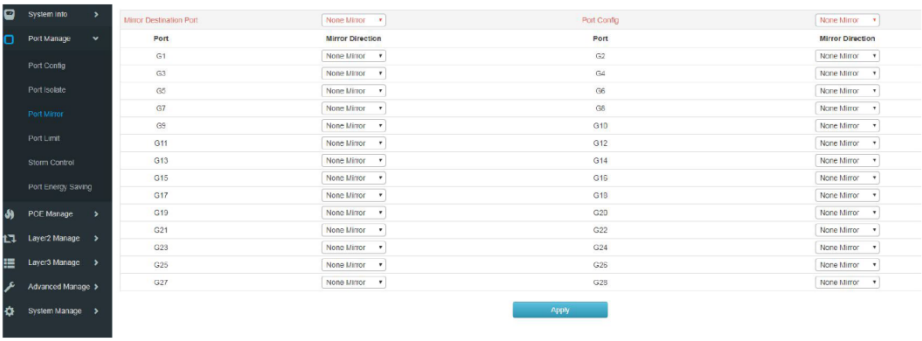


На данной странице WEB интерфейса представлены настройки для изоляции портов. Изолированные порты могут обмениваться

информацией только с указанными портами. Данная функция способна обеспечить защиту портов при Net Storm и Broadcast Storm.

- Select all – поле с красным шрифтом, где можно включить изоляцию сразу для всех портов. При этом изолированные порты не смогут обмениваться трафиком друг с другом.
- Port Isolation – персональная настройка (вкл/выкл) изоляции для выбранного порта.

10.3.3 Зеркалирование портов (Port mirroring)



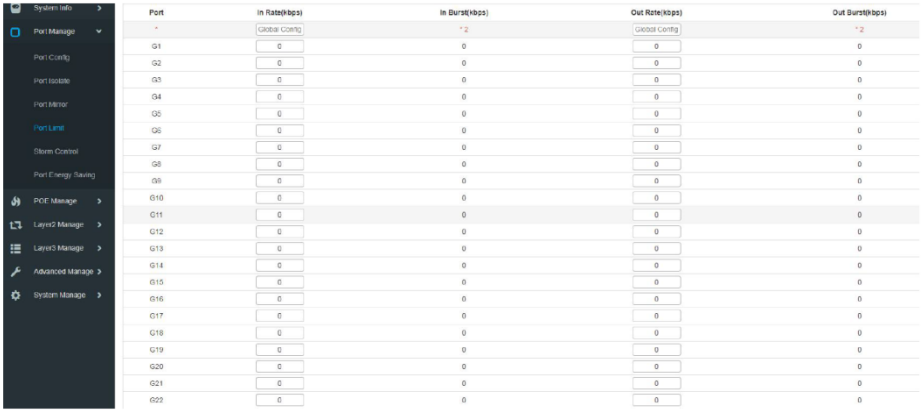
На данной странице WEB интерфейса коммутатора представлены настройки функции зеркалирования – возможности копирования отправляемого/принимаемого трафика на выбранный порт с целью мониторинга и выявления проблем.

- Mirror target port – выбор порта, на который будет дублироваться трафик с интересуемого порта.
- Port Management – настройка порта.

– Not Mirroring – не дублировать трафик на порт-зеркало;
– Receiving image – дублировать только принимаемый трафик на порт-зеркало;
– Send mirroring – дублировать только отправляемый трафик на порт-зеркало;

- Global mirroring – дублировать весь (принимаемый/отправляемый) трафик на порт-зеркало.
- Mirror Direction – настройки зеркалирования для выбранного порта в соответствии с опциями в управлении портами (Port Managment). Опции в Port Management скофигурованы для всех портов.

10.3.4 Ограничение скорости портов (Port Speed Limit)



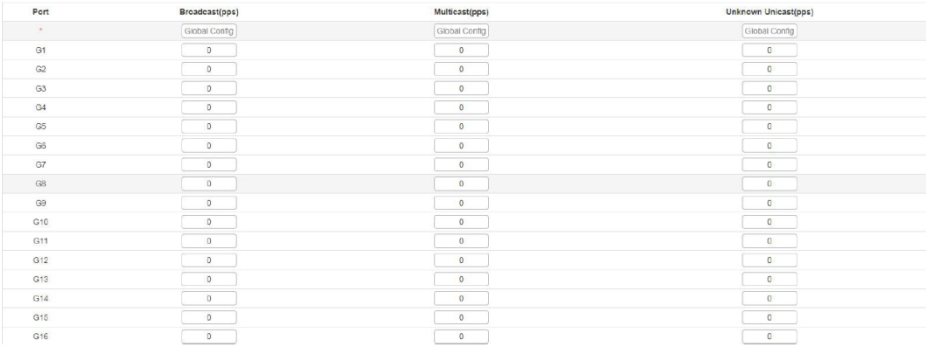
На данной странице WEB интерфейса находятся настройки по ограничению пропускной способности портов (как входящей, так и исходящей).

- ✓ Entrance Rate – в этом поле можно задать скорость приема трафика
- ✓ Exit rate – в этом поле можно задать скорость передачи трафика

Внимание!

Нельзя одновременно использовать ограничение скорости и функцию подавления Net Storm и Broadcast Storm. Активация любой из функций автоматически отключает другую.

10.3.5 Защита от Net Storm и Broadcast Storm (Storm Control)



Port	Broadcast(pps)	Multicast(pps)	Unknown Unicast(pps)
*	Global Config	Global Config	Global Config
G1	0	0	0
G2	0	0	0
G3	0	0	0
G4	0	0	0
G5	0	0	0
G6	0	0	0
G7	0	0	0
G8	0	0	0
G9	0	0	0
G10	0	0	0
G11	0	0	0
G12	0	0	0
G13	0	0	0
G14	0	0	0
G15	0	0	0
G16	0	0	0

Широковещательный шторм (Broadcast Storm) возникает в результате значительного увеличения количества broadcast пакетов в сети. Данное явление значительно снижает общую производительность сети.

На данной странице WEB интерфейса находятся настройки механизма защиты от Broadcast Storm. Всего поддерживается 3 типа пакетов: Broadcast пакеты, Multicast пакеты, Неизвестные Unicast пакеты.

В течение интервала обнаружения коммутатор отслеживает количество полученных пакетов выбранных типов на порте и сравнивает его с максимальным указанным значением. Когда скорость передачи таких пакетов превышает указанный порог, срабатывает механизм Storm Control.

На странице доступны следующие настройки:

- ✓ Broadcast (pps) – поле отвечает за максимальную скорость приема broadcast пакетов. При достижении указанного лимита остальные broadcast пакеты не будут обрабатываться. Доступный диапазон значений 0 – 1000000. 0 означает, что лимит не установлен.
- ✓ Multicast (pps) – поле отвечает за максимальную скорость приема multicast пакетов. При достижении указанного лимита остальные multicast пакеты не будут обрабатываться. Доступный диапазон значений 0 – 1000000. 0 означает, что лимит не установлен.

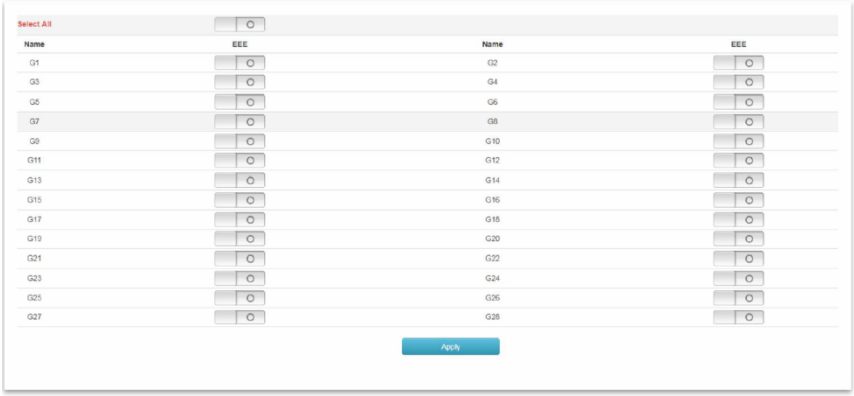
- ✓ Unknown unicast (pps) – поле отвечает за максимальную скорость приема неизвестных Unicast пакетов. При достижении указанного лимита остальные unicast пакеты не будут обрабатываться. Доступный диапазон значений 0 – 1000000. 0 означает, что лимит не установлен.

Значение «Глобальная настройка» (Global Config) позволяет устанавливать лимит для всех портов сразу. После настройки следует нажать Apply Page Setting (Применить настройки страницы).

Внимание!

Нельзя одновременно использовать ограничение скорости и функцию подавления Net Storm и Broadcast Storm. Активация любой из функций автоматически отключает другую.

10.3.6 Функция энергосбережения для портов (Port Energy Saving)



На данной странице WEB интерфейса представлена возможность активировать функцию энергосбережения EEE для выбранных портов.

- ✓ Select all – вкл/выкл функции энергосбережения для всех портов;
- ✓ EEE – вкл/выкл функции энергосбережения для выбранного порта.

10.4 Управление настройками 2 уровня (Layer 2 Managment)

10.4.1 Таблица MAC адресов (MAC Address Table)

Основная задача коммутатора Ethernet – пересылать пакет с данными на канальном уровне в соответствующий порт в соответствии с MAC адресом.

Таблица MAC адресов содержит всю необходимую информацию для пересылки пакетов между портами. Таблица MAC адресов является основой для реализации быстрой пересылки пакетов. При этом записи в таблице MAC адресов можно обновлять как вручную, так и автоматически (learning). Большая часть MAC адресов в таблице создается автоматически, но в некоторых случаях привязка MAC адресов вручную может ускорить саму функцию коммутирования.

Функция фильтрации MAC адресов позволяет коммутатору не обрабатывать пакеты, которые не должны быть обработаны в соответствии с правилами. Фильтрация MAC адресов позволяет повысить общий уровень безопасности сети.

- Add the MAC address – окно в котором пользователь может внести MAC адрес вручную.

- MAC Address – MAC адрес, который нужно добавить;
- Vlan – выбранная VLAN. VLAN 1 зарезервирована системой под физические порты коммутатора;
- Port – соответствующий порт коммутатора.

Кнопка Add – добавить MAC адресс, кнопка Cancel – отмена.

Чтобы удалить запись из таблицы MAC адресов сначала выберите запись, а затем нажмите Delete, чтобы завершить удаление.

- Lease time remaining – поле для указания времени аренды адреса, после которого адрес удаляется из таблицы. Необходимо только для автоматической адресации. MAC адреса, добавленные вручную не требуют указания времени аренды.

Внимание!

Если порт (или устройство) изменено вручную, или указан некорректный MAC, то запись в таблице должна быть удалена, иначе коммутатор не сможет пересылать пакеты корректно.

Примечание!

Если время устаревания MAC адресов (время аренды) слишком велико, то таблица MAC адресов будет забита устаревшими MAC адресами и коммутатор не сможет обновить адреса в таблице для новых подключенных устройств.

Если время устаревания MAC адресов (время аренды) слишком мало, то таблица MAC адресов будет обновляться слишком быстро. Это приведет к тому, что коммутатор не сможет найти необходимые записи в таблице и будет пересылать пакеты с данными на все порты, снижая общую эффективность коммутации.

Рекомендуется использовать значение по умолчанию.

10.4.2 VLAN (VLAN Config)

VLAN (Virtual Local Area Network, виртуальная локальная сеть) — это функция в роутерах и коммутаторах, позволяющая на одном физическом сетевом интерфейсе (Ethernet, Wi-Fi интерфейсе) создать несколько виртуальных локальных сетей. VLAN используют для создания логической топологии сети, которая никак не зависит от физической топологии.

По сравнению с обычной локальной сетью (LAN) виртуальная локальная сеть (VLAN) имеет ряд преимуществ:

- Контроль области широковещательного (Broadcast) домена. Распространение broadcast пакетов ограничено только этой VLAN, таким образом, достигается сохранение пропускной способности сети, а также повышаются возможности по обработке пакетов в сети.

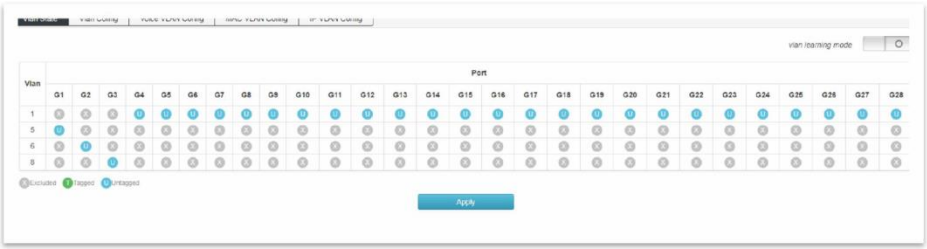
- Повышенная безопасность сети. Поскольку пакеты передаются на канальном уровне и изолированы с помощью broadcast домена, то узлы в каждой VLAN не могут связываться напрямую и должны использовать сетевой уровень (L3) для обмена пакетами.

- Упрощенное управление сетью. Хосты одной рабочей группы могут находиться в разных регионах.

VLAN на основе портов (port-based) строится таким образом, что VLAN назначаются на основе номера интерфейса коммутатора. Администратор сети задает разные PVID для каждого интерфейса (порта) коммутатора.

Когда пакет с данными поступает на порт коммутатора, последний проверяет VLAN тэг (VLAN tag) и PVID порта. Если VLAN тэга нет, то коммутатор присваивает тэг в соответствии с PVID порта. Если VLAN тэг у принимаемого пакета уже существует, то коммутатор не присваивает новый тэг, даже если порт сконфигурирован как PVID.

10.4.2.1 VLAN Static



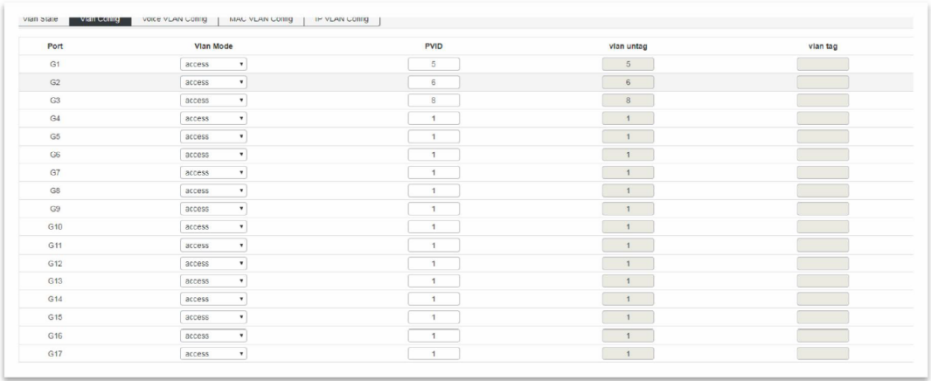
Запоминание VLAN (VLAN Learning)

Каждая VLAN имеет свою собственную таблицу сопоставления MAC Адреса и порта. Таким образом, один и тот же MAC адрес может отображаться в нескольких таблицах сопоставления.

Режим VLAN Learning строится на том, что происходит проверка всей таблицы MAC адресов с помощью комбинации MAC адрес + VID в качестве индекса. Если номера VID всегда разные, то MAC адреса могут повторяться.

Это также означает, что ранее изученный MAC адрес в каждой VLAN принадлежит данной VLAN и не будет совместно использоваться с другими VLAN.

10.5.2.2 Настройка VLAN (VLAN Config)



На данной странице WEB интерфейса представлены настройки для VLAN и настройки VLAN для каждого порта.

- VLAN Mode – режим работы VLAN
  - Access – порт принадлежит только одной VLAN. По умолчанию все пакеты помечаются Untag (без метки);
  - Trunk – порт может принадлежать нескольким VLAN, получать/отправлять пакеты от нескольких VLAN. В сети очень часто VLAN настроены на разных коммутаторах. По умолчанию все пакеты помечаются VLAN tag;
  - Hybrid – порт может пропускать пакеты нескольких VLAN, получать/отправлять пакеты от нескольких VLAN. Такой режим работы VLAN может использоваться для объединения сетевых и пользовательских устройств. Правило генерирования метки (тегирование) для трафика может быть гибко настроено в зависимости от фактического состояния устройства, подключенного к порту.

- PVID – Port VLAN ID – идентификатор VID для порта. Если пакет, полученный портом, не содержит VLAN тэг, то коммутатор помечает пакет на основе значения PVID и пересылает пакет. Когда VLAN разделены в сети PVID является важным параметром каждого порта. У PVID 2 применения:
  - Когда порт получает пакет без метки, коммутатор присваивает VLAN тэг на основе PVID;
  - Когда порт получает широковещательный (broadcast) пакет, коммутатор передает пакет в VLAN, ассоциированную с портом.

- VLAN untag – не помечать пакеты меткой VLAN tag
- VLAN tag – пометить пакеты меткой VLAN tag

Пример конфигурации:

Добавить порт G2 в VLAN10.

Добавить порты G2-G6 в VLAN10

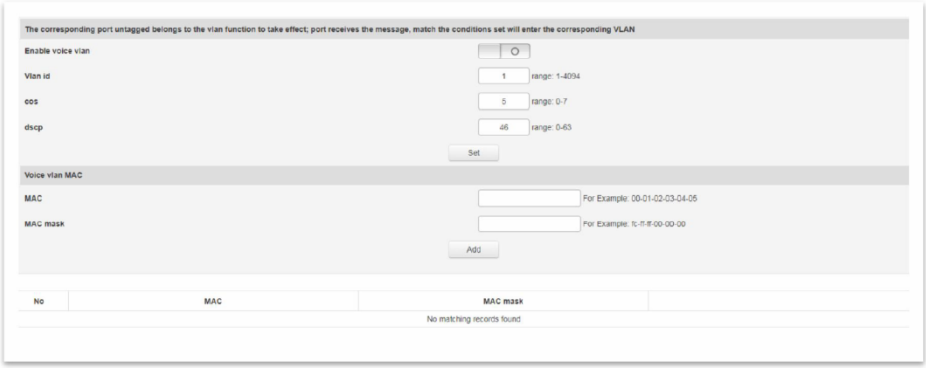
Добавить порт G9 к нескольким VLAN

При настройке порта, как порта принадлежащего нескольким VLAN следует изменить режим работы на Trunk или Hybrid, а затем настроить VLAN tag.

10.4.2.3 Voice VLAN Configuration

Голосовая VLAN это VLAN предназначенная для передачи голосового трафика между пользователями.

Создав голосовую VLAN и добавив порт, к которому подключено устройство VoIP вы сможете разрешить передачу голосового трафика. Такой подход улучшает качество передаваемого через сеть голоса, облегчает настройку QoS.



- ✓ Enable Voice VLAN – вкл/выкл голосовой VLAN
- ✓ VLAN ID – идентификатор VLAN, может быть от 1 до 4094. VLAN1 – значение по умолчанию. Остальные VLAN, в которых порт является участником, должны быть переведен в режим Untag.
- ✓ COS – поле для ввода значения CoS (Class of Service) в диапазоне от 0 до 7. Повышает/понижает приоритет обработки голосового трафика.
- ✓ Dscp – поле для ввода значения dscp (Точка кода дифференцированных услуг) в диапазоне от 0 до 63. Повышает/понижает приоритет обработки голосового трафика.
- ✓ MAC – поле для ввода OUI адреса особого VoIP телефона или голосового клиента. Например, 0812-f231-05e1
- ✓ MAC Mask – поле для ввода значения маски, например ffff-ff00-0000

Примечание!

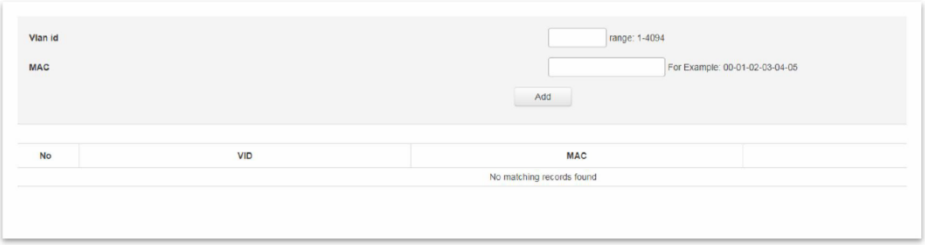
- VLAN1 нельзя указать, как Voice VLAN. Рекомендуется создать другую VLAN для передачи голосового трафика;
- В одно и тоже время только одна VLAN может быть настроена, как Voice VLAN;
- Сопоставление VLAN, стекирование VLAN не разрешены к использованию на порте, задействованном в Voice VLAN.

10.4.2.4 Настройка VLAN на базе MAC адресов (MAC VLAN Configuration)

MAC VLAN – еще один метод разделения VLAN сетей. MAC VLAN сеть разделена в соответствии с MAC адресами каждого хоста. Если пакет без пометок VLAN (untag) получен на порте, то к нему добавляется VLAN ID согласно таблицы.

Преимущества – при изменении физического месторасположения конечного пользователя нет необходимости перенастраивать VLAN. После привязки устройство, соответствующее MAC адресу может использовать порты пока оно подключено к порту-участнику соответствующей VLAN без изменения конфигурации VLAN. Использование MAC VLAN метода повышает безопасность конечных пользователей, а также расширяет гибкость доступа.

Недостатки – применимо только в сценариях, где сетевая карта устройства не заменяется продолжительно время, а сетевое окружение относительно простое. Все участники такой сети должны быть определены заранее.



- ✓ VLAN ID – поле для ввода идентификатора VLAN, которая должна быть добавлена. От 1 до 4094. При этом 1 – значение VID по умолчанию и не может быть использовано. Остальные VLAN, в которых порт является участником, должны быть переведен в режим Untag.
- ✓ MAC – поле для ввода MAC адреса клиента.

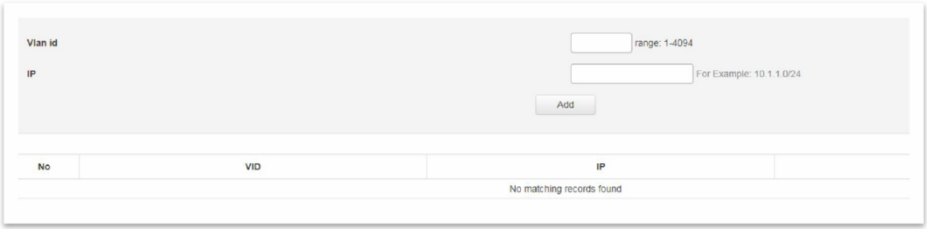
Нажмите Add (Добавить), чтобы завершить создание MAC VLAN.

10.4.2.5 Настройка VLAN на базе IP адресов (IP VLAN Configuration)

VLAN, основанная на протоколе IP, назначает разные VID'ы для пакетов в зависимости от IP адреса, на который адресованы пакеты.

Преимущества – VLAN'ы разделены на основе IP адреса и типа сервиса. Это удобно для управления такой сетью и ее обслуживания.

Недостатки – таблица сопоставления всех IP протоколов и VID'ов должна быть настроена заранее. Необходимо проанализировать формат адресов различных IP протоколов, выполнить соответствующие преобразования – все это потребляет больше ресурсов коммутатора и сказывается на конечной скорости обработки пакетов в сети.



- ✓ VLAN ID – поле для ввода идентификатора VLAN, которая должна быть добавлена. От 1 до 4094. При этом 1 – значение VID по умолчанию и не может быть использовано. Остальные VLAN, в

которых порт является участником, должны быть переведен в режим Untag.

- ✓ IP – поле для ввода IP адреса клиента.

10.4.3 Агрегирование каналов (Link Aggregation)

Физические порты могут быть объедены в один логический порт для оптимизации нагрузки входящего/исходящего трафика на каждый порт-участник логического порта. Весь трафик может быть разделен между всеми портами-участниками группы агрегации для увеличения пропускной способности.

В то же время каждый порт-участник группы агрегации динамически резервирует друг друга, что повышает общую надежность соединения.

Порты-участники одной и той же группы агрегации должны быть сконфигурированы одинаково (STP, QoS, VLAN, атрибуты порта, MAC Address Learning и тд).

10.4.3.1 Настройки постоянной агрегации (Static Aggregation Config)

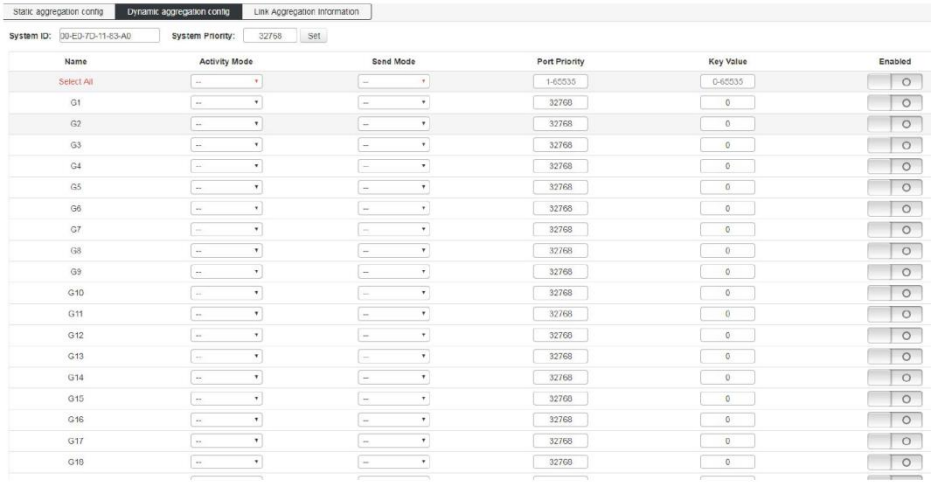
На данной странице WEB интерфейса коммутатора есть возможность вручную настроить группу агрегации. LACP статус для порта, настроенного вручную – отключен.

Нажмите Create (Создать), чтобы в появившемся окне задать ID группы и подтвердить (Establish) ее создание.

- Delete – выберите группу агрегации, которую необходимо удалить и нажмите Delete (Удалить).
- Load Balancing Mode – выбор метода балансировки.

– Src MAC – распределение на основе MAC адреса источника;
– Dst MAC – распределение на основе MAC адреса конечного устройства;
– Src&Dst MAC – распределение на основе MAC адреса источника и MAC адреса конечного устройства. По умолчанию;
– Src IP – распределение на основе IP адреса источника
– Dst IP – распределение на основе IP адреса конечного устройства
– Src&Dst IP – распределение на основе IP адреса источника и MAC адреса конечного устройства

10.4.3.2 Настройки динамической агрегации (Dynamic Aggregation Config)



Протокол LACP (Link Aggregation Control Protocol) используется для динамического агрегирования каналов, а также для расформирования ранее созданной группы агрегации.

- System Priority – приоритет устройства определяется вместе с MAC адресом системы. Устройство с самым высоким значением будет доминировать при создании группы агрегации или ее расформирования. Значение по умолчанию – 32768.
- Activity Mode – периодичность посылки LACP пакетов.
  - Active Mode – порт автоматически посылает LACP пакеты с периодичностью, указанной в поле Send Mode.
  - Passive Mode – порт не посылает автоматически пакеты LACP, а реагирует только на пакеты LACP отправленные с однорангового устройства.
- Send Mode – выбор скорости посылки LACP пакетов.
  - Slow – медленная скорость;
  - Fast – быстрая скорость;

- No Send Mode – не посылать LACP пакеты.

- Port Priority – приоритет порта-участника группы агрегации. Чем меньше значение, тем предпочтительнее порт. Значение по умолчанию – 32768.
- Key value – ключ группы агрегации. Для участников одной группы ключ должен быть одинаковый.
- Enabled/Disabled – вкл/выкл динамической агрегации каналов LACP. По умолчанию выкл.

10.4.3.3 Информация о группах агрегации (Link Aggregation Information)

На данной странице WEB интерфейса находится детальная статистика по группам агрегации, включая количество портов-участников, приоритеты, режим балансировки и значения ключей для постоянной или динамической агрегации.

- ✓ Aggregation Group – имя группы агрегации;
- ✓ Mode – режим агрегации (динамический или постоянный);
- ✓ Number of Ports – порты-участники группы агрегации;
- ✓ Port List – порты, которые должны войти в группу агрегации;
- ✓ Load Balancing – режим балансировки портов внутри группы.

10.4.4 Настройка протокола STP (STP Configuration)

Семейство протоколов STP/RSTP/MSTP предназначены для предотвращения возникновения сетевых петель в локальной сети, в том числе и при использовании кольцевой топологии подключения.

Устройства, на которых поддерживается работа данных протоколов способны обнаруживать петли в сети при взаимодействии друг с другом и блокировать определенные порты, пока топология не станет похоже на древовидную (tree).

Протокол	Особенности
STP (IEEE 802.1D)	Позволяет сформировать древовидную топологию подключения без петель для исключения влияния broadcast шторма. Время восстановления топологии – медленное
RSTP (IEEE 802.1W)	Позволяет сформировать древовидную топологию подключения без петель для исключения влияния broadcast шторма. Время восстановления топологии – быстрое
MSTP (IEEE 802.1S)	Позволяет сформировать древовидную топологию подключения без петель для исключения влияния broadcast шторма. Время восстановления топологии – быстрое. MSTP используется обычно для VLAN сетей.

10.4.4.1 Глобальная настройка (Global Configuration)

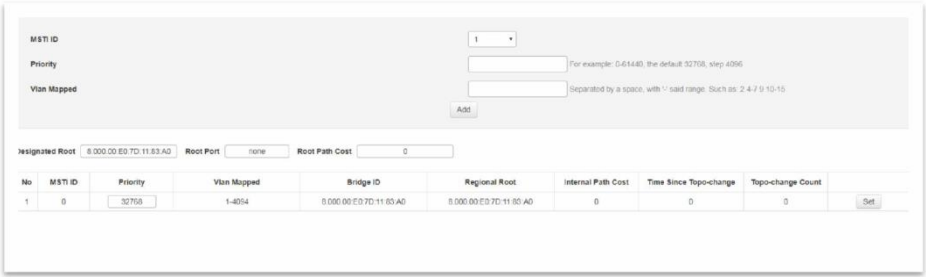
На данной странице WEB интерфейса представлены глобальные настройки STP протоколов.

- Enable Spanning Tree – включение/выключение применения протоколов STP.
- Protocol Version – версия протокола
  - STP;
  - RSTP;
  - MSTP.
- Max Age – время жизни сообщения. Диапазон возможных значений от 6 – 40 сек. Значение по умолчанию – 20 сек.
- Hello Time – период в течение которого было отправлено сообщение. Устройство Bridge передает такие пакеты окружающим устройствам.
- Forward Delay – задержка перед сменой состояния порта. Диапазон от 4 до 30 сек. Значение по умолчанию – 15 сек.
- Max Hops – максимальное количество хопов (переходов). Диапазон значений от 0 до 20. Большое количество хопов используется для искусственного ограничения размера сети.

- Revision Level – уровень ревизии MSTP. Используется для определения имени домена с таблицей сопоставления VLAN.
- Configuration Name – значение по умолчанию MAC адрес основной платы в коммутаторе.

Необходимо нажать кнопку Apply (Принять) для того, чтобы настройки вступили в силу.

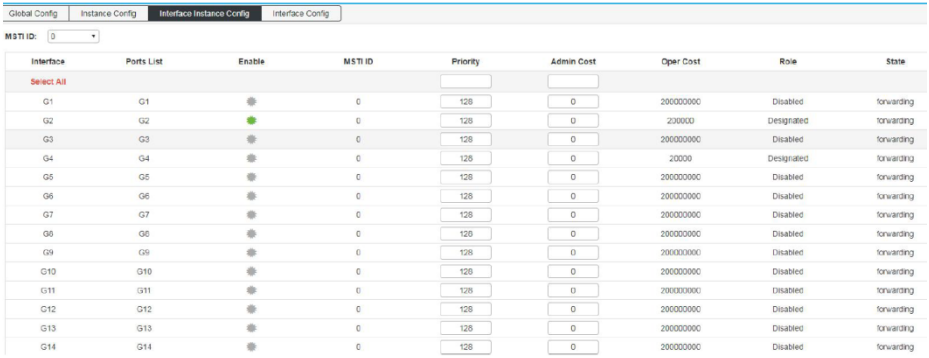
10.4.4.2 Настройка instance (Instance Config)



- ✓ MSTI ID – выбор идентификатора MSTI;
- ✓ Priority – значение приоритета для выбранного instance. Доступный диапазон значений от 0 до 65535. Значение по умолчанию – 32768;
- ✓ VLAN Mapped – VLAN'ы, пакеты с которых могут быть перенаправлены.

Кнопка Add – добавить.

10.4.4.3 Настройка instance для портов (Interface Instance Config)



На данной странице WEB интерфейса находятся инструменты для настройки портов при работе с протоколом MSTP.

- MSTID – выбор настроенного instance из выпадающего списка.
- Priority – выбор значения приоритета для порта. Данное значение может влиять на роль порта в MSTI. При изменении значения приоритета порта, механизм протокола MSTP пересчитывает роль интерфейса и осуществляет переход между состояниями.
- Path Cost – стоимость пути. Значение определяет, будет ли порт являться корневым (root). Меньшее значение отвечает за более высокий приоритет.
- Role – роль порта в выстраиваемой древовидной топологии.
  - Disable – порт без физического подключения;
  - Designated – порт, отвечающий за перенаправление данных в нисходящие сегменты сети или устройства;
  - Root – порт с наименьшим показателем Path Cost, отвечает за перенаправление данных корневому мосту (root bridge);
  - Alternate – резервный порт root порта или master порта;

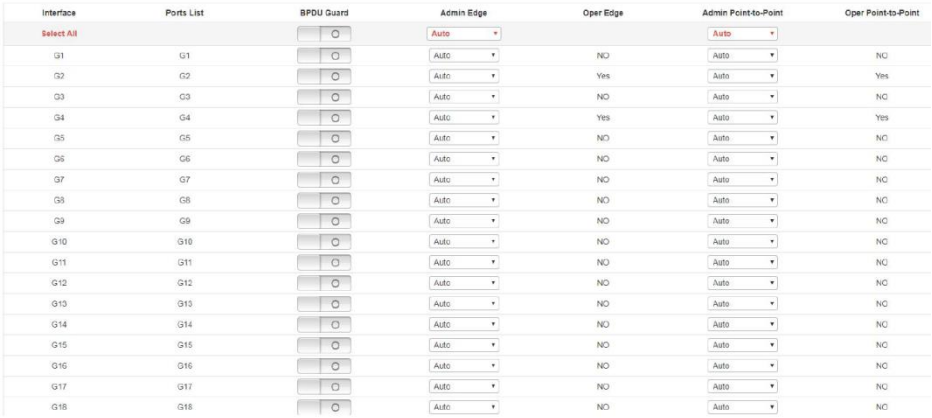
  - Master Port – порт, отвечающий за подключение MSTP доменов к общему корневому порту с наименьшим показателем Path Cost;
  - Backup Port – резервный порт.
- Status – текущий статус порта.
  - Discarding – порт без физического подключения;
  - Forwarding – порт принимает и отправляет данные, занимается приемом/отправкой пакетов протокола и выполняет обучение на основе адресов (address learning);
  - Blocking – порт не принимает и не отправляет данные. Также не занимается обучением на основе адресов и не отправляет пакеты протокола;
  - Learning – порт принимает/отправляет пакеты протокола, выполняется обучение на основе адресов. Данные не принимаются и не передаются.
- Description – соотношение STP Cost и пропускной способности.

Полоса пропускания	STP Cost
4 Мбит/с	250
10 Мбит/с	100
16 Мбит/с	62
45 Мбит/с	39
100 Мбит/с	19
155 Мбит/с	14
622 Мбит/с	6
1 Гбит/с	4
10 Гбит/с	2

Примечание:

Порт, напрямую подключенный к терминалу, установите как Edge порт и включите BPDU защиту (BPDU Guard). Таким образом, порт можно быстро перевести в состояние пересылки, а сеть может быть защищена.

10.4.4.4 Настройка портов для STP (Interface Config)



Interface	Ports List	BPDU Guard	Admin Edge	Oper Edge	Admin Point-to-Point	Oper Point-to-Point
Select All			Auto		Auto	
G1	G1		Auto	NO	Auto	NO
G2	G2		Auto	Yes	Auto	Yes
G3	G3		Auto	NO	Auto	NO
G4	G4		Auto	Yes	Auto	Yes
G5	G5		Auto	NO	Auto	NO
G6	G6		Auto	NO	Auto	NO
G7	G7		Auto	NO	Auto	NO
G8	G8		Auto	NO	Auto	NO
G9	G9		Auto	NO	Auto	NO
G10	G10		Auto	NO	Auto	NO
G11	G11		Auto	NO	Auto	NO
G12	G12		Auto	NO	Auto	NO
G13	G13		Auto	NO	Auto	NO
G14	G14		Auto	NO	Auto	NO
G15	G15		Auto	NO	Auto	NO
G16	G16		Auto	NO	Auto	NO
G17	G17		Auto	NO	Auto	NO
G18	G18		Auto	NO	Auto	NO

На данной странице WEB интерфейса коммутатора находятся настройки портов для работы с STP протоколом.

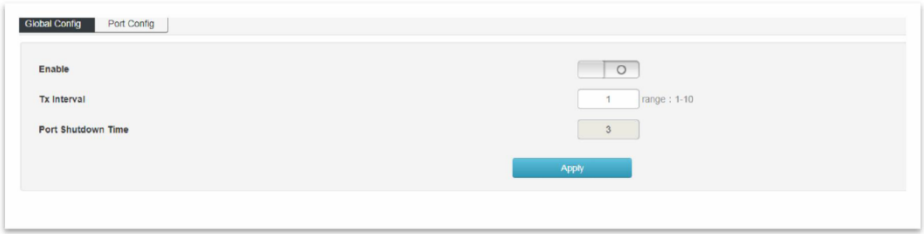
- BPDU Guard – вкл/выкл защиты BPDU. С включенной функцией BPDU Guard порт, который принимает BPDU пакеты, будет отключен. Отключенный порт сможет быть восстановлен только администратором сети вручную.
- Admin Edge – Edge порт должен быть подключен непосредственно к терминалу пользователя вместо коммутатора или другого сегмента. Порт Edge способен быстро изменить свое состояние на состояние пересылки (forwarding)
- Admin Point-to-Point, Oper Point-to-Point – да/нет. Состояние порта, когда он:
  - Auto – задействован в соединении точка-точка. Автоопределение;
  - Force-true – задействован в соединении точка-точка;
  - Force-false – не задействован с соединении точка-точка.

10.4.5 Защита от петель (Loop protection)

Когда используемая топология подключения стабильна, коммутатор получает BPDU пакеты от вышестоящего коммутатора. Если подключение неисправно или используется однонаправленное подключение, то коммутатор не сможет получать пакеты BPDU. STP топология пересчитывается, заблокированный порт переводится в состояние пересылки. В середине возникает петля.

Функция защиты от петель (Loop Protection) предотвращает развитие таких событий. Если порт не получает BPDU, то он будет блокирован независимо от выбранной роли порта.

10.4.5.1 Глобальные настройки (Global Config)

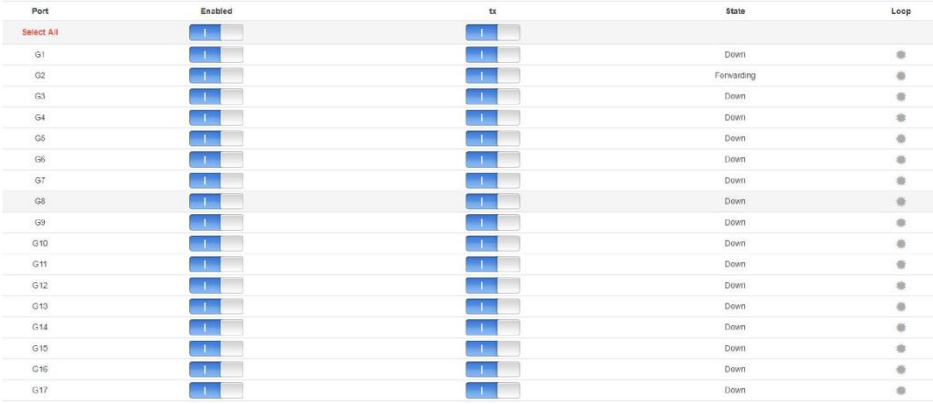


На данной странице находятся глобальные настройки функции Loop Protection.

- ✓ Enable – вкл/выкл функции Loop Protection;
- ✓ Tx Interval – интервал проверки приема BPDU пакетов. По умолчанию 1 сек. Доступные значение 1-10 сек.
- ✓ Port Shutdown Time – время блокировки порта. По умолчанию 3 сек.

Apply – запомнить настройки.

10.4.5.2 Настройка портов для Loop Protection (Port Config)



- ✓ Port – номер конкретного физического порта коммутатора;
- ✓ Enabled – вкл/выкл функции Loop Protection для порта;
- ✓ Tx – вкл/выкл отправки портом пакетов с информацией об обнаружении петли;
- ✓ State – текущее состояние порта
  - Down – отключен;
  - Forwarding – прием/передача пакетов в нормальном режиме;
  - Blocking – порт заблокирован. Порт не сможет принимать/передавать данные, пока не будет разблокирован.
- ✓ Loop – индикатор обнаружения петли на порте.

10.4.6 Функция DHCP Snooping

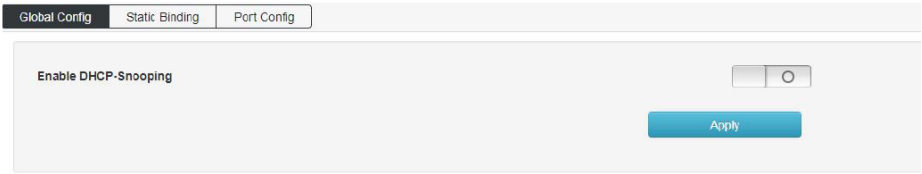
DHCP Snooping – это функция 2 уровня (Layer2), которая позволяет отбрасывать трафик DHCP, определенный как неприемлимый.

DHCP Snooping предотвращает несанкционированные (мошеннические) DHCP-серверы, предлагающие IP-адреса DHCP-клиентам.

Функция DHCP Snooping выполняет следующие действия:

- ✓ Проверяет сообщения DHCP из ненадежных источников и отфильтровывает недействительные сообщения.
- ✓ Создает и поддерживает базу данных привязки DHCP Snooping, которая содержит информацию о ненадежных хостах с арендованными IP-адресами.
- ✓ Использует базу данных привязки DHCP Snooping для проверки последующих запросов от ненадежных хостов.

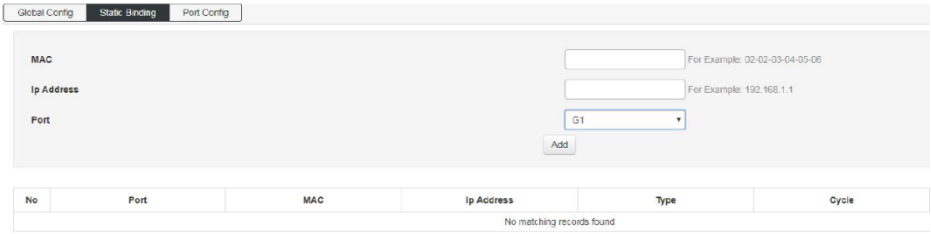
10.4.6.1 Глобальные настройки DHCP Snooping (Global Config)



На данной странице WEB интерфейса находятся глобальные настройки функции DHCP Snooping.

Для подтверждения настроек используйте кнопку Принять (Apply).

10.4.6.2 Постоянная привязка (Static Binding)



На данной странице WEB интерфейса коммутатора находятся настройки постоянной привязки MAC и IP адресов. Таблица привязки помогает избежать атаки с использованием истощения DHCP.

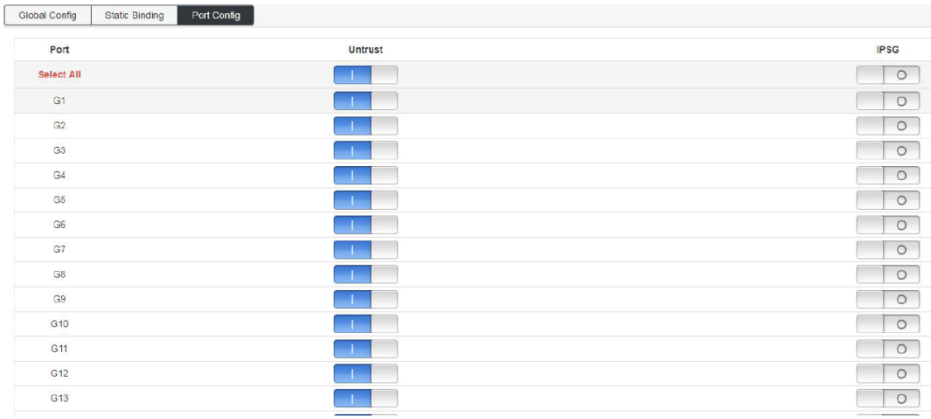
- ✓ MAC – поле для ввода MAC адреса.
- ✓ IP Address – поле для ввода IP адреса.
- ✓ Port – привязка к выбранному порту коммутатора.

Для завершения привязки нажмите кнопку Add (Добавить)

Итоговый результат выглядит следующим образом:

No	Port	MAC	Ip Address	Type	Cycle	
1	G10	a6-a6-a6-a6-a6-a8	192.168.18.101	Dynamic	3750	Binding Add
2	G10	b0-e5-ed-a4-83-41	192.168.18.103	Dynamic	4440	Binding Add
3	G16	20-60-58-66-33-10	192.168.1.166	Static	0	Add

10.4.6.3 Управление портами (Port Config)



На данной странице WEB интерфейса коммутатора есть инструменты для объявления портов доверенными/недоверенными и тд.

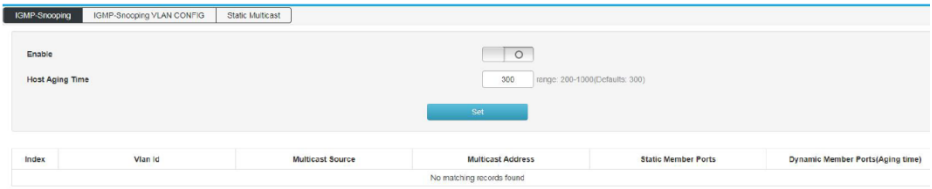
- ✓ Untrust – вкл/выкл объявления порта доверенным (trust) и недоверенными (untrust).
- ✓ IPSG – вкл/выкл фильтрации исходных IP адресов на основе таблицы привязки.

10.4.7 Функция IGMP Snooping

IGMP snooping — функция отслеживания сетевого трафика IGMP, который позволяет сетевым устройствам канального уровня (коммутаторам) отслеживать IGMP-обмен между потребителями и поставщиками (маршрутизаторами) многоадресного (multicast) IP-трафика, формально происходящий на более высоком (сетевом) уровне.

После включения IGMP snooping коммутатор начинает анализировать все IGMP-пакеты между подключенными к нему компьютерами-потребителями и маршрутизаторами-поставщиками multicast трафика. Обнаружив IGMP-запрос потребителя на подключение к multicast группе, коммутатор включает порт, к которому тот подключён, в список её членов (для ретрансляции группового трафика). И наоборот: услышав запрос 'IGMP Leave' (покинуть), удаляет соответствующий порт из списка группы.

10.4.7.1 Глобальные настройки IGMP snooping (IGMP Snooping)



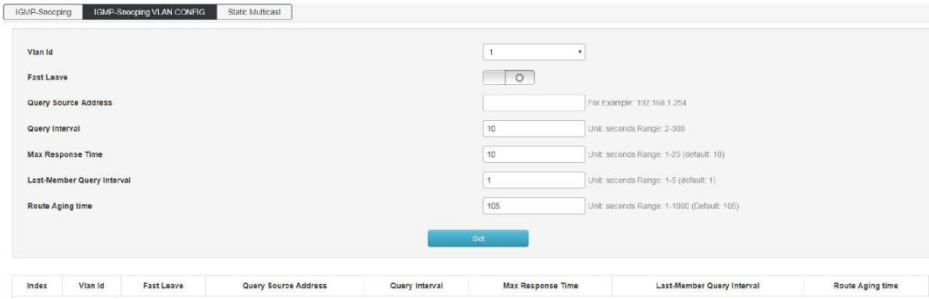
На данной странице WEB интерфейса находятся глобальные настройки функции IGMP Snooping.

Enable – вкл/выкл функции IGMP Snooping;

Host Aging Time – когда порт-участник добавляется в группу многоадресной (multicast) рассылки, коммутатор выполняет проверку с заданным в этом поле временем. Если порт не получает в течение времени Aging time пакет отчета, то порт перестает быть участником группы многоадресной (multicast) рассылки.

Для подтверждения нажмите кнопку Set

10.4.7.2 Настройка IGMP Snooping для VLAN (IGMP Snooping VLAN Config)



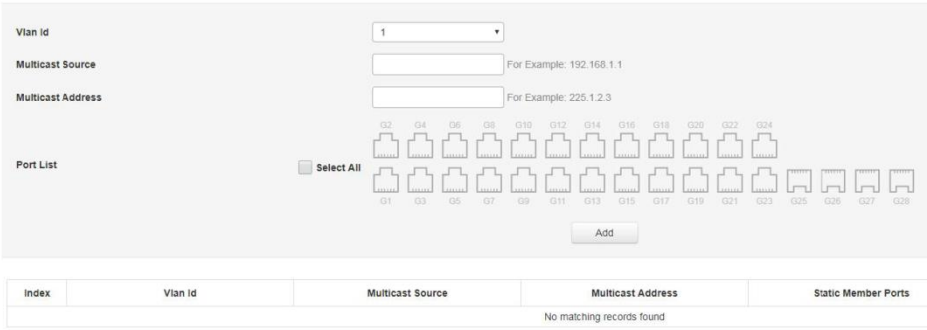
На данной странице WEB интерфейса находятся настройки группы многоадресной рассылки, созданной с помощью IGMP Snooping основанной на широковещательном домене VLAN. Различные VLAN можно настроить с различными параметрами IGMP.

- VLAN ID – идентификатор VLAN, для которой необходимо включить IGMP Snooping.
- Fast Leave – вкл/выкл. Если порт покидает группу многоадресной рассылки, то коммутатор получает IGMP Leave сообщение и удаляет порт из группы многоадресной рассылки.
- Query Source Address – IP адрес источника запросов.
- Query Interval – интервал отправления запросов.
- Max Response Time – время отклика на запрос.
- Lost-Member Query Interval – интервал отправления запросов

Примечание !

Fast leave будет иметь эффект, только если хост поддерживает IGMP v2 или IGMP v3.

10.4.7.3 Постоянный мультикастинг (Static Multicast)



На данной странице WEB интерфейса коммутатора находятся настройки постоянного мультикастинга, который в отличие от предыдущего метода обеспечивает изоляцию VLAN, безопасность, а также гарантирует пропускную способность.

- VLAN ID – поле для ввода идентификатора multicast VLAN;
- Multicast Source – поле для ввода IP адреса multicast сервера;
- Multicast Address – поле для ввода IP адреса multicast сервера, который должен быть multicast адресом;
- Port List – выбор порта для добавления в группу многоадресной рассылки.

Multicast адрес:

Диапазон multicast адресов	Примечание
224.0.0.0 – 224.0.0.255	Пул адресов, зарезервированный для протоколов маршрутизации, обнаружения и обслуживания
224.0.1.0 – 224.0.1.255	Пул адресов для видео и конференц-связи. Данный публичный пул адресов можно использовать в интернете
239.0.0.0 – 239.255.255.255	Пул адресов для LAN. Не может быть использован для интернета

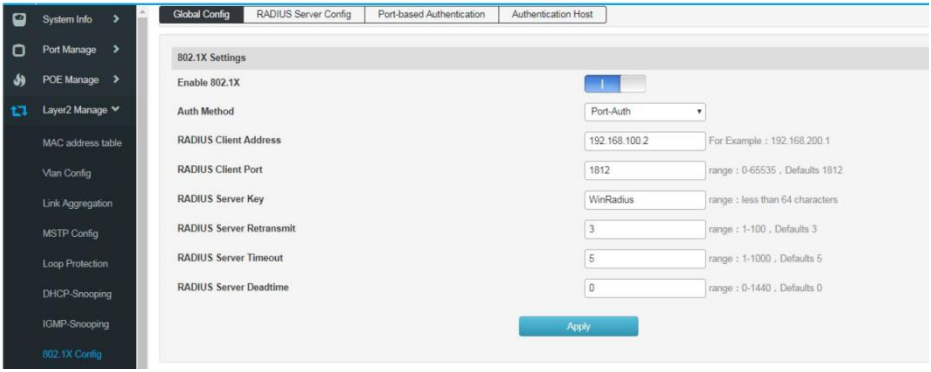
10.4.8 Настройка 802.1x (802.1x Configuration)

802.1x — это стандарт, который используется для аутентификации и авторизации пользователей и рабочих станций в сети передачи данных.

Благодаря стандарту 802.1x можно предоставить пользователям права доступа к корпоративной сети и ее сервисам в зависимости от группы или занимаемой должности, которой принадлежит тот или иной пользователь.

Так, подключившись к беспроводной сети или к сетевой розетке в любом месте корпоративной сети, пользователь будет автоматически помещен в тот VLAN, который предопределен политиками группы, к которой привязана учетная запись пользователя или его рабочей станции в AD. К данному VLAN будет привязан соответствующий список доступа ACL (статический, либо динамический, в зависимости от прав пользователя) для контроля доступа к корпоративным сервисам. Кроме списков доступа, к VLAN можно привязать политики QoS для контроля полосы пропускания.

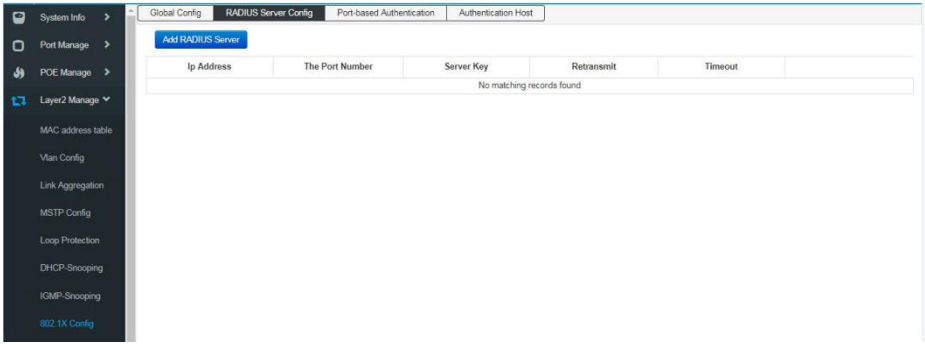
10.4.8.1 Глобальные настройки 802.1x (Global Config)



На данной странице WEB интерфейса находятся глобальные настройки для стандарта безопасности 802.1x.

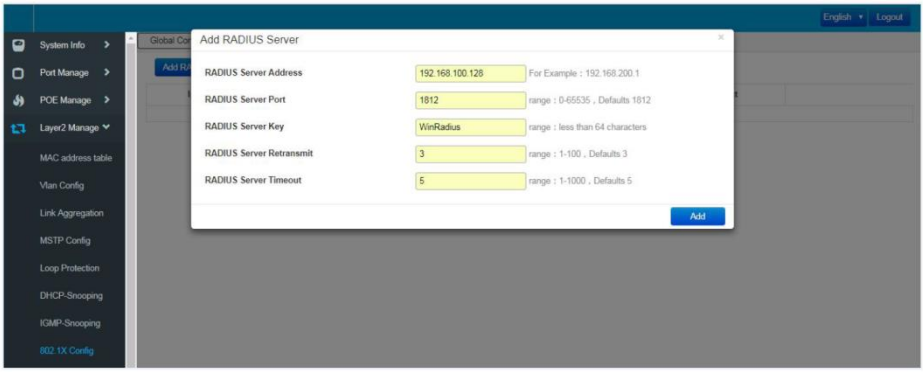
- Enable 802.1X – вкл/выкл использования стандарта 802.1x
- Auth Method – выбор метода аутентификации
  - Port-based – все пользователи, после первого, удачного авторизованного пользователя, могут использовать сеть. Если первый, удачно авторизованный пользователь отключается, остальные пользователи также теряют доступ к сети;
  - MAC-based – пользователи получают доступ к сети на основе заранее одобренных MAC адресов.
- RADIUS Client Address – поле для указания IP адреса клиента RADIUS.
- RADIUS Client Port – поле для указания порта, связывающегося с RADIUS клиентом.
- Radius Client Server Key – ключ для пакетов от RADIUS сервера.
- Radius Client Server Retransmit – количество повторных передач пакетов RADIUS сервера. В случае, если совокупное количество передач превысит максимальное значение и RADIUS сервер не реагирует, коммутатор уведомит об ошибке аутентификации. Значение по умолчанию – 5.
- Radius Client Server Timeout – время ожидания ответа от сервера RADIUS. Значение по умолчанию – 5 сек.
- Radius Client Server Deadtime – время, после которого RADIUS сервер считается недоступным/отключенным. Диапазон 0 – 1440.

10.4.8.2 Настройки сервера RADIUS (RADIUS Server Config)



На данной странице WEB интерфейса коммутатора находятся инструменты для добавления и настройки сервера RADIUS.

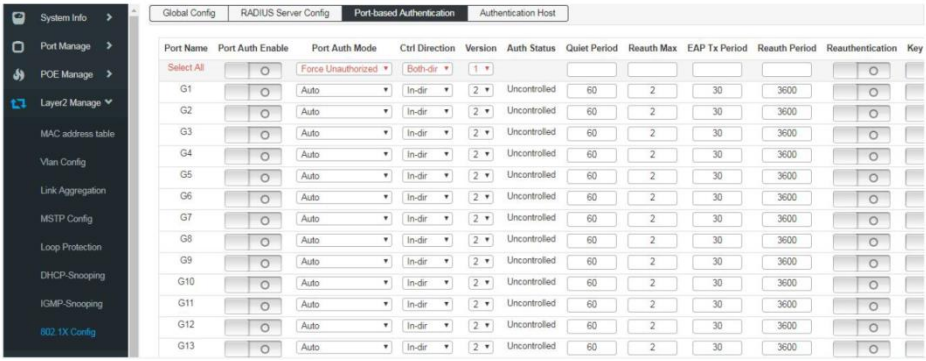
Нажмите кнопку Add RADIUS Server (Добавить сервер RADIUS)



И заполните поля, как на рисунке ниже, используя свои данные. Результат добавления отобразится в таблице, где его можно перенастроить кнопкой Set или удалить кнопкой Del.

- RADIUS Server Address – поле для указания IP адреса клиента RADIUS;
- RADIUS Server Port – поле для указания порта, связывающегося с RADIUS клиентом;
- RADIUS Server Key – ключ для пакетов от RADIUS сервера;
- RADIUS Server Retransmit – количество повторных передач пакетов RADIUS сервера;
- RADIUS Server Timeout – время ожидания ответа от сервера RADIUS.

10.4.8.3 Аутентификация на основе портов (Port-based Authentiction)



- Port Auth Enable – вкл/выкл аутентификации по стандарту 802.1x для выбранного порта.
- Port Auth Mode – режим выполнения аутентификации
  - Auto – в автоматическом режиме;
  - Forced Certified – порт получает доступ к сети без аутентификации;
  - Forced Non-Certified – порт всегда проходит аутентификацию.
- Auth Status – статус выполнения аутентификации на порте.

- Quiet Period – период после неудачной аутентификации пользователя на порте, в течение которого не может быть выполнена повторная аутентификация.
- Reauth Max – максимальное количество повторных аутентификаций.
- EAP Tx Period – интервал для EAP цикла аутентификации.
- Reauthentication – вкл/выкл возможности повторной аутентифиации.

10.5 Управление настройками 3 уровня (Layer3 Management)

10.5.1 Настройка интерфейсов (Interface Setting)

На данной странице WEB интерфейса представлены настройки IPv4 IPv6 адресов для выбранных интерфейсов.

Для создания нового интерфейса нажмите кнопку Create Interface

- ✓ Interface Name – выбор имени сетевого интерфейса;
- ✓ IPv4 Address – поле для ввода Ipv4 адреса сетевого интерфейса.

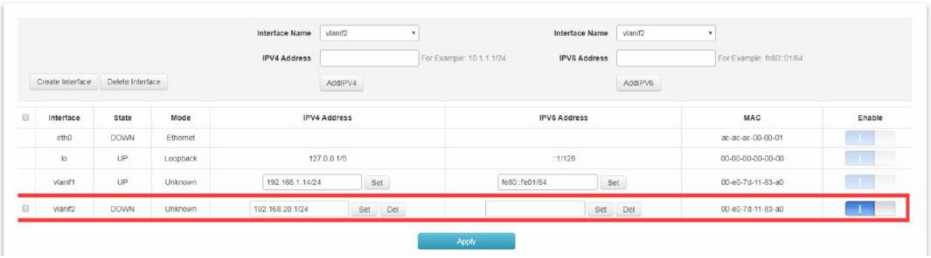


Таблица интерфейсов отображает следующую информацию:

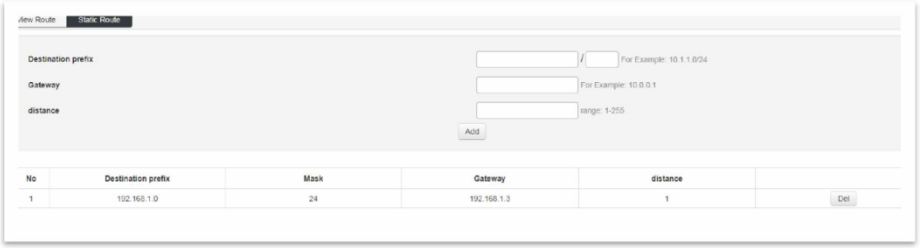
- Interface – поле отображает имя интерфейса;
- State – поле отображает текущее состояние интерфейса
  - UP – активен;
  - DOWN – не активен
- Mode – поле отображает текущий режим работы интерфейса.
- IPv4 Address – поле отображает IPv4 адрес.
- IPv4 Address – поле отображает IPv6 адрес, если он был задан.
- MAC – поле отображает MAC адрес интерфейса.
- Enable – вкл/откл выбранного интерфейса.

10.5.2 Настройка маршрутизации (Routing Configuration)

10.5.2.1 Просмотр маршрутов (View the routing)

На данной странице WEB интерфейса коммутатора отображается список маршрутов: прямых подключений (direct connection), маршрутов заданных вручную (static routing) и динамических маршрутов (dynamic routing).

10.5.2.2 Постоянные маршруты, заданные вручную (Static Routing)



Постоянные маршруты задаются вручную системным администратором. В сети с простой структурой сетевому администратору достаточно задать постоянные маршруты для надежного подключения всех устройств. Данный вид маршрутизации применяется в небольших сетях с фиксированной топологией.

Выбор правильной постоянной маршрутизации поможет избежать проблем с выбором маршрутов, а также увеличит скорость пересылки пакетов. При изменении сети администратор должен вносить корректировки в постоянную маршрутизацию.

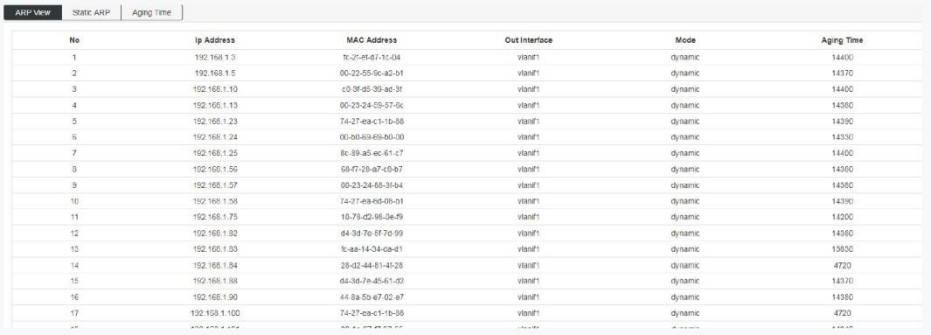
На данной странице WEB интерфейса коммутатора находятся инструменты для создания записей постоянной маршрутизации.

- ✓ Destination prefix – IP адрес в сети, маршрут к которому необходимо задать.
- ✓ Gateway – IP адрес шлюза (следующего узла в маршруте)
- ✓ Distance – значение приоритета для маршрута. Чем значение меньше, тем выше приоритет.

Созданный маршрут будет отображаться во вкладке View Route.

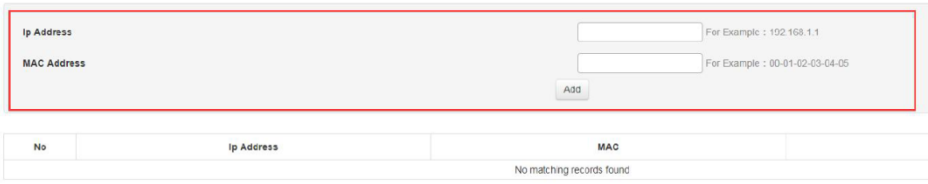
10.5.2.3 Настройка протокола ARP (The ARP configuration)

ARP (Address Resolution Protocol — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения MAC-адреса по IP-адресу другого компьютера.



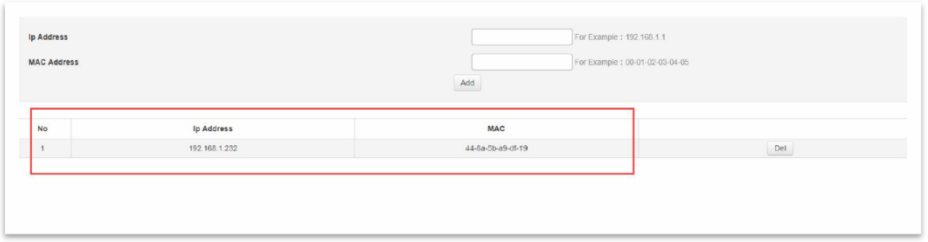
Для настройки постоянной ARP (static ARP):

1) перейдите на вкладку Static ARP



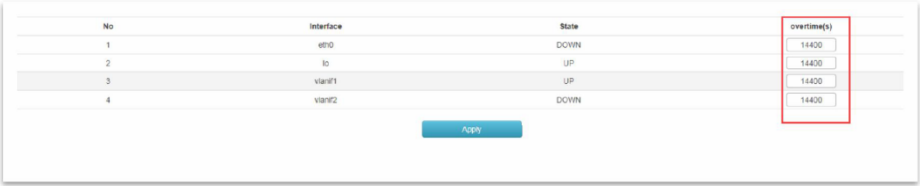
2) Введите IP адрес в поле IP Address;
3) Введите MAC адрес в поле MAC Address;
4) Нажмите кнопку Add.

Итоговый результат отобразится в таблице:



Для настройки времени устаревания ARP:

1) перейдите в раздел ARP Aging Time



2) Введите время устаревания ARP в секундах в поле overtime(s);
3) Нажмите кнопку Apply (принять).

10.5.3 Настройка DHCP сервера (DHCP Server Configuration)

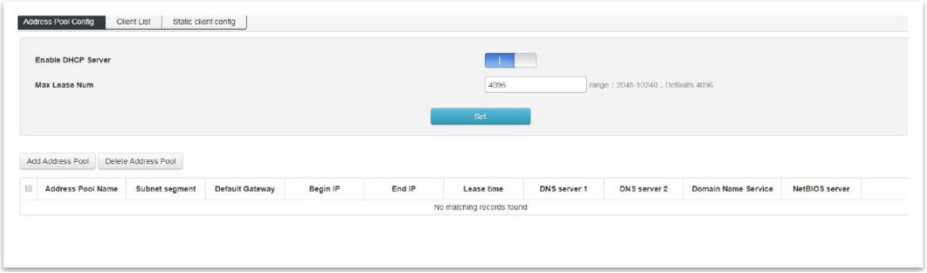
DHCP (Dynamic Host Configuration Protocol) — протокол, отвечающий за динамическую выдачу IP адресов устройствам сети. Упрощает работу системного администратора - специалисту не требуется каждый раз вручную назначать IP адреса новым устройствам.

Настройка DHCP сводится к заданию пула адресов, какие будут закрепляться за клиентскими устройствами.

Схемы раздачи IP адресов:

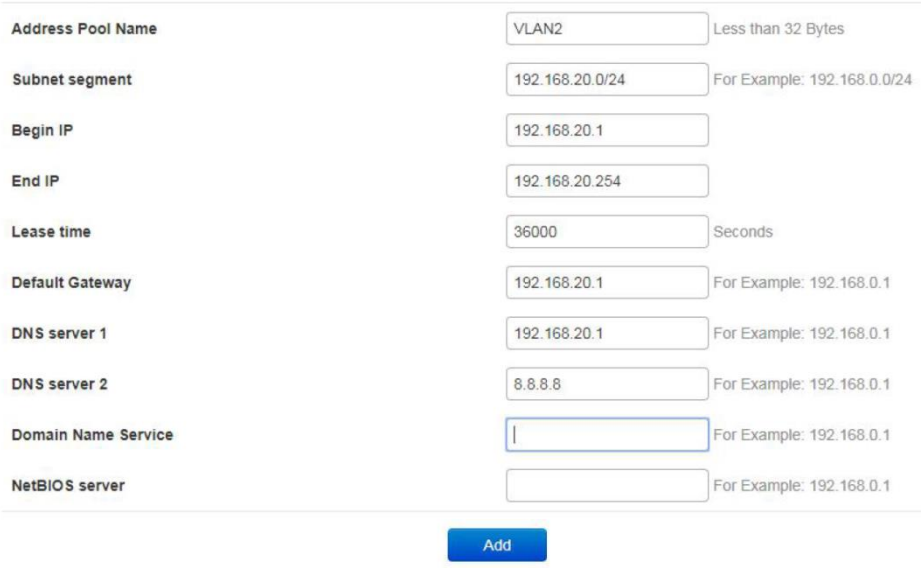
- ✓ динамическая - ПК получает IP-адрес на определенный срок. После этого сетевой адрес может быть закреплен за другим компьютером. Применяется на 95% всех серверов.
- ✓ автоматическая - разница с предыдущим вариантом раздачи только в том, что компьютер получает не динамический, а статический IP-адрес.
- ✓ ручная - системный администратор составляет таблицу соответствия MAC и IP-адресов. Применяется в сетях с высокими требованиями к безопасности.

10.5.3.1 Настройка пула IP адресов для DHCP (Address Pool Config)



- ✓ Enable DHCP Server – вкл/выкл автоматической раздачи IP адресов с помощью DHCP.
- ✓ Max Lease Num – максимальное количество назначаемых IP адресов. Диапазон 2048-10240. Значение по умолчанию – 4096.

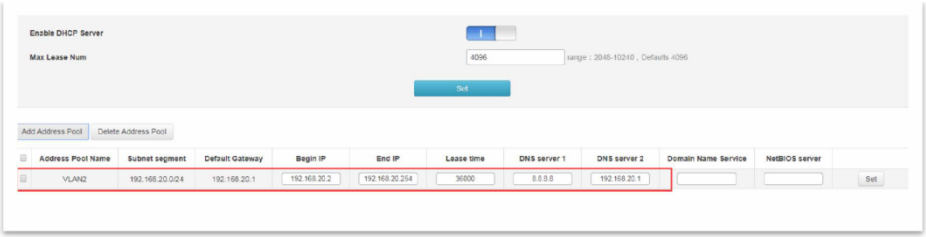
Чтобы задать пул IP адресов нажмите кнопку Add Address Pool



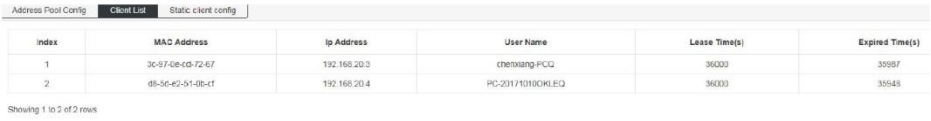
- Address Pool Name – имя создаваемого пула IP адресов.
- Subnet Segment – сегмент подсети.
- Begin IP – начальный IP адрес в пуле.
- End IP – конечный IP адрес в пуле.
- Lease Time – время аренды IP адресов в секундах.
- Default Gateway – IP адрес шлюза по умолчанию.
- DNS Server 1 – адрес DNS сервера.
- DNS Server 2 – адрес резервного DNS сервера.
- Domain Name Server – IP адрес.
- NetBIOS Server – сервер WINS.

Нажмите Add (добавить), чтобы завершить добавление пула IP адресов.

Итоговый результат будет виден в таблице:

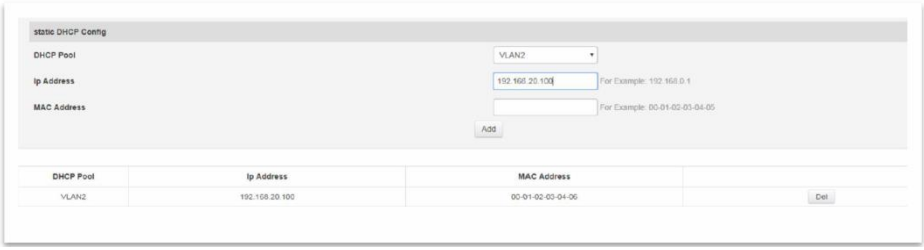


10.5.3.2 Список клиентов с назначенными IP адресами (Client List)



- ✓ MAC Address – MAC адрес клиента.
- ✓ IP Address – IP адрес клиента.
- ✓ User Name – Имя пользователя.
- ✓ Lease Time(s) – Время аренды выданного IP адреса в сек.
- ✓ Expired Times(s) – Оставшееся время аренды IP адреса в сек.

10.5.3.3 Назначение постоянного IP сервера клиентам (Static Client Configuration)

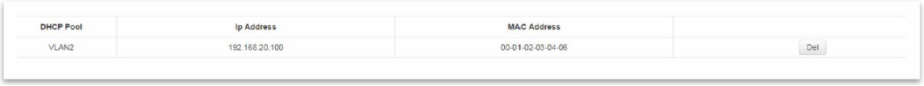


На данной странице WEB интерфейса находятся инструменты для присвоения постоянного IP адреса клиентам при работе DHCP сервера.

- ✓ DHCP Pool – выбор пула IP адресов из выпадающего списка.
- ✓ IP Address – IP адрес из списка, который будет назначен устройству с заданным MAC адресом.
- ✓ MAC Address – MAC адрес устройства, которому будет назначен постоянный IP адрес.

Нажмите Add (добавить), чтобы завершить процедуру.

Итоговый результат:



10.5.4 Настройка DHCP Relay (DHCP Relay)

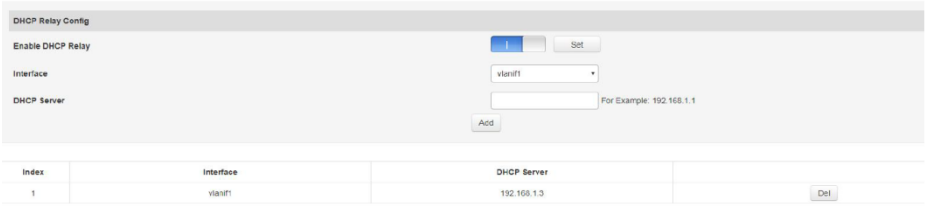
Функция DHCP Relay (стандарт RFC 3046) применяется для предоставления DHCP-серверу данных о полученном запросе. В частности, к этим данным можно отнести:

- ✓ Адрес DHCP-ретранслятора, с которого шёл запрос;
- ✓ Номер порта ретранслятора, через который поступил запрос;

При настройке, коммутатора в режиме DHCP Relay можно значительно повысить эффективность сети за счёт сокращения количества DHCP-серверов, которые при другой схеме понадобились бы для каждой подсети. В данном случае коммутатор сам переадресует DHCP-запрос от клиента к удалённому DHCP-серверу и добавит указанные выше данные.

В общем случае, назначение функции DHCP Relay – это привязка IP-адреса, выдаваемого DHCP-сервером, к порту коммутатора, к которому подключён клиент, либо к ретранслятору, с которого поступил запрос, что может помочь с систематизацией IP-адресов в локальной сети при использовании DHCP-сервера.

10.5.4.1 Активация функции DHCP Relay (Enable DHCP Relay)



- ✓ Enable DHCP Relay – вкл/выкл функции DHCP Relay
- ✓ Interface – выбор соответствующего интерфейса.
- ✓ DHCP Server – IP адрес DHCP сервера.

Нажмите Add, чтобы завершить настройку.

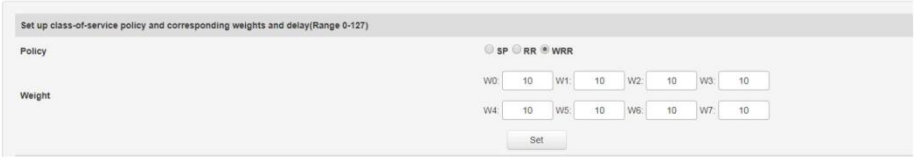
10.6 Дополнительные настройки (Advanced Settings)

10.6.1 Настройка QoS (QoS Configuration)

QoS (quality of service «качество обслуживания») – технология предоставления различным классам трафика различных приоритетов в обслуживании. То есть QoS — технология, которая может гарантировать пропуск в полном объеме определенному виду трафика в заданных технологических рамках.

Основная задача QoS — обеспечить гарантированную передачу определенных пакетов данных незаметно для пользователя. С помощью технологии QoS можно гарантировать, что у пользователей не возникнет проблем при скачивании файлов, видеозвонках, разговорах по IP-телефонии, просмотре каких-либо онлайн-документов в локальной или глобальной сети.

10.6.1.1 Глобальная настройка QoS (Global Configuration)



При полной загрузке сети, множество пакетов пытаются использовать ресурсы сети одновременно. Данная задача может быть решена путем распределения ресурсов с использованием очередей. Есть несколько механизмов для организации очередей:

- ✓ Strict Priority (SP) – строгая очередь на основе приоритетов. Этот механизм организации очереди относится ко второму уровню (Layer2).
- ✓ Weighted Fair Queue (WFQ) – взвешенные справедливые очереди. Этот механизм работает с IP заголовками пакетов и относится к третьему уровню (Layer3).
- ✓ Weighted Round Robin (WRR) – взвешенный цикличесткий алгоритм. Этот механизм организации очереди относится ко второму уровню (Layer2).

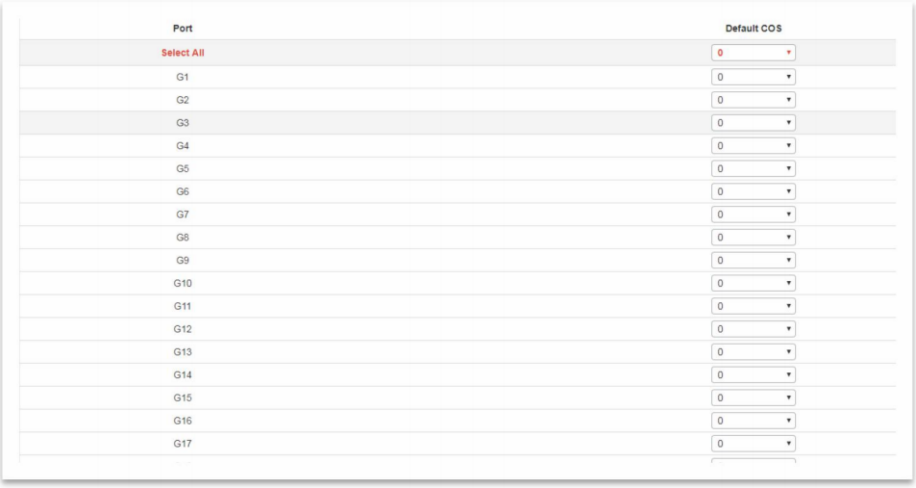
И др.

На данной странице WEB интерфейса находятся глобальные настройки для функции QoS.

- Policy – выбор механизма формирования очередей для выделения ресурсов сети трафику
  - SP – механизм создания строгих очередей на основе приоритетов;
  - RR – механизм создания очередей на основе выбора из множества очередей;
  - WRR – механизм создания взвешенных справедливых очередей.
- Weight – значение веса для 8 очередей. Если выбран механизм создания очередей RR или SP значение Weight не учитывается.

10.6.1.2 Настройка класса обслуживания для портов (Port Management)

CoS – или класс обслуживания применяется в составе QoS и также является механизмом для распределения ресурсов сети и ее пропускной способности для трафика.



На данной странице WEB интерфейса находятся настройки класса обслуживания для каждого выбранного порта.

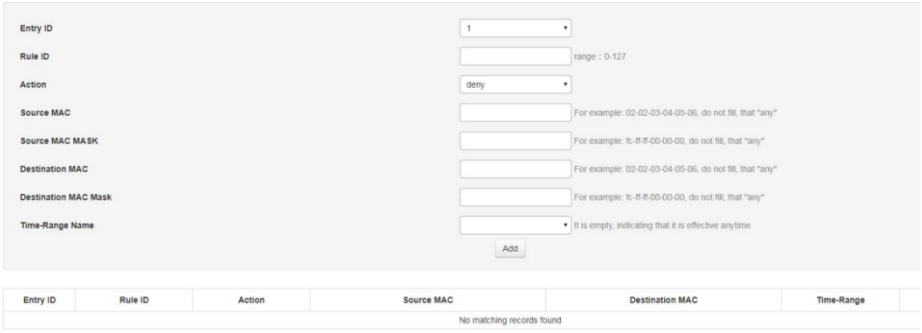
10.6.2 Настройки ACL (ACL Configuration)

С разрастанием сети и увеличением трафика, проходящего внутри сети, контроль безопасности и разделение пропускной способности становится необходимой частью сетевого управления. Фильтрация пакетов на основе ACL (Лист контроля доступа) позволяет эффективно бороться с неавторизованными пользователями в сети.

ACL может быть разделен на несколько групп:

- ✓ Basic IP ACL – правила, сформулированные на IP адресе источника отправки пакета. Диапазон идентификаторов ACL: 100-999.
- ✓ Advanced IP ACL – расширенные правила на основе информации 3 и 4 уровней (Layer3, 4) такой как, IP адрес источника отправки пакета, конечный IP адрес, тип протокола для заголовка, особенности протокола и тд. Диапазон идентификаторов ACL: 100-999.
- ✓ MAC ACL – правила на основе информации 2 уровня (Layer2) такой как MAC адрес источника отправки пакетов, конечный MAC адрес, приоритет VLAN и тд. Диапазон идентификаторов ACL: 1-32.

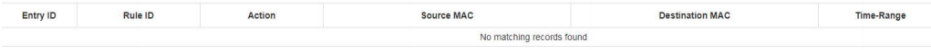
10.6.2.1 Настройки ACL на основе MAC адресов (MAC ACL Configuration)



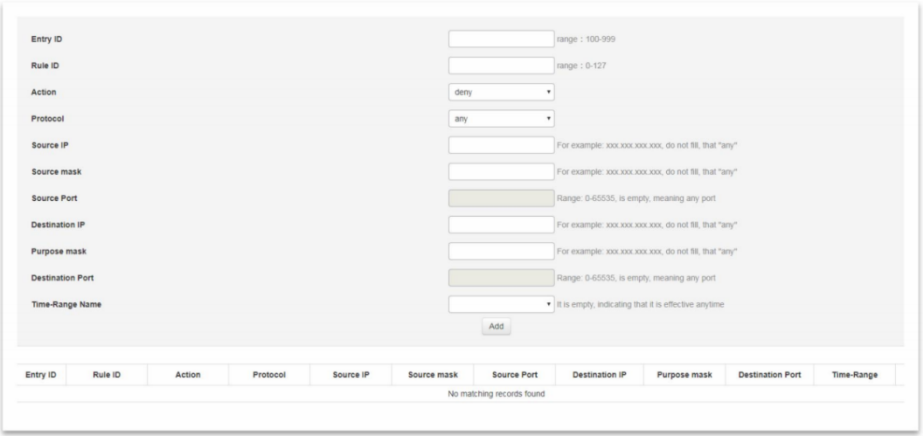
На данной странице WEB интерфейса коммутатора находятся настройки ACL на основе MAC адресов.

- Entry ID – идентификатор записи.
- Rule ID – идентификатор правила.
- Action – выбор действия:
  - Allow – разрешить передачу пакетов;
  - Deny – не передавать пакеты.
- Source MAC – MAC адрес источника отправки пакетов.
- Source MAC mask – маска MAC адреса источника отправки пакетов.
- Destination MAC – MAC адрес назначения.
- Destination MAC mask – маска для MAC адреса назначения.
- Time-Range Name – выбор временного диапазона для правила. По умолчанию правило применяется постоянно (unlimitted).

Нажмите кнопку Add (добавить), чтобы завершить настройку. Пример отобразиться в таблице ниже настроек.



10.6.2.2 Настройки ACL на основе IP адресов (IP ACL Configuration)



На данной странице WEB интерфейса коммутатора находятся настройки для ACL на основе IP адресов.

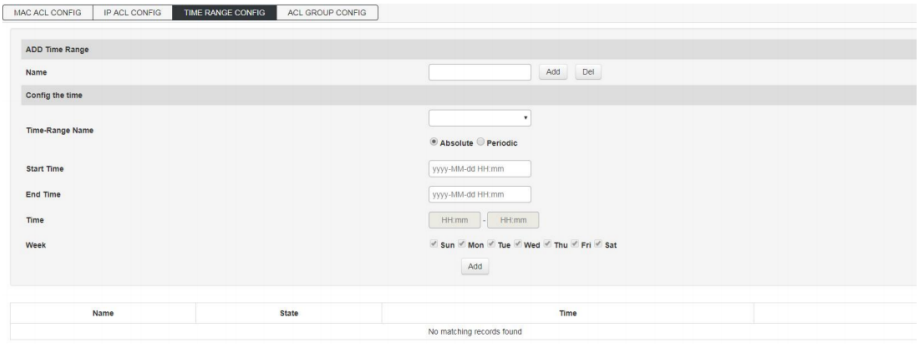
- Entry ID – идентификатор записи.
- Rule ID – идентификатор правила.
- Action – выбор действия:
  - Allow – разрешить передачу пакетов;
  - Deny – разрешить передачу пакетов.
- Protocol – информация протокола.
- Source IP – IP адрес источника отправки пакетов.
- Source IP mask – маска IP адреса отправки пакетов.
- Source Port – номер порта (для TCP/UDP протокола) источника отправки пакетов.
- Destination IP – IP адрес назначения.
- Purpose mask – маска IP адреса назначения.
- Destination port – номер порта (для TCP/UDP протокола) назначения.
- Time-Range Name – выбор временного диапазона для правила. По умолчанию правило применяется постоянно (unlimitted).

Нажмите кнопку Add (добавить), чтобы завершить настройку. Пример отобразиться в таблице ниже настроек.

Entry ID	Rule ID	Action	Protocol	Source IP	Source mask	Source Port	Destination IP	Purpose mask	Destination Port	Time-Range	
110	120	deny	icmp	192.168.20.5	192.168.20.55		any	any		5555	Del

10.6.2.3 Настройка времени действия применяемых правил ACL (Time–Range Configuration)

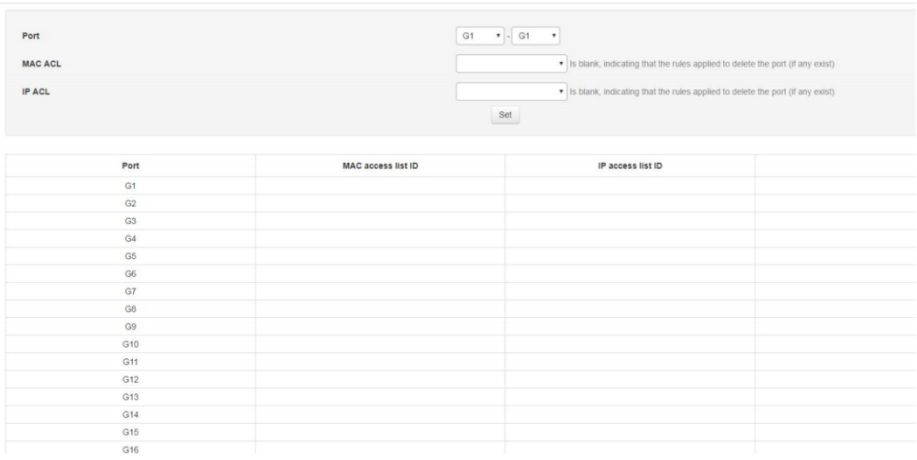
На данной странице WEB интерфейса коммутатора находятся настройки времени применения правил ACL. Такую фильтрацию трафика можно назвать временной фильтрацией, так как выбранные правила ACL будут применяться в выбранные промежутки времени (по расписанию).



- Name – общее имя для временного диапазона.
- Time-Range Name – выбор из выпадающего списка ранее созданных имен временных диапазонов. А также тип применения:
  - Absolute – постоянный диапазон времени применения правил;
  - Periodic – периодический диапазон времени применения правил ACL.
- Start time – время начала применения правил. Год, месяц, день, час, минута.
- End Time – время окончания применения правил. Год, месяц, день, час, минута.
- Time – время от и до для применения выбранных правил по расписанию. Час:минута начала – Час:минута окончания.
- Week – выбор дня недели, в который/которые будут применяться выбранные правила фильтрации трафика.

10.6.2.4 (ACL Group Configuration)

После того, как Вы создали список правил ACL его можно применять к любому порту коммутатора. На данной странице WEB интерфейса коммутатора находятся инструменты для привязки списка ACL к выбранному порту.



- ✓ Port – выбор порта, для которого нужно применить правило/правила ACL;
- ✓ MAC ACL – выбор из выпадающего списка ранее сформированных правил ACL на основе MAC адресов.
- ✓ IP ACL – выбор из выпадающего списка ранее сформированных правил ACL на основе IP адресов.

Для окончания настроек нажмите кнопку Set (Установить).

10.6.3 Настройка протокола управления SNMP (SNMP Configuration)

SNMP (англ. Simple Network Management Protocol — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP.

Управляемые протоколом SNMP сети состоят из трех ключевых компонентов:

- ✓ Управляемое устройство;
- ✓ Агент — программное обеспечение, запускаемое на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства;
- ✓ Система сетевого управления (Network Management System, NMS) — программное обеспечение, взаимодействующее с менеджерами для поддержки комплексной структуры данных, отражающей состояние сети

Так как адреса объектов устройств определяются в цифровом формате, их сложно запомнить. Для упрощения применяются базы управляющей информации (MIB). Базы MIB описывают структуру управляемых данных на подсистеме устройства; они используют иерархическое пространство имён, содержащее идентификаторы объектов (OID-ы). Каждый OID состоит из двух частей: текстового имени и SNMP адреса в цифровом виде

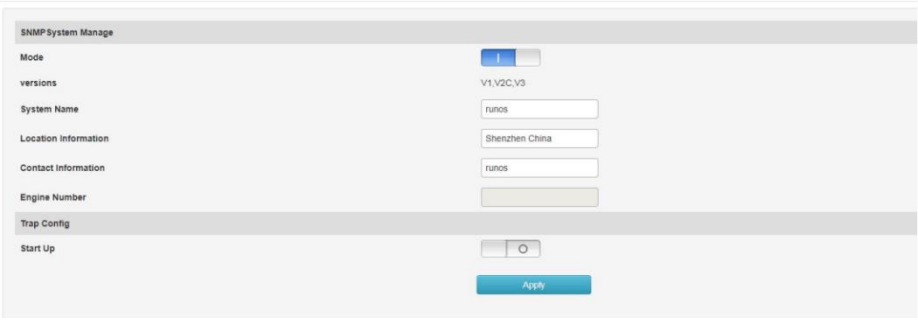
Коммутатор поддерживает SNMP 3 версий. Различия между ними заключаются в следующем:

- ✓ SNMPv1 – изначальная реализация протокола SNMP. SNMPv1 работает с такими протоколами, как UDP, IP, CLNS, DDP и IPX. SNMPv1 широко используется и де-факто является протоколом сетевого управления в Интернет-сообществе.
- ✓ SNMPv2c – пересматривает Версию 1 и включает в себя улучшения в области производительности, безопасности, конфиденциальности и связях между менеджерами. Протокол ввел GetBulkRequest, альтернативу итерационному применению

GetNextRequest для получения большого количества управляющих данных через один запрос.

- ✓ SNMPv3 – версия 3 является самой лучшей с точки зрения безопасности. Добавлена криптографическая защита, улучшена общая концепция и введена новая терминология. В отличие от SNMPv1 и v2, в SNMPv3 каждое сообщение содержит параметры безопасности, которые закодированы как строка октетов. Значение этих параметров зависит от используемой модели безопасности

10.6.3.1 Общие настройки протоколов SNMP (SNMP Configuration)



На данной странице WEB интерфейса коммутатора содержатся общие настройки протокола SNMP.

- Mode – вкл/выкл поддержки протокола SNMP.
- Versions – версии протокола SNMP.
- System Name – имя коммутатора.
- Location Information – дополнительная информация о местоположении коммутатора в сети.
- Contact Information – информация для связи.

- Start Up – вкл/выкл функции SNMP Trap – информация об ошибках, критических событиях и пр. отправляемая в систему управления сетью NMS.

Для завершения настройки нажмите кнопку Apply (Принять)

10.6.4 (RMON Configuration)

RMON – протокол мониторинга компьютерных сетей, основанный на протоколе SNMP.

В основе RMON, как и в основе SNMP, лежит сбор и анализ информации о характере данных, передаваемых по сети. Как и в SNMP, сбор информации осуществляется аппаратно-программными агентами, данные от которых поступают на компьютер, где установлено приложение управления сетью (NMS).

Отличие RMON от SNMP состоит, в первую очередь, в характере собираемой информации: если в SNMP эта информация характеризует только события, происходящие на том устройстве, где установлен агент, то RMON требует, чтобы получаемые данные характеризовали трафик между сетевыми устройствами.

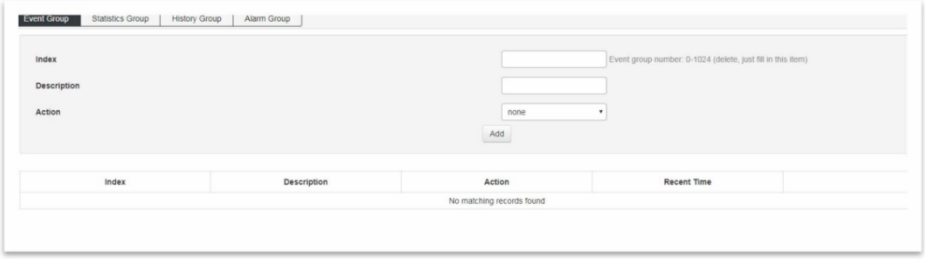
RMON поддерживает следующие группы событий (согласно RFC1757):

- ✓ Statistic group – первая группа «статистики». В ней собирается общая информация о трафике в данном сегменте и степени использования пропускной способности сети - количестве переданных байтов и сетевых пакетов, числе ошибок и коллизий и так далее.
- ✓ History group – Группа «предыстории» отвечает за сбор информации, определенной в группе статистики, в течение определенного времени (от одной секунды до одного часа). В результате оказывается возможным проанализировать текущие тенденции в работе сети и сравнить текущее состояние с базовым - это позволит выявить нежелательные явления в

работе сети раньше, чем они превратятся в серьезную проблему (например, пока сбои в работе оборудования не привели к его полному отказу).

- ✓ Events group – в группе «событий», определяется, когда следует отправлять аварийный сигнал приложению управления, когда - перехватывать пакеты, и вообще - как реагировать на те или иные события, происходящие в сети, например, на превышение заданных в группе alarms пороговых значений: следует ли ставить в известность приложение управления, или надо просто запротоколировать данное событие и продолжать работать. События могут и не быть связаны с передачей аварийных сигналов - например, направление пакета в буфер перехвата тоже представляет собой событие.
- ✓ Alarms group – группа «аварийных сигналов» позволяет пользователю определить ряд пороговых уровней (эти пороги могут относиться к самым разным вещам - любому параметру из группы статистики, амплитуде или скорости его изменения и многому другому), по превышении которых генерируется аварийный сигнал

10.6.4.1 Настройки группы событий (Event Group)

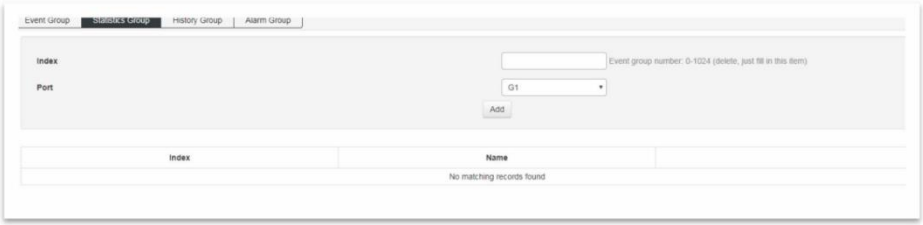


На данной странице WEB интерфейса коммутатора находятся настройки группы событий протокола RMON.

- Index – индекс группы событий от 0 до 1024
- Description – описание события.
- Action – действия при обнаружении события:
  - None – не предпринимать никаких действий;
  - Log – занести запись о событии в журнал событий коммутатора.
  - Trap – отправить сообщение об обнаружении события управляющему хосту;
  - Log&Trap – отправить сообщение об обнаружении события управляющему хосту и занести запись о событии в журнал событий коммутатора.

Нажмите кнопку Add (Добавить), чтобы закончить настройку.

10.6.4.2 Настройки группы статистики (Statistic Group)

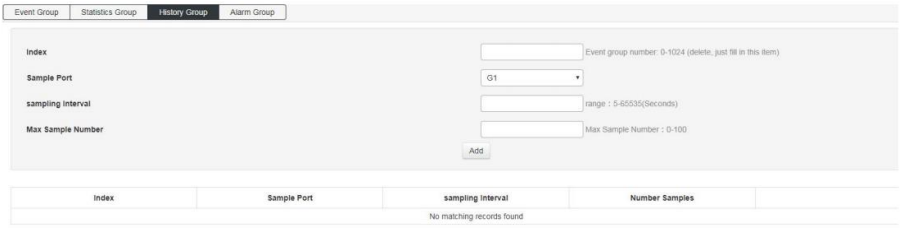


На данной странице WEB интерфейса коммутатора находятся настройки «статистики» протокола RMON.

- Index – индекс записи от 1 до 65535.
- Port – выбор порта коммутатора, который должен учитываться.

Нажмите кнопку Add (Добавить), чтобы закончить настройку.

10.6.4.3 Настройка группы предыстории (History Group)

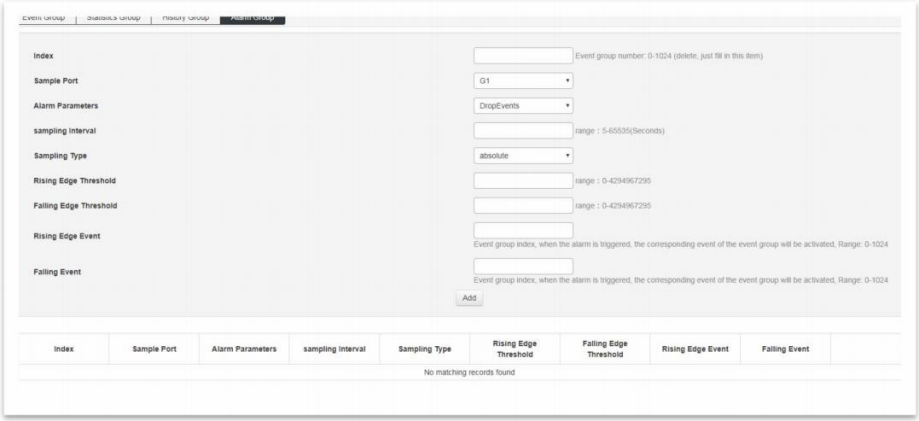


На данной странице WEB интерфейса коммутатора находятся настройки «предыстории» протокола RMON.

- Index – индекс записи о выборке.
- Sample Port – порт для выборки.
- Sampling Interval – интервал для выборки на порте. По умолчанию 1800 сек.
- Max Sample Number – поле для ввода максимального количества отображаемых записей выборки, которые могут быть сохранены в текущую запись с заданным ранее индексом. Диапазон значений 1 – 100. Значение по умолчанию – 50.

Нажмите кнопку Add (Добавить), чтобы закончить настройку.

10.6.4.4 Настройка группы тревожных сигналов (Alarm Group)



- Index – индекс записи об тревожном событии.
- Sample Port – порт, с которого регистрируются тревожные записи.
- Alarm Parameters – параметры тревожных событий.
- Sampling Interval – интервал обнаружения тревожного события. По умолчанию 1800 сек.
- Sampling Type – выбор метода обнаружения тревожного события:
  - Absolute – прямое сравнение результатов выборки с указанным порогом по окончанию интервала обнаружения;
  - Delta – сравнение результата вычитания текущего значения с указанным порогом.
- Rising Edge Threshold – поле для указания порога нарастания, после которого срабатывает механизм обнаружения тревожного события. Значение по умолчанию – 100.
- Falling Edge Threshold – поле для указания порога спада, после которого срабатывает механизм обнаружения тревожного события. Значение по умолчанию – 100.
- Rising Edge Event – идентификатор тревожного события, после превышения порога Rising Edge Threshold
- Falling Event – идентификатор тревожного события, после падения ниже порога Falling Edge Threshold.

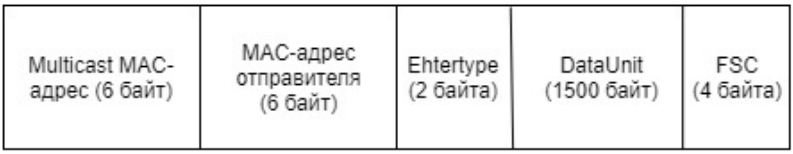
Нажмите кнопку Add (Добавить), чтобы закончить настройку.

10.6.5 Настройка протокола LLDP (LLDP Configuration)

LLDP – протокол канального уровня (Layer2), позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

Собранные данные запрашиваются с помощью протокола SNMP (протокол сетевого управления). Для работы LLDP необходимо прямое подключение между устройствами (например, сеть, построенная на коммутаторе).

LLDP вставляет свое сообщение в Ethernet-пакет и передает его через аплинк. Коммутатор, получивший сообщение идентифицирует его по определенному mac-адресу получателя (уникальному для протокола) и не передает дальше.



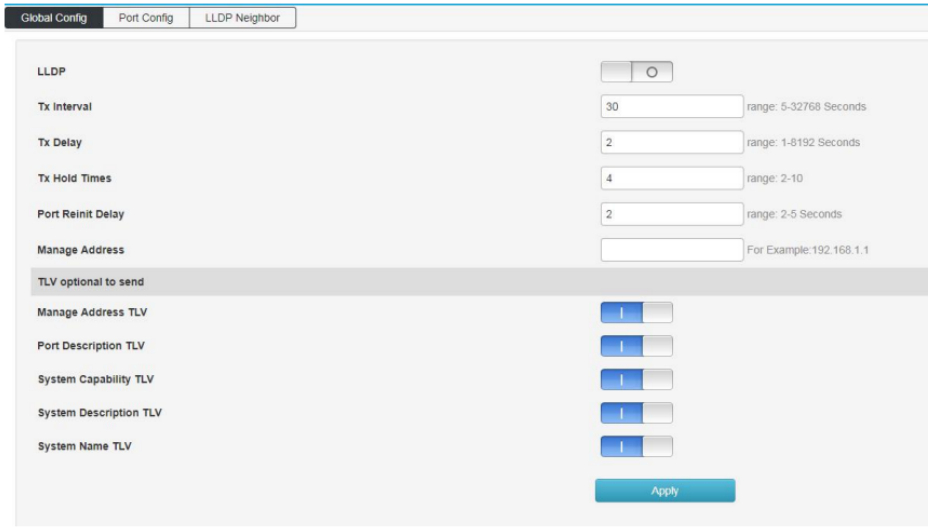
Вся основная информация, передаваемая из сообщений LLDP, содержится в DataUnit (LLDPDU) в виде TLV.

TLV, в свою очередь, является методом записи коротких данных в телекоммуникационных протоколах.

Тип TLV	Имя TLV	Описание
0	End of LLDPDU	Определяет окончание блока LLDPDU. Любая информация за пределами этого значения не будет обрабатываться.
1	Chassis ID	Определяет идентификатор шасси для подключенного устройства.
2	Port ID	Определяет идентификатор информации о порте, с которого отправлен пакет.
3	Time To Live (TTL)	Время жизни информации о устройствах-соседях
4	Port Description	Описание порта устройств–соседей

Тип TLV	Имя TLV	Описание
5	System Name	Системное имя, используемое для уведомления устройств-соседей
6	System Specification	Описание системной информации для устройств-соседей. В том числе аппаратная версия и версия прошивки.
7	System Capability	Информация для устройств–соседей о совместимости.
8	Management address	Уведомление устройств–соседей об адресе, с которого можно управлять устройством.

10.6.5.1 Глобальные настройки LLDP (Global Config)



На данной странице WEB интерфейса коммутатора находятся глобальные настройки протокола LLDP.

- ✓ LLDP – вкл/выкл протокола LLDP.
- ✓ Tx Interval – интервал отправки LLDP пакетов от 5 до 32768 сек. Значение по умолчанию – 30 сек.
- ✓ Tx Delay – Задержка перед отправкой пакета LLDP. От 2 до 10 сек. Значение по умолчанию – 4 сек.
- ✓ Tx Hold Times – Время жизни (TTL) для пакетов LLDP. От 2 до 10 сек. Значение по умолчанию – 4 сек.
- ✓ Port Reint Delay – Время для реинициализации порта. От 2 до 5 сек. Значение по умолчанию 2 сек.
- ✓ Manage Address – IP адрес, по которому управляется коммутатор и который должны знать устройства–соседи.
- ✓ Manage Address TLV – передавать/не передавать информацию о адресе управления коммутатором.
- ✓ Port Description TLV – передавать/не передавать информацию с описанием порта.
- ✓ System Capability TLV – передавать/не передавать информацию о совместимости.
- ✓ System Description TLV – передавать/не передавать описание системы, включая аппаратную версию и версию прошивки.
- ✓ System Name – передавать/не передавать системное имя (имя коммутатора).

Нажмите кнопку Apply (Принять), чтобы закончить настройку.

10.6.5.2 Настройка приема/передачи LLDP пакетов на портах (Port Config)

На данной странице WEB интерфейса есть возможность вкл/выкл отдельно прием и передачу LLDP пакетов на выбранных портах.

10.6.5.3 Информация полученная от устройств-соседей по LLDP (LLDP Neighbour)

На данной странице WEB интерфейса коммутатора находится таблица с информацией, полученной от устройств-соседей в локальной сети с помощью протокола LLDP. Информация предоставляется только для чтения.

10.6.6 Настройка протокола синхронизации времени NTP (NTP Configuration)

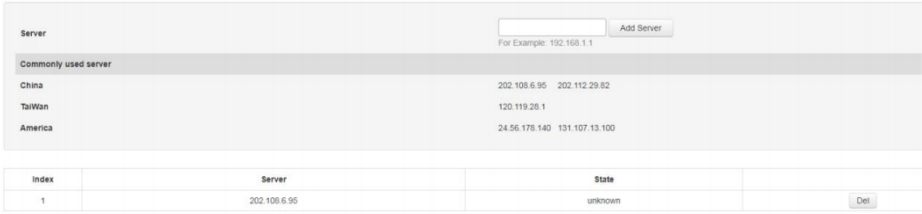
NTP (англ. Network Time Protocol — протокол сетевого времени) — сетевой протокол для синхронизации внутренних часов коммутатора с часами ПК, подключенного к коммутатору.

10.6.6.1 Глобальные настройки NTP (NTP Global Config)

На данной странице WEB интерфейса коммутатора находятся глобальные настройки NTP.

- ✓ Mode – вкл/выкл протокола синхронизации времени NTP.
- ✓ Time zone setting – выбор часового пояса
- ✓ Time gap – интервал синхронизации времени. Значение по умолчанию 300 сек.

10.6.6.2 Настройки сервера NTP (NTP Server Config)



На данной странице WEB интерфейса коммутатора находятся настройки синхронизации часов коммутатора с часами на удаленном сервере с помощью протокола NTP.

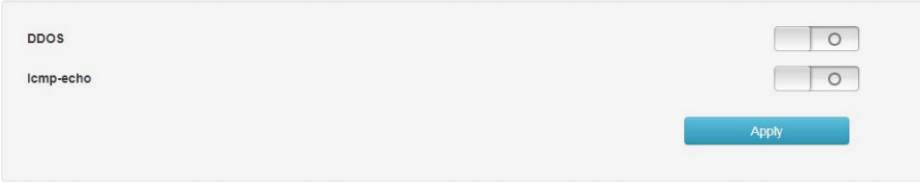
- ✓ Server – поле для ввода IP адреса сервера NTP. Например: 24.56.178.140 – для Америки.

Нажмите кнопку add Server, чтобы добавить новый сервер NTP в таблицу. Удалить сервер из таблицы серверов можно с помощью кнопки Del.

10.6.7 Механизм защиты от сетевых атак (Anti-attack)

DDoS – Distributed Denial of Service или распределенные сетевые атаки типа «отказ в обслуживании». Работают по принципу переполнения буфера коммутатора с помощью большого количества запросов на обслуживание.

ICMP – атака, нацеленная на уязвимость протокола ICMP, которая позволяет вызывать «отказ в обслуживании». Коммутатор позволяет блокировать атаки по принципу эхо запросов.



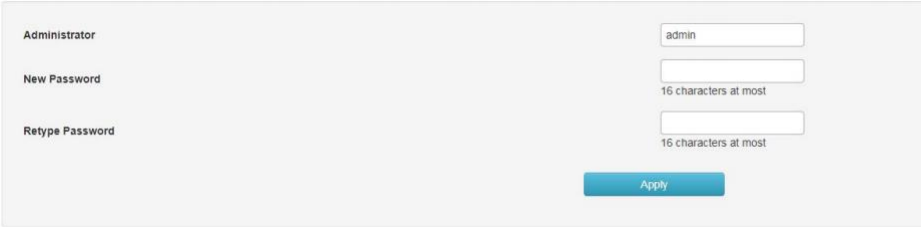
Данная страница WEB интерфейса коммутатора содержит в себе инструменты для предотвращения сетевых атак типа DDOS и ICMP-Echo.

- ✓ DDOS – вкл/выкл механизм защиты от атак типа DDOS
- ✓ ICMP-ECHO – вкл/выкл механизма защиты от атак с помощью ICMP эхо-запросов.

Чтобы завершить настройку, нажмите кнопку Apply (Принять).

10.7 Настройки системы (System Managment)

10.7.1 Настройки пользователя (User Settings)

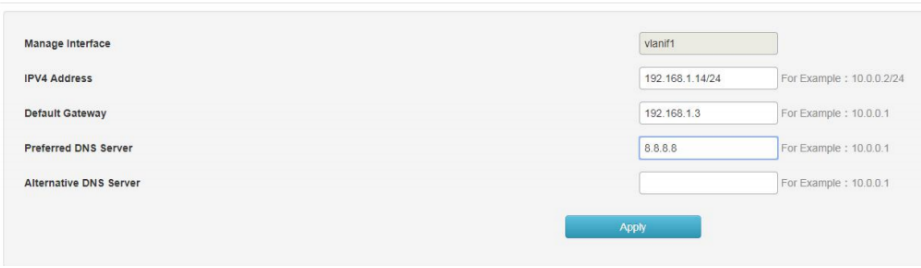


На данной странице WEB интерфейса коммутатора находятся настройки пользователя, с правами администратора.

- ✓ Administrator – логин (имя) администратора управления коммутатором;
- ✓ New Password – новый пароль;
- ✓ Retype Password – поле для повторного ввода пароля.

Чтобы завершить настройку, нажмите кнопку Apply (Принять).

10.7.2 Сетевые настройки (Network Settings)

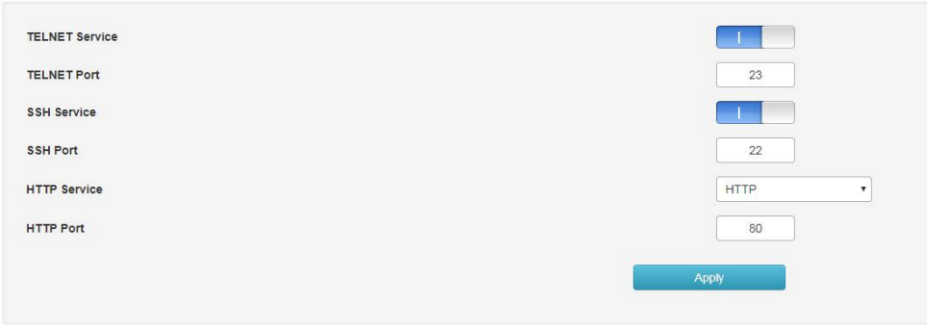


На данной странице WEB интерфейса коммутатора находятся настройки IP адреса управления коммутатором, шлюза и DNS сервера.

- ✓ IPV4 Address – поле для ввода IP адреса, который будет использоваться для управления коммутатором.
- ✓ Default Gateway – IP адрес шлюза по умолчанию. Указывается, в случае подключения коммутатора к интернету.
- ✓ Preferred DNS Server – IP адрес предпочтительного DNS сервера.
- ✓ Alternative DNS Server – IP адрес альтернативного (резервного) DNS сервера.

Чтобы завершить настройку, нажмите кнопку Apply (Принять).

10.7.3 Настройка способов управления коммутатором (Service Configuration)



На данной странице WEB интерфейса коммутатора находятся настройки для активации различных способов управления коммутатором.

- ✓ TELNET Service – вкл/выкл управления коммутатором через TELNET.
- ✓ TELNET Port – номер порта для управления коммутатором через TELNET.
- ✓ SSH Service – вкл/выкл управления коммутатором через SSH.
- ✓ SSH Port – номер порта для управления коммутатором через SSH.
- ✓ HTTP Service – вкл/выкл управления коммутатором через HTTP.

- ✓ HTTP Port – номер порта для управления коммутатором через HTTP (WEB)

Чтобы завершить настройку, нажмите кнопку Apply (Принять).

10.7.3.1 Управление через TELNET (TELNET Service)

Формат команды: Telnet *192.168.254.1 xx*
Где:

- ✓ 192.168.254.1 это текущий IP адрес коммутатора;
- ✓ 23 – порт из поля «TELNET Port».

10.7.3.2 Управление через SSH (SSH Service)

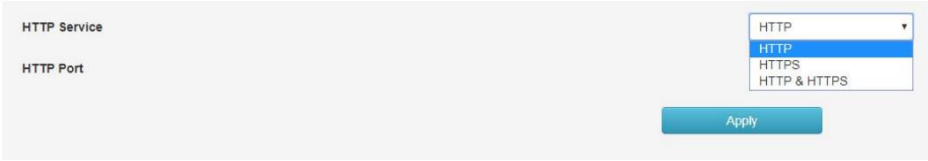
SSH – сетевой протокол прикладного уровня, позволяющий производить удалённое управление коммутатором.

Схож по функциональности с протоколами Telnet, но, в отличие от него, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования.

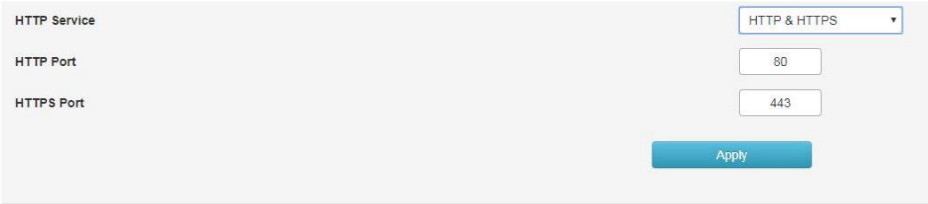
По умолчанию коммутатор использую протокол SSHv2 и порт 22.

10.7.3.3 Управление через HTTP (HTTP Service)

Данный способ управления коммутатором позволяет выбирать из 3 доступных WEB протоколов и их комбинаций:



- ✓ HTTP – использовать только HTTP;
- ✓ HTTPS – использовать только HTTPS;
- ✓ HTTP&HTTPS – поддерживается и HTTP и HTTPS.



- ✓ Порт HTTP по умолчанию – 80.
- ✓ Порт HTTPS по умолчанию – 443.

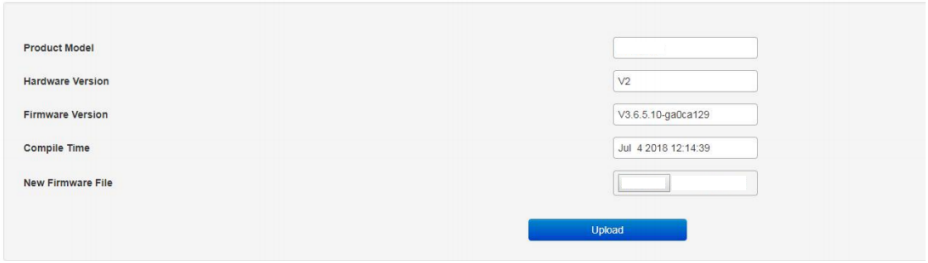
Пример подключения через WEB: *https://192.168.254.1*

10.7.4 Сброс к заводским настройкам (Configuration Management)

На данной странице WEB интерфейса коммутатора находится кнопка, с помощью которой можно сбросить настройки коммутатора к заводским значениям.

При этом будет установлен IP адрес управления 192.168.254.1. Рекомендуется производить данную процедуру сброса, только убедившись, что необходимая конфигурация коммутатора выгружена в файл на USB флеш накопитель.

10.7.5 Обновление прошивки (Firmware Upgrade)



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

Порядок обновления следующий:

1) Выберите файл с прошивкой на ПК с помощью кнопки в поле New Fimware File (Новый файл с прошивкой)
2) Нажмите кнопку UPLOAD и дождитесь окончанию загрузки файла. По окончанию загрузки коммутатор будет перезагружен.
3) В поле Firmware Version (Версия прошивки) – будет отражена версия текущей, обновленной прошивки.

Внимание!

- ✓ Не прерывайте процедуру обновления прошивки
- ✓ Не перезагружайте коммутатор самостоятельно во время обновления прошивки во избежание дальнейших технических проблем с устройством.
- ✓ Свяжитесь с авторизованным сервисным центром, если были перебои с подачей электропитания во время обновления прошивки и коммутатор перестал работать корректно.

10.7.6 Диагностические тесты (Diagnostic Test)

В коммутаторе предусмотрено несколько диагностических тестов:

- ✓ Ping Detection – тест с помощью запросов с использованием протокола ICMP (команда PING);
- ✓ Tracert Detection – тест для определения маршрута, по которому проходят пакеты до заданного узла;
- ✓ Network Cable Detection – тест кабельного соединения (целостность пар в кабеле, длина каждой из пар в кабеле).

10.7.6.1 Тест с помощью Ping (Ping Detection)

С помощью команды Ping администратор сети может проверить целостность подключения, активность сетевого устройства и тд.

Тест с помощью Ping состоит из 3 этапов:

1) Отправка ICMP запроса на интересующее сетевое устройство;
2) Если сеть исправна (исправно устройство), вернется ответ от устройства в виде статистики;
3) Если сеть неисправна, то ответ вернется с информацией о том, что устройство недостижимо или превышен таймаут запроса.

- ✓ IP Address – поле для ввода IP адреса интересующего устройства в сети.

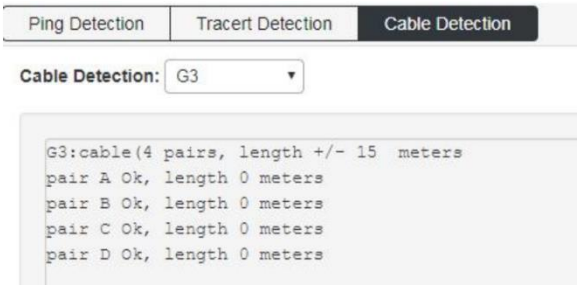
Нажмите кнопку PING, чтобы приступить к тестированию.

10.7.6.2 Тест с помощью Tracert (Tracert Detection)

На данной странице WEB интерфейса коммутатора содержится инструмент для тестирования Tracert – позволяющий проверить маршрут прохождения пакетов до заданного узла.

Результаты трассировки отображают, какое количество промежуточных устройств L3 уровня (коммутаторов, маршрутизаторов и тд) находится между коммутатором и интересующим хостом. При этом выводится информация о задержке прохождения пакетов и IP адреса промежуточных устройств.

10.7.6.3 Тест кабельного соединения (Cable Detection)



На данной странице WEB интерфейса находится инструмент, который может помочь сетевому администратору с диагностикой кабельного соединения на выбранном порте.

- ✓ Cable Detection – выбор порта, соединение с которым требуется проверить.

Результаты выводят количество пар в кабеле, примерную длину кабеля, а также состояние каждой пары в кабеле и их длину.

Перед повторным тестированием необходимо подождать не менее 5 сек, чтобы исключить ошибки при диагностике.

10.7.7 Перезагрузка коммутатора (Restart the system)

На данной странице WEB интерфейса коммутатора находится кнопка для принудительной перезагрузки устройства. Все несохраненные настройки будут сброшены к предыдущим значениям.

Для перезагрузки нажмите кнопку Restart

11. Технические характеристики**

Модель	**SW-32G4X-1L**
Общее кол-во портов	36
Кол-во портов Combo GE (RJ45+SFP)	8 (8xRJ45 + 8xSFP)
Кол-во портов SFP (не Combo порты)	16xGE SFP (1 Гбит/с) 4x10G «SFP+» (10 Гбит/с)
Топологии подключения	звезда каскад кольцо
Буфер пакетов	1,5 МБ
Таблица MAC-адресов	16 К
Пропускная способность коммутационной матрицы (Switching fabric)	128 Гбит/с
Скорость обслуживания пакетов (Forwarding rate)	96 MPPS
Поддержка jumbo frame	10 КБ
Размер flash памяти	16 МБ
Стандарты и протоколы	• IEEE 802.3 – 10Base-T • IEEE 802.3u – 100Base-TX • IEEE 802.3ab – 1000Base-T • IEEE 802.3z – 1000 Base-X • IEEE 802.3ae – 10G Base-SR/LR • 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 • G.8032 – ERPS Ethernet loop protection switch

Модель	**SW-32G4X-1L**
Функциии уровня L2	• IEEE 802.1D (STP) • IEEE 802.1w (RSTP) • IEEE 802.1s (MSTP) • VLAN / VLAN Group, Voice VLAN • Link Aggregation IEEE 802.3ad with LACP • IGMP Snooping v1/v2/v3 • DHCP Snooping • IGMP Static Multicast Addresses • Storm Control
Функции уровня L3	• ARP Configuration • Routing Configuration • DHCP server • DHCP Relay • Support RIP V1/V2 protocols • Support OSPF V1/V2 protocols
Качество обслуживания (QoS)	8 очередей / порт
Безопасность	• Management System User Name/Password Protection • IEEE 802.1x Port-based Access Control • HTTP & SSL (Secure Web) • SSH v1/v2(Secured Telnet Session)
Управление	• Управление через Web-интерфейс • CLI • Telnet • SNMP
Индикаторы	✓ PWR 1/2 – питание ✓ SYS – состояние системы ✓ Master – режим Master при стекировании
Грозозащита	6kV, 8/20us Для портов RJ-45
Питание	AC 90-253V с резервированием
Энергопотребление	<10 Вт
Охлаждение	Активное (вентиляторы в корпусе) Front-to-Back вентиляция
Размеры (ШхВхГ) (мм)	440x44x320
Способ монтажа	в 19” стойку
Рабочая температура	-10...+50 °C

Модель	**SW-32G4X-1L**
Дополнительно	✓ Порт OOB – управление раздельно с каналом передачи данных. ✓ Порт Console – консольный порт для управления через RJ45-RS-232 интерфейс с помощью CLI команд. ✓ Порт Micro USB (дублер порта Console) – консольный порт для управления через USB с помощью CLI команд. ✓ Порт USB – порт для загрузки/сохранения текущей конфигурации. ✓ Стекирование до 8 устройств.

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

12. Гарантия

Гарантия на все оборудование OSNOVO – 60 месяцев с даты продажи.

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

Составил: Елагин С.А.