

OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Управляемый (L3) коммутатор с 10G портами SW-24G4X-1L на 28 портов (24xGE RJ-45 с PoE + 4x10G «SFP+»)

SW-24G4X-1L



Прежде чем приступать к эксплуатации изделия,
внимательно прочтите настояще руководство

www.osnovo.ru

Содержание

1. Назначение	7
2. Комплектация	8
3. Особенности оборудования	8
4. Внешний вид и описание элементов	8
4.1 Внешний вид и описание разъемов и индикаторов	8
5. Подключение	12
5.1 Схема подключения	12
5.2 Подключение питания	13
6. Проверка работоспособности	14
7. Подготовка перед управлением коммутатором через WEB	15
8. Подготовка перед управлением коммутатором через порт CONSOLE	18
9. Подготовка перед управлением коммутатором через Telnet/SSH	20
10. WEB интерфейс управления коммутатором	22
10.1 Общий вид WEB интерфейса	22
10.2 Системная информация (System Info)	23
10.2.1 Общая информация о системе (Global Info)	23
10.2.2 Накопленная статистика работы (Statistic Info)	24
10.2.3 Журналы событий (Log Info)	25
10.2.3.1 Список журналов (Log List)	26
10.2.3.2 Экспорт журналов событий (Log Save)	27
10.3 Управление портами (Port Management)	28
10.3.1 Настройки портов (Port Configuration)	28
10.3.2 Изоляция портов (Port Isolation)	29
10.3.3 Зеркалирование портов (Port mirroring)	30
10.3.4 Ограничение скорости портов (Port Speed Limit)	31
10.3.5 Защита от Net Storm и Broadcast Storm (Storm Control)	32

10.3.6 Функция энергосбережения для портов (Port Energy Saving)	33
10.4 Управление питанием PoE (PoE Management)	34
10.4.1 Управление питанием PoE для портов (Port PoE Config)	34
10.4.2 Информация об оборудовании (Equipment Information)	35
10.4.3 Настройка подачи PoE по расписанию (Timing Supply Config)	35
10.4.3.1 Установка периода подачи PoE (Time Range Config)	35
10.4.3.2 Применение периода подачи PoE для портов (Timing Supply Config)	36
10.4.3.3 Функция PoE AI Config (PoE AI Config)	37
10.5 Управление настройками 2 уровня (Layer 2 Management)	38
10.5.1 Таблица MAC адресов (MAC Address Table)	38
10.5.2 VLAN (VLAN Config)	40
10.5.2.1 VLAN Static	41
10.5.2.2 Настройка VLAN (VLAN Config)	42
10.5.2.3 Voice VLAN Configuration	44
10.5.2.4 Настройка VLAN на базе MAC адресов (MAC VLAN Configuration)	45
10.5.2.5 Настройка VLAN на базе IP адресов (IP VLAN Configuration)	46
10.5.3 Агрегирование каналов (Link Aggregation)	47
10.5.3.1 Настройки постоянной агрегации (Static Aggregation Config)	48
10.5.3.2 Настройки динамической агрегации (Dynamic Aggregation Config)	49
10.5.3.3 Информация о группах агрегации (Link Aggregation Information)	50
10.5.4 Настройка протокола STP (STP Configuration)	51
10.5.4.1 Глобальная настройка (Global Configuration)	52
10.5.4.2 Настройка instance (Instance Config)	53
10.5.4.3 Настройка instance для портов (Interface Instance Config) ...	54

10.5.4.4 Настройка портов для STP (Interface Config)	56
10.5.5 Защита от петель (Loop protection)	57
10.5.5.1 Глобальные настройки (Global Config).....	57
10.5.5.2 Настройка портов для Loop Protection (Port Config).....	58
10.5.6 Функция DHCP Snooping	58
10.5.6.1 Глобальные настройки DHCP Snooping (Global Config)	59
10.5.6.2 Постоянная привязка (Static Binding)	59
10.5.6.3 Управление портами (Port Config)	60
10.5.7 Функция IGMP Snooping	61
10.5.7.1 Глобальные настройки IGMP snooping (IGMP Snooping)	61
10.5.7.2 Настройка IGMP Snooping для VLAN (IGMP Snooping VLAN Config)	62
10.5.7.3 Постоянный мультикастинг (Static Multicast)	63
10.5.8 Настройка 802.1x (802.1x Configuration).....	64
10.5.8.1 Глобальные настройки 802.1x (Global Config)	64
10.5.8.2 Настройки сервера RADIUS (RADIUS Server Config)	66
10.5.8.3 Аутентификация на основе портов (Port-based Authentiction)	67
10.6 Управление настройками 3 уровня (Layer3 Management).....	68
10.6.1 Настройка интерфейсов (Interface Setting)	68
10.6.2 Настройка маршрутизации (Routing Configuration)	69
10.6.2.1 Просмотр маршрутов (View the routing)	69
10.6.2.2 Постоянные маршруты, заданные вручную (Static Routing)	70
10.6.2.3 Настройка протокола ARP (The ARP configuration).....	71
10.6.3.1 Настройка пула IP адресов для DHCP (Address Pool Config)	73
10.6.3.2 Список клиентов с назначенными IP адресами (Client List) .	74
10.6.3.3 Назначение постоянного IP сервера клиентам (Static Client Configuration)	75

10.6.4 Настройка DHCP Relay (DHCP Relay)	76
10.6.4.1 Активация функции DHCP Relay (Enable DHCP Relay)	76
10.7 Дополнительные настройки (Advanced Settings)	77
10.7.1 Настройка QoS (QoS Configuration)	77
10.7.1.1 Глобальная настройка QoS (Global Configuration)	77
10.7.1.2 Настройка класса обслуживания для портов (Port Management)	78
10.7.2 Настройки ACL (ACL Configuration)	79
10.7.2.1 Настройки ACL на основе MAC адресов (MAC ACL Configuration)	79
10.7.2.2 Настройки ACL на основе IP адресов (IP ACL Configuration)	80
10.7.2.3 Настройка времени действия применяемых правил ACL (Time–Range Configuration)	82
10.7.2.4 (ACL Group Configuration)	83
10.7.3 Настройка протокола управления SNMP (SNMP Configuration)	84
10.7.3.1 Общие настройки протоколов SNMP (SNMP Configuration)	85
10.7.4 (RMON Configuration)	86
10.7.4.1 Настройки группы событий (Event Group)	87
10.7.4.2 Настройки группы статистики (Statistic Group)	88
10.7.4.3 Настройка группы предыстории (History Group)	89
10.7.4.4 Настройка группы тревожных сигналов (Alarm Group)	89
10.7.5 Настройка протокола LLDP (LLDP Configuration)	91
10.7.5.1 Глобальные настройки LLDP (Global Config)	92
10.7.5.2 Настройка приема/передачи LLDP пакетов на портах (Port Config)	94
10.7.5.3 Информация полученная от устройств-соседей по LLDP (LLDP Neighbour)	94

10.7.6 Настройка протокола синхронизации времени NTP (NTP Configuration)	95
10.7.6.1 Глобальные настройки NTP (NTP Global Config)	95
10.7.6.2 Настройки сервера NTP (NTP Server Config)	95
10.7.7 Механизм защиты от сетевых атак (Anti-attack).....	96
10.8 Настройки системы (System Management)	97
10.8.1 Настройки пользователя (User Settings)	97
10.8.2 Сетевые настройки (Network Settings)	97
10.8.3 Настройка способов управления коммутатором (Service Configuration)	98
10.8.3.1 Управление через TELNET (TELNET Service).....	99
10.8.3.2 Управление через SSH (SSH Service).....	99
10.8.3.3 Управление через HTTP (HTTP Service).....	99
10.8.4 Сброс к заводским настройкам (Configuration Management).100	100
10.8.5 Обновление прошивки (Firmware Upgrade)	100
10.8.6 Диагностические тесты (Diagnostic Test)	101
10.8.6.1 Тест с помощью Ping (Ping Detection)	102
10.8.6.2 Тест с помощью Tracert (Tracert Detection).....	102
10.8.6.3 Тест кабельного соединения (Cable Detection)	103
10.8.7 Перезагрузка коммутатора (Restart the system)	103
11. Технические характеристики*	104
12. Гарантия	106

1. Назначение

Управляемый (L3) коммутатор с 10G портами SW-24G4X-1L на 28 портов (24xGE RJ-45 с PoE + 4x10G «SFP+») предназначен для объединения сетевых устройств, передачи данных между ними.

24 основных порта коммутатора поддерживают PoE стандартов IEEE 802.3 af/at с максимальной мощностью на порт – 30 Вт. Суммарный PoE бюджет коммутатора на 24 порта – 400 Вт (по 16.6 Вт на порт).

4 «SFP+» порта работают на скорости 10G и способны без задержек передавать весь объем трафика на сервер или другое устройство.

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 и тд.)

Кроме того коммутатор поддерживают работу в кольцевой топологии (Ring) благодаря поддержке протоколов IEEE 802.1s (MSTP) и IEEE 802.1w (RSTP).

С помощью кнопок на передней панели в коммутаторе предусмотрена быстрая активация функций:

- ✓ QOS – вкл/выкл приоритезации видеотрафика;
- ✓ Ai POE – автоматическое определение «зависших» PoE устройств;
- ✓ CCTV – увеличение расстояния передачи данных до 250м на портах 1-8 (скорость 10 Мбит/с без PoE);
- ✓ VLAN – изоляция портов 1-24 друг от друга (могут обмениваться данными только с SFP+ портами) для защиты от сетевого шторма.

Коммутатор SW-24G4X-1L может быть использован на предприятиях малого и среднего бизнеса:

- для подключения к сетям операторов связи и к сетям более крупным предприятий (интерфейсы 10G);
- в высокопроизводительных системах IP видеонаблюдения (в том числе с питанием IP камер по PoE);
- для организации VoIP телефонии (в том числе – с питанием по PoE конечных устройств).

2. Комплектация

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

3. Особенности оборудования

- ✓ Высокопроизводительные Uplink-порты 10G (4 x 10G «SFP+»);
- ✓ Значительный PoE бюджет – 400Вт;
- ✓ Поддержка Ai PoE – автоматическое определение «зависших» PoE устройств;
- ✓ Возможность передачи данных на 250м при 10 Мбит/с (1-8 порты);
- ✓ Управление через WEB интерфейс;
- ✓ Поддержка функций L2 (VLAN, QOS, LACP, LLDP, IGMP snooping) и L3 (ARP, DHCP, Routing RIP V1/V2);
- ✓ Поддержка кольцевой топологии подключения (STP, RSTP, MSTP).

4. Внешний вид и описание элементов

4.1 Внешний вид и описание разъемов и индикаторов



Рис. 1 Коммутатор SW-24G4X-1L, внешний вид

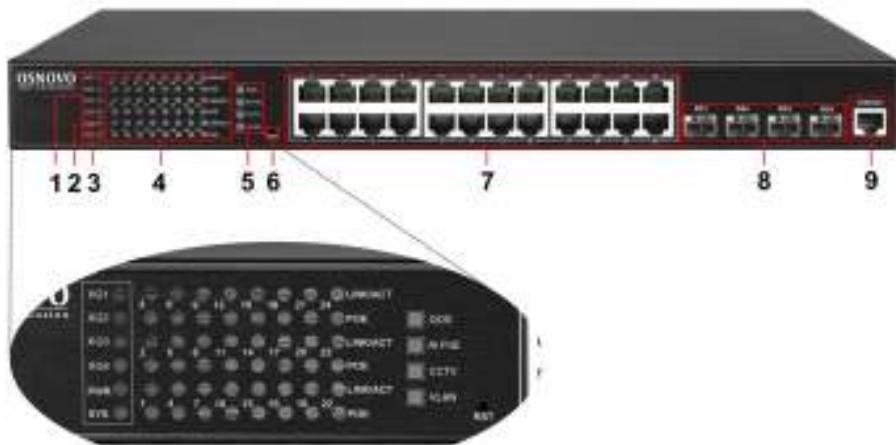


Рис.2 Коммутатор SW-24G4X-1L, разъемы, кнопки и индикаторы на передней панели

Таб. 1 Коммутатор SW-24G4X-1L, назначение разъемов, кнопок и индикаторов на передней панели

№ п/п	Обозначение	Назначение
1	XG1 XG2 XG3 XG4	LED индикаторы работы «SFP+» портов (8) <u>Горит/мигает</u> – соединение установлено на соответствующем оптическом порте <u>Не горит</u> – соединения нет, проверьте SFP+ модуль/оптический кабель
2	PWR	LED индикатор питания <u>Горит</u> – питание подается <u>Не горит</u> – питание не подается, проверьте подключение коммутатора к сети AC 230V
3	SYS	LED индикатор работы системы <u>Мигает</u> – система работает корректно. <u>Не горит</u> – система работает в неправильном режиме. Прошивка коммутатора повреждена.

№ п/п	Обозначение	Назначение
4	1-24 Link/Act POE	<p>PoE – LED индикаторы PoE портов 1-24 (7)</p> <p><u>Горит</u> – к соответствующему порту подключено PoE устройство. Питание PoE подается.</p> <p><u>Не горит</u> – подключено устройство без питания по PoE.</p> <p>Link/Act – LED индикаторы сетевой активности портов 1-24 (7)</p> <p><u>Горит/мигает</u> – установлено соединение, идет передача данных</p> <p><u>Не горит</u> – соединение не установлено.</p>
5	QOS Ai PoE CCTV VLAN	<p>Кнопки для быстрой активации соответствующих режимов работы коммутатора:</p> <ul style="list-style-type: none"> ▪ QOS – повышает приоритет видеотрафика до высокого. Может потребоваться в гибридной, разветвленной сети. ▪ Ai PoE – автоматическое определение «зависших» PoE устройств и их автоматическая перезагрузка. ▪ CCTV – возможность передачи данных на 250м для портов 1-8 со скоростью 10 Мбит/с без PoE. ▪ VLAN – изоляция портов друг от друга. Используется для предотвращения возникновения net storm. Порты 1-24 могут передавать трафик только на Uplink порты.
6	RST	Микрокнопка для сброса коммутатора к заводским настройкам.
7	1 - 24	Разъемы RJ-45 с 1 по 24й для подключения сетевых устройств на скорости 10/100/1000 Мбит/с, в том числе с PoE (IEEE 802.3 af/at)

№ п/п	Обозначение	Назначение
8	XG1 XG2 XG3 XG4	«SFP+» порты для подключения коммутатора к оптической линии связи на скорости 10 Гбит/с используя SFP+ модули 10G (приобретаются отдельно).
9	Console	Разъем RJ-45 для подключения уличного коммутатора к СОМ порту. Позволяет загружать в уличный коммутатор прошивку в случае аварийной ситуации



Рис. 3 Коммутатор SW-24G4X-1L, разъемы и кнопки на задней панели

Таб. 2 Коммутатор SW-24G4X-1L, назначение разъемов, кнопок и на задней панели

№ п/п	Обозначение	Назначение
1	-	Разъем для подключения коммутатора к сети AC 230V кабелем из комплекта поставки.
2	ON OFF	Кнопка для вкл/выкл коммутатора.
3		Посадочное место для предохранителя (подлежит проверке/замене в случае проблем с питанием). Извлекается с помощью отвертки.
4		Винтовая клемма для подключения заземления

5. Подключение

5.1 Схема подключения

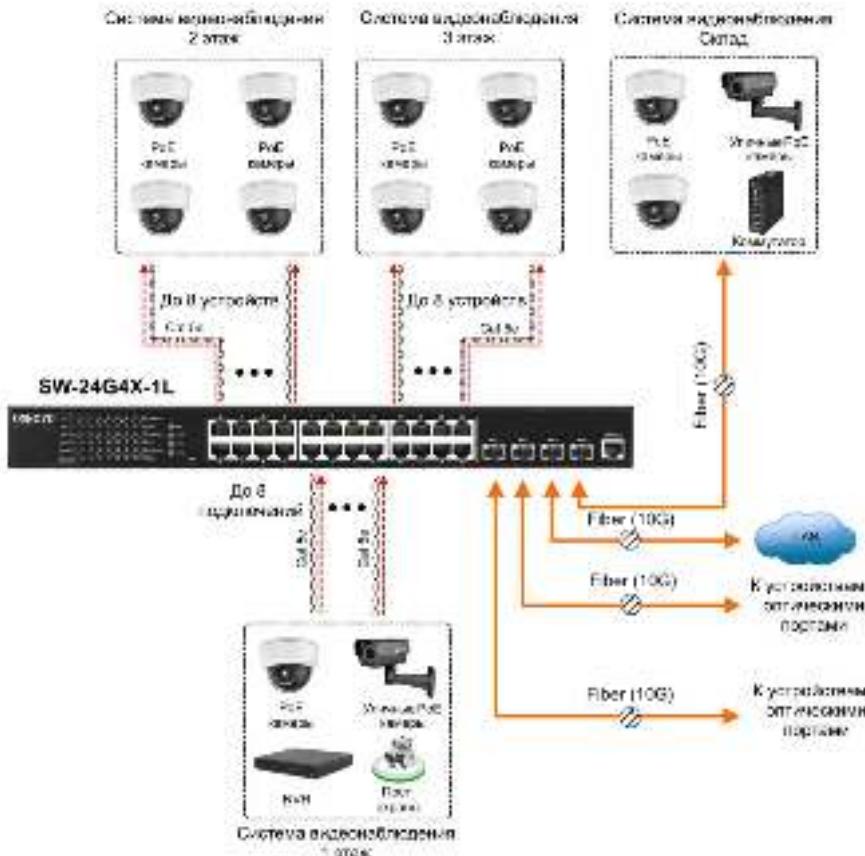


Рис. 4 Схема подключения коммутатора SW-24G4X-1L на примере построения системы видеонаблюдения на предприятии

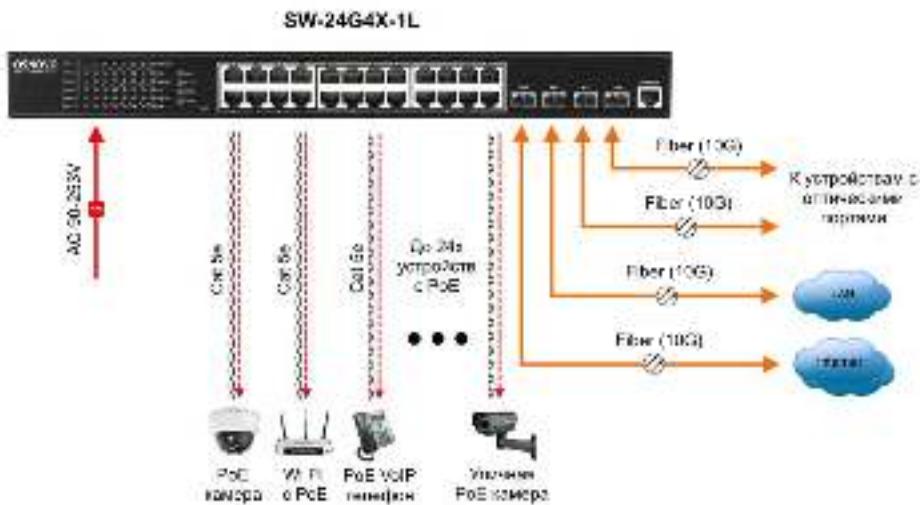


Рис.5 Типовая схема подключения коммутатора SW-24G4X-1L

5.2 Подключение питания



Рис. 6 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 вилку шнура питания (3) к розетке сети переменного тока AC 230V;
- 4) Переведите переключатель питания в положение ON.

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:

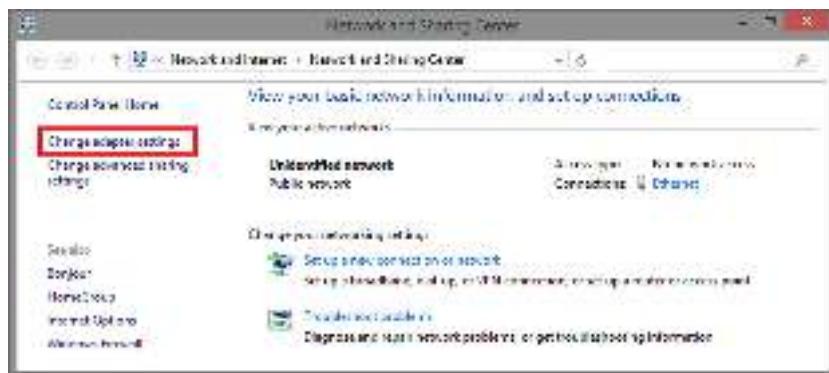
Причины потери в оптической линии могут быть вызваны:

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

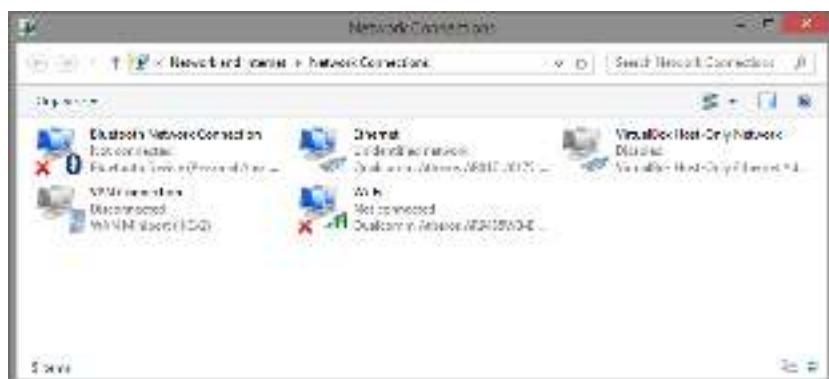
7. Подготовка перед управлением коммутатором через WEB.

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

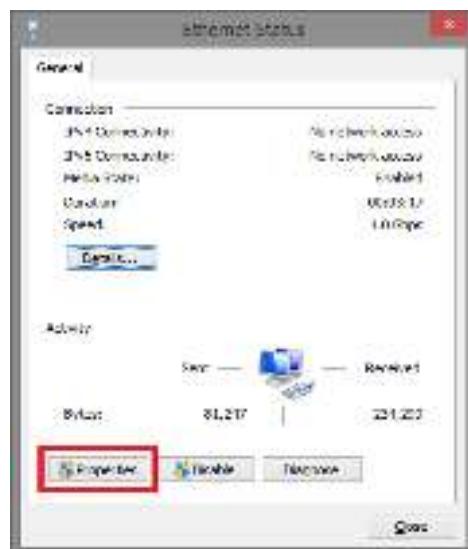
1. Откройте «Центр управления сетями и общим доступом» (Network and Sharing in Control Panel) и нажмите «Изменение параметров адаптера» (Change adapter setting) как на рисунке ниже.



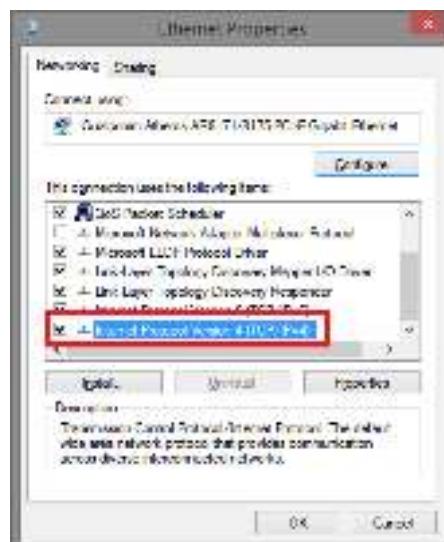
2. В появившемся окне «Сетевые подключения» (Network Connections) отображены все сетевые подключения, доступные вашему ПК. Сделайте двойной клик на подключении, которое вы используете для сети Ethernet



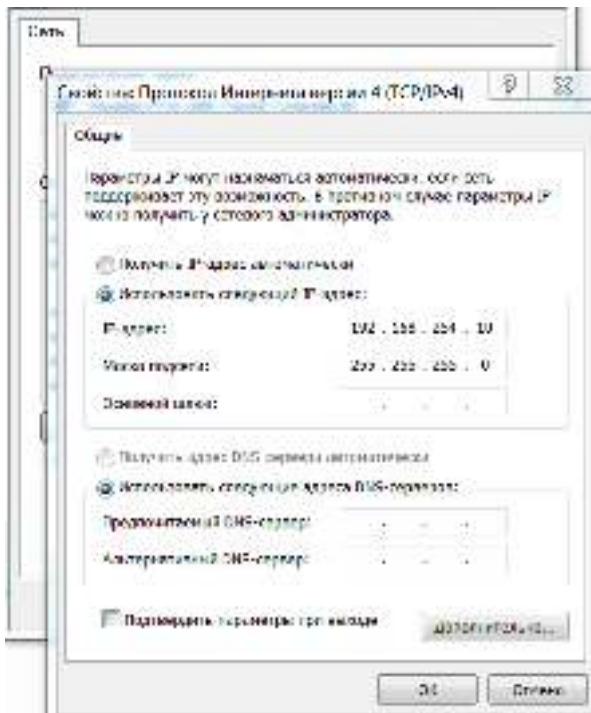
3. В появившемся окне «Состояние - Подключение по локальной сети» (Ethernet Status) нажмите кнопку «Свойства» (Properties) как показано ниже.



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 OK, чтобы сохранить и применить настройки.

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

По умолчанию:

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

8. Подготовка перед управлением коммутатором через порт CONSOLE

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

Скачайте и установите на ПК, с которого будет проводиться конфигурирование коммутатора программу-эммулятор 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**



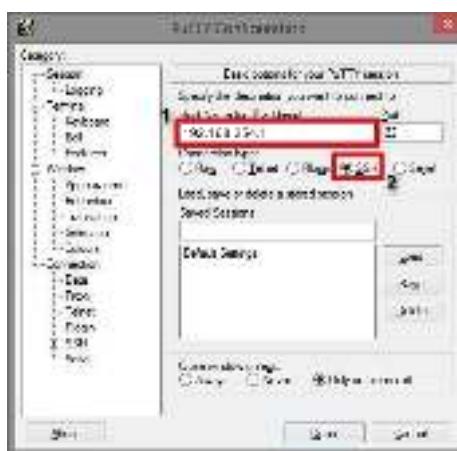
9. Подготовка перед управлением коммутатором через Telnet/SSH

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.



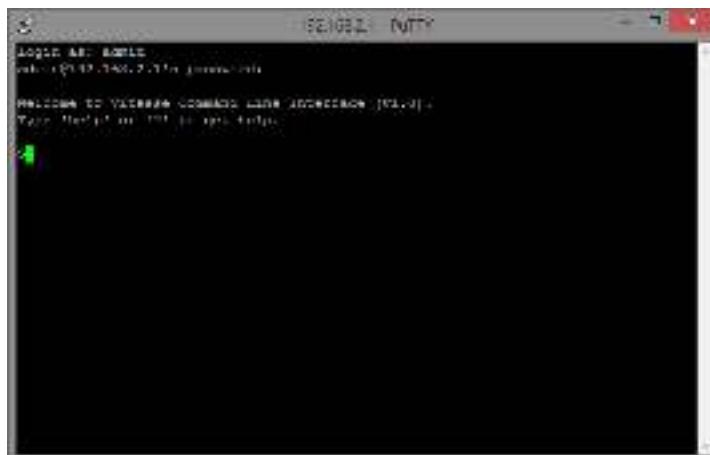
3. Если вы подключаетесь к коммутатору через SSH впервые, вы увидите окно PuTTY Security Alert. Нажмите Yes (Да) для продолжения.



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)

Best Friend Number	Business Contact Identifier	Best Friend Contact Identifier	Customer Contact Identifier
User Screening	Indicates if user has been flagged		
1	0	0	0
2	11111111111111111111	11111111111111111111	11111111111111111111
3	1	1	1
4	11111111111111111111	11111111111111111111	11111111111111111111
5	0	0	0
6	00000000000000000000	00000000000000000000	00000000000000000000
7	0	0	0
8	00000000000000000000	00000000000000000000	00000000000000000000
9	0	0	0
10	0	0	0
11	0	0	0
12	0	0	0
13	0	0	0
14	0	0	0
15	0	0	0
16	0	0	0
17	0	0	0
18	0	0	0
19	0	0	0
20	0	0	0
21	0	0	0
22	0	0	0
23	0	0	0
24	0	0	0
25	0	0	0
26	0	0	0
27	0	0	0
28	0	0	0
29	0	0	0
30	0	0	0
31	0	0	0
32	0	0	0
33	0	0	0
34	0	0	0
35	0	0	0
36	0	0	0
37	0	0	0
38	0	0	0
39	0	0	0
40	0	0	0
41	0	0	0
42	0	0	0
43	0	0	0
44	0	0	0
45	0	0	0
46	0	0	0
47	0	0	0
48	0	0	0
49	0	0	0
50	0	0	0
51	0	0	0
52	0	0	0
53	0	0	0
54	0	0	0
55	0	0	0
56	0	0	0
57	0	0	0
58	0	0	0
59	0	0	0
60	0	0	0
61	0	0	0
62	0	0	0
63	0	0	0
64	0	0	0
65	0	0	0
66	0	0	0
67	0	0	0
68	0	0	0
69	0	0	0
70	0	0	0
71	0	0	0
72	0	0	0
73	0	0	0
74	0	0	0
75	0	0	0
76	0	0	0
77	0	0	0
78	0	0	0
79	0	0	0
80	0	0	0
81	0	0	0
82	0	0	0
83	0	0	0
84	0	0	0
85	0	0	0
86	0	0	0
87	0	0	0
88	0	0	0
89	0	0	0
90	0	0	0
91	0	0	0
92	0	0	0
93	0	0	0
94	0	0	0
95	0	0	0
96	0	0	0
97	0	0	0
98	0	0	0
99	0	0	0
100	0	0	0
101	0	0	0
102	0	0	0
103	0	0	0
104	0	0	0
105	0	0	0
106	0	0	0
107	0	0	0
108	0	0	0
109	0	0	0
110	0	0	0
111	0	0	0
112	0	0	0
113	0	0	0
114	0	0	0
115	0	0	0
116	0	0	0
117	0	0	0
118	0	0	0
119	0	0	0
120	0	0	0
121	0	0	0
122	0	0	0
123	0	0	0
124	0	0	0
125	0	0	0
126	0	0	0
127	0	0	0
128	0	0	0
129	0	0	0
130	0	0	0
131	0	0	0
132	0	0	0
133	0	0	0
134	0	0	0
135	0	0	0
136	0	0	0
137	0	0	0
138	0	0	0
139	0	0	0
140	0	0	0
141	0	0	0
142	0	0	0
143	0	0	0
144	0	0	0
145	0	0	0
146	0	0	0
147	0	0	0
148	0	0	0
149	0	0	0
150	0	0	0
151	0	0	0
152	0	0	0
153	0	0	0
154	0	0	0
155	0	0	0
156	0	0	0
157	0	0	0
158	0	0	0
159	0	0	0
160	0	0	0
161	0	0	0
162	0	0	0
163	0	0	0
164	0	0	0
165	0	0	0
166	0	0	0
167	0	0	0
168	0	0	0
169	0	0	0
170	0	0	0
171	0	0	0
172	0	0	0
173	0	0	0
174	0	0	0
175	0	0	0
176	0	0	0
177	0	0	0
178	0	0	0
179	0	0	0
180	0	0	0
181	0	0	0
182	0	0	0
183	0	0	0
184	0	0	0
185	0	0	0
186	0	0	0
187	0	0	0
188	0	0	0
189	0	0	0
190	0	0	0
191	0	0	0
192	0	0	0
193	0	0	0
194	0	0	0
195	0	0	0
196	0	0	0
197	0	0	0
198	0	0	0
199	0	0	0
200	0	0	0
201	0	0	0
202	0	0	0
203	0	0	0
204	0	0	0
205	0	0	0
206	0	0	0
207	0	0	0
208	0	0	0
209	0	0	0
210	0	0	0
211	0	0	0
212	0	0	0
213	0	0	0
214	0	0	0
215	0	0	0
216	0	0	0
217	0	0	0
218	0	0	0
219	0	0	0
220	0	0	0
221	0	0	0
222	0	0	0
223	0	0	0
224	0	0	0
225	0	0	0
226	0	0	0
227	0	0	0
228	0	0	0
229	0	0	0
230	0	0	0
231	0	0	0
232	0	0	0
233	0	0	0
234	0	0	0
235	0	0	0
236	0	0	0
237	0	0	0
238	0	0	0
239	0	0	0
240	0	0	0
241	0	0	0
242	0	0	0
243	0	0	0
244	0	0	0
245	0	0	0
246	0	0	0
247	0	0	0
248	0	0	0
249	0	0	0
250	0	0	0
251	0	0	0
252	0	0	0
253	0	0	0
254	0	0	0
255	0	0	0
256	0	0	0
257	0	0	0
258	0	0	0
259	0	0	0
260	0	0	0
261	0	0	0
262	0	0	0
263	0	0	0
264	0	0	0
265	0	0	0
266	0	0	0
267	0	0	0
268	0	0	0
269	0	0	0
270	0	0	0
271	0	0	0
272	0	0	0
273	0	0	0
274	0	0	0
275	0	0	0
276	0	0	0
277	0	0	0
278	0	0	0
279	0	0	0
280	0	0	0
281	0	0	0
282	0	0	0
283	0	0	0
284	0	0	0
285	0	0	0
286	0	0	0
287	0	0	0
288	0	0	0
289	0	0	0
290	0	0	0
291	0	0	0
292	0	0	0
293	0	0	0
294	0	0	0
295	0	0	0
296	0	0	0
297	0	0	0
298	0	0	0
299	0	0	0
300	0	0	0
301	0	0	0
302	0	0	0
303	0	0	0
304	0	0	0
305	0	0	0
306	0	0	0
307	0	0	0
308	0	0	0
309	0	0	0
310	0	0	0
311	0	0	0
312	0	0	0
313	0	0	0
314	0	0	0
315	0	0	0
316	0	0	0
317	0	0	0
318	0	0	0
319	0	0	0
320	0	0	0
321	0	0	0
322	0	0	0
323	0	0	0
324	0	0	0
325	0	0	0
326	0	0	0
327	0	0	0
328	0	0	0
329	0	0	0
330	0	0	0
331	0	0	0
332	0	0	0
333	0	0	0
334	0	0	0
335	0	0	0
336	0	0	0
337	0	0	0
338	0	0	0
339	0	0	0
340	0	0	0
341	0	0	0
342	0	0	0
343	0	0	0
344	0	0	0
345	0	0	0
346	0	0	0
347	0	0	0
348	0	0	0
349	0	0	0
350	0	0	0
351	0	0	0
352	0	0	0
353	0	0	0
354	0	0	0
355	0	0	0
356	0	0	0
357	0	0	0
358	0	0	0
359	0	0	0
360	0	0	0
361	0	0	0
362	0	0	0
363	0	0	0
364	0	0	0
365	0	0	0
366	0	0	0
367	0	0	0
368	0	0	0
369	0	0	0
370	0	0	0
371	0	0	0
372	0	0	0
373	0	0	0
374	0	0	0
375	0	0	0
376	0	0	0
377	0	0	0
378	0	0	0
379	0	0	0
380	0	0	0
381	0	0	0
382	0	0	0
383	0	0	0
384	0	0	0
385	0	0	0
386	0	0	0
387	0	0	0
388	0	0	0
389	0	0	0
390	0	0	0
391	0	0	0
392	0	0	0
393	0	0	0
394	0	0	0
395	0	0	0
396	0	0	0
397	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 00:17	5	Link	mono	92	Interface[92] state change to up
1970-01-01 00:17	5	Link	mono	93	Interface[93] state change to down.
1970-01-01 00:01	5	Link	mono	92	Interface[92] state change to up
1970-01-01 00:01	5	Bridge	poc	92	Interface[92] poc power shape state change
1970-01-01 00:01	5	Status	poc	92	Interface[92] poc power good state change.
1970-01-01 00:01	5	Contact	poc	92	Interface[92] poc disconnect
1970-01-01 00:01	5	Bridge	poc	92	Interface[92] poc power enable state change
1970-01-01 00:01	5	Status	poc	92	Interface[92] poc power good state change.
1970-01-01 00:01	5	Link	mono	92	Interface[92] state change to down.
1970-01-01 00:02	5	Link	mono	18	Interface[18] state change to up
1970-01-01 00:00	5	Link	mono	92	Interface[92] state change to up
1970-01-01 00:00	5	Link	mono	18	Interface[18] state change to up
1970-01-01 00:00	5	Link	mono	92	Interface[92] state change to up
1970-01-01 00:00	5	Link	mono	18	Interface[18] state change to up
1970-01-01 00:00	5	Link	mono	92	Interface[92] 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.

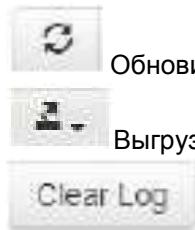
Максимальное количество записей в журнале – 512.

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





10.3 Управление портами (Port Management)

10.3.1 Настройки портов (Port Configuration)

№	Название	Мак-адрес	Скорость	Дуплекс	Максимальный трафик	Приоритет	Макс. нагрузка	Проверка	Статус
1	Port 1	00:0C:29:00:00:01	100	Full	1000	1	100	OK	Green
2	Port 2	00:0C:29:00:00:02	100	Full	1000	2	100	OK	Green
3	Port 3	00:0C:29:00:00:03	100	Full	1000	3	100	OK	Green
4	Port 4	00:0C:29:00:00:04	100	Full	1000	4	100	OK	Green
5	Port 5	00:0C:29:00:00:05	100	Full	1000	5	100	OK	Green
6	Port 6	00:0C:29:00:00:06	100	Full	1000	6	100	OK	Green
7	Port 7	00:0C:29:00:00:07	100	Full	1000	7	100	OK	Green
8	Port 8	00:0C:29:00:00:08	100	Full	1000	8	100	OK	Green
9	Port 9	00:0C:29:00:00:09	100	Full	1000	9	100	OK	Green
10	Port 10	00:0C:29:00:00:0A	100	Full	1000	10	100	OK	Green
11	Port 11	00:0C:29:00:00:0B	100	Full	1000	11	100	OK	Green
12	Port 12	00:0C:29:00:00:0C	100	Full	1000	12	100	OK	Green
13	Port 13	00:0C:29:00:00:0D	100	Full	1000	13	100	OK	Green
14	Port 14	00:0C:29:00:00:0E	100	Full	1000	14	100	OK	Green
15	Port 15	00:0C:29:00:00:0F	100	Full	1000	15	100	OK	Green
16	Port 16	00:0C:29:00:00:10	100	Full	1000	16	100	OK	Green
17	Port 17	00:0C:29:00:00:11	100	Full	1000	17	100	OK	Green
18	Port 18	00:0C:29:00:00:12	100	Full	1000	18	100	OK	Green
19	Port 19	00:0C:29:00:00:13	100	Full	1000	19	100	OK	Green
20	Port 20	00:0C:29:00:00:14	100	Full	1000	20	100	OK	Green
21	Port 21	00:0C:29:00:00:15	100	Full	1000	21	100	OK	Green
22	Port 22	00:0C:29:00:00:16	100	Full	1000	22	100	OK	Green
23	Port 23	00:0C:29:00:00:17	100	Full	1000	23	100	OK	Green
24	Port 24	00:0C:29:00:00:18	100	Full	1000	24	100	OK	Green
25	Port 25	00:0C:29:00:00:19	100	Full	1000	25	100	OK	Green
26	Port 26	00:0C:29:00:00:1A	100	Full	1000	26	100	OK	Green
27	Port 27	00:0C:29:00:00:1B	100	Full	1000	27	100	OK	Green
28	Port 28	00:0C:29:00:00:1C	100	Full	1000	28	100	OK	Green
29	Port 29	00:0C:29:00:00:1D	100	Full	1000	29	100	OK	Green
30	Port 30	00:0C:29:00:00:1E	100	Full	1000	30	100	OK	Green
31	Port 31	00:0C:29:00:00:1F	100	Full	1000	31	100	OK	Green
32	Port 32	00:0C:29:00:00:10	100	Full	1000	32	100	OK	Green
33	Port 33	00:0C:29:00:00:11	100	Full	1000	33	100	OK	Green
34	Port 34	00:0C:29:00:00:12	100	Full	1000	34	100	OK	Green
35	Port 35	00:0C:29:00:00:13	100	Full	1000	35	100	OK	Green
36	Port 36	00:0C:29:00:00:14	100	Full	1000	36	100	OK	Green
37	Port 37	00:0C:29:00:00:15	100	Full	1000	37	100	OK	Green
38	Port 38	00:0C:29:00:00:16	100	Full	1000	38	100	OK	Green
39	Port 39	00:0C:29:00:00:17	100	Full	1000	39	100	OK	Green
40	Port 40	00:0C:29:00:00:18	100	Full	1000	40	100	OK	Green
41	Port 41	00:0C:29:00:00:19	100	Full	1000	41	100	OK	Green
42	Port 42	00:0C:29:00:00:1A	100	Full	1000	42	100	OK	Green
43	Port 43	00:0C:29:00:00:1B	100	Full	1000	43	100	OK	Green
44	Port 44	00:0C:29:00:00:1C	100	Full	1000	44	100	OK	Green
45	Port 45	00:0C:29:00:00:1D	100	Full	1000	45	100	OK	Green
46	Port 46	00:0C:29:00:00:1E	100	Full	1000	46	100	OK	Green
47	Port 47	00:0C:29:00:00:10	100	Full	1000	47	100	OK	Green
48	Port 48	00:0C:29:00:00:11	100	Full	1000	48	100	OK	Green
49	Port 49	00:0C:29:00:00:12	100	Full	1000	49	100	OK	Green
50	Port 50	00:0C:29:00:00:13	100	Full	1000	50	100	OK	Green
51	Port 51	00:0C:29:00:00:14	100	Full	1000	51	100	OK	Green
52	Port 52	00:0C:29:00:00:15	100	Full	1000	52	100	OK	Green
53	Port 53	00:0C:29:00:00:16	100	Full	1000	53	100	OK	Green
54	Port 54	00:0C:29:00:00:17	100	Full	1000	54	100	OK	Green
55	Port 55	00:0C:29:00:00:18	100	Full	1000	55	100	OK	Green
56	Port 56	00:0C:29:00:00:19	100	Full	1000	56	100	OK	Green
57	Port 57	00:0C:29:00:00:1A	100	Full	1000	57	100	OK	Green
58	Port 58	00:0C:29:00:00:1B	100	Full	1000	58	100	OK	Green
59	Port 59	00:0C:29:00:00:1C	100	Full	1000	59	100	OK	Green
60	Port 60	00:0C:29:00:00:1D	100	Full	1000	60	100	OK	Green
61	Port 61	00:0C:29:00:00:1E	100	Full	1000	61	100	OK	Green
62	Port 62	00:0C:29:00:00:10	100	Full	1000	62	100	OK	Green
63	Port 63	00:0C:29:00:00:11	100	Full	1000	63	100	OK	Green
64	Port 64	00:0C:29:00:00:12	100	Full	1000	64	100	OK	Green
65	Port 65	00:0C:29:00:00:13	100	Full	1000	65	100	OK	Green
66	Port 66	00:0C:29:00:00:14	100	Full	1000	66	100	OK	Green
67	Port 67	00:0C:29:00:00:15	100	Full	1000	67	100	OK	Green
68	Port 68	00:0C:29:00:00:16	100	Full	1000	68	100	OK	Green
69	Port 69	00:0C:29:00:00:17	100	Full	1000	69	100	OK	Green
70	Port 70	00:0C:29:00:00:18	100	Full	1000	70	100	OK	Green
71	Port 71	00:0C:29:00:00:19	100	Full	1000	71	100	OK	Green
72	Port 72	00:0C:29:00:00:1A	100	Full	1000	72	100	OK	Green
73	Port 73	00:0C:29:00:00:1B	100	Full	1000	73	100	OK	Green
74	Port 74	00:0C:29:00:00:1C	100	Full	1000	74	100	OK	Green
75	Port 75	00:0C:29:00:00:1D	100	Full	1000	75	100	OK	Green
76	Port 76	00:0C:29:00:00:1E	100	Full	1000	76	100	OK	Green
77	Port 77	00:0C:29:00:00:10	100	Full	1000	77	100	OK	Green
78	Port 78	00:0C:29:00:00:11	100	Full	1000	78	100	OK	Green
79	Port 79	00:0C:29:00:00:12	100	Full	1000	79	100	OK	Green
80	Port 80	00:0C:29:00:00:13	100	Full	1000	80	100	OK	Green
81	Port 81	00:0C:29:00:00:14	100	Full	1000	81	100	OK	Green
82	Port 82	00:0C:29:00:00:15	100	Full	1000	82	100	OK	Green
83	Port 83	00:0C:29:00:00:16	100	Full	1000	83	100	OK	Green
84	Port 84	00:0C:29:00:00:17	100	Full	1000	84	100	OK	Green
85	Port 85	00:0C:29:00:00:18	100	Full	1000	85	100	OK	Green
86	Port 86	00:0C:29:00:00:19	100	Full	1000	86	100	OK	Green
87	Port 87	00:0C:29:00:00:1A	100	Full	1000	87	100	OK	Green
88	Port 88	00:0C:29:00:00:1B	100	Full	1000	88	100	OK	Green
89	Port 89	00:0C:29:00:00:1C	100	Full	1000	89	100	OK	Green
90	Port 90	00:0C:29:00:00:1D	100	Full	1000	90	100	OK	Green
91	Port 91	00:0C:29:00:00:1E	100	Full	1000	91	100	OK	Green
92	Port 92	00:0C:29:00:00:10	100	Full	1000	92	100	OK	Green
93	Port 93	00:0C:29:00:00:11	100	Full	1000	93	100	OK	Green
94	Port 94	00:0C:29:00:00:12	100	Full	1000	94	100	OK	Green
95	Port 95	00:0C:29:00:00:13	100	Full	1000	95	100	OK	Green
96	Port 96	00:0C:29:00:00:14	100	Full	1000	96	100	OK	Green
97	Port 97	00:0C:29:00:00:15	100	Full	1000	97	100	OK	Green
98	Port 98	00:0C:29:00:00:16	100	Full	1000	98	100	OK	Green
99	Port 99	00:0C:29:00:00:17	100	Full	1000	99	100	OK	Green
100	Port 100	00:0C:29:00:00:18	100	Full	1000	100	100	OK	Green

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
 - 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)

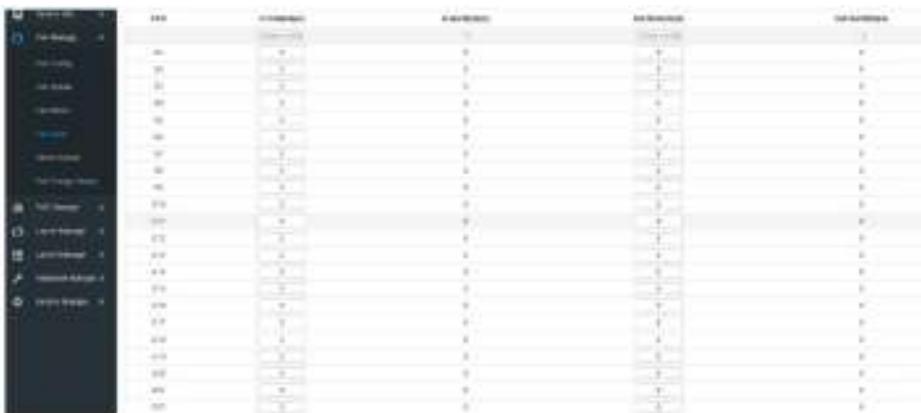


На данной странице WEB интерфейса коммутатора представлены настройки функции зеркалирования – возможности копирования отправляемого/принимаемого трафика на выбранный порт с целью мониторинга и выявления проблем.

- 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 Management). Опции в Port Management сконфигурированы 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)



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)

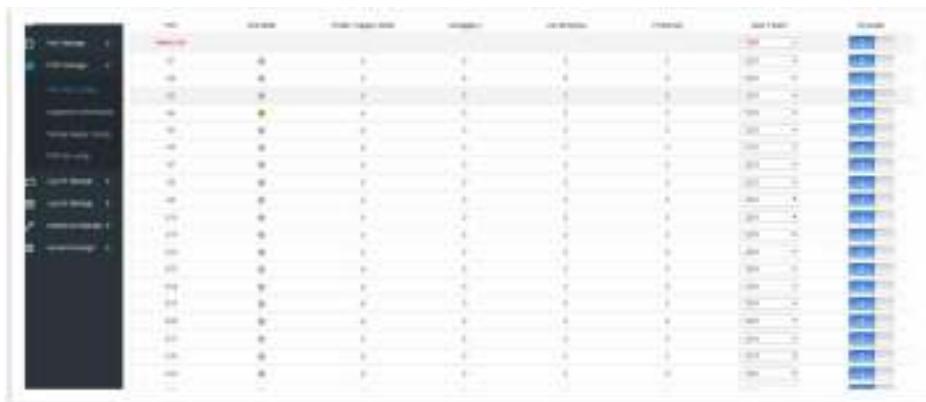


На данной странице WEB интерфейса представлена возможность активировать функцию энергосбережения EEE для выбранных портов.

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

10.4 Управление питанием PoE (PoE Management)

10.4.1 Управление питанием PoE для портов (Port PoE Config)



На данной странице WEB интерфейса коммутатора представлены настройки PoE для портов, которые поддерживают эту функцию. В частности доступно ограничение максимальной мощности на порте, и глобальное вкл/выкл PoE на порте.

- ✓ MAX power – поле, в котором можно выбрать максимальную выдаваемую на порт мощность PoE;
- ✓ On/Off – переключатель, отвечающий за вкл/выкл PoE на порте.

Внимание!

Общее значение выдаваемой мощности PoE по каждому порту не должно превышать значения Maximum Total Power Supply (Общая мощность источника питания) в разделе Smart PoE Configuration.

10.4.2 Информация об оборудовании (Equipment Information)



На данной странице WEB интерфейса представлена информация по потребляемой мощности PoE, напряжению PoE и температуре на каждом PoE контроллере.

Если температура на любом из чипов отображается красным – это значит, что температура слишком высокая и необходимо снизить нагрузку или принять иные меры по охлаждению коммутатора.

10.4.3 Настройка подачи PoE по расписанию (Timing Supply Config)

На данной странице WEB интерфейса представлены настройки, позволяющие задавать время (год/месяц/день/час/минута/секунда), в которое коммутатор включит подачу PoE на выбранном порте.

Также можно задавать период в неделях/часах/минутах/секундах в течение которого будет осуществляться подача PoE на порте.

10.4.3.1 Установка периода подачи PoE (Time Range Config)



- Add time Range > Name – поле, где можно задать имя временного диапазона. Это могут быть цифры, буквы. Нажмите Add, чтобы завершить создание временного диапазона. Del – чтобы удалить.
- Config the time – настройки временного диапазона
 - Time-Range Name – выбор (выпадающий список) временного диапазона из ранее добавленных;
 - Start Time – установка начального значения временного диапазона. Тип параметра – absolute;
 - End Time – установка конечного значения временного диапазона;
 - Time – установка циклического значения времени;
 - Week – число дней для заданного цикла.

Примечание!

Прежде чем задавать временной диапазон подачи PoE необходимо синхронизировать время системы коммутатора с временем в ОС кнопкой на первой странице WEB интерфейса (Global Info)

10.4.3.2 Применение периода подачи PoE для портов (Timing Supply Config)

Port	Port Status	Power Output Type	Periodic	OneShot	Max Off Time Length	Timing Power Supply
00-0001	Up	●	○	○	00:00:00	●
00-0002	Up	●	○	○	00:00:00	●
00-0003	Up	●	○	○	00:00:00	●
00-0004	Up	●	○	○	00:00:00	●
00-0005	Up	●	○	○	00:00:00	●
00-0006	Up	●	○	○	00:00:00	●
00-0007	Up	●	○	○	00:00:00	●
00-0008	Up	●	○	○	00:00:00	●
00-0009	Up	●	○	○	00:00:00	●
00-0010	Up	●	○	○	00:00:00	●
00-0011	Up	●	○	○	00:00:00	●
00-0012	Up	●	○	○	00:00:00	●
00-0013	Up	●	○	○	00:00:00	●
00-0014	Up	●	○	○	00:00:00	●
00-0015	Up	●	○	○	00:00:00	●
00-0016	Up	●	○	○	00:00:00	●
00-0017	Up	●	○	○	00:00:00	●
00-0018	Up	●	○	○	00:00:00	●
00-0019	Up	●	○	○	00:00:00	●
00-0020	Up	●	○	○	00:00:00	●
00-0021	Up	●	○	○	00:00:00	●
00-0022	Up	●	○	○	00:00:00	●
00-0023	Up	●	○	○	00:00:00	●
00-0024	Up	●	○	○	00:00:00	●
00-0025	Up	●	○	○	00:00:00	●
00-0026	Up	●	○	○	00:00:00	●
00-0027	Up	●	○	○	00:00:00	●
00-0028	Up	●	○	○	00:00:00	●
00-0029	Up	●	○	○	00:00:00	●
00-0030	Up	●	○	○	00:00:00	●
00-0031	Up	●	○	○	00:00:00	●
00-0032	Up	●	○	○	00:00:00	●

На данной странице WEB интерфейса находятся инструменты для активации ранее заданного временного диапазона подачи PoE для выбранных портов.

Кроме того на странице отображаются данные о напряжении PoE, потребляемом от порта токе в mA, состояние подключения (есть/нет подключение).

- ✓ Power off Time Range – выбор из выпадающего списка ранее созданного временного диапазона под заданным именем.
Нажмите Select all (выбрать все), чтобы применить данный диапазон ко всем портам;
- ✓ Timing Power Supply – вкл/выкл функции подачи PoE по расписанию (временному диапазону).

10.4.3 Функция PoE AI Config (PoE AI Config)



На данной странице WEB интерфейса представлены настройки функции PoE AI, которая позволяет автоматически перезагружать подключенные PoE устройства в случае зависания.

Функция срабатывает в случае, если на порте с подключенным PoE устройством не наблюдается сетевой активности (прием/передача трафика) в течение заданного промежутка времени. В таком случае PoE будет отключено на порте на 10 сек, после чего восстановлено.

Кроме того, данная функция отвечает также за отключение порта в случае, если общая потребляемая мощность превысила указанную в поле Max Total Power.

- ✓ PoE AI – вкл/выкл режима антивискания PoE AI. Также может быть вкл/выкл кнопкой на передней панели коммутатора.
 - ✓ Max Total Power – поле, где задается максимальная совокупная мощность PoE на все порты.
 - ✓ Zero Flow Interval – время в сек, по истечении которого, в случае отсутствия приема/передачи трафика на порте, коммутатор отключает PoE на порте, а затем включает через 10 сек.

10.5 Управление настройками 2 уровня (Layer 2 Management)

10.5.1 Таблица MAC адресов (MAC Address Table)

Category	Sub-Category	Product ID	Description	Stock Level	Unit Price
Electronics	Smartphones	SPR-0001	iPhone 12 Pro Max	500	\$1,200
Electronics	Laptops	LAP-0001	MacBook Pro M1	300	\$1,000
Electronics	Tablets	TAB-0001	Surface Pro 7	200	\$800

Основная задача коммутатора Ethernet – пересыпать 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 пересыпать пакеты с данными на все порты, снижая общую эффективность коммутации.

Рекомендуется использовать значение по умолчанию.

10.5.2 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.

10.5.2.1 VLAN Static



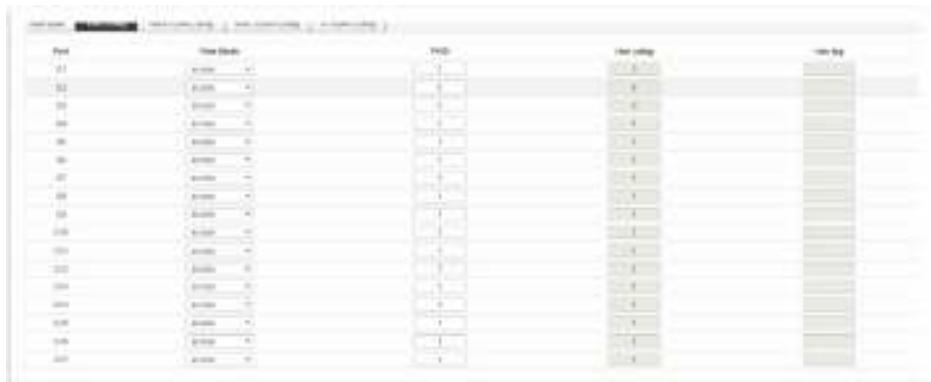
Запоминание VLAN (VLAN Learning)

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 пересыпает 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, ассоцииированную 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

Port	Vlan Mode	Pvid
G1	access	1
G2	access	10
G3	access	10
G4	access	10
G5	access	10

Добавить порт G9 к нескольким VLAN

Port	Vlan Mode	PVID	inet tag
G1	802.1Q	1	0
G2	802.1Q	10	10
G3	802.1Q	10	10
G4	802.1Q	10	10
G5	802.1Q	10	10
G6	802.1Q	10	10
G7	802.1Q	1	1
G8	802.1Q	1	1
G9	802.1Q	1	1

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

10.5.2.3 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.

10.5.2.4 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 устройства, 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.

10.5.2.5 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 переведены в режим Untag.
- ✓ IP – поле для ввода IP адреса клиента.

10.5.3 Агрегирование каналов (Link Aggregation)

Физические порты могут быть объединены 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.

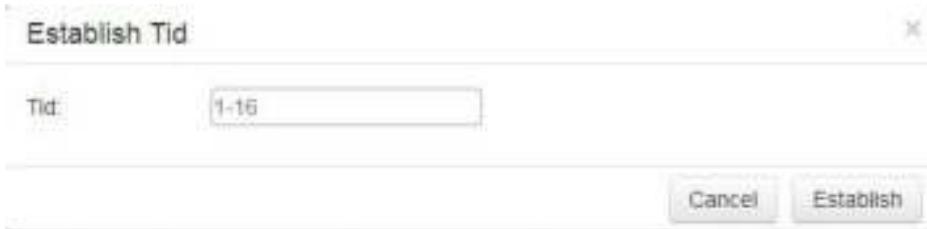
Порты-участники одной и той же группы агрегации должны быть сконфигурированы одинаково (STP, QoS, VLAN, атрибуты порта, MAC Address Learning и тд).

10.5.3.1 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

10.5.3.2 Настройки динамической агрегации (Dynamic Aggregation Config)

Имя порта	Порты в группе	Логика синхронизации	Порты в группе	Порты в группе	Порты в группе	Порты в группе
Port 1	—	—	—	—	—	—
Port 2	—	—	—	—	—	—
Port 3	—	—	—	—	—	—
Port 4	—	—	—	—	—	—
Port 5	—	—	—	—	—	—
Port 6	—	—	—	—	—	—
Port 7	—	—	—	—	—	—
Port 8	—	—	—	—	—	—
Port 9	—	—	—	—	—	—
Port 10	—	—	—	—	—	—
Port 11	—	—	—	—	—	—
Port 12	—	—	—	—	—	—
Port 13	—	—	—	—	—	—
Port 14	—	—	—	—	—	—
Port 15	—	—	—	—	—	—
Port 16	—	—	—	—	—	—
Port 17	—	—	—	—	—	—
Port 18	—	—	—	—	—	—
Port 19	—	—	—	—	—	—
Port 20	—	—	—	—	—	—
Port 21	—	—	—	—	—	—
Port 22	—	—	—	—	—	—
Port 23	—	—	—	—	—	—
Port 24	—	—	—	—	—	—
Port 25	—	—	—	—	—	—
Port 26	—	—	—	—	—	—
Port 27	—	—	—	—	—	—
Port 28	—	—	—	—	—	—
Port 29	—	—	—	—	—	—
Port 30	—	—	—	—	—	—
Port 31	—	—	—	—	—	—
Port 32	—	—	—	—	—	—
Port 33	—	—	—	—	—	—
Port 34	—	—	—	—	—	—
Port 35	—	—	—	—	—	—
Port 36	—	—	—	—	—	—
Port 37	—	—	—	—	—	—
Port 38	—	—	—	—	—	—
Port 39	—	—	—	—	—	—
Port 40	—	—	—	—	—	—
Port 41	—	—	—	—	—	—
Port 42	—	—	—	—	—	—
Port 43	—	—	—	—	—	—
Port 44	—	—	—	—	—	—
Port 45	—	—	—	—	—	—
Port 46	—	—	—	—	—	—
Port 47	—	—	—	—	—	—
Port 48	—	—	—	—	—	—
Port 49	—	—	—	—	—	—
Port 50	—	—	—	—	—	—
Port 51	—	—	—	—	—	—
Port 52	—	—	—	—	—	—
Port 53	—	—	—	—	—	—
Port 54	—	—	—	—	—	—
Port 55	—	—	—	—	—	—
Port 56	—	—	—	—	—	—
Port 57	—	—	—	—	—	—
Port 58	—	—	—	—	—	—
Port 59	—	—	—	—	—	—
Port 60	—	—	—	—	—	—
Port 61	—	—	—	—	—	—
Port 62	—	—	—	—	—	—
Port 63	—	—	—	—	—	—
Port 64	—	—	—	—	—	—
Port 65	—	—	—	—	—	—
Port 66	—	—	—	—	—	—
Port 67	—	—	—	—	—	—
Port 68	—	—	—	—	—	—
Port 69	—	—	—	—	—	—
Port 70	—	—	—	—	—	—
Port 71	—	—	—	—	—	—
Port 72	—	—	—	—	—	—
Port 73	—	—	—	—	—	—
Port 74	—	—	—	—	—	—
Port 75	—	—	—	—	—	—
Port 76	—	—	—	—	—	—
Port 77	—	—	—	—	—	—
Port 78	—	—	—	—	—	—
Port 79	—	—	—	—	—	—
Port 80	—	—	—	—	—	—
Port 81	—	—	—	—	—	—
Port 82	—	—	—	—	—	—
Port 83	—	—	—	—	—	—
Port 84	—	—	—	—	—	—
Port 85	—	—	—	—	—	—
Port 86	—	—	—	—	—	—
Port 87	—	—	—	—	—	—
Port 88	—	—	—	—	—	—
Port 89	—	—	—	—	—	—
Port 90	—	—	—	—	—	—
Port 91	—	—	—	—	—	—
Port 92	—	—	—	—	—	—
Port 93	—	—	—	—	—	—
Port 94	—	—	—	—	—	—
Port 95	—	—	—	—	—	—
Port 96	—	—	—	—	—	—
Port 97	—	—	—	—	—	—
Port 98	—	—	—	—	—	—
Port 99	—	—	—	—	—	—
Port 100	—	—	—	—	—	—

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 расформировании. Значение по умолчанию – 32768.
- Activity Mode – периодичность посылки LACP пакетов.
 - Active Mode – порт автоматически посыпает LACP пакеты с периодичностью, указанной в поле Send Mode.
 - Passive Mode – порт не посыпает 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 посыпать 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.

10.5.3.3 Информация о группах агрегации (Link Aggregation Information)

Группа агрегации	Название группы	Модель	Порты	Порты	Балансировка	
Имя	Номер	Модель	Номера Порта	Активные Порты	Номера Порта	Балансировка
Group 1	Group 1	Group 1	1, 2, 3, 4	1, 2, 3, 4	1, 2, 3, 4	RoundRobin

Для каждого участника группы агрегации определены активные порты и режим балансировки трафика.

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.

10.5.4 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.

10.5.4.1 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.

10.5.4.2 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.

10.5.4.3 Настройка instance для портов (Interface Instance Config)

The screenshot shows a table of port configurations for MSTP. The columns include Port ID, Priority, Designated, Root ID, Root Priority, Root Cost, Designated Cost, Designated Role, and Type. Most ports have a priority of 0 and a cost of 0. Port 1 has a priority of 128 and a cost of 100. Port 48 is designated as the root bridge.

Порты	Priority	Дизайнер	Root ID	Root Priority	Root Cost	Designated Cost	Designated Role	Type	Mode
1	0			0	0	0	0	Designated	Learning
2	0			0	0	0	0	Designated	Learning
3	0			0	0	0	0	Designated	Learning
4	0			0	0	0	0	Designated	Learning
5	0			0	0	0	0	Designated	Learning
6	0			0	0	0	0	Designated	Learning
7	0			0	0	0	0	Designated	Learning
8	0			0	0	0	0	Designated	Learning
9	0			0	0	0	0	Designated	Learning
10	0			0	0	0	0	Designated	Learning
11	0			0	0	0	0	Designated	Learning
12	0			0	0	0	0	Designated	Learning
13	0			0	0	0	0	Designated	Learning
14	0			0	0	0	0	Designated	Learning
15	0			0	0	0	0	Designated	Learning
16	0			0	0	0	0	Designated	Learning
17	0			0	0	0	0	Designated	Learning
18	0			0	0	0	0	Designated	Learning
19	0			0	0	0	0	Designated	Learning
20	0			0	0	0	0	Designated	Learning
21	0			0	0	0	0	Designated	Learning
22	0			0	0	0	0	Designated	Learning
23	0			0	0	0	0	Designated	Learning
24	0			0	0	0	0	Designated	Learning
25	0			0	0	0	0	Designated	Learning
26	0			0	0	0	0	Designated	Learning
27	0			0	0	0	0	Designated	Learning
28	0			0	0	0	0	Designated	Learning
29	0			0	0	0	0	Designated	Learning
30	0			0	0	0	0	Designated	Learning
31	0			0	0	0	0	Designated	Learning
32	0			0	0	0	0	Designated	Learning
33	0			0	0	0	0	Designated	Learning
34	0			0	0	0	0	Designated	Learning
35	0			0	0	0	0	Designated	Learning
36	0			0	0	0	0	Designated	Learning
37	0			0	0	0	0	Designated	Learning
38	0			0	0	0	0	Designated	Learning
39	0			0	0	0	0	Designated	Learning
40	0			0	0	0	0	Designated	Learning
41	0			0	0	0	0	Designated	Learning
42	0			0	0	0	0	Designated	Learning
43	0			0	0	0	0	Designated	Learning
44	0			0	0	0	0	Designated	Learning
45	0			0	0	0	0	Designated	Learning
46	0			0	0	0	0	Designated	Learning
47	0			0	0	0	0	Designated	Learning
48	128			0	100	0	Root	Root	Learning

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.

10.5.4.4 Настройка портов для STP (Interface Config)

Имя интерфейса	Максимальный поток	Сервисный порт	Максимальный поток	Порт Edge	Статус порта	Максимальный поток	Порт Point-to-Point
Ethernet 0/0	100	0	100	Auto	Enabled	100	0
Ethernet 0/1	100	0	100	Auto	Enabled	100	0
Ethernet 0/2	100	0	100	Auto	Enabled	100	0
Ethernet 0/3	100	0	100	Auto	Enabled	100	0
Ethernet 0/4	100	0	100	Auto	Enabled	100	0
Ethernet 0/5	100	0	100	Auto	Enabled	100	0
Ethernet 0/6	100	0	100	Auto	Enabled	100	0
Ethernet 0/7	100	0	100	Auto	Enabled	100	0
Ethernet 0/8	100	0	100	Auto	Enabled	100	0
Ethernet 0/9	100	0	100	Auto	Enabled	100	0
Ethernet 0/10	100	0	100	Auto	Enabled	100	0
Ethernet 0/11	100	0	100	Auto	Enabled	100	0
Ethernet 0/12	100	0	100	Auto	Enabled	100	0
Ethernet 0/13	100	0	100	Auto	Enabled	100	0
Ethernet 0/14	100	0	100	Auto	Enabled	100	0
Ethernet 0/15	100	0	100	Auto	Enabled	100	0
Ethernet 0/16	100	0	100	Auto	Enabled	100	0
Ethernet 0/17	100	0	100	Auto	Enabled	100	0
Ethernet 0/18	100	0	100	Auto	Enabled	100	0
Ethernet 0/19	100	0	100	Auto	Enabled	100	0
Ethernet 0/20	100	0	100	Auto	Enabled	100	0
Ethernet 0/21	100	0	100	Auto	Enabled	100	0
Ethernet 0/22	100	0	100	Auto	Enabled	100	0
Ethernet 0/23	100	0	100	Auto	Enabled	100	0
Ethernet 0/24	100	0	100	Auto	Enabled	100	0
Ethernet 0/25	100	0	100	Auto	Enabled	100	0
Ethernet 0/26	100	0	100	Auto	Enabled	100	0
Ethernet 0/27	100	0	100	Auto	Enabled	100	0
Ethernet 0/28	100	0	100	Auto	Enabled	100	0
Ethernet 0/29	100	0	100	Auto	Enabled	100	0
Ethernet 0/30	100	0	100	Auto	Enabled	100	0
Ethernet 0/31	100	0	100	Auto	Enabled	100	0
Ethernet 0/32	100	0	100	Auto	Enabled	100	0
Ethernet 0/33	100	0	100	Auto	Enabled	100	0
Ethernet 0/34	100	0	100	Auto	Enabled	100	0
Ethernet 0/35	100	0	100	Auto	Enabled	100	0
Ethernet 0/36	100	0	100	Auto	Enabled	100	0
Ethernet 0/37	100	0	100	Auto	Enabled	100	0
Ethernet 0/38	100	0	100	Auto	Enabled	100	0
Ethernet 0/39	100	0	100	Auto	Enabled	100	0
Ethernet 0/40	100	0	100	Auto	Enabled	100	0
Ethernet 0/41	100	0	100	Auto	Enabled	100	0
Ethernet 0/42	100	0	100	Auto	Enabled	100	0
Ethernet 0/43	100	0	100	Auto	Enabled	100	0
Ethernet 0/44	100	0	100	Auto	Enabled	100	0
Ethernet 0/45	100	0	100	Auto	Enabled	100	0
Ethernet 0/46	100	0	100	Auto	Enabled	100	0
Ethernet 0/47	100	0	100	Auto	Enabled	100	0
Ethernet 0/48	100	0	100	Auto	Enabled	100	0
Ethernet 0/49	100	0	100	Auto	Enabled	100	0
Ethernet 0/50	100	0	100	Auto	Enabled	100	0
Ethernet 0/51	100	0	100	Auto	Enabled	100	0
Ethernet 0/52	100	0	100	Auto	Enabled	100	0
Ethernet 0/53	100	0	100	Auto	Enabled	100	0
Ethernet 0/54	100	0	100	Auto	Enabled	100	0
Ethernet 0/55	100	0	100	Auto	Enabled	100	0
Ethernet 0/56	100	0	100	Auto	Enabled	100	0
Ethernet 0/57	100	0	100	Auto	Enabled	100	0
Ethernet 0/58	100	0	100	Auto	Enabled	100	0
Ethernet 0/59	100	0	100	Auto	Enabled	100	0
Ethernet 0/60	100	0	100	Auto	Enabled	100	0
Ethernet 0/61	100	0	100	Auto	Enabled	100	0
Ethernet 0/62	100	0	100	Auto	Enabled	100	0
Ethernet 0/63	100	0	100	Auto	Enabled	100	0
Ethernet 0/64	100	0	100	Auto	Enabled	100	0
Ethernet 0/65	100	0	100	Auto	Enabled	100	0
Ethernet 0/66	100	0	100	Auto	Enabled	100	0
Ethernet 0/67	100	0	100	Auto	Enabled	100	0
Ethernet 0/68	100	0	100	Auto	Enabled	100	0
Ethernet 0/69	100	0	100	Auto	Enabled	100	0
Ethernet 0/70	100	0	100	Auto	Enabled	100	0
Ethernet 0/71	100	0	100	Auto	Enabled	100	0
Ethernet 0/72	100	0	100	Auto	Enabled	100	0
Ethernet 0/73	100	0	100	Auto	Enabled	100	0
Ethernet 0/74	100	0	100	Auto	Enabled	100	0
Ethernet 0/75	100	0	100	Auto	Enabled	100	0
Ethernet 0/76	100	0	100	Auto	Enabled	100	0
Ethernet 0/77	100	0	100	Auto	Enabled	100	0
Ethernet 0/78	100	0	100	Auto	Enabled	100	0
Ethernet 0/79	100	0	100	Auto	Enabled	100	0
Ethernet 0/80	100	0	100	Auto	Enabled	100	0
Ethernet 0/81	100	0	100	Auto	Enabled	100	0
Ethernet 0/82	100	0	100	Auto	Enabled	100	0
Ethernet 0/83	100	0	100	Auto	Enabled	100	0
Ethernet 0/84	100	0	100	Auto	Enabled	100	0
Ethernet 0/85	100	0	100	Auto	Enabled	100	0
Ethernet 0/86	100	0	100	Auto	Enabled	100	0
Ethernet 0/87	100	0	100	Auto	Enabled	100	0
Ethernet 0/88	100	0	100	Auto	Enabled	100	0
Ethernet 0/89	100	0	100	Auto	Enabled	100	0
Ethernet 0/90	100	0	100	Auto	Enabled	100	0
Ethernet 0/91	100	0	100	Auto	Enabled	100	0
Ethernet 0/92	100	0	100	Auto	Enabled	100	0
Ethernet 0/93	100	0	100	Auto	Enabled	100	0
Ethernet 0/94	100	0	100	Auto	Enabled	100	0
Ethernet 0/95	100	0	100	Auto	Enabled	100	0
Ethernet 0/96	100	0	100	Auto	Enabled	100	0
Ethernet 0/97	100	0	100	Auto	Enabled	100	0
Ethernet 0/98	100	0	100	Auto	Enabled	100	0
Ethernet 0/99	100	0	100	Auto	Enabled	100	0
Ethernet 0/100	100	0	100	Auto	Enabled	100	0

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 соединением точка-точка.

10.5.5 Защита от петель (Loop protection)

Когда используемая топология подключения стабильна, коммутатор получает BPDU пакеты от вышестоящего коммутатора. Если подключение неисправно или используется одностороннее 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.

10.5.5.1 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 значения 1-10 сек.
- ✓ Port Shutdown Time – время блокировки порта. По умолчанию 3 сек.

Apply – запомнить настройки.

10.5.5.2 Настройка портов для Loop Protection (Port Config)

Index	Element	#	Line	Loc
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
34				
35				
36				
37				
38				
39				
40				
41				
42				
43				
44				
45				
46				
47				
48				
49				
50				
51				
52				
53				
54				
55				
56				
57				
58				
59				
60				
61				
62				
63				
64				
65				
66				
67				
68				
69				
70				
71				
72				
73				
74				
75				
76				
77				
78				
79				
80				
81				
82				
83				
84				
85				
86				
87				
88				
89				
90				
91				
92				
93				
94				
95				
96				
97				
98				
99				
100				
101				
102				
103				
104				
105				
106				
107				
108				
109				
110				
111				
112				
113				
114				
115				
116				
117				
118				
119				
120				
121				
122				
123				
124				
125				
126				
127				
128				
129				
130				
131				
132				
133				
134				
135				
136				
137				
138				
139				
140				
141				
142				
143				
144				
145				
146				
147				
148				
149				
150				
151				
152				
153				
154				
155				
156				
157				
158				
159				
160				
161				
162				
163				
164				
165				
166				
167				
168				
169				
170				
171				
172				
173				
174				
175				
176				
177				
178				
179				
180				
181				
182				
183				
184				
185				
186				
187				
188				
189				
190				
191				
192				
193				
194				
195				
196				
197				
198				
199				
200				
201				
202				
203				
204				
205				
206				
207				
208				
209				
210				
211				
212				
213				
214				
215				
216				
217				
218				
219				
220				
221				
222				
223				
224				
225				
226				
227				
228				
229				
230				
231				
232				
233				
234				
235				
236				
237				
238				
239				
240				
241				
242				
243				
244				
245				
246				
247				
248				
249				
250				
251				
252				
253				
254				
255				
256				
257				
258				
259				
260				
261				
262				
263				
264				
265				
266				
267				
268				
269				
270				
271				
272				
273				
274				
275				
276				
277				
278				
279				
280				
281				
282				
283				
284				
285				
286				
287				
288				
289				
290				
291				
292				
293				
294				
295				
296				
297				
298				
299				
300				
301				
302				
303				
304				
305				
306				
307				
308				
309				
310				
311				
312				
313				
314				
315				
316				
317				
318				
319				
320				
321				
322				
323				
324				
325				
326				
327				
328				
329				
330				
331				
332				
333				
334				
335				
336				
337				
338				
339				
340				
341				
342				
343				
344				
345				
346				
347				
348				
349				
350				
351				
352				
353				
354				
355				
356				
357				
358				
359				
360				
361				
362				
363				
364				
365				
366				
367				
368				
369				
370				
371				
372				
373				
374				
375				
376				
377				
378				
379				
380				
381				
382				
383				
384				
385				
386				
387				
388				
389				
390				
391				
392				
393				
394				
395				
396				
397				
398				
399				
400				
401				
402				
403				
404				
405				
406				
407				
408				
409				
410				
411				
412				
413				
414				
415				
416				
417				
418				
419				
420				
421				
422				
423				
424				
425				
426				
427				
428				
429				
430				
431				
432				
433				
434				
435				

- ✓ 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.

10.5.6 Функция DHCP Snooping

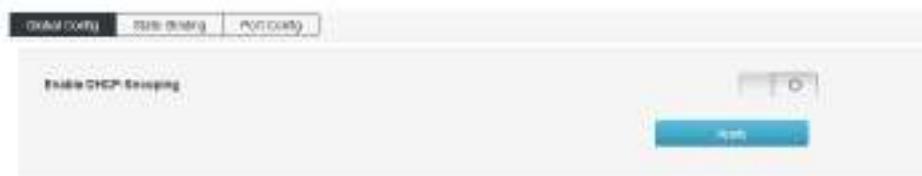
DHCP Snooping – это функция 2 уровня (Layer2), которая позволяет отбрасывать трафик DHCP, определенный как неприемлемый.

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.

10.5.6.1 Глобальные настройки DHCP Snooping (Global Config)



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

Для подтверждения настроек используйте кнопку Принять (Apply).

10.5.6.2 Постоянная привязка (Static Binding)

MAC	IP Address	Port	Age
00:0C:29:00:00:01	192.168.10.100	Ethernet 1/0/1	00:00:00:00:00:00
MAC-таблица коммутатора			
IP	Port	MAC	Age

На данной странице WEB интерфейса коммутатора находятся настройки постоянной привязки MAC и IP адресов. Таблица привязки помогает избежать атак 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:

№	Название	MAC	IP address	Тип	Порты	Опции	Удалить	Добавить
1	192.168.1.100	00-0C-29-00-00-01	192.168.1.100/24	Приемник	1-256			
2	192.168.1.101	192-00-00-00-00-01	192.168.1.101/24	Приемник	2-160			
3	192.168.1.102	00-0C-29-00-00-02	192.168.1.102/24	Приемник	3-160			

10.5.6.3 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 недоверенным (untrust).
- ✓ IPSG – вкл/выкл фильтрации исходных IP адресов на основе таблицы привязки.

10.5.7 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 подключен, в список её членов (для ретрансляции группового трафика). И наоборот: услышав запрос 'IGMP Leave' (покинуть), удаляет соответствующий порт из списка группы.

10.5.7.1 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

10.5.7.2 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.

10.5.7.3 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

10.5.8 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.

10.5.8.1 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/отключенными. Диапазон 0 – 1440.

10.5.8.2 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.

10.5.8.3 Аутентификация на основе портов (Port-based Authentication)

Port Name	Port Auth Enable	Port Auth Mode	ESSID	Channel	Beacon	Multi-Status	Beacon Period	Beacon Map	ESSID Period	Beacon Period	Authentication Mode
port 1-1	+	802.1x+TLS	802.1x+TLS	6	+	disabled	300	0	300	0	802.1x+TLS
port 1-2	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-3	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-4	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-5	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-6	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-7	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-8	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-9	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-10	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-11	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x
port 1-12	-	802.1x	802.1x	6	+	disabled	300	0	300	0	802.1x

- 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 аутентификации.

10.6 Управление настройками 3 уровня (Layer3 Management)

10.6.1 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 вводаIpv4 адреса сетевого интерфейса.

Interface	State	Mode	IPv4 Address	IPv6 Address	MAC	Enable
Ethernet 1	UP	Normal	192.168.1.100	2001:DB8::1	00:0C:29:00:00:01	On
Ethernet 2	DOWN	Normal				Off
Ethernet 3	UP	Normal	192.168.1.101	2001:DB8::2	00:0C:29:00:00:02	On
Ethernet 4	UP	Normal	192.168.1.102	2001:DB8::3	00:0C:29:00:00:03	On

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.
- IPv6 Address – поле отображает IPv6 адрес, если он был задан.
- MAC – поле отображает MAC адрес интерфейса.
- Enable – вкл/откл выбранного интерфейса.

10.6.2 Настройка маршрутизации (Routing Configuration)

10.6.2.1 Просмотр маршрутов (View the routing)

Id	Оригинал	Тип	Трасса	Дистанция	Статус	Тип маршрута
1	192.168.1.100	Direct	192.168.1.100	0	Up	Direct connection
2	192.168.1.101	Static	192.168.1.101	0	Up	Static routing
3	192.168.1.102	Dynamic	192.168.1.102	0	Up	Dynamic routing

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

10.6.2.2 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.



10.6.2.3 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

IP Address:	<input type="text" value="192.168.1.11"/>	Mac Address:	<input type="text" value="00:0C:29:00:00:00"/>
MAC Address:	<input type="text" value="00:0C:29:00:00:00"/>		
	<input type="button" value="OK"/>		
From:	IP Address:	Mac ID:	
You are trying to access from:			

- 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).

10.6.3 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.

10.6.3.1 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:	VLAN2	Less than 32 bytes.
Subnet segment:	192.168.20.0/24	For Example: 192.168.0.0/24
Begin IP:	192.168.20.1	
End IP:	192.168.20.254	
Lease time:	36000	Seconds
Default Gateway:	192.168.20.1	For Example: 192.168.0.1
DNS server 1:	192.168.20.1	For Example: 192.168.0.1
DNS server 2:	0.0.0.0	For Example: 192.168.0.1
Domain Name Service:		For Example: 192.168.0.1
NetBIOS server:		For Example: 192.168.0.1

[Add](#)

- 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:

Address Pool Name	Subnet Segment	Default Gateway	Start IP	End IP	Lease time	DNS server 1	DNS server 2	Domain Name Server	NetBIOS Server
Pool 1	192.168.1.0/24	192.168.1.1	192.168.1.1	192.168.1.254	2400	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1

10.6.3.2 Список клиентов с назначенными IP адресами (Client List)

IP Address	MAC Address	IP Address	User Name	Lease Time	Expires Time
192.168.1.100	00:0C:29:00:00:0A	192.168.1.100	user1	00:00:00:00:00:00	00:00:00:00:00:00

- ✓ 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.

10.6.3.3 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:



10.6.4 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.

10.6.4.1 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.

10.7 Дополнительные настройки (Advanced Settings)

10.7.1 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.

10.7.1.1 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 циклический 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.

10.7.1.2 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.

10.7.2 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.

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

The screenshot shows a configuration page for MAC ACL rules. On the left, there's a sidebar with navigation links: 'Layer 2', 'Action', 'Protocol', 'Source MAC', 'Source MAC Range', 'Destination MAC', 'Destination MAC Range', 'Priority', 'Protocol MAC Range', and 'Other Related Items'. The main area has several input fields:

- 'Layer 2' dropdown set to 'Layer 2'.
- 'Action' dropdown set to 'Allow'.
- 'Protocol' dropdown set to 'Any'.
- 'Source MAC' dropdown set to 'Any'.
- 'Source MAC Range' dropdown set to 'Any'.
- 'Destination MAC' dropdown set to 'Any'.
- 'Destination MAC Range' dropdown set to 'Any'.
- 'Priority' dropdown set to 'Any'.
- 'Protocol MAC Range' dropdown set to 'Any'.
- 'Other Related Items' dropdown set to 'Any'.

At the bottom, there are tabs for 'Layer 2', 'Basic', 'Advanced', 'Protocol MAC', 'Other Related Items', and 'Help'.

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 (unlimited).

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



10.7.2.2 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 – запретить 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 (unlimited).

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

Entry ID	Rule ID	Protocol	Source IP	Source Mask	Source Port	Destination IP	Destination Mask	Destination Port	Time-Range
100	100	-	192.168.1.100	255.255.255.0	100	192.168.1.101	255.255.255.0	100	-

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

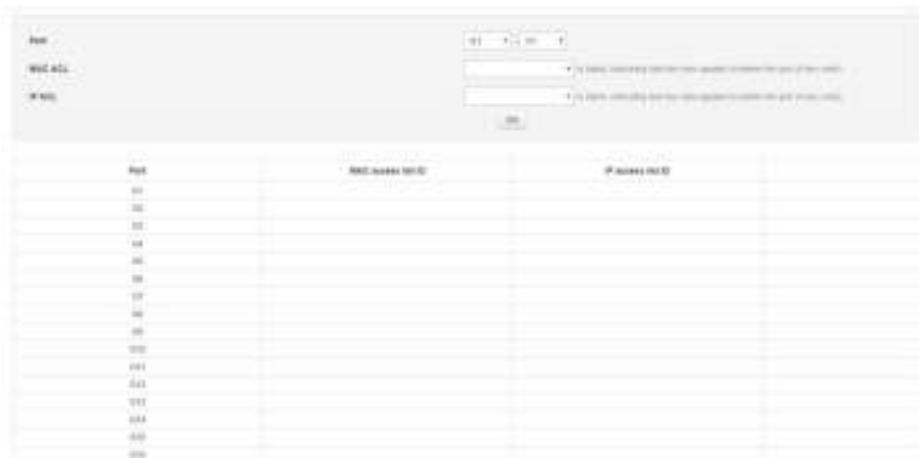
На данной странице WEB интерфейса коммутатора находятся настройки времени применения правил ACL. Такую фильтрацию трафика можно назвать временной фильтрацией, так как выбранные правила ACL будут применяться в выбранные промежутки времени (по расписанию).



- 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.

10.7.2.4 (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).

10.7.3 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 управляемой 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

10.7.3.1 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)

10.7.4 (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

10.7.4.1 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.

10.7.4.2 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.

10.7.4.3 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.

10.7.4.4 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.

10.7.5 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 (独一无二ному для протокола) и не передает дальше.

Multicast MAC-адрес (6 байт)	MAC-адрес отправителя (6 байт)	Ehtertype (2 байта)	DataUnit (1500 байт)	FSC (4 байта)
------------------------------	--------------------------------	---------------------	----------------------	---------------

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.

10.7.5.1 Глобальные настройки LLDP (Global Config)

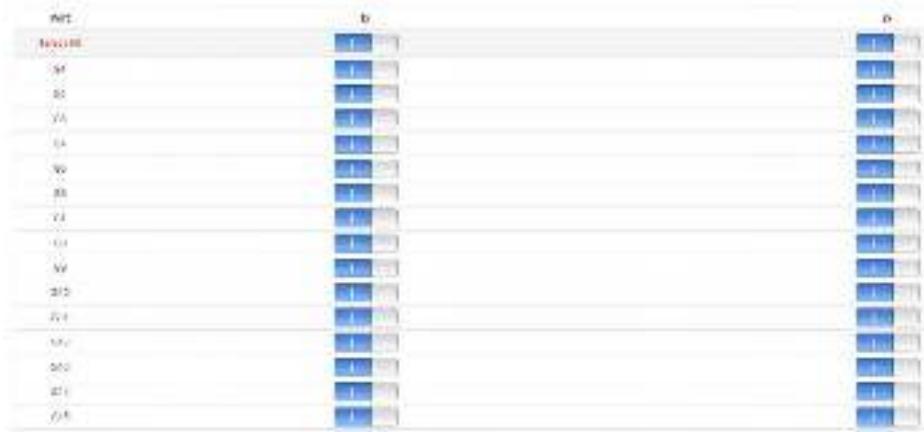
The screenshot displays the 'Global Config' tab of the LLDP configuration page. The left sidebar lists configuration items: LLDP, System Name, System Description, and System Capabilities. On the right, there are input fields for 'System Name' (containing 'D-Link DGS-1000G Switch'), 'System Description' (containing 'D-link DGS-1000G'), and 'System Capabilities' (containing 'Layer 2'). Below these are four checkboxes for 'LLDP Enabled' (selected), 'Port-based LLDP' (selected), 'System capability TLV' (selected), and 'System description TLV' (selected). A preview window on the right shows the current LLDP settings. At the bottom is a large blue 'Apply' button.

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 управляет 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.

10.7.5.2 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.

10.7.5.3 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.

10.7.6 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.

10.7.6.1 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.

10.7.6.2 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.

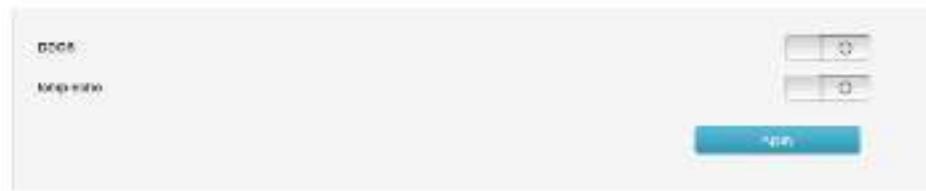
- ✓ Server – поле для ввода IP адреса сервера NTP. Например: 24.56.178.140 – для Америки.

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

10.7.7 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).

10.8 Настройки системы (System Management)

10.8.1 Настройки пользователя (User Settings)

The screenshot shows the 'User Settings' section of a network switch's configuration interface. On the left, there are three input fields: 'Login' (containing 'admin'), 'New Password' (containing '1234567890'), and 'Retype Password' (containing '1234567890'). Below these fields is a blue 'Apply' button.

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).

10.8.2 Сетевые настройки (Network Settings)

The screenshot shows the 'Network Settings' section of a network switch's configuration interface. On the left, there are three input fields: 'IP Address' (containing '192.168.1.1'), 'Gateway' (containing '192.168.1.2'), and 'DNS' (containing '8.8.8.8'). Below these fields is a blue 'Apply' button.

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).

10.8.3 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).

10.8.3.1 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».

10.8.3.2 Управление через SSH (SSH Service)

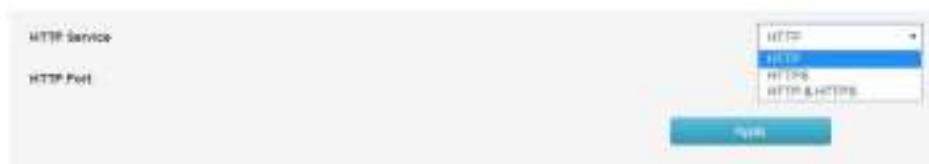
SSH – сетевой протокол прикладного уровня, позволяющий производить удалённое управление коммутатором.

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

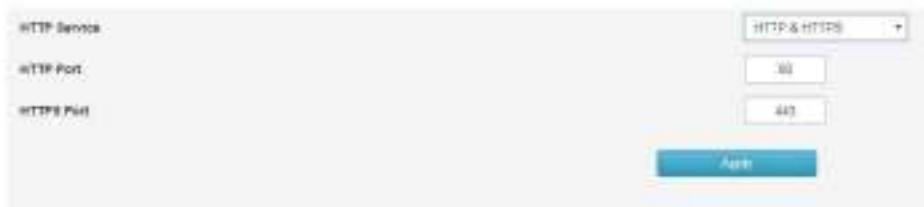
По умолчанию коммутатор использует протокол SSHv2 и порт 22.

10.8.3.3 Управление через HTTP (HTTP Service)

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



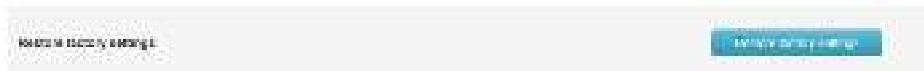
- ✓ HTTP – использовать только HTTP;
- ✓ HTTPS – использовать только HTTPS;
- ✓ HTTP&HTTPS – поддерживается и HTTP и HTTPS.



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

Пример подключения через WEB: <https://192.168.254.1>

10.8.4 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.

10.8.5 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 Firmware 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.

10.8.6 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).

10.8.6.1 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.

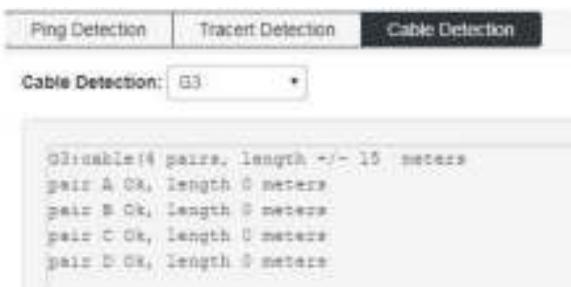
Нажмите кнопку PING, чтобы приступить к тестированию.

10.8.6.2 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.

10.8.6.3 Тест кабельного соединения (Cable Detection)



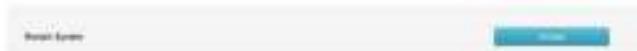
На данной странице WEB интерфейса находится инструмент, который может помочь сетевому администратору с диагностикой кабельного соединения на выбранном порте.

- ✓ 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.

10.8.7 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-24G4X-1L
Общее кол-во портов	28
Кол-во портов FE+PoE	-
Кол-во портов FE	-
Кол-во портов GE+PoE	24
Кол-во портов GE (не Combo порты)	
Кол-во портов Combo GE (RJ45+SFP)	-
Кол-во портов SFP (не Combo порты)	4x10G «SFP+» (10Гбит/с)
Встроенные оптические порты	-
Мощность PoE на один порт (макс.)	30 Вт
Суммарная мощность PoE всех портов (макс.)	400 Вт
Стандарты PoE	IEEE 802.3af IEEE 802.3at
Метод подачи PoE	Метод А 1/2(+), 3/6(-)
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)	95.232 МППС

Модель	SW-24G4X-1L
Поддержка jumbo frame	10 КБ
Размер flash памяти	16 МБ
Стандарты и протоколы	<ul style="list-style-type: none"> • IEEE 802.3 – 10BaseT • IEEE 802.3u – 100BaseTX • IEEE 802.3ab – 1000BaseT • IEEE 802.3z – 1000 BaseSX/LX • 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
Функции уровня L2	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • ARP Configuration • Routing Configuration • DHCP server • DHCP Relay • Support RIP V1/V2 protocols
Качество обслуживания (QoS)	8 очередей / порт
Безопасность	<ul style="list-style-type: none"> • Management System User Name/Password Protection • IEEE 802.1x Port-based Access Control • HTTP & SSL (Secure Web) • SSH v2.0 (Secured Telnet Session)

Модель	SW-24G4X-1L
Управление	<ul style="list-style-type: none"> • Управление через Web-интерфейс • CLI • Telnet • SNMP
Индикаторы	<ul style="list-style-type: none"> ✓ PWR – питание ✓ SYS – состояние системы ✓ XG1-XG4 – линк на SFP+ портах ✓ PoE – индикаторы PoE ✓ Link/Act – подключение/сет.активность
Грозозащита	4 kV, 8/20us для портов RJ-45
Питание	AC90-253V
Энергопотребление	<10 Вт – без PoE 410Вт – с PoE
Охлаждение	Активное (вентиляторы в корпусе)
Размеры (ШxВxГ) (мм)	440x44x320
Способ монтажа	в 19" стойку
Рабочая температура	-10...+50 °C
Дополнительно	Кнопки QOS Ai PoE CCTV VLAN для включения соответствующих режимов работы

* 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.

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

Составил: Елагин С.А.