**Инструкция по использованию приложения**

1. Форма авторизации
   * 1. Логин
     2. Пароль
     3. Адрес хоста

Логин и пароль проверяются при вводе регулярным выражением, допускающим только латиницу, цифры и символы “.” и “\_”.

IP маршрутизатора также проверяется регулярным выражением, которое гарантирует, что запись будет в виде четырех десятичных чисел значением от 0 до 255, разделенных точками.

1. Форма конфигурирования маршрутизатора

В случае успешной аутентификации открывается форма настройки маршрутизатора. Она содержит несколько категорий. Переключение между этими категориями осуществляется с помощью бокового выезжающего меню.

Меню включает в себя семь пунктов:

* + - 1. Основные настройки;
      2. Другие настройки;
      3. PoE настройка;
      4. Настройка портов;
      5. Wi-Fi;
      6. VLAN;
      7. Информация о фирме.

Рассмотрим каждую секцию более подробно.

1. **Основные настройки**

Эта вкладка содержит в себе следующие настройки:

1. Адрес хоста;
2. Маска подсети;
3. MAC-адрес;
4. Модель;
5. Версия прошивки;
6. Native VLAN;
7. Storm control;
8. Шлюз;
9. Описание.

Адрес хоста, маска подсети и шлюз проверяются тем же регулярным выражением, что IP маршрутизатора на форме авторизации. Пользователь заранее уведомляется о неизменяемости некоторых полей: поле является неизменяемым, если около поля ввода установлена метка “\*”. Такими являются поля, содержащие MAC-адрес, модель маршрутизатора, версию прошивки.

Если пользователь изменяет IP-адрес хоста, маску подсети или шлюз, то маршрутизатору посылается запрос на перезагрузку и пользователь автоматически деавторизовывается, т.е. переносится на форму авторизации.

Есть возможность выбрать Native VLAN, который создан для повышения безопасности маршрутизатора. Если его установить, то указанный VLAN сможет получать все пакеты, не отнесённые ни к одной VLAN.

**VLAN** (Virtual Local Area Network) — представляет собой логическую сеть группировка, которая ограничивает широковещательный домен. Это позволяет изолировать сетевой трафик, поэтому только члены VLAN получают трафик из одних и тех же VLAN членов.

Также можно включить\выключить функцию контроля так называемого широковещательного шторма. Допустимые значения: выключено, 10%, 20%, 40%.

**Широковещательный шторм** (англ. Broadcast storm) — лавина (всплеск) широковещательных пакетов (на втором уровне модели OSI — кадров). Размножение широковещательных сообщений активным сетевым оборудованием приводит к экспоненциальному росту их числа и парализует работу сети. Считается нормальным, если широковещательные пакеты составляют не более 10 % от общего числа пакетов в сети.

Широковещательный шторм может возникать как результат появления некорректно сформированных широковещательных сообщений, в том числе действиями злоумышленников. Также довольно часто к шторму приводит некорректная настройка протокола Spanning Tree, поскольку в заголовке пакетов Ethernet нет информации о времени жизни кадра, как, например, у пакетов IP.

**Spanning Tree Protocol** (STP, протокол остовного дерева) — канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

1. **Другие настройки**

Эта секция включает следующие вкладки:

1. Аккаунт;
2. Восстановление;
3. Перезагрузка;
4. Обновление.

Аккаунт

1. Логин;
2. Старый пароль;
3. Новый пароль;
4. Подтверждение пароля.

На этой вкладке пользователь может сменить пароль. После завершения операции нужно будет повторно авторизоваться.

Восстановление

По нажатию на кнопку «Сбросить» произойдет восстановление системы, что приведет к сбросу настроек к заводским. Пользователь будет автоматически деавторизован.

Перезагрузка

По нажатию на кнопку «Перезагрузить» произойдет перезагрузка маршрутизатора. Пользователь будет автоматически деавторизован.

Обновление

На этой вкладке можно выбрать файл c последним обновлением прошивки (расширение .bin) и затем подождать пока пересылка файла пройдет успешно. Далее произойдет автоматическая перезагрузка маршрутизатора и деавторизация пользователя.

1. **PoE настройка**

В этой секции лишь одна вкладка: настройка питания через Ethernet.

**Power over Ethernet (PoE)** — технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными, через стандартную витую пару в сети Ethernet. Данная технология предназначается для IP-телефонии, точек доступа беспроводных сетей, IP-камер, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Отображаются следующие параметры для каждого из портов:

1. Состояние;
2. Потребление энергии (Вт);
3. Текущее использование энергии (мА);
4. Предельная мощность (Вт);
5. Приоритет.

Есть возможность обновления отображаемых данных на странице, а также изменения некоторых параметров, в частности, состояния и приоритета.

1. **Настройка портов**

Данная секция позволяет просмотреть\настроить некоторые параметры портов. включает несколько вкладок:

1. Состояние;
2. Настройка;
3. Счетчики;
4. Магистральный порт.
   1. Состояние

Для каждого из портов отображает список параметров. Эта форма не является редактируемой. Есть возможность обновления данных.

Параметры:

1. Соединение;
2. Скорость;
3. Дуплекс;
4. Управление потоком.
   1. Настройка

Для каждого из портов позволяет редактировать список параметров. Есть возможность обновления данных, что отображаются на странице.

1. Режим;
2. Управление потоком;
3. Приоритет 802.1р;
4. Базовый приоритет;
5. Описание порта.

Режим скорости может принимать одно из значений: Auto, 100 Мб (Full), 100 Мб (Half), 10 Мб (Full), 10 Мб (Half).

Можно включить\выключить управление потоком и функцию приоритетов 802.1p.

Стандарт IEEE 802.1p определяет поведение коммутаторов при обработке маркированных кадров с использованием приоритезации. Коммутатор, поддерживающий приоритезацию, должен иметь для каждого порта несколько выходных очередей, в которые помещаются кадры в зависимости от их приоритета. Дисциплина обслуживания этих очередей определяется при конфигурировании маршрутизатора. Необходимость приоритезации трафика появляется с введением мультимедийных приложений, чувствительных к задержкам.

Базовый приоритет может быть нормальным либо высоким.

* 1. Счетчики

Форма отображает значения списка параметров для каждого из портов. А именно:

* Количество RX-пакетов;

Количество пакетов, полученных на порт (включая одноадресные пакеты);

* Количество RX-байт;

Количество октетов данных (в том числе и в плохих пакетах), полученных на порт.

* Количество ошибок;
* Количество TX-пакетов;

Количество пакетов, переданных на порт (включая одноадресные пакеты);

* Количество TX-байт;

Количество октетов данных (в том числе и в плохих пакетах), переданных по порту.

* Количество коллизий.
  1. Магистральный порт

**Магистральный порт** или **Trunk port** — это канал типа «точка-точка» между коммутатором и другим сетевым устройством. Магистральные подключения служат для передачи трафика нескольких VLAN через один канал и обеспечивают им доступ ко всей сети.

После включения функции магистрального порта, порт 7 и порт 8 должны быть подключены к другому сетевому устройству, которое

также поддерживает функцию магистрального порта, чтобы удвоить пропускную способность между ними. В противном случае, если подключенное устройство не поддерживает эту функцию, то это вызовет петлю сети и вешает всю сеть.

1. **Wi-Fi**

Эта форма включает в себя две вкладки:

1. Wi-Fi
2. Доступные сети
   1. Wi-Fi

Здесь производится настройка точки доступа.

1. Имя беспроводной сети (SSID);
2. Частотный диапазон;
3. Статус.
   1. Доступные сети

На этой вкладке есть возможность подключить маршрутизатор к Wi-Fi сети. В этом случае возможна потеря соединения с ним. Пользователь об этом заранее предупреждается. Есть возможность обновления списка доступных сетей.

1. **VLAN**

Как уже было сказано, виртуальная локальная сеть (VLAN) представляет собой логическую сетевую группировку, которая ограничивает широковещательный домен (второй уровень OSI). Это позволяет изолировать сетевой трафик, поэтому только члены VLAN получают трафик из одних и тех же VLAN членов. В принципе, создание VLAN от маршрутизатора является логическим эквивалентом переподключения группы сетевых устройств к другому маршрутизатору. Тем не менее, все сетевые устройства по-прежнему подключаются к одному устройству физически.

Обозначение членства в VLAN может производиться несколькими способам. В нашем случае, осуществляется по порту (port-based). В этом случае порту коммутатора вручную назначается одна VLAN. Только одна VLAN может получать все пакеты, не отнесённые ни к одной VLAN, так называемая, Native VLAN. Сетевой коммутатор будет добавлять метки данной VLAN ко всем принятым кадрам, не имеющим никаких меток.

По умолчанию, включена поддержка VLAN на стандарте IEEE 802.1Q.

**IEEE 802.1Q** — открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN.

VLAN позволяет сети быть сегментированной для того, чтобы уменьшить размер широковещательных доменов. VLAN также может обеспечить уровень безопасности вашей сети. IEEE 802.1Q VLAN будет отображаться только пакеты между станциями, которые являются членами VLAN.

802.1Q не изменяет заголовки кадра, поэтому сетевые устройства, которые не поддерживают этот стандарт, могут передавать трафик без учёта его принадлежности к VLAN. 802.1Q помещает внутрь фрейма тег, который передает информацию о принадлежности трафика к VLAN.

Приложение позволяет выбрать один из трех режимов:

* Без VLAN;
* VLAN на основе портов;
* 802.1Q VLAN

Ниже на скриншотах отображены 2 состояния этой формы: при выбранных «Без VLAN» и «VLAN на основе портов» режимах. При выборе этих режимов отображается таблице, в которой с помощью checkbox-ов можно указать принадлежность каждого из портов к какой-то VLAN.

В случае 802.1Q VLAN есть два новых параметра:

* PVID (Port VLAN identifier)

Можем присвоить PVID для выбранного порта. Диапазон: 1-4094.

PVID будут вставлены во все немаркированные кадров, входящих в указанный порт.

* Тегирование трафика
* Untagged: исходящие кадры без VLAN-тега;
* Tagged: исходящие кадры с VLAN-тегом.

**7. Информация о фирме**

Выводится информация о фирме-производителе и о способах связаться с ней.