Инструкция по настройке соединения между двумя подсетями через маршрутизаторы EDR-810-VPN-2GSFP

Для организации защищенного канала связи между двумя удаленными подсетями необходимо настроить VPN-туннель.

В данной инструкции рассматривается пример построения Open VPN-туннеля между двумя маршрутизаторами EDR-810-VPN-2GSFP.

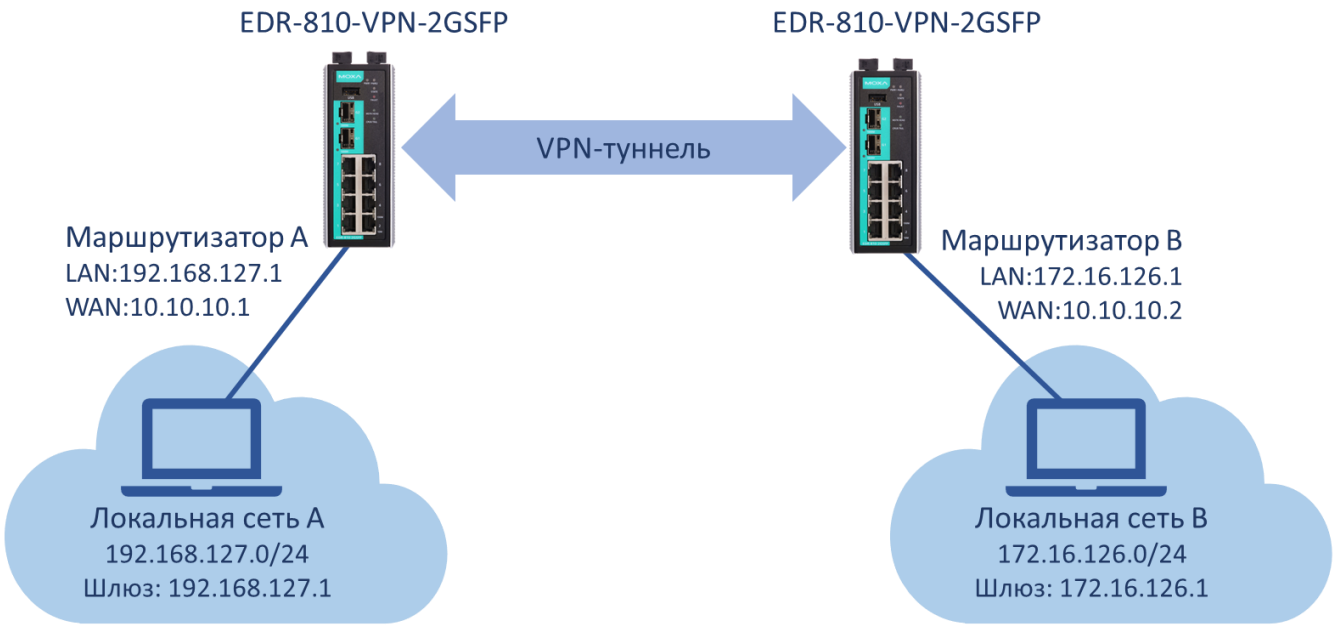


рис. 1 «Схема сети»

В таблице 1 указана адресация всей системы, согласно которой будем настраивать оборудование.

Таблица 1 «Адресация сети»

	IP-адрес	Маска подсети	Основной шлюз
Маршрутизатор A LAN-интерфейс	192.168.127.1	255.255.255.0	
Маршрутизатор A WAN-интерфейс	10.10.10.1	255.255.255.240	xxx.xxx.xxx.xxx
Ноутбук подсети A	192.168.127.13	255.255.255.0	192.168.127.1
Маршрутизатор B LAN-интерфейс	172.16.126.1	255.255.255.0	
Маршрутизатор B WAN-интерфейс	10.10.10.2	255.255.255.240	xxx.xxx.xxx.xxx
Ноутбук подсети B	172.16.126.13	255.255.255.0	172.16.126.1

xxx.xxx.xxx.xxx – основной шлюз WAN сети зависит от построения системы или выдается провайдером связи. В примере на рисунке 1 – соединение между маршрутизатором сети A и B прямое, поэтому шлюз указывать не нужно.

Все настройки маршрутизаторов осуществляются через web-интерфейс.

По умолчанию маршрутизаторы EDR-810-VPN-2GSFP имеют следующие параметры:

ip-адрес: 192.168.127.254
логин: admin
пароль: moxa

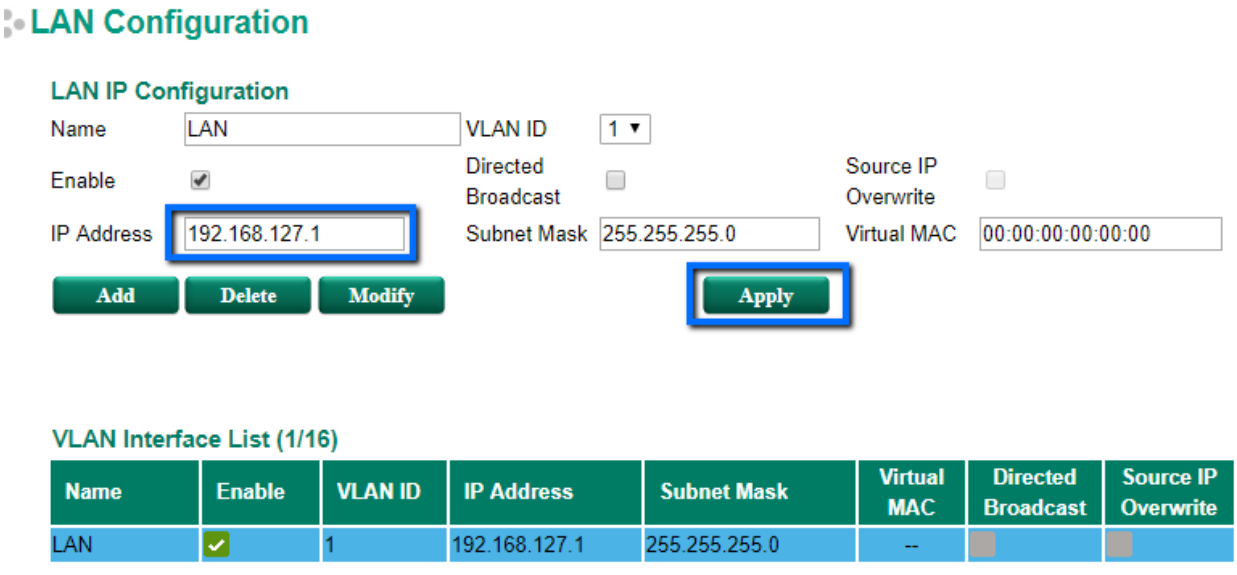
В целях безопасности рекомендуется изменить данные для входа.

После внесения любых изменений в настройки маршрутизатора необходимо нажимать кнопку **Apply** для сохранения изменений.

1. Настройка Маршрутизатора A

1.1. Настройка LAN-интерфейса

IP-адрес и маска подсети (согласно Таблице 1) задаются в разделе ***Network – Interface - LAN***



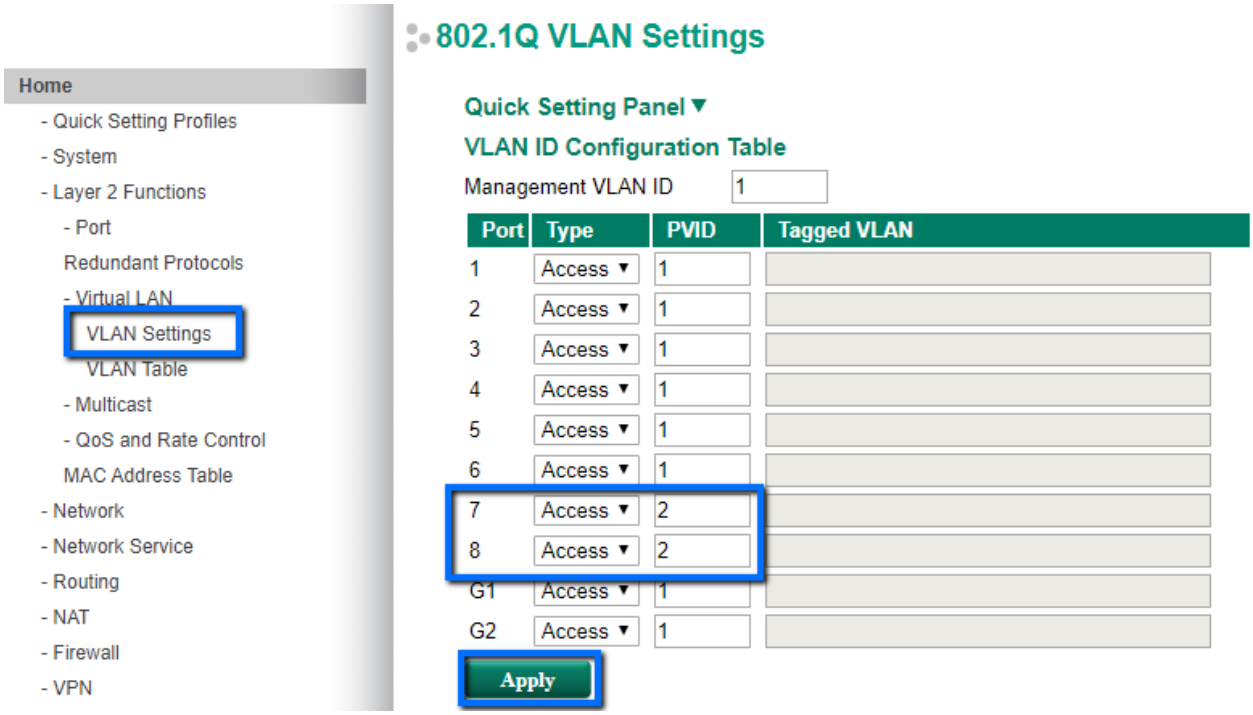
1.2. Настройка WAN-интерфейса

Маршрутизатор EDR-810 имеет 10 портов, каждый из которых можно назначить LAN или WAN-интерфейсом. Поэтому прежде, чем задавать адресацию на WAN-интерфейсе, нужно установить порты, которые будут относиться к WAN. Для этого необходимо поместить их в отдельную VLAN.

- Настройка VLAN

VLAN настройки осуществляются в разделе ***Layer 2 Functions - Virtual LAN - VLAN Settings***.

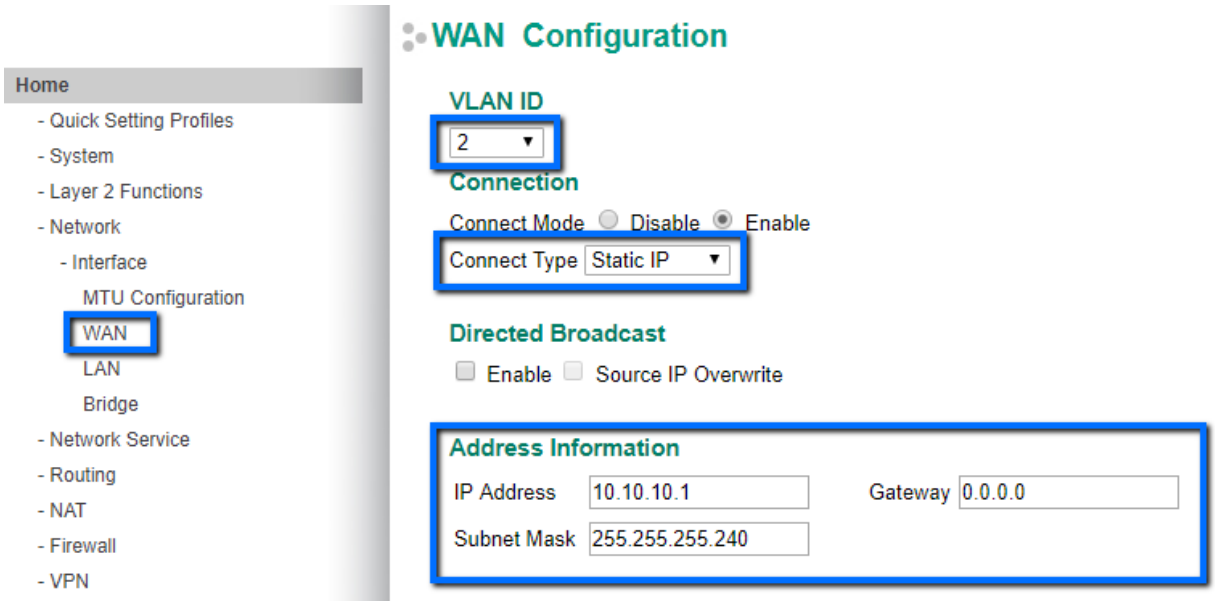
Порты 7 и 8 маршрутизатора будут относиться к WAN-интерфейсу. На этих портах указываем VLAN ID 2.



Когда отдельная VLAN для WAN-портов создана, можно перейти к назначению адресации.

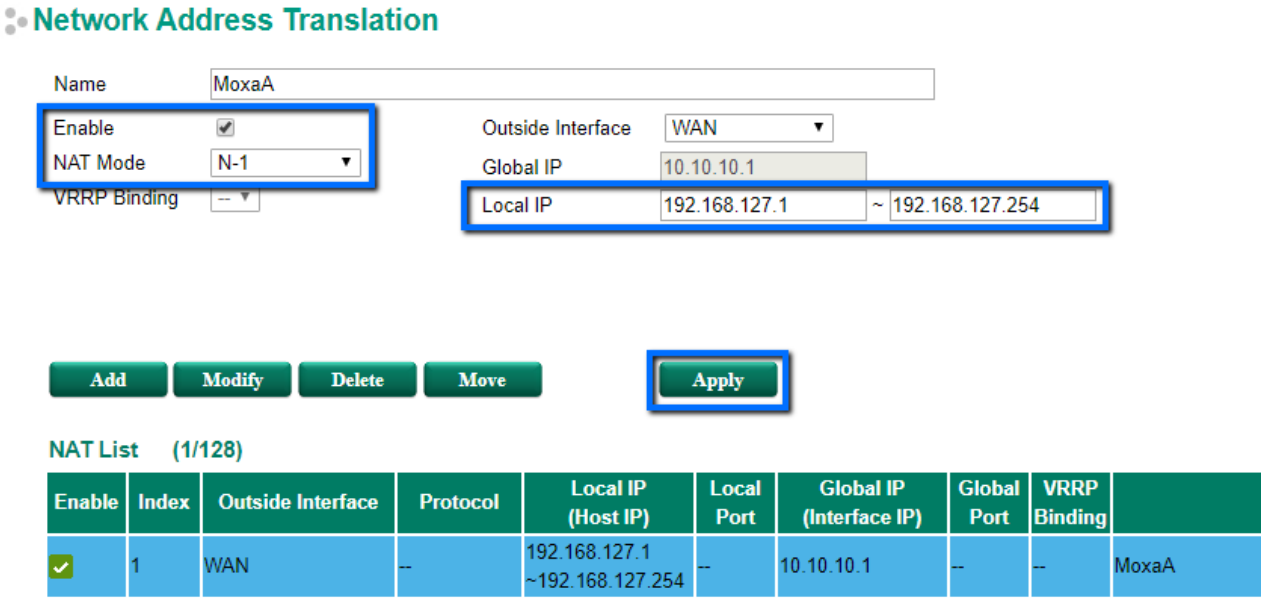
- Адресация WAN-интерфейса

В разделе ***Network – Interface – WAN*** назначается IP-адрес, маска сети и шлюз по умолчанию согласно Таблице 1.



1.3. Настройка NAT

Для того чтобы маршрутизатор подменял адреса локальной сети на внешний адрес при передаче во внешнюю сеть, необходимо настроить NAT в разделе ***NAT - NAT Setting***

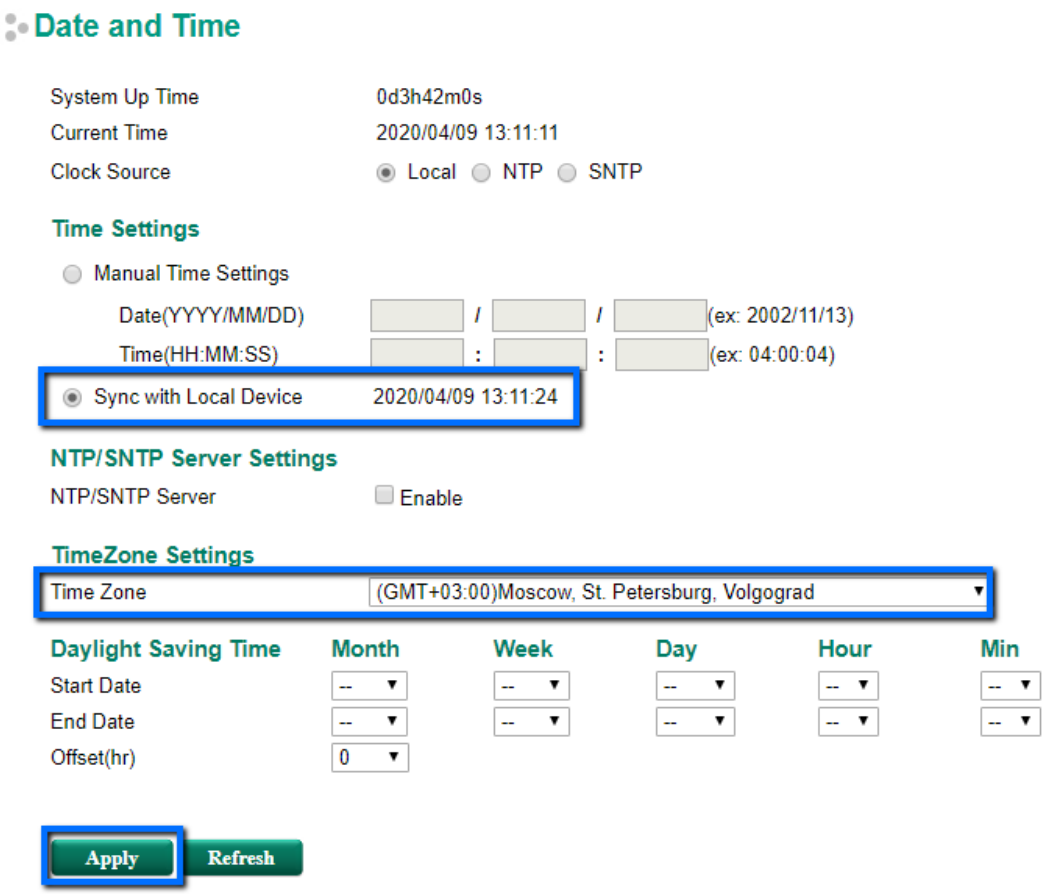


1.4. Настройка даты и времени

Для выполнения корректного соединения между VPN-сервером и VPN-клиентом необходимо, чтобы маршрутизаторы были синхронизированы в настройках даты и времени.

Настройка системного времени осуществляется в разделе ***System - Date and Time.***

Можно осуществить синхронизацию локальную или по протоколу SNTP.



2. Настройка Маршрутизатора B

Для настройки Маршрутизатора B необходимо повторить шаги 1.1 – 1.4, указывая параметры в соответствии с Таблицей 1.

3. Настройка VPN-туннеля

3.1. Предустановка сертификатов безопасности

Аутентификация при установке Open VPN-туннеля осуществляется с помощью сертификатов безопасности, а авторизация пользователя с помощью логина и пароля.

Сгенерировать сертификаты безопасности можно с помощью различных программ, а также можно создать их на самом маршрутизаторе.

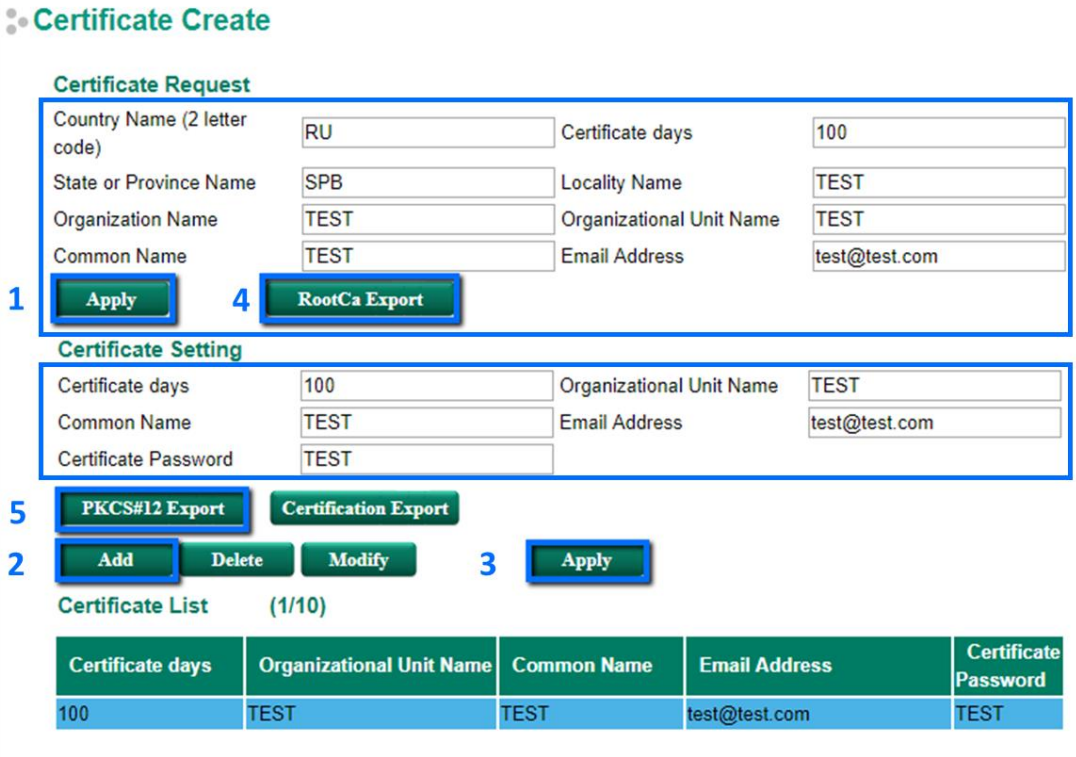
- Создание сертификатов безопасности

В разделе ***Certificate Management - CA Server - Certificate Create*** нужно выполнить несколько шагов:

- Заполнить таблицу ***Certificate Request***, нажать кнопку ***Apply***
- Заполнить таблицу ***Certificate Setting***, нажать кнопку ***Add*** и затем ***Apply***
- Выгрузить сертификат ***RootCA*** с помощью кнопки ***RootCA Export***
- Сгенерировать сертификат с помощью кнопки ***PKCS#12 Export***

(необходимо время на создание файлов с сертификатами, нужно немного подождать и повторно нажать на кнопки ***Export***)

Нужно создать сертификаты на одном маршрутизаторе и загрузить их на два маршрутизатора (на VPN-сервер и VPN-клиент).



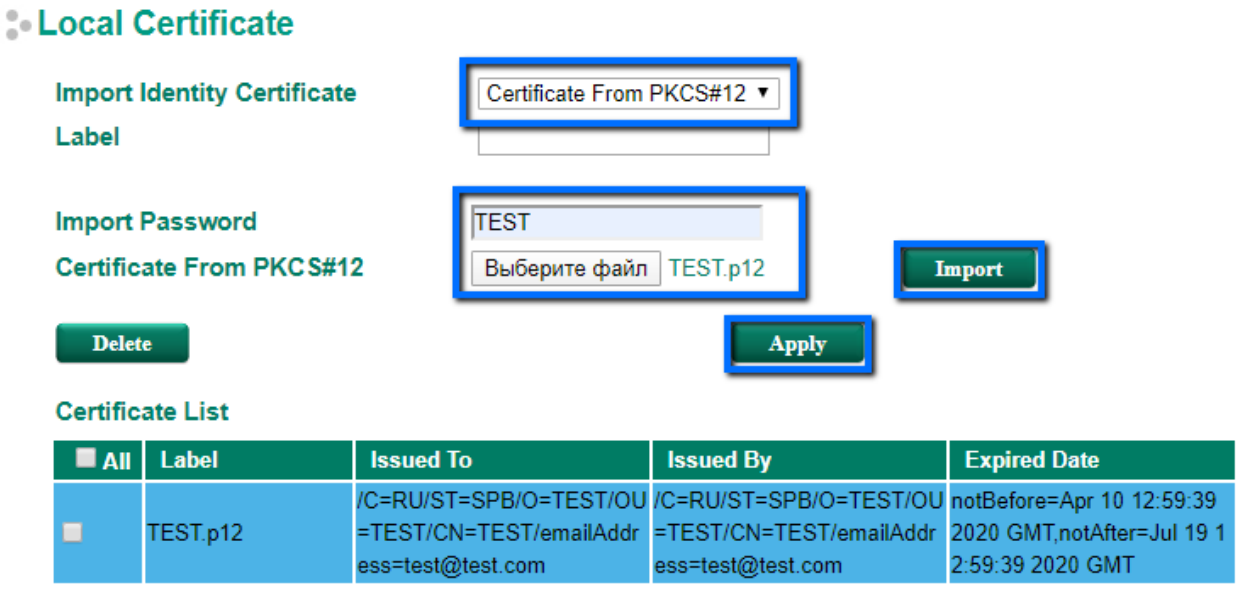
- Загрузка сертификатов на маршрутизаторы

Оба сертификата нужно загрузить на каждый маршрутизатор в раздел ***Certificate Management***, но в разные подразделы в соответствии с таблицей 2.

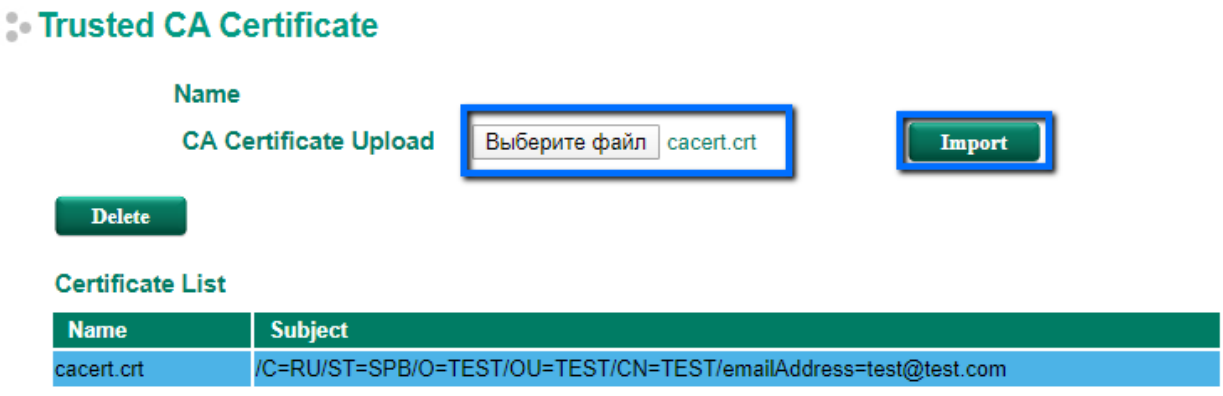
Таблица 2 «Сертификаты безопасности»

Место загрузки	Тип сертификата	Название сертификата
Trusted CA Certificate	RootCA	Cacert.crt
Local Certificate	PKCS	TEST.p12

В раздел ***Certificate Management - Local Certificate*** загружается PKCS сертификат



В раздел ***Certificate Management - Trusted CA Certificate*** загружается Root сертификат



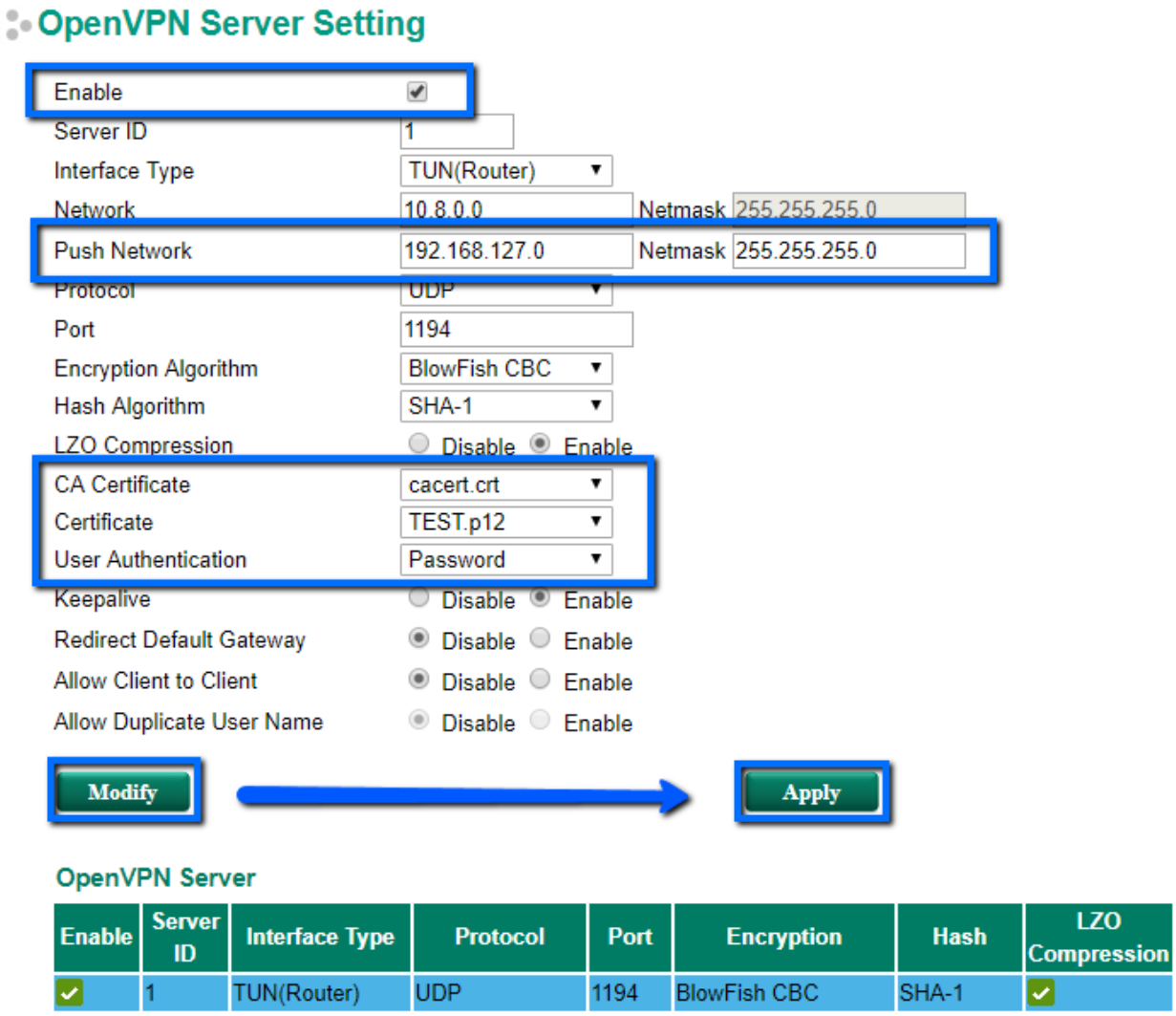
3.2. Настройка Open VPN-сервера

Маршрутизатор A будет выступать в качестве Open VPN-сервера, то есть будет ожидать подключения от удаленной подсети.

Настройки Open VPN Сервера осуществляются в разделе нужно активировать VPN-туннель в разделе ***VPN – OpenVPN.***

- Активация Open VPN-сервера

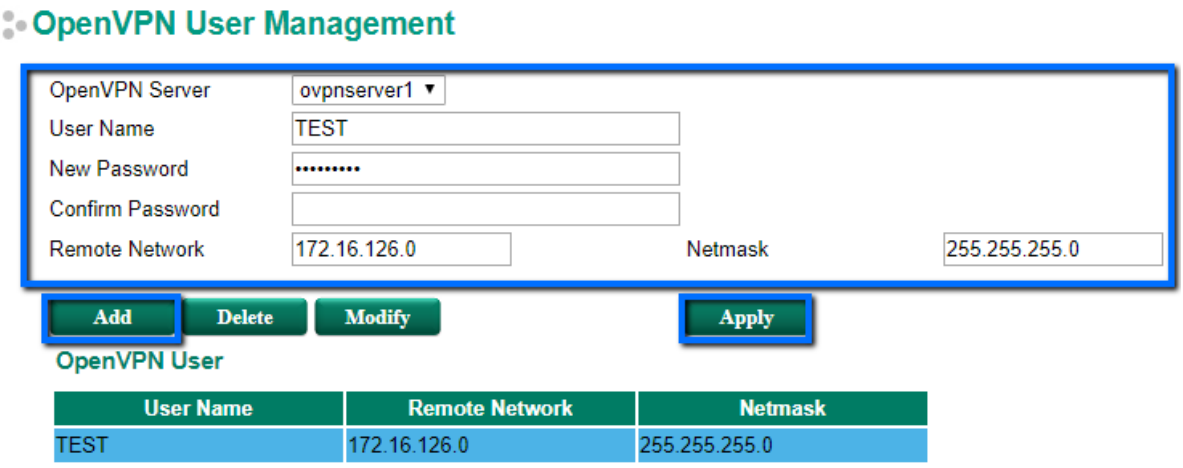
В разделе ***VPN – OpenVPN - OpenVPN Server - Server Setting*** активируется VPN туннель. В качестве ***Push Network*** указывается локальная сеть Сервера, а ***Network*** – любая незадействованная виртуальная подсеть.



Сертификаты безопасности автоматически будут установлены те, что были загружены в соответствующие разделы. Для авторизации пользователей выбирается вариант - ***password***.

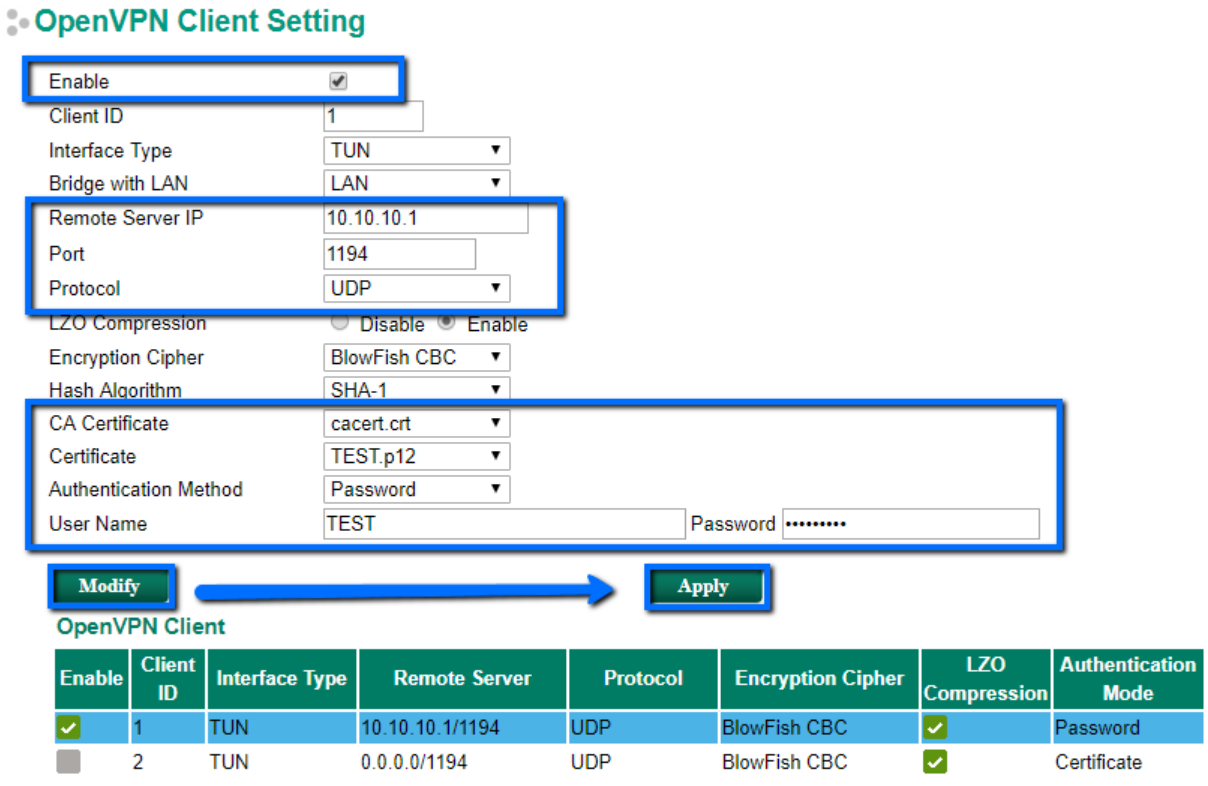
- Создание таблицы пользователей

В разделе ***VPN – OpenVPN - OpenVPN Server - User Management*** нужно указать локальную подсеть удаленного Open VPN-клиента и придумать логин и пароль для пользователей.



3.3. Настройка Open VPN-клиента

В разделе ***VPN – OpenVPN - OpenVPN Client - Client Setting*** выполняются настройки Open VPN-клиента.



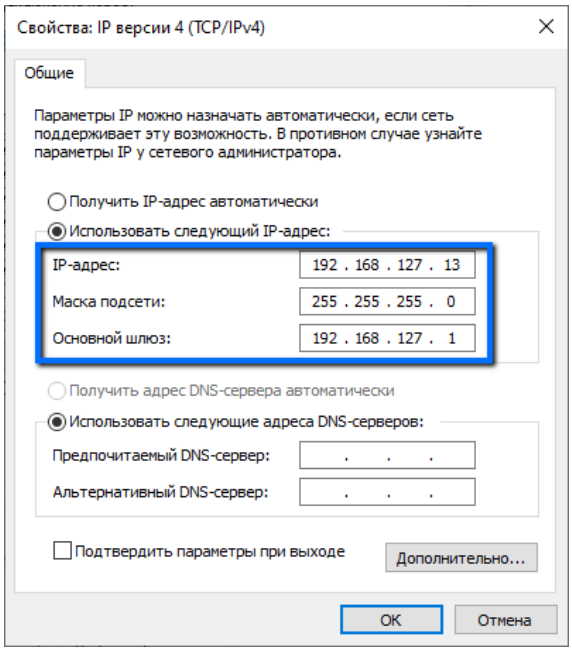
В качестве ***Remote Server*** нужно указать WAN ip-адрес Маршрутизатора А и выбрать такие же сертификаты, как установлены на VPN-сервере.

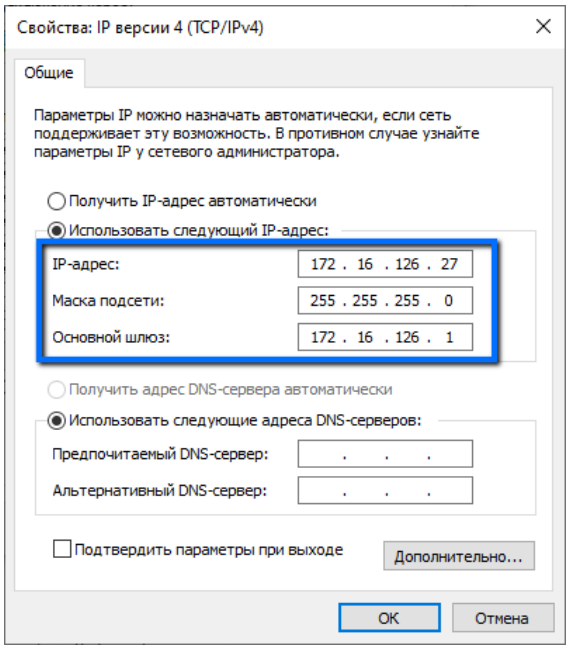
User Name и ***Password*** должны соответствовать данным, указанным в настройках пользователей на VPN-сервере.

3.4. Настройка устройств в локальных сетях

На устройствах в локальных сетях необходимо указать основной шлюз – LAN адрес маршрутизатора в соответствии с Таблицей 1.

Для локальной сети A: 192.168.127.1
Для локальной сети B: 172.16.126.1

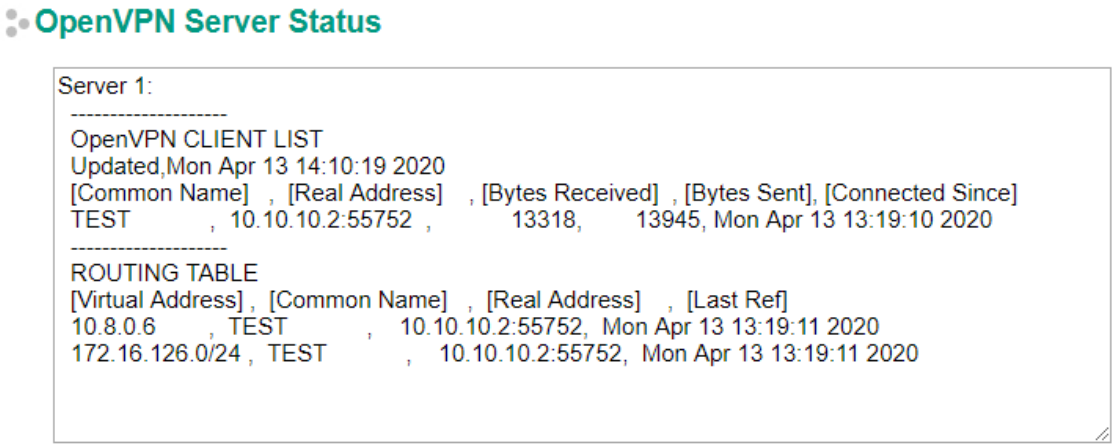




3.5. Диагностика VPN-соединения

После выполнения вышеуказанных настроек на двух маршрутизаторах будет установлено VPN-соединение.

На VPN-сервере в разделе ***VPN – OpenVPN - OpenVPN Server - OpenVPN Server Status*** появится запись об установленном VPN-соединении с определенным клиентом и добавится маршрут для доступа в новую подсеть.



На VPN-клиенте в разделе ***VPN – OpenVPN - OpenVPN Client - OpenVPN Client Status*** появится информация об успешном соединении.

OpenVPN Client Status

```
Client 1:
  State: Connected
  OpenVPN STATISTICS
  Updated,Mon Apr 13 15:06:37 2020
  TUN/TAP read bytes,0
  TUN/TAP write bytes,0
  TCP/UDP read bytes,4407
  TCP/UDP write bytes,3082
  Auth read bytes,832
  pre-compress bytes,0
  post-compress bytes,0
  pre-decompress bytes,0
  post-decompress bytes,0
  END

Client 2:
  client is not enabled
```

Кроме того, при успешном установлении VPN-туннеля на маршрутизаторах загорится индикатор VPN.