

Инструкция по настройке VPN-соединения между модемом OnCell G3110 и маршрутизатором EDR-G903

Оборудование.

1. Маршрутизатор EDR-G903
2. Модем OnCellG3110
3. 2 компьютера

Топология сети

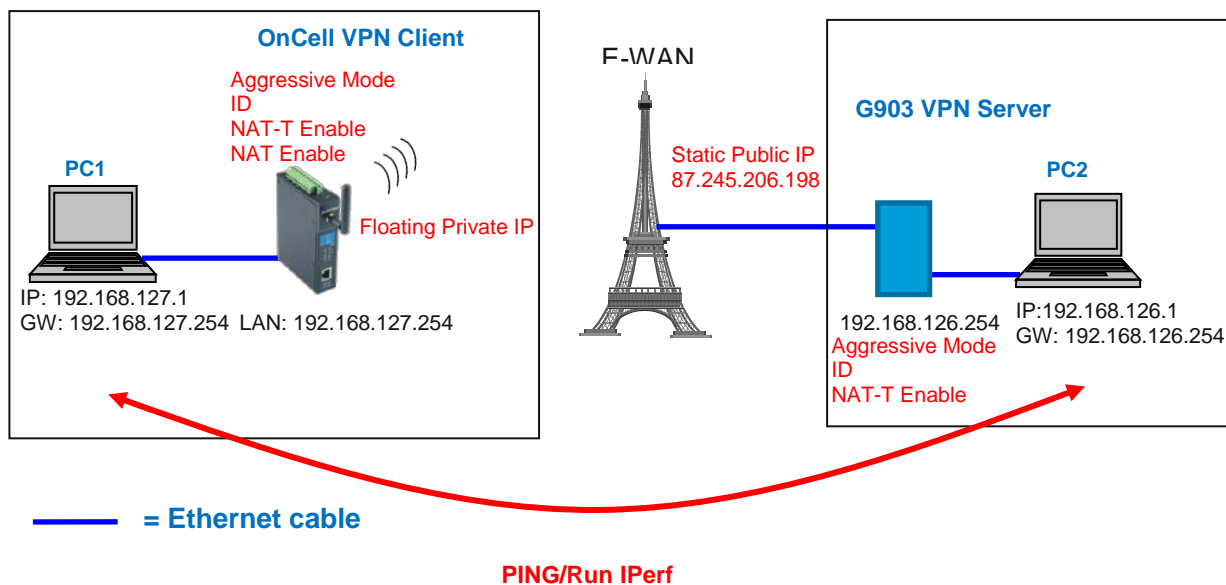


Рис. 1

С одной стороны имеем модем OnCell G3110, имеющий выход в интернет через Floating IP, выделяемый провайдером. Модем является шлюзом для сети 192.168.127.X и имеет в этой сети IP-адрес 192.168.127.254. С другой стороны – маршрутизатор, имеющий выход в интернет через статический IP-адрес, выделенный провайдером (в рассматриваемом примере – 87.245.206.198). Маршрутизатор является шлюзом для сети 192.168.126.X и имеет в этой сети IP-адрес 192.168.126.254. Модем является VPN-клиентом, а коммутатор VPN-сервером. **Обратите внимание, что при настройке туннеля VPN по протоколу IPSec, необходимо, чтобы локальные сети с одной и с другой стороны не пересекались!**

Настройка VPN-сервера.

1. С помощью браузера откройте WEB-интерфейс коммутатора EDR-G903.
2. В пункте меню Network/Interface/WAN1 укажите конфигурацию, выданную провайдером (статический IP-адрес, маску подсети, шлюз и DNS-сервер). Нажмите кнопку Activate.

WAN1 Configuration

Connection
 Connect Mode Disable Enable
 Connect Type

Address Information
 IP Address Gateway
 Subnet Mask

PPTP Dialup
 PPTP Connection Enable
 User Name IP Address
 Password

DNS (Optional for dynamic IP or PPPoE Type)
 Server 1 Server 2 Server 3

Рис. 2

- В пункте меню Network/Interface/LAN укажите конфигурацию порта LAN в локальной сети. Нажмите кнопку Activate.

LAN Configuration

LAN IP Configuration
 IP Address (ex. 192.168.1.1)
 Subnet Mask (ex. 255.255.255.0)

Рис. 3

- Настройте правило NAT в пункте меню NAT/NAT Setting, как показано на рисунке 4. В поле LAN IP Range укажите диапазон IP-адресов локальной сети, для которых будет действовать данное правило NAT. Нажмите кнопку New/Insert и Activate.

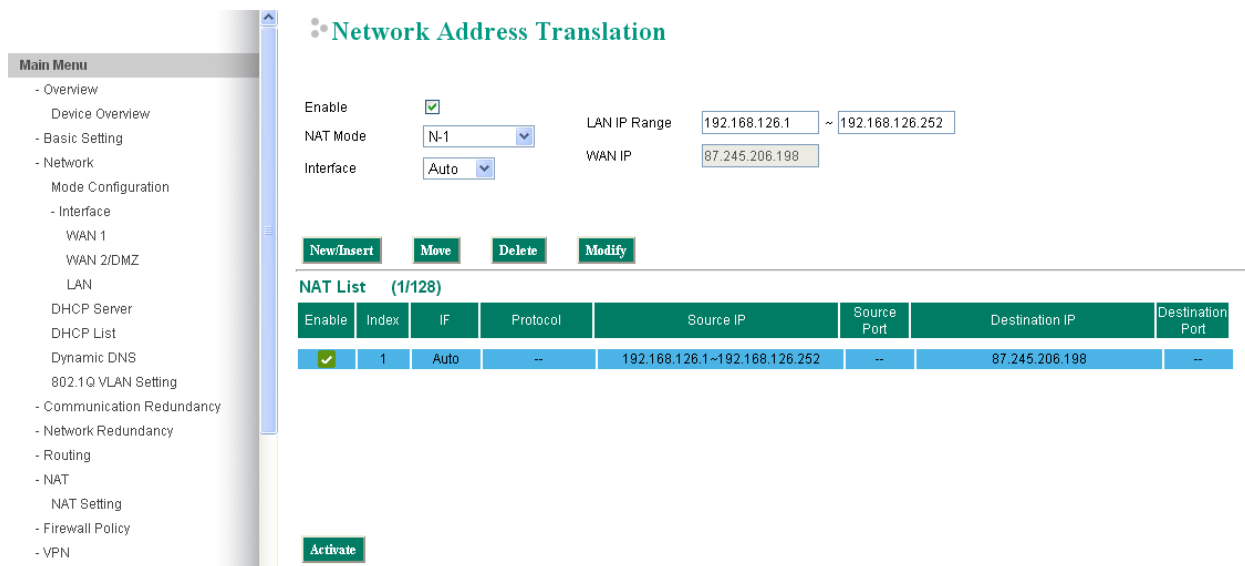


Рис. 4

5. Включите VPN-сервер в пункте меню VPN/IPSec/Global Settings. Там же включите функцию IPsec NAT-T Enable, нажмите кнопку Activate.



Рис. 5

6. Задайте настройки VPN-тоннеля. В пункте меню VPN/IPSec/IPsec Setting задайте настройки, как показано на рисунках 6 и 7. Адреса локальной и удалённой сети укажите свои (в примере - 192.168.126.0 и 192.168.127.0 соответственно).

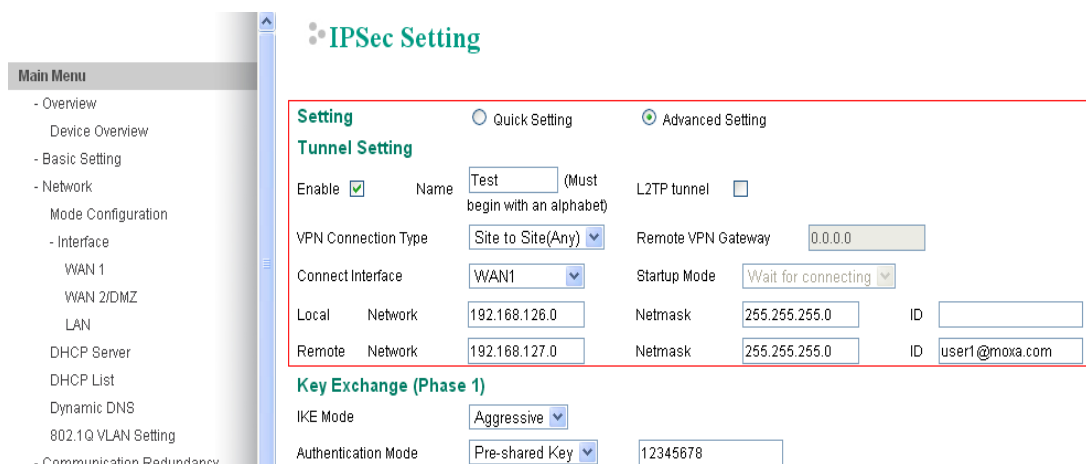


Рис. 6

В поле Pre-Shared Key укажите секретный ключ, с помощью которого устройства будут получать доступ к VPN-серверу. Для безопасности ваших данных, выберите как можно более сложный ключ. В ключ примере – 12345678 – не является безопасным.

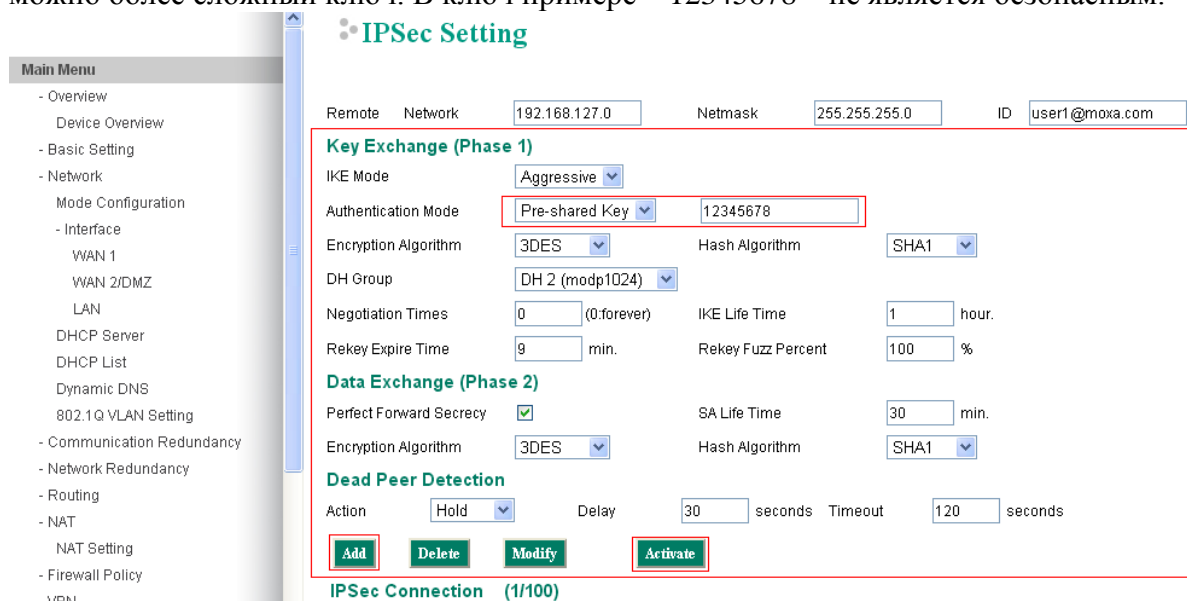


Рис. 7

Далее нажмите кнопки Add и Activate. Настройка VPN-сервера закончена.

Настройка VPN-клиента.

1. С помощью браузера откройте WEB-интерфейс модема OnCell G3110.
2. В пункте меню Network Settings/Basic Network Settings укажите конфигурацию интерфейса LAN. Нажмите кнопку Submit.

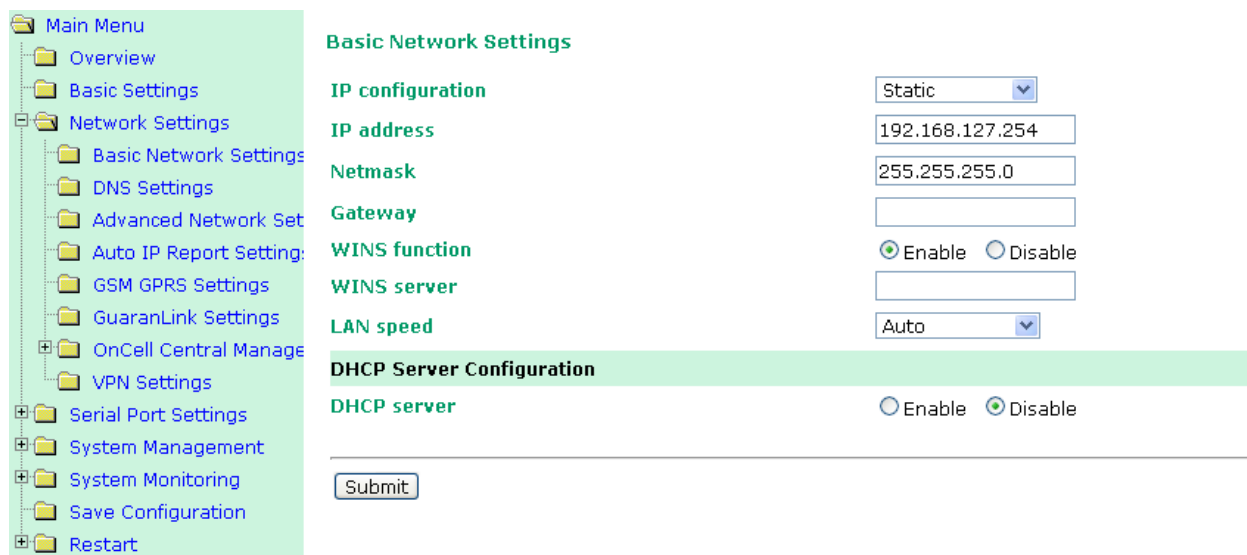


Рис. 8

3. В пункте меню Network Settings/GSM GPRS Settings выберите тип соединения GPRS. Точку доступа APN уточните у оператора мобильной связи (в примере – internet). Нажмите кнопку Submit.

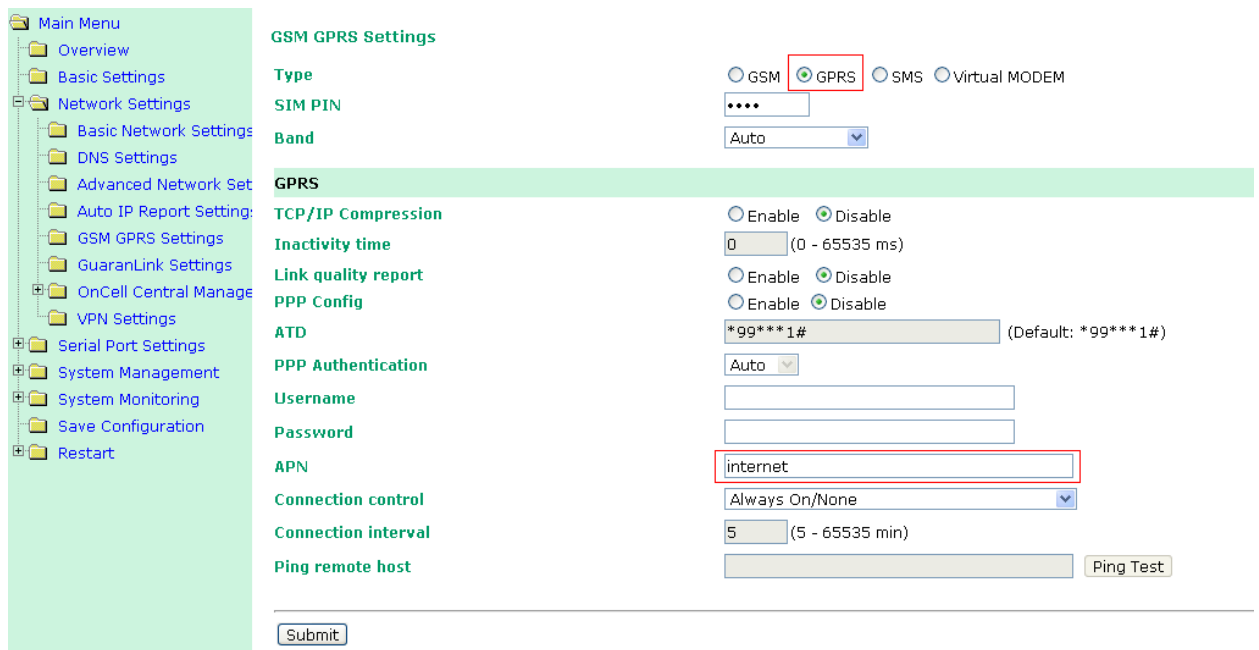


Рис. 9

4. Проверьте соединение с сетью Internet с помощью команды Ping. Например, проверьте доступность маршрутизатора по его внешнему IP-адресу. В рассматриваемом примере – 87.245.206.198.

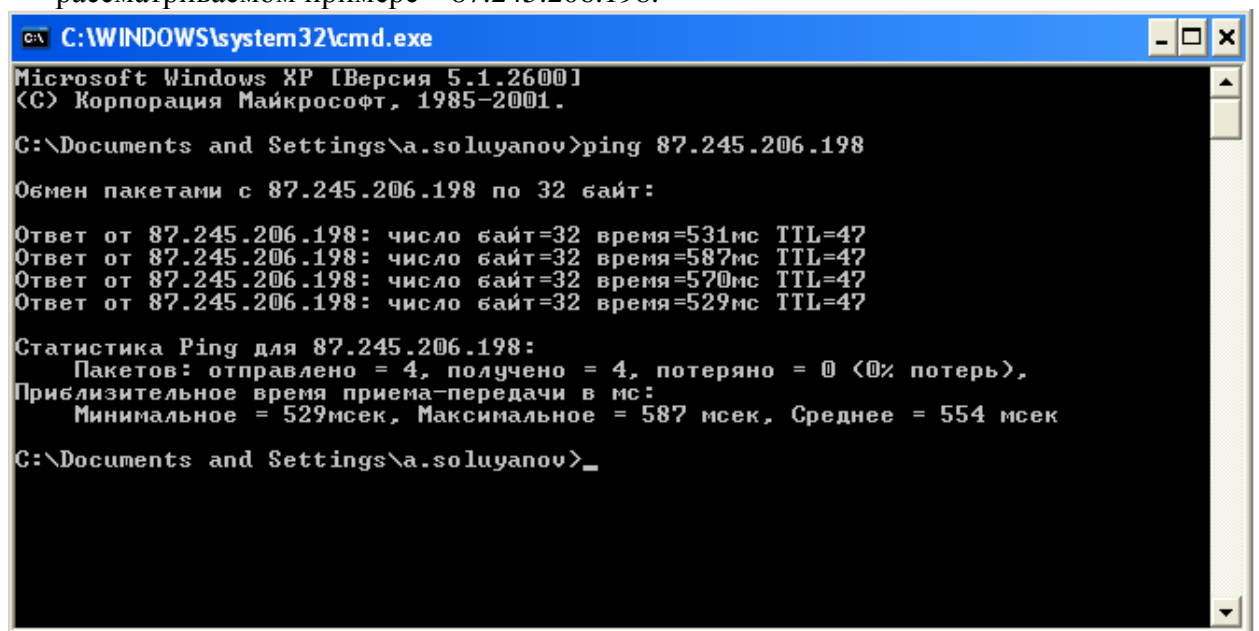


Рис. 10

5. В пункте меню Network Settings/VPN Settings укажите настройки VPN-клиента, как показано на рисунках 11 и 12.

Рис. 11

В полях Remote subnet IP и Local subnet IP укажите адреса ваших удалённой и локальной сетей соответственно. Значения полей Pre-shared key (PSK) и IP/FQDN/User_FQDN должны совпадать с теми значениями, которые были указаны в настройках VPN-сервера.

Рис. 12

Обратите внимание на то, что значения параметров SA lifetime Phase 1 и SA lifetime Phase 2 указываются в секундах. В настройках VPN-сервера параметр SA lifetime Phase 1 соответствует параметру IKE Lifetime и указывается в часах (в примере – 1 час), см рис 7; параметр SA lifetime Phase 2 имеет то же название, но указывается в минутах (в примере – 30 минут), см. рис. 7. **Значения соответствующих параметров должны совпадать, не забудьте произвести пересчёт величин!!!** Нажмите кнопку Submit. Настройка VPN-клиента завершена.

Результат.

Для проверки правильности настройки перейдите в пункт меню System Monitoring/System Status/System Log. В поле System Log при корректной настройке

всех параметров должно появиться сообщение о том, что фазы 1 и 2 создания туннеля VPN завершены.

The screenshot shows a 'System Log' window with a tree view on the left and a log list on the right. The log entries include:

- 2000/01/08 00:42:22 [Network] VPN phase2 renew key
- 2000/01/08 00:42:23 [Network] VPN phase2 renew key success
- 2000/01/08 01:04:55 [Network] VPN phase2 renew key
- 2000/01/08 01:04:56 [Network] VPN phase2 renew key success
- 2000/01/08 01:20:21 [Network] VPN start phase1 aggr. mode connect
- 2000/01/08 01:20:22 [Network] VPN start encryption
- 2000/01/08 01:20:22 [Network] VPN phase1 pass
- 2000/01/08 01:20:23 [Network] VPN phase2 pass
- 2000/01/08 01:42:54 [Network] VPN phase2 renew key
- 2000/01/08 01:42:56 [Network] VPN phase2 renew key success
- 2000/01/08 02:05:27 [Network] VPN phase2 renew key
- 2000/01/08 02:05:29 [Network] VPN phase2 renew key success
- 2000/01/08 02:20:54 [Network] VPN start phase1 aggr. mode connect
- 2000/01/08 02:20:55 [Network] VPN start encryption
- 2000/01/08 02:20:55 [Network] VPN phase1 pass
- 2000/01/08 02:20:57 [Network] VPN phase2 pass
- 2000/01/08 02:22:09 [Network] Ethernet Link Down
- 2000/01/08 02:43:28 [Network] VPN phase2 renew key
- 2000/01/08 02:43:30 [Network] VPN phase2 renew key success

Buttons at the bottom: Select all, Clear log, Refresh.

Аналогично в WEB-интерфейсе маршрутизатора EDR-G903 можно увидеть статус VPN-туннеля. Выберите пункт меню VPN/IPSec/IPSec Status. При корректной настройке все параметров IPsec Connection List будет выглядеть следующим образом:

The screenshot shows the 'IPSec Status' page with a table titled 'IPSec Connection List'. The table has the following data:

Name	Local Subnet	Local Gateway	Remote Gateway	Remote Subnet	Key Exchange (Phase 1)	Data Exchange (Phase 2)
Test	192.168.126.0/24	87.245.206.198	0.0.0.0	192.168.127.0/24	established	established

Для проверки доступности сетей на противоположных концах VPN-туннеля используйте команду Ping.