RBMTX

Instrukcja Obsługi

GSM/LTE

wersja polska

TELEORIGIN
www.teleorgin.com

Elproma Elektronika Sp. z.o.o
Ul. Szymanowskiego 13;
05-092 Łomianki k/Warszawy

e-mail: info@teleorigin.com
Tel. +48 (022) 751 76 80
Fax. +48 (022) 751 76 81

Index

1 Opakowanie i zawartość

1.1 Opakowanie

Oryginalne pudełko przedstawiono poniżej:

Na opakowaniu znajduje się naklejka odpowiadająca naklejce znajdującej się na modemie. Numer seryjny jednoznacznie identyfikuje modem i zapewnia, że jest on oryginalnym produktem. Więcej informacji na temat naklejek znajduje się w rozdziale 2.4. Etykieta produktu

1.2 Zawartość opakowania

W opakowaniu znajdują się:

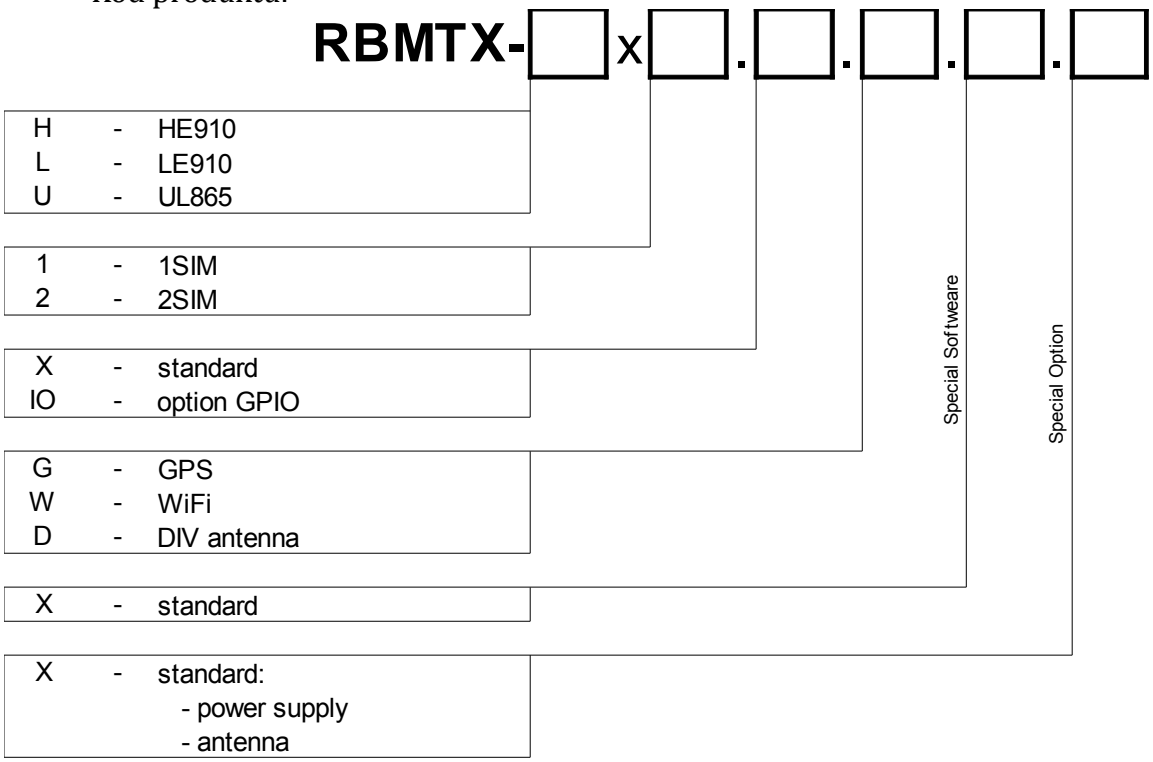
A) Modem RBMTX
B) Antena GSM (SMA)

1.3 Wersje modemu

Możliwe jest rozbudowanie podstawowej wersji modemu o dodatkowe funkcjonalności i interfejsy. W tabeli poniżej przedstawiono różne konfiguracje modemu.

Opcja	Typowo	Opcje
Zasilanie	9...30V	-
CPU	IMX286 450MHz	
Pamięć	128MB RAM, 512MB MicroSD (część wykorzystana dla systemu Linux, pojemność karty może ulec zmianie)	NAND FLASH lub DATAFLASH
RS232	Konsola systemowa	Drugi RS485 zamiast RS232
RS485	1	2
Złącza we/wy	-	4 wejścia cyfrowe, 4 wyjścia cyfrowe, wejście AC, 2 wejścia analogowe, I^2C, interfejs CAN, wyjście zasilające 3.3V, audio I/O, miniUSB 2.0
Połączenie	HSPA+ (GSM, GPRS, EDGE)	UMTS, LTE
SIM	Zewnętrzna	Wewnętrzna
Audio	-	Mikrofon mono, wejście stereo LINE IN, wyjście stereo LINE OUT,lub wyjście do głośnika SPK OUT
LAN	Ethernet 10/100Mbps	Modem WiFi

Kod produktu:



Przykład: **RBMTX-Hx1.X.G.X.X** – modem HSPA+ z GPS, 1 SIM holder

2 Opis ogólny

2.1 Panel przedni

2.2 Panel tylni

2.3 Złącza zewnętrzne

2.3.1 Interfejsy i złącza

2.3.1.1 Złącze SMA anteny GSM

Złącze SMA wykorzystywane jest do podłączenia zewnętrznej anteny GSM. Aby modem mógł zalogować się do sieci GSM należy podłączyć antenę. Rodzaj anteny zależy od technologii sieci GSM. W przypadku, gdy sygnał jest mocny proszę użyć anteny załączonej w opakowaniu. W przypadku, gdy zasięg sieci GSM jest niski lub bardzo słaby, należy użyć np. anteny kierunkowej (wewnątrz budynku, np. w miejscu gdzie zasięg jest wystarczający).

Ważne: *W przypadku gdy żadna antena nie jest podłączona do modemu, nie jest możliwe zalogowanie urządzenia w sieci GSM.*

2.3.1.2 Port szeregowy modemu (RS232/RS485)

Urządzenie występuje w wersji z portem szeregowym RS232 lub RS485. Port szeregowy RS232/RS485 (na złączu RJ-45) znajduje się na przednim panelu urządzenia. Port ten może zostać konfigurowany pod indywidualne potrzeby klienta.

version		
RS232 RS485	2x RS485	RB-MTX
		RJ45
A	A1	1
5V	5V	2
B	B1	3
GND	GND	4
TX	A2	5
RX	B2	6
RTS	NC	7
CTS	NC	8

	Rb-MTX	RS232	RS485
	RJ45	DB9F	DB9F
A	1	nc	1
5V	2	2	2
B	3	3	nc
GND	4	nc	nc
TX	5	5	5
RX	6	ns	6
RTS	7	7	nc
CTS	8	8	nc

2.3.1.3 Złącze RJ-45

Złącze RJ-45 znajduje się na przednim panelu modemu RBMTX i używane jest do komunikacji z komputerem PC lub laptopem (Ethernet). W celu uruchomienia stron konfiguracyjnych modemu podłącz kabel typu UTP pomiędzy złączem RJ-45 komputera, a złączem RJ-45 terminala. Strona konfiguracyjna dostępna jest pod adresem IP określonym w konfiguracji modemu (ustawienie fabryczne to 192.168.1.234).

2.3.1.4 Złącze zasilania

Modem RBMTX powinien być zasilany napięciem z zakresu 6..30V, aby zapewnić optymalne zasilanie urządzenia, szczególnie w celu uniknięcia stanów nieustalonych pochodzących od zasilaczy indukcyjnych.

2.3.1.5 We/wy audio

Wejścia i wyjście audio dostępne są jako opcja. Możliwe jest wyposażenie modemu w następujące we/wy:

- SPK/LINE OUT – głośnik zewnętrzny lub linia zewnętrzna
- LINE IN
- MIC IN – wejście mikrofonowe

2.3.1.6 Złącze 20-pinowe

RBMTX dostępny jest w wersji ze złączem 20-pinowym również jako opcja. Szczegółowy opis złącza znajduje się w poniższej tabeli

PIN Górny rząd*	*Funkcja*		*PIN* Dolny rząd*	*Funkcja*
1	ADC IN1		2	ADC IN2
3	DAC OUT		4	NC
5	GND (nie jest to we. zasilania)		6	NC
7	IN1		8	IN2
9	IN3		10	IN4
11	OUT1		12	OUT2
13	OUT3		14	OUT4
15	I2C SDA		16	I2C SCL
17	CAN L		18	CAN H
19	GND (nie jest to we. zasilania)		20	wyjście +3.3V, 75mA (maks.)

GND – masa. **Proszę nie łączyć bezpośrednio z linią minus zasilania.**
NC – nie podłączono.

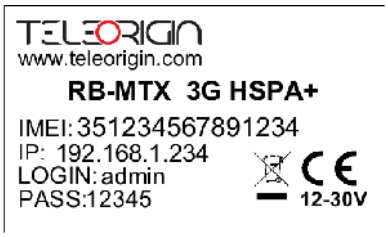
2.3.2 Karty SIM

Złącze/złącza na kartę SIM znajdują się na przednim panelu RBMTX. Aby umieścić kartę SIM **należy wcisnąć żółty przycisk i wyjąć czarną „szufladkę" na kartę**. Po umieszczeniu karty należy włożyć ją do modemu (patrz obrazek). Aby możliwe było korzystanie z usług sieci GSM należy umieścić w modemie aktywną kartę SIM.

2.4 Etykieta produktu

Na etykiecie produktu znajdują się następujące informacje:

- Numer seryjny produktu
- Symbol przekreślonego kosza i certyfikatu CE oraz zakresy napięcia zasilania
- 15 cyfrowy kod kreskowy
- Nazwa modelu



Etykieta na urządzeniu

Etykieta na pudełku

3 Podstawowe funkcje i usługi

Podstawowe funkcje i usługi modemu zawarto w tabeli poniżej.

Funkcja/usługa	Opis
Obsługiwane częstotliwości	Wszystkie wersje: • GSM 900 Class 4 (2W) • DCS 1800 Class 1 (1W) • EDGE 900MHz Class E2 (0.5W) • EDGE 1800MHz Class E2 (0.4W) Wersja HSPA+: • WCDMA FDD B1, B2, B4, B5, B8 Class 3 (0.25W) Wersja UMTS: • WCDMA FDD B1, B8 Class 3 (0.25W) Wersja LTE: • WCDMA FDD B1, B5, B8 Class 3 (0.25W) • LTE FDD B3, B7, B20 Class 3 (0.2W)
Transfer danych	⇗ HSPA+ (downlink 21 Mbit/s, uplink 5,76 Mbit/s) ⇗ UMTS (downlink 7,2 Mbit/s, uplink 5,76 Mbit/s) ⇗ EDGE (Multi-slot class 10, max BR downlink 236,8 Kb/s) ⇗ GPRS (Multi-slot class 10, max BR downlink 85,6 Kb/s) ⇗ CSD (Max BR 14,4 Kb/s) ⇗ TCP/IP, UDP/IP, SSL, HTTP, HTTPS, FTP, SMTP, POP3, IBM MQTT ⇗ Protokół Class B GSM 07.10 multiplexing
WiFi	Standardowo: ⇗ 802.11b/g/n, 802.3, 802.3u Transfer danych ⇗ do 150 Mbps
Interfejsy (wersja podstawowa)	⇗ Złącze anteny GSM: SMA ⇗ 2x SIM: 3V standard ⇗ RS232 lub RS485 przez RJ-45 (DB9 do specjalnego użytku*) ⇗ RJ-45 (x2) ⇗ Złącze zasilania
Opcje*	⇗ Dual SIM ⇗ Interfejsy I/O (CAN, wyjście 3.3V, miniUSB) ⇗ Audio I/O ⇗ Złącze anteny WiFi SMA
Inne	Wymiary: ⇗ Max. 83 x 60 x 34 mm (bez złącz) Temperatura pracy: ⇗ Min. 0°C Max. 45°C

*opcjonalnie

4 Korzystanie z modemu

4.1 Rozpoczynanie pracy z modemem

W celu uruchomienia modemu wykonaj następujące kroki:

4.1.1 Włożenie karty SIM

- Wciśnij żółty przycisk na przednim panelu i wyjmij „szyfladkę" na kartę SIM
- Umieść kartę(y) SIM jak pokazano na obrazku:

*modemy dostępne są z jedną lub z dwoma złączami na kartę SIM

4.1.2 Podłączenie anteny

- Przykręć antenę GSM lub obie anteny: GSM i GPS (opcje dodatkowe) do złącza SMA:

4.1.3 Podłączenie zasilania

- Podłącz kabel zasilacza do złącza PWR znajdującego się na tylnym panelu modemu.

4.1.4 Podłączenie kabla UTP do gniazda RJ-45

- Podłącz kabel UTP do gniazda RJ-45 jak pokazano na rysunku.

4.2 Konfiguracja modemu

Modem konfiguruje się poprzez przeglądarkę internetową ułatwiając tym samym obsługę modemu. Konfiguracja modemu opisana jest w następnych podrozdziałach. Ustawienia podzielono na kategorie umożliwiające proste odnalezienie poszukiwanej opcji. Przy przełączaniu pomiędzy zakładkami opcje zapamiętywane są w sposób automatyczny w pamięci modemu. W celu zapamiętania ustawień na koniec konfiguracji należy kliknąć w „Save Settings". Możliwe jest także anulowanie nowych ustawień przez wybór odpowiedniej opcji z menu znajdującego się na dole ekranu.

Uwaga: Pamięć cache resetowana jest przy restarcie lub rozłączeniu zasilania

Uwaga: Dostęp do niektórych zakładek uwarunkowany jest wersją modemu

4.2.1 Ustanowienie połączenia

Po podłączeniu niezbędnych kabli (4.1 Rozpoczynanie pracy z modemem) możliwe jest ustanowienie połączenia z siecią. Uruchom ustawienia protokołu TCP/IP (**Połączenia sieciowe -> Połączenie lokalne -> Protokół internetowy (TCP/IP) -> Właściwości**) i ustaw swój adres IP jako: 192.168.1.x. Teraz strona konfiguracyjna modemu dostępna jest pod adresem **192.168.1.234**.

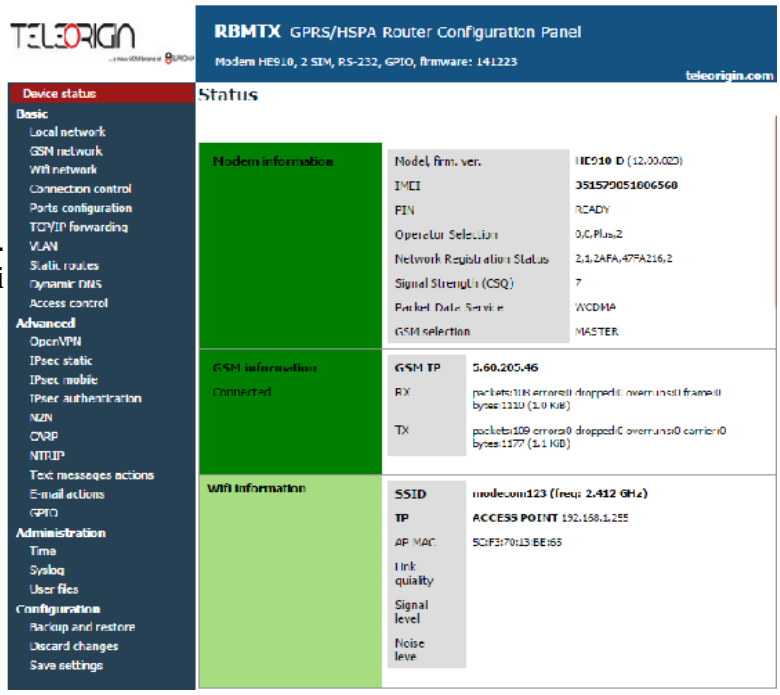
4.2.2 Status modemu (Device status)

Otwórz przeglądarkę WWW i wpisz adres 192.168.1.234. Zostaniesz poproszony o podanie nazwy użytkownika i hasła. Standardowe ustawienia to:

Nazwa użytkownika: **admin**

Hasło: **12345**

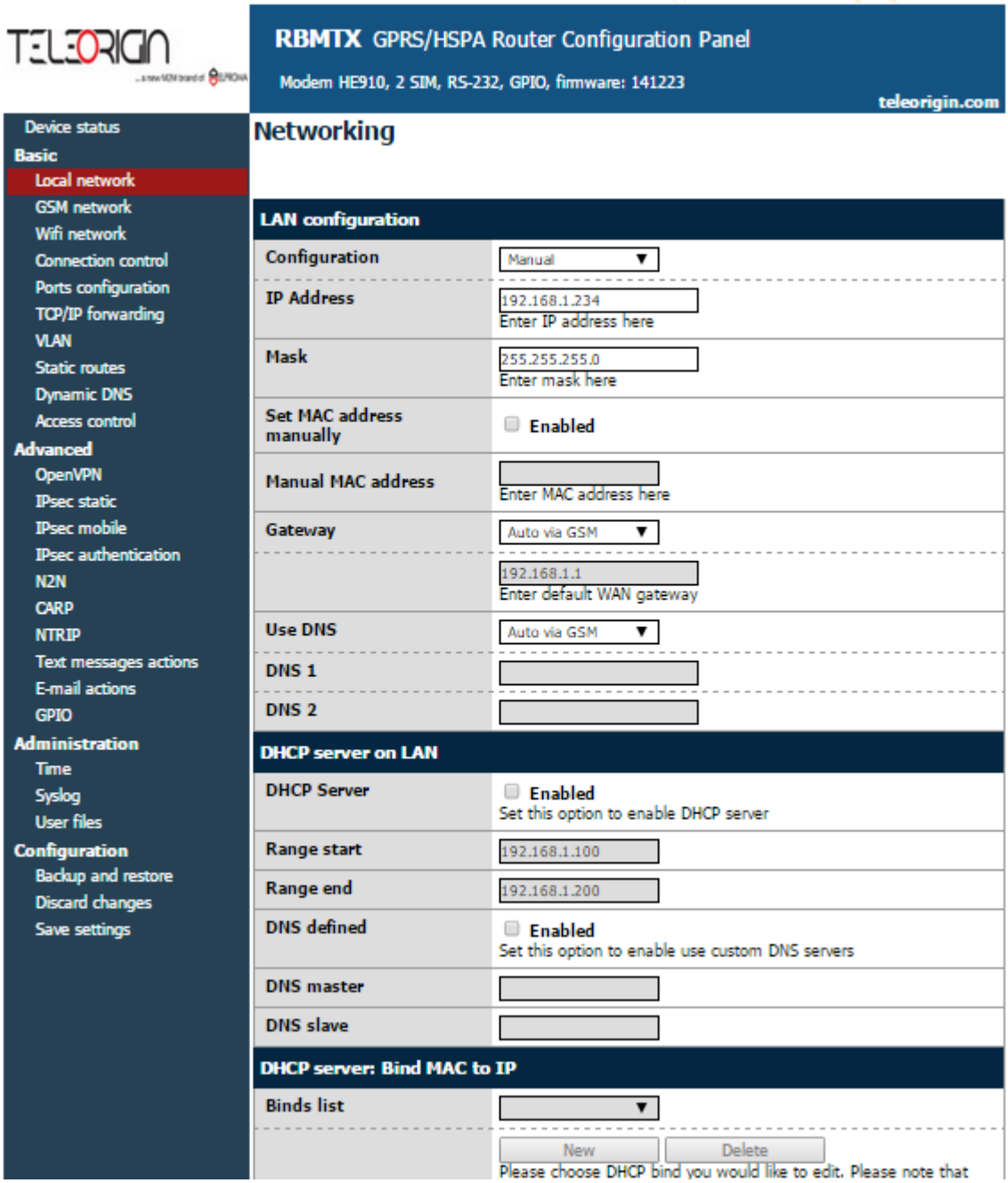
Jeżeli wszystko skonfigurowane jest poprawnie pojawi się następujące okno:



Jest to strona statusu modemu. Zawiera ona status połączenia do sieci oraz parametry PPP połączenia.

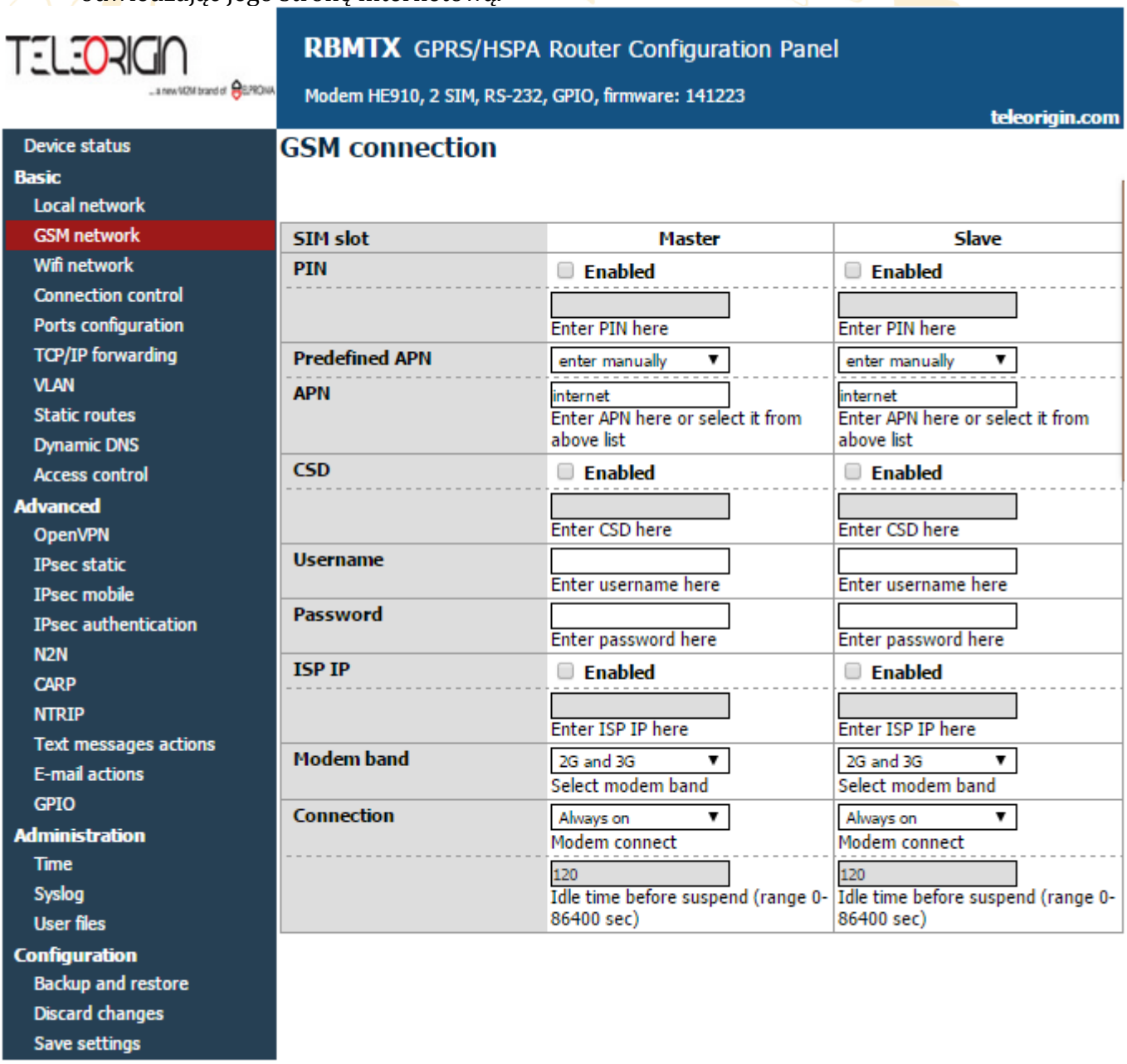
4.2.3 Sieć lokalna LAN (Local network)

Na stronie konfiguracji LAN dostępne są ustawienia niezbędnych parametrów połączenia LAN. Tutaj możliwe jest ustawianie adresu IP (bądź ustawienie automatycznego wyboru IP z użyciem DHCP), maski podsieci, domyślnego punktu dostępu czy też adresu DNS. Ostatnie dwie mogą zostać ustawione ręcznie bądź pobrane z sieci GSM lub DHCP. Dodatkowo modem może pracować jako serwer DHCP. Możliwe jest zdefiniowanie jego zakresu pracy lub zestawu powiązań IP-MAC.



4.2.4 Sieć GSM (GSM network)

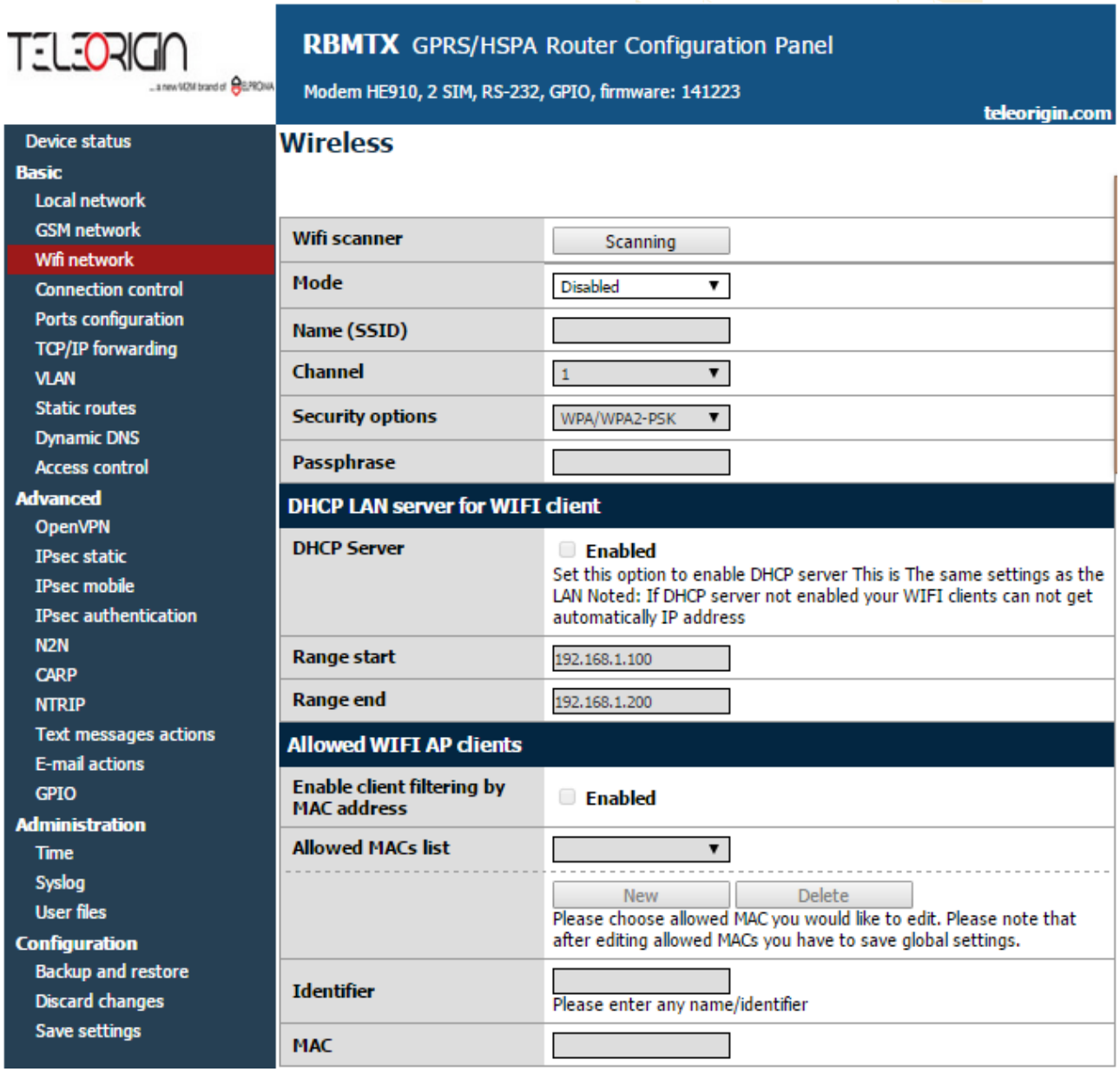
Zakładka GSM network zawiera parametry związane z połączeniem internetowym (punkty dostępowe APN, nazwa użytkownika, hasło, CSD, ISP IP oraz rodzaj sieci) dla karty **MASTER SIM**. Niezbędna jest znajomość tych parametrów w celu korzystania z połączenia internetowego. Powinny one zostać dostarczone przez Twojego operatora. Możesz także znaleźć je kontaktując się z operatorem lub odwiedzając jego stronę internetową.



W przypadku, gdy karta SIM posiada PIN należy zaznaczyć pole Enabled i wpisać kod PIN w pole poniżej. Wychodzące połączenia realizowane są zawsze przez MASTER SIM.

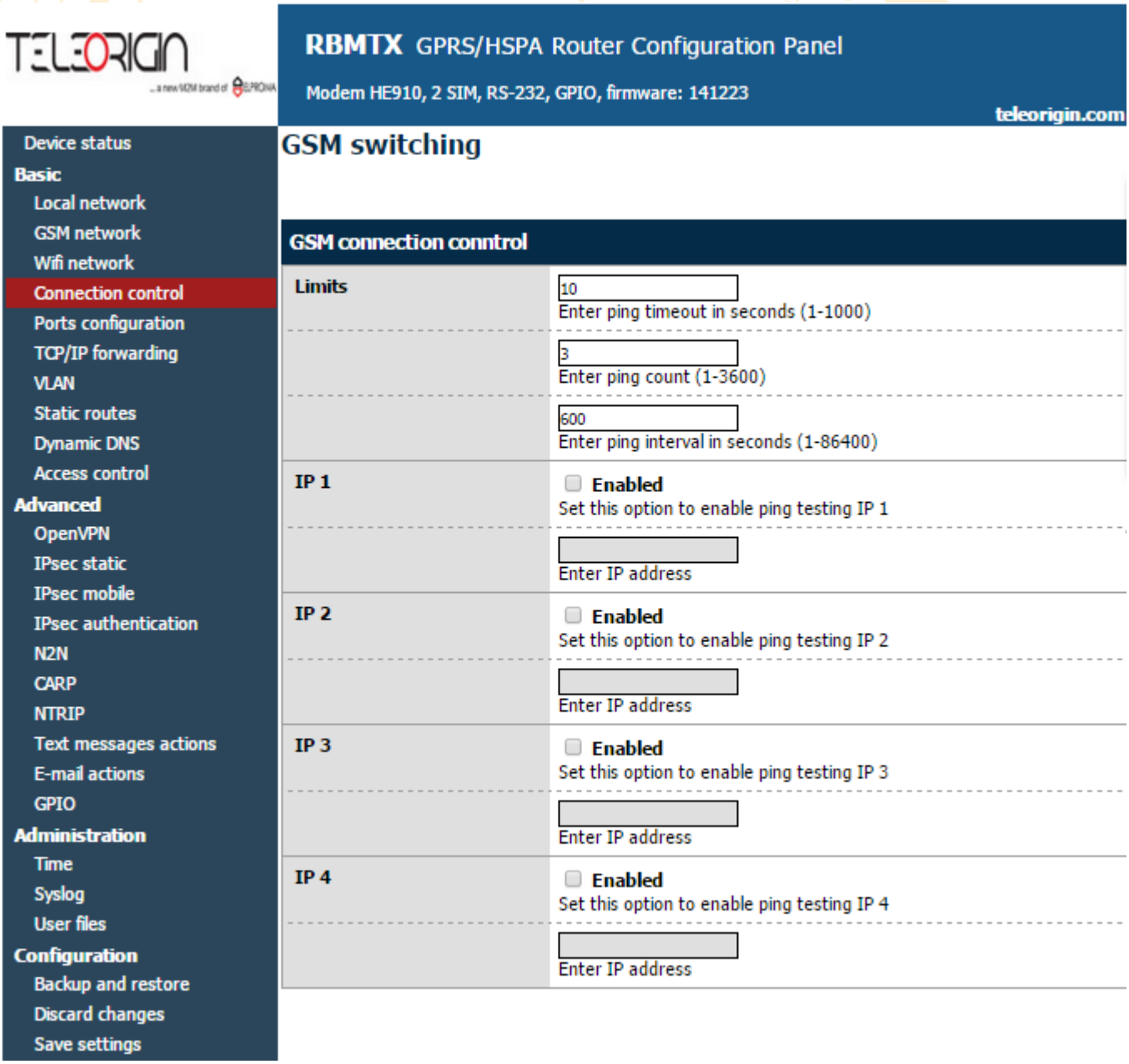
4.2.5 WiFi network

Zakładka “WiFi network” jest dostępna tylko dla routera RBMTX z opcją WiFi. W tym menu można ustawić parametry sieci WiFi. Aby wyszukać wszystkie dostępne sieci WiFi należy użyć przycisku “Scanning”. Zostaniesz przeniesiony do strony z listą dostępnych sieci. Można ustawić tryb WiFi (Access point or Station), podać nazwę i hasło danej sieci. Jest także opcja włączenia serwera DHCP i dozwolonych klientów AP.



4.2.6 Ustawienia połączeń (Connection control)

Zakładka ta zawiera parametry definiujące sposób przełączania pomiędzy kartami Slave i Master. Możliwe jest zdefiniowanie czasu dla operacji testowania połączenia (ping), ustawienie liczby prób oraz do 4 adresów IP. W poniższym przykładzie (obrazek) po trzech 10-sekundowych próbach karta zostanie przełączona z Master na Slave bądź odwrotnie.



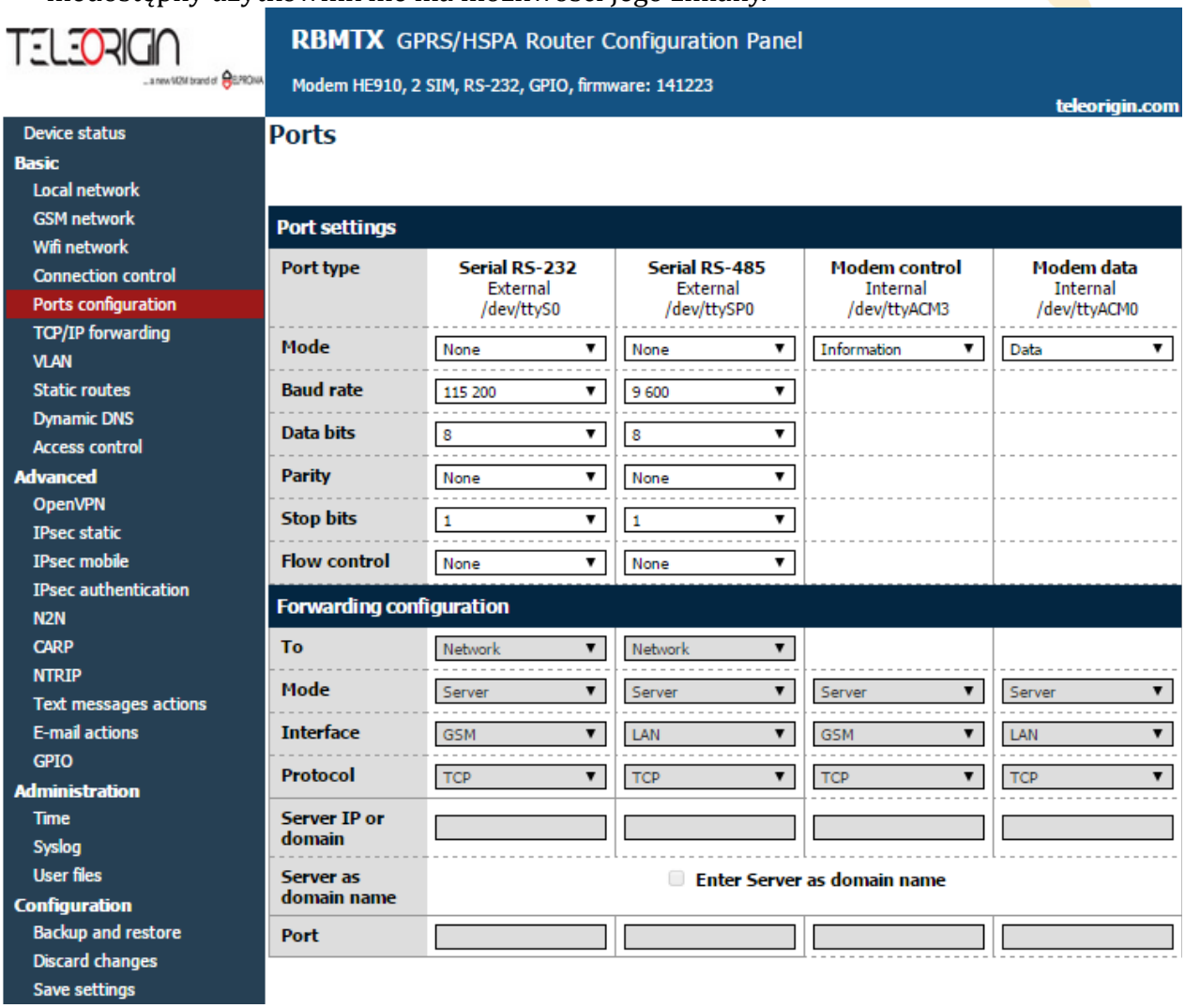
4.2.7 Ustawienia portów (Ports configuration)

Możliwe jest ustawienie parametrów portu szeregowego RS232. W zakładce RS232 Port znajdują się trzy konfigurowane porty: /dev/ttyS0, /dev/ttyACM0 oraz /dev/ttyS1 lub /dev/ttyUSB0 (w zależności od wersji modemu).

Każdy z portów może pracować w innym trybie. Port /dev/ttyS0 może pracować w trybie Terminal, ModBus lub NTRIP. Pozostałe dwa porty mogą także pracować jako port modemu (sterowanie i dane) lub port odbierający wiadomości SMS (patrz 4.2.19. SMS Actions).

Każdy port może być przekierowany (forwarding) na port TCP/UDP (jakoś serwer lub klient). Ponadto port /dev/ttyS0 można przekierować na sterowanie modemem lub transfer danych – w tym przypadku żaden inny tryb nie może zostać uruchomiony na tym porcie.

Uruchomienie niektórych trybów dla dev/ttyS0 i /dev/ttyS1 umożliwia ustawienie parametrów takich jak: liczba bitów na sekundę (baud rate), bity danych, parzystość (parity), bity stopu i protokół. W przypadku gdy jakiś parametr jest niedostępny użytkownik nie ma możliwości jego zmiany.

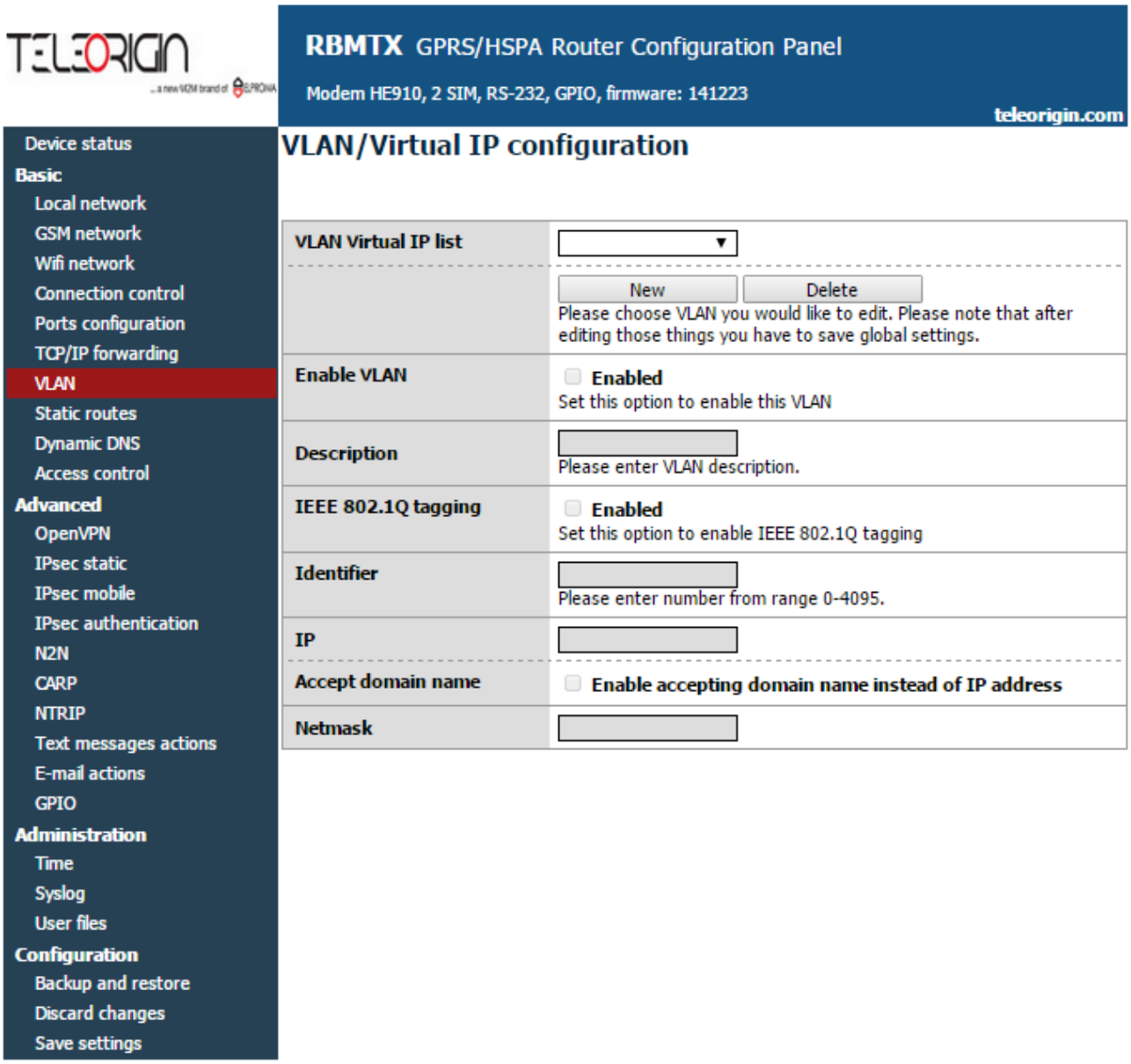


4.2.8 TCP/IP forwarding

Możliwe jest ustawienie pojedynczych portów lub zakresów portów, które będą przekierowane na dany adres IP. Aby dodać nową regułę dotyczącą pojedynczego portu należy przejść do zakładki TCP/IP Forwarding i w sekcji Single Port rules kliknąć przycisk New. Następnie wpisać identyfikator (dowolną nazwę określającą naszą regułę), zaznaczyć pole Enabled, wpisać zewnętrzny (External) i Przy dodawaniu nowej reguły lub zmianie zakładki stan edytowanej reguły jest zapamiętywany. Możliwe jest też usuwanie reguł za pomocą przycisku Delete. Po zmianach w konfiguracji należy dodatkowo kliknąć Save Settings, aby zapisać całą konfigurację. Analogicznie możemy dodawać reguły dotyczące zakresów portów w sekcji Port range rules. Możemy też określić adres IP dla niezaufanej sieci w sekcji DMZ.

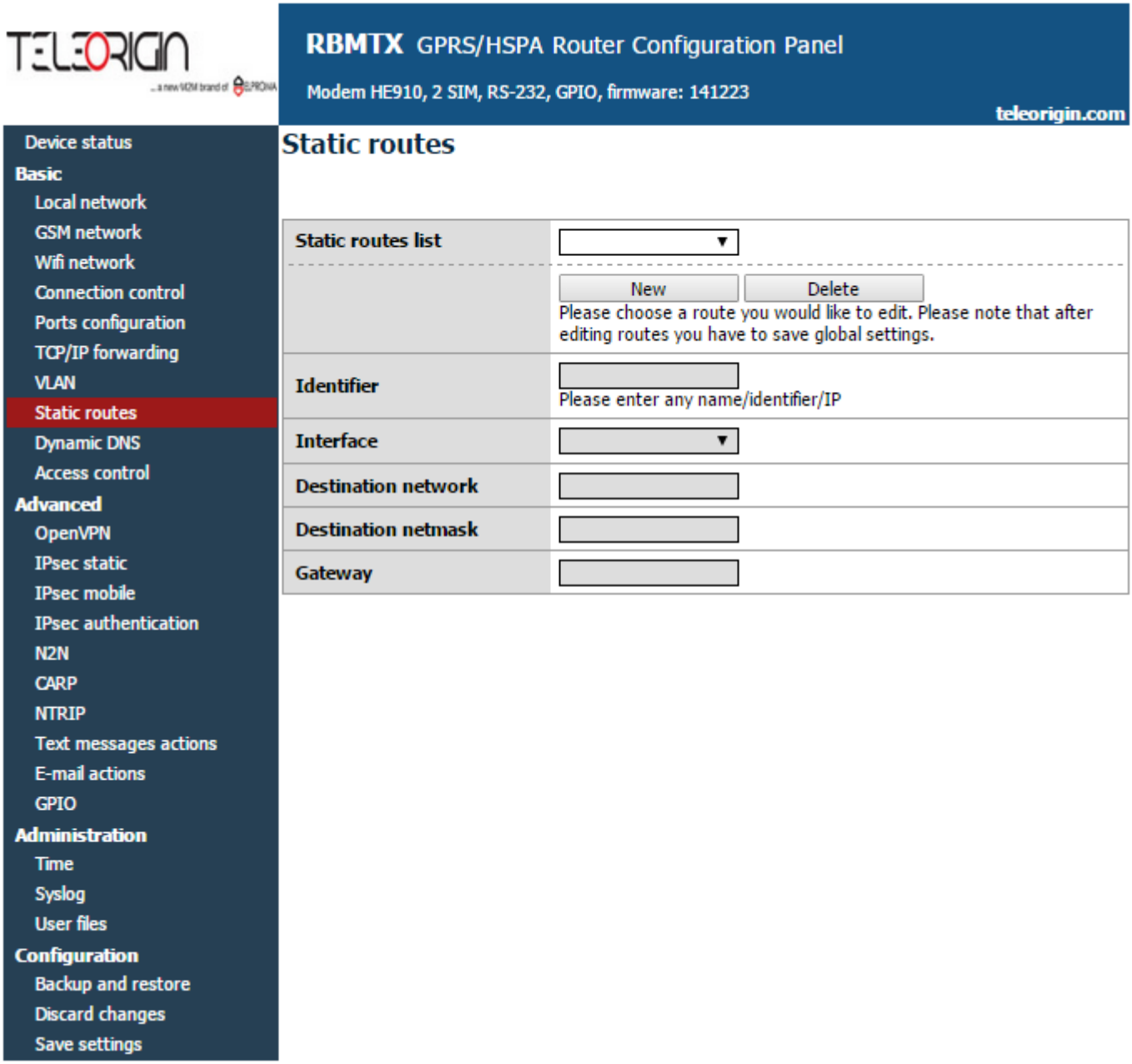
4.2.9 VLAN

Zakładka VLAN umożliwia użytkownikowi na stworzenie wirtualnego adresu IP. Należy zdefiniować IP, maskę podsieci oraz identyfikator z zakresu 0-4095. Zaznaczając IEEE 802.1Q tagging virtual IP staje się częścią VLAN.



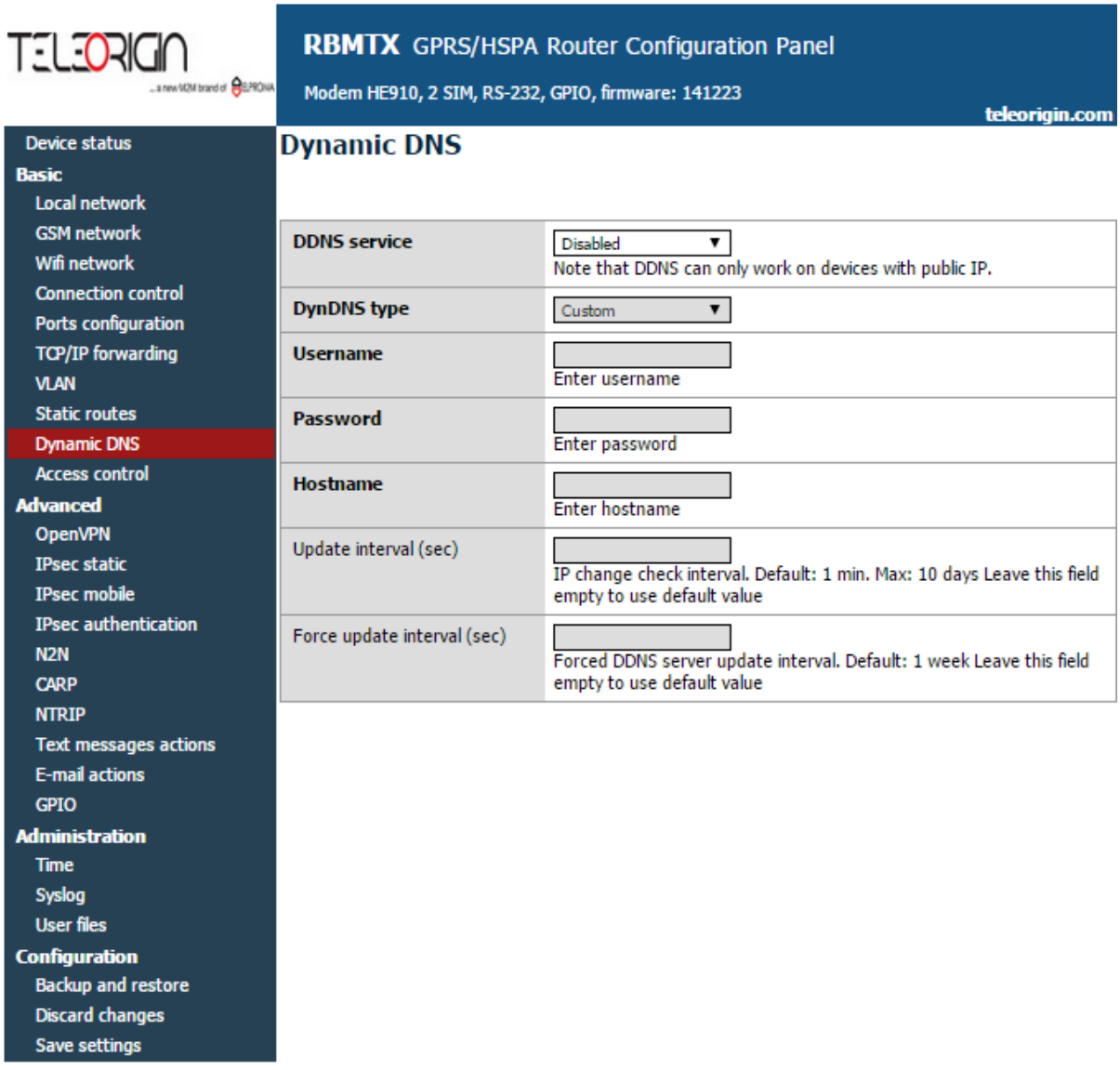
4.2.10 Static routes

Zakładka Static routes umożliwia zdefiniowanie routingu pod własne preferencje. Klikając w przycisk New dodajemy nowe połączenie (routing). Pozostałe pola pozwalają na wprowadzenie identyfikatora (użyć w celu rozróżnienia routingu w konfiguracji na stronie www), wybór interfejsu, docelowej sieci, maski oraz serwera gateway.



4.2.11 Dynamic DNS

Dynamic DNS to usługa, która pozwala na udostępnienie urządzenia pod określonym adresem internetowym niezależnie od zmian jego adresu IP. Aby było to możliwe potrzebne jest utworzenie konta na jednym z serwisów internetowych obsługujących tę usługę. Aktualnie obsługiwane serwisy przez modem MTX to DynDNS.org oraz No-IP.com. Po założeniu konta w jednym z serwisów ustawiamy w zakładce Dynamic DNS usługodawcę, dla dyndns.org dodatkowo rodzaj usługi, nazwę użytkownika, hasło, nazwę hosta oraz dwa parametry: update interval i force update interval. Pierwszy z nich określa jak często następuje sprawdzenie, czy adres IP uległ zmianie i ewentualne powiadomienie o tym fakcie usługodawcy, drugi określa czas pomiędzy wymuszonymi aktualizacjami, tzn. takimi, które występują nawet gdy adres IP się nie zmienił. W razie wątpliwości można pozostawić te pola puste-zostaną wtedy użyte domyślne wartości.



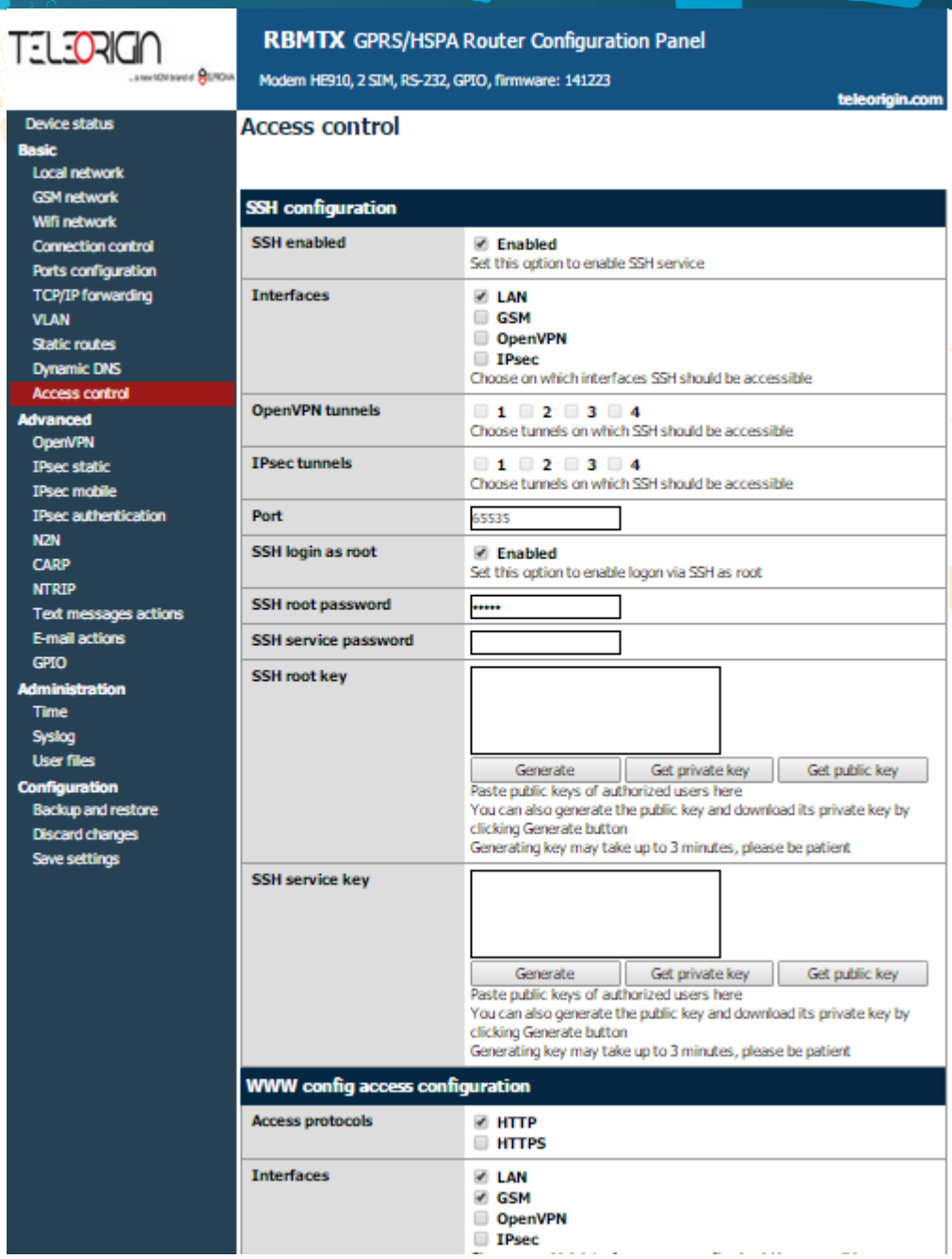
4.2.12 Access control

Zakładka Access Control służy do zmiany ustawień dostępu do modemu. Pierwsza sekcja zawiera konfigurację protokołu SSH. Możemy włączyć lub wyłączyć protokół, ustalić, na których portach i interfejsach będzie możliwe logowanie (dotyczy to także tuneli OpenVPN i IPsec). Możliwe jest również zablokowanie logowania przez SSH jako root oraz zmiana kluczy i haseł dla użytkowników root i service. Po kliknięciu przycisku Delete hasło zostaje usunięte, tzn. jego podanie nie będzie wymagane przy logowaniu. Po zmianie/usunięciu hasła należy pamiętać o zapisie całej konfiguracji przy pomocy przycisku Save Configuration w menu głównym. Przy logowaniu priorytet ma uwierzytelnienie kluczem, to znaczy, że jeżeli podamy klucz publiczny oraz ustawimy hasło użytkownika to klient posługujący się zaufanym kluczem nie będzie proszony dodatkowo o podanie hasła, a klient nie posiadający klucza będzie mógł zalogować się za pomocą hasła. W pola SSH root key i SSH service key możliwe jest wklejenie kilku kluczy.

UWAGA: Konto service służy do wgrywania aktualizacji oprogramowania. Wyłączenie protokołu SSH spowoduje brak możliwości aktualizacji.

Istnieje możliwość wygenerowania pary kluczy bezpośrednio na modemie. W tym celu należy kliknąć przycisk Generate. Proces tworzenia kluczy może trwać kilka minut (w tym czasie nie należy przełączać zakładek ani zmieniać innych ustawień), a po jego zakończeniu zostanie wyświetlony komunikat potwierdzający wykonanie operacji. Publiczny klucz zostanie automatycznie wklejony w pole z kluczami (jeżeli pole nie było puste jego zawartość zostanie zachowana, a wygenerowany klucz będzie pierwszy na liście). Odtąd możliwe będzie ściąganie klucza prywatnego i publicznego za pomocą przycisków Get private key oraz Get public key. Aby logować się przy pomocy klucza w systemie Linux należy ściągnąć klucz prywatny i umieścić go w katalogu /home/user/.ssh/ zmieniając jego nazwę na id_rsa.

W sekcji WWW config access configuration możliwa jest zmiana ustawień dotyczących konfiguracji www. Możemy ustalić, z jakich protokołów chcemy korzystać, na jakich interfejsach ma być dostępna konfiguracja (dotyczy to także tuneli OpenVPN i IPsec), na jakich portach będą dostępne wersje HTTP i HTTPS konfiguracji. Możliwa jest także zmiana hasła (zmiana ta jest natychmiastowa i nie wymaga zapisywania konfiguracji). Dla bezpieczeństwa odznaczenie jednocześnie dostępu HTTP i HTTPS jest niemożliwe.


TELEORIGIN
RBMTX GPRS/HSPA Router Configuration Panel
Modem HE910, 2 SIM, RS-232, GPIO, firmware: 141223
teleorigin.com
Device status
Basic
Local network
GSM network
Wifi network
Connection control
Ports configuration
TCP/IP forwarding
VLAN
Static routes
Dynamic DNS
Access control
Advanced
OpenVPN
IPsec static
IPsec mobile
IPsec authentication
NZN
CARP
NTRIP
Text messages actions
E-mail actions
GPIO
Administration
Time
Syslog
User files
Configuration
Backup and restore
Discard changes
Save settings
Access control
SSH configuration
SSH enabled
Enabled
Set this option to enable SSH service
Interfaces
LAN
GSM
OpenVPN
IPsec
Choose on which interfaces SSH should be accessible
OpenVPN tunnels
1 2 3 4
Choose tunnels on which SSH should be accessible
IPsec tunnels
1 2 3 4
Choose tunnels on which SSH should be accessible
Port
65535
SSH login as root
Enabled
Set this option to enable logon via SSH as root
SSH root password
SSH service password
SSH root key
Generate
Get private key
Get public key
Paste public keys of authorized users here
You can also generate the public key and download its private key by clicking Generate button
Generating key may take up to 3 minutes, please be patient
SSH service key
Generate
Get private key
Get public key
Paste public keys of authorized users here
You can also generate the public key and download its private key by clicking Generate button
Generating key may take up to 3 minutes, please be patient
WWW config access configuration
Access protocols
HTTP
HTTPS
Interfaces
LAN
GSM
OpenVPN
IPsec

4.2.13 Open VPN

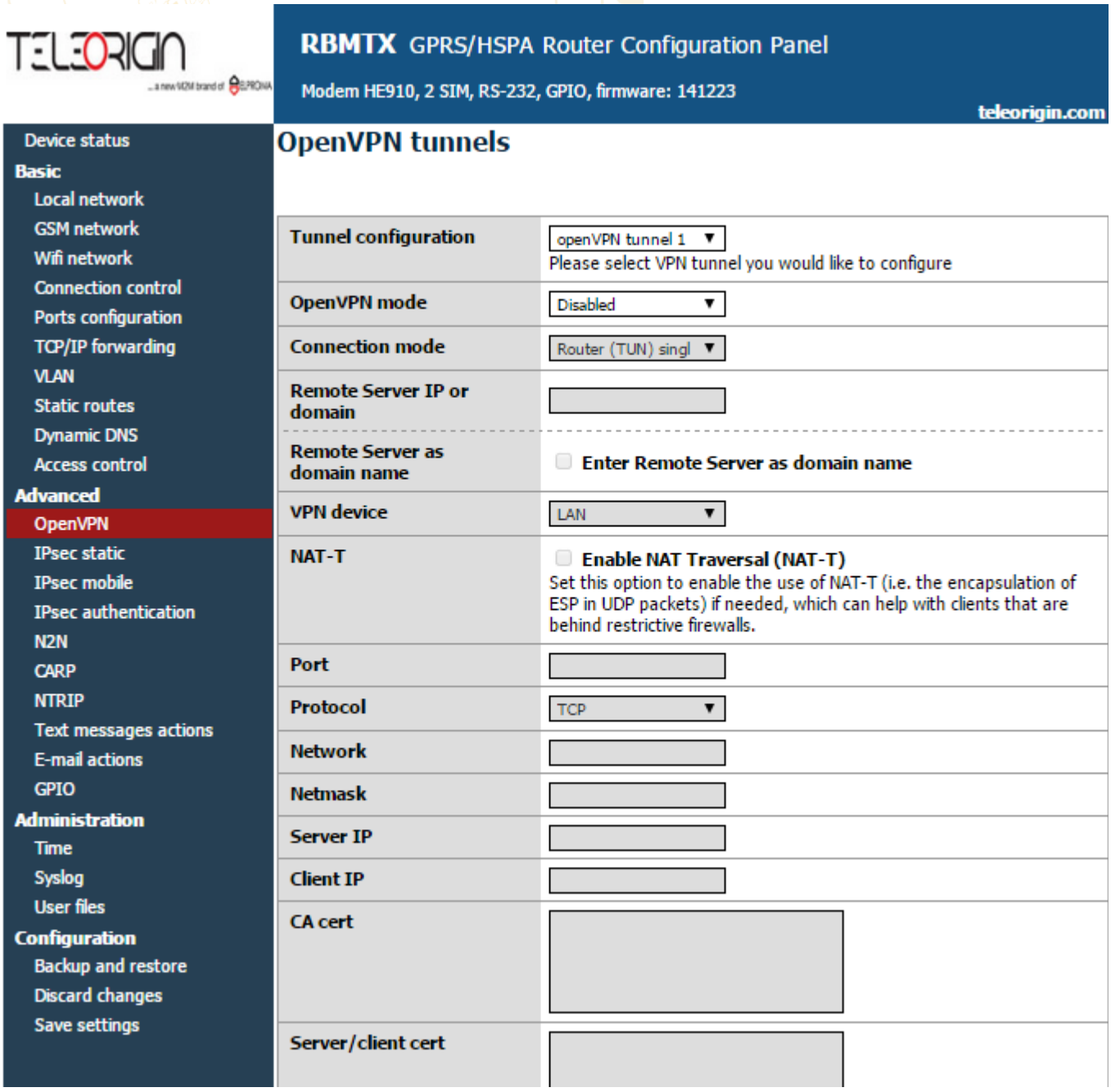
Możliwe jest połączenie modemu do sieci VPN lub ustanowienie własnej z użyciem oprogramowania OpenVPN. W zakładce OpenVPN istnieje możliwość zdefiniowania do czterech połączeń VPN (tuneli). Aby wyświetlić ustawienia konkretnego tunelu wybieramy go z listy Tunnel configuration. Następnie należy wybrać czy modem ma być serwerem czy klientem oraz jeden z dostępnych typów połączenia: tun lub tap. Połączenie typu tun może być zrealizowane pomiędzy dwoma urządzeniami lub większą ich liczbą. W zależności od wyboru w dalszej części konfiguracji będziemy musieli podać adres IP sieci i maskę lub adres klienta i serwera.

W przypadku gdy urządzenie ma pracować jako serwer należy ustawić port na którym urządzenie ma nasłuchiwać przychodzące połączenia (fabrycznie dla sieci VPN używany jest port 1194, pamiętaj by odblokować ten port w zakładce firewall). Następnie, proszę wybrać urządzenie które realizować ma połączenie: eth (zewnętrzny port RJ-45) lub ppp (połączenie przez sieci komórkowe). Należy wybrać także odpowiedni protokół: TCP lub UDP (użyj drugiej opcji w przypadku gdy nie wiesz która opcja jest odpowiednia). W przypadku połączenia typu tun niezbędne jest podanie adresów IP serwera i klienta (zalecamy używanie adresów typu: 10.x.x.x). Dla połączenia tap wprowadź adres podsieci VPN oraz maskę podsieci (np. 10.1.0.0 oraz 255.255.255.0). W większości przypadków Twoje urządzenie zarezerwuje pierwszy adres IP z puli dostępnych adresów (czyli 10.1.0.1 gdy używasz adresów 10.1.0.0).

W przypadku gdy urządzenie jest ustawione jako klient, poza parametrami serwera wymienionymi powyżej trzeba podać dodatkowe. Wpisz adres IP serwera VPN w pole Remote Server IP oraz port nasłuchiwania w pole Port.

Po wprowadzeniu wszystkich niezbędnych informacji użytkownik powinien wypełnić cztery pola certyfikatów, które generowane są na dowolnym komputerze (sprawdź VPN online help w celu uzyskania dodatkowych informacji). Zawartość plików powinna zostać wklejona w odpowiednie pola w karcie konfiguracji VPN. Istnieje możliwość dodatkowego zabezpieczenia połączenia VPN poprzez ustalenie wspólnego klucza TLS i wpisania go w pole TLS key dla wszystkich urządzeń w sieci VPN.

Ostatnia opcja to przełączanie kompresji LZO (zalecane włączenie w celu poprawy komunikacji sieciowej) oraz dodatkowy parametr w polu Additional configuration.


RBMTX GPRS/HSPA Router Configuration Panel
Modem HE910, 2 SIM, RS-232, GPIO, firmware: 141223
teleorigin.com
Device status
Basic
Local network
GSM network
Wifi network
Connection control
Ports configuration
TCP/IP forwarding
VLAN
Static routes
Dynamic DNS
Access control
Advanced
OpenVPN
IPsec static
IPsec mobile
IPsec authentication
N2N
CARP
NTRIP
Text messages actions
E-mail actions
GPIO
Administration
Time
Syslog
User files
Configuration
Backup and restore
Discard changes
Save settings
OpenVPN tunnels
Tunnel configuration
openVPN tunnel 1
Please select VPN tunnel you would like to configure
OpenVPN mode
Disabled
Connection mode
Router (TUN) singl
Remote Server IP or domain
Remote Server as domain name
Enter Remote Server as domain name
VPN device
LAN
NAT-T
Enable NAT Traversal (NAT-T)
Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
Port
Protocol
TCP
Network
Netmask
Server IP
Client IP
CA cert
Server/client cert

4.2.14 IPsec static/IPsec mobile

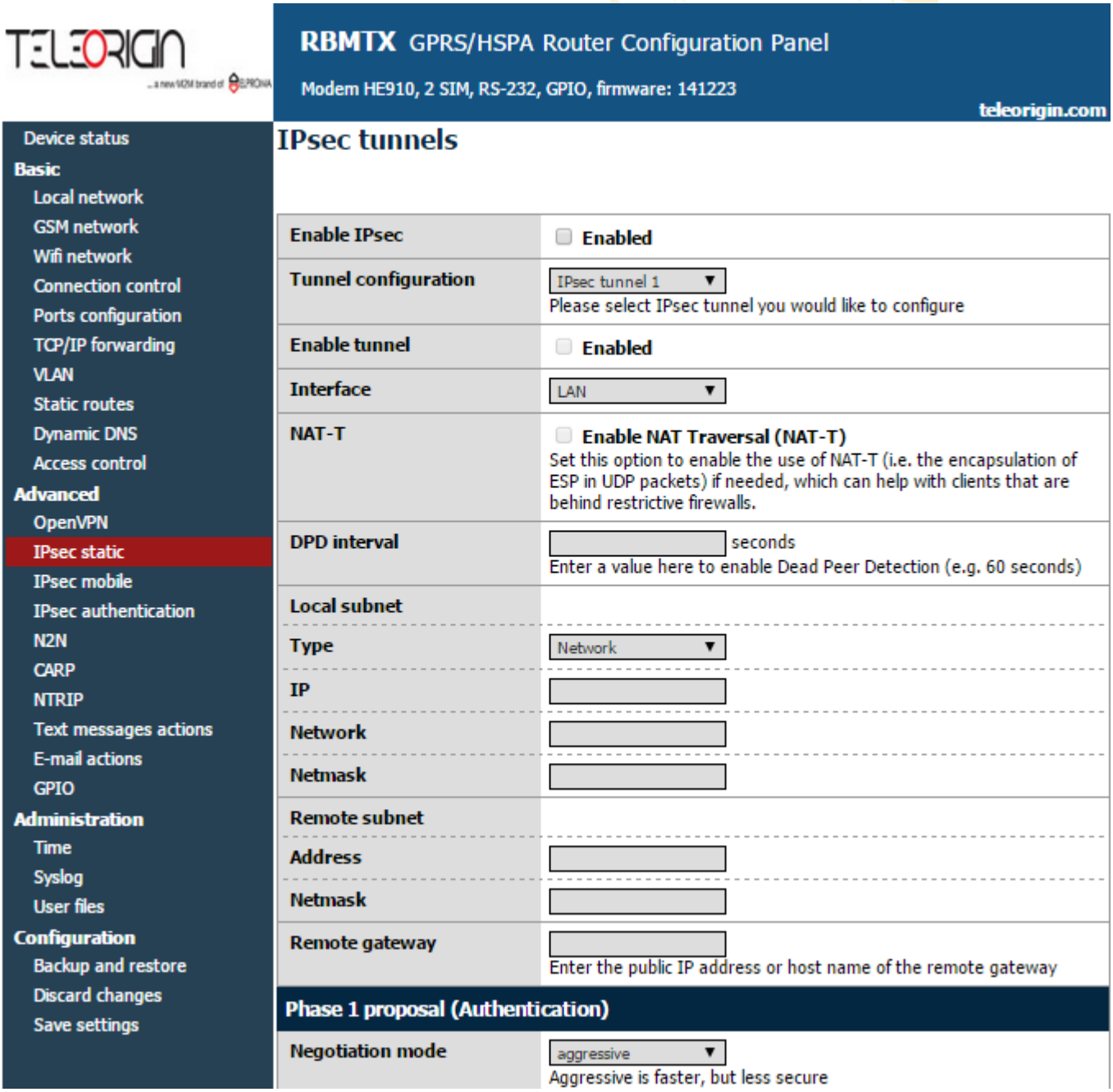
IPsec to zbiór protokołów internetowych pozwalający na stworzenie bezpiecznego połączenia pomiędzy urządzeniami. Do konfiguracji takiego połączenia na modemie MTX służą trzy zakładki konfiguracji: Tunnels, Mobile Clients, Keys and Certificates.

Aby włączyć program obsługujący protokół należy przede wszystkim w zakładce Tunnels zaznaczyć opcję Enable Ipsec. Pod tą opcją mamy pole wyboru pozwalające nam na przełączanie pomiędzy konfiguracjami czterech tuneli. Aby włączyć dany tunel wybieramy go z listy, a następnie zaznaczamy pole Enable tunnel. Następnie należy wybrać interfejs sieciowy, przez który zostanie przeprowadzone połączenie. Nie sposób omówić wszystkich możliwości nawiązywania połączenia za pomocą protokołu IPsec, dlatego poniżej zostanie opisana przykładowa konfiguracja.

Załóżmy, że chcemy połączyć ze sobą dwa modemy MTX o adresach 123.45.67.1 oraz 123.45.67.2. Pole DPD interval określa czas, po którym połączenie zostanie zamknięte jeżeli drugie urządzenie nie odpowie. Dla ustalenia uwagi wpiszmy 3600 sekund. Kolejnym ustawieniem jest określenie lokalnej podsieci, z której pakiety będą przekazywane poprzez bezpieczne połączenie. Możemy tu wybrać Single host (tylko nasz MTX), Network (sieć kilku urządzeń) lub LAN subnet (podsieć lokalnej sieci). Ponieważ nie wiemy, czy nie będziemy chcieli dodać więcej urządzeń w przyszłości wybierzemy opcję Network, w pole IP wpisując 192.168.36.1, w pole Network 192.168.36.0, a w pole Netmask 255.255.255.0. Oczywistym powinno być, że wybrany adres IP powinien być zgodny z wybraną siecią i jej maską. W pola Address i Netmask w sekcji remote subnet musimy wpisać podsieć lokalną, którą określimy na drugim urządzeniu. Na drugim urządzeniu wpiszemy w sekcji Local subnet IP=192.168.35.1, Network=192.168.35.0 i Netmask=255.255.255.0, dlatego też w pola Address i Netmask tej sekcji musimy wpisać Address=192.168.35.0 i Netmask=255.255.255.0 (czyli po prostu przepisujemy pola Network i Netmask z sekcji Local subnet na drugim urządzeniu). Oczywiście w sekcji remote subnet na drugim urządzeniu należy przepisać odpowiednie pola z pierwszego urządzenia. Kolejnym polem jest Remote gateway, gdzie wpisujemy adres IP drugiego urządzenia, tzn. wpisujemy na krzyż: w pierwszym urządzeniu 123.45.67.2, a w drugim 123.45.67.1.

Następnym krokiem jest zdefiniowanie dwóch faz negocjacji połączenia. W Musimy określić jakim identyfikatorem będzie się przedstawiać nasze urządzenie. Najczęstszym wyborem jest My IP Address (mój adres IP) lub RSA Cert Subject (ale tylko wtedy, gdy używamy do autoryzacji certyfikatów, o czym za chwilę). Algorytm szyfrowania (Encryption algorithm) i algorytm funkcji skrótu (Hash algorithm) określamy wedle własnego uznania, należy jednak pamiętać, żeby na wszystkich urządzeniach ustawić te same ustawienia. Najszybszym algorytmem szyfrowania jest z reguły Blowfish, a najwolniejszym (ale i najbezpieczniejszym)-AES. Następnym ustawieniem jest DH key group, czyli długość kodu Diffiego-Hellmana. Tu również ustawienia po obu stronach połączenia powinny być zgodne. W polu Lifetime należy określić maksymalny czas negocjacji w fazie pierwszej, przykładowo 180 sekund, czyli 3 minuty. Jeżeli nie jesteśmy pewni co wpisać możemy pozostawić to pole puste. Najważniejszym ustawieniem fazy pierwszej jest Authentication method, czyli metoda uwierzytelnienia. Najprostszą metodą jest Pre-shared key (PSK), czyli

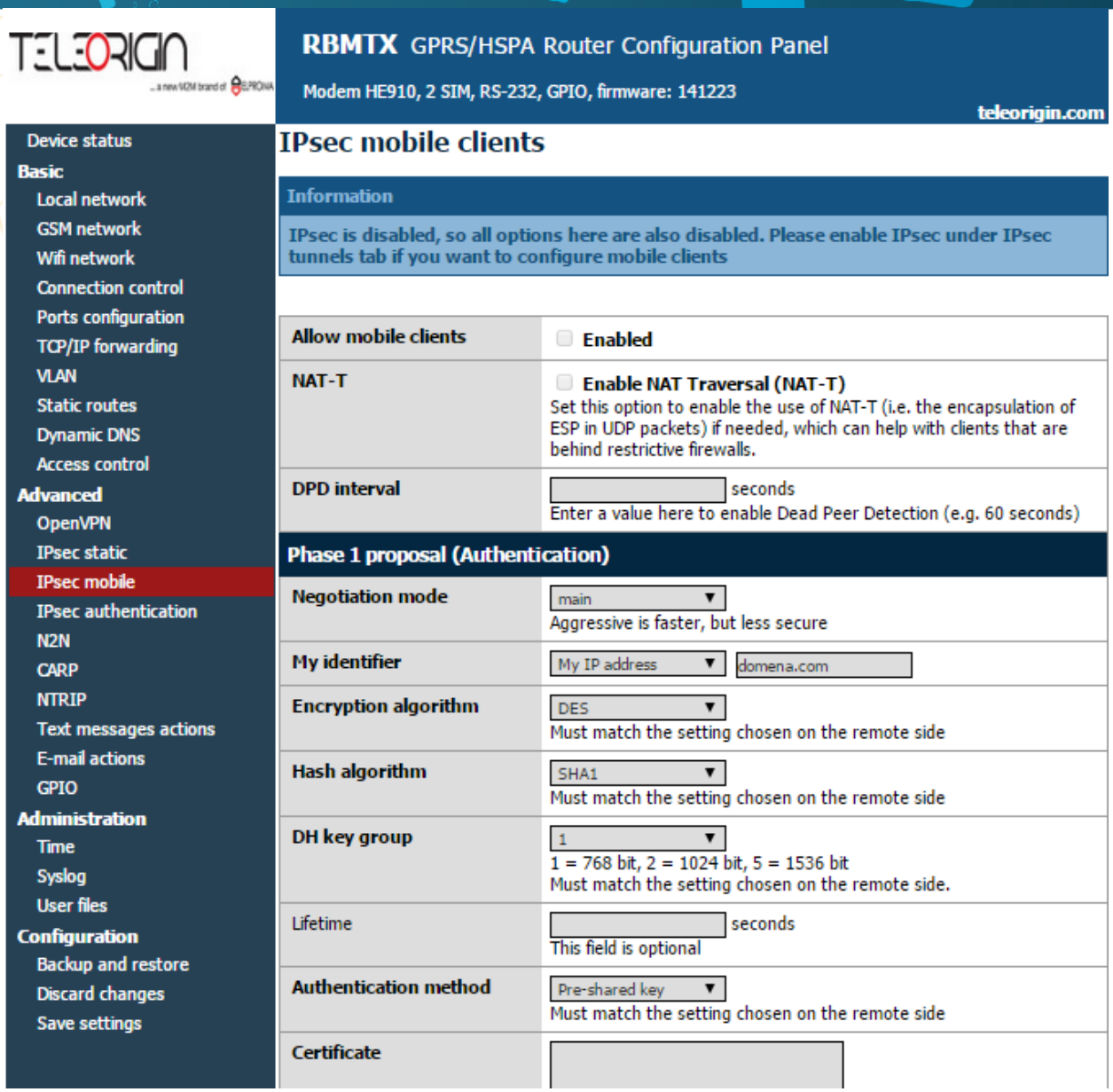
mówiąc prościej hasło, które jest zgodne dla obu stron. Jeżeli zależy nam na lepszym bezpieczeństwie możemy wybrać RSA signature. Ta metoda jest jednak bardziej kłopotliwa, gdyż wymaga wygenerowania certyfikatów i kluczy. Jeżeli zdecydujemy się na tę metodę mamy dwie możliwości: podać własny klucz, własny certyfikat oraz certyfikat drugiego urządzenia (peer certificate) lub własny klucz, certyfikat i certyfikat CA (sposób dodawania certyfikatów CA został opisany w dalszej części rozdziału).



W drugiej fazie negocjacji należy ustalić protokół: AH (tylko uwierzytelnienie) lub ESP (uwierzytelnienie z szyfrowaniem), algorytmy szyfrowania i funkcji skrótu (można zaznaczyć kilka, ważne, aby przynajmniej jeden pokrywał się po obu stronach), długość klucza PFS (Perfect Forward Secrecy) oraz czas trwania drugiej fazy negocjacji (to pole można zostawić puste aby użyć wartości domyślnej).

Po zapisaniu ustawień powinniśmy mieć gotowe bezpieczne połączenie IPsec. Jeżeli wybraliśmy metodę autoryzacji poprzez certyfikaty RSA nie określając certyfikatu partnera (peer certificate), musimy dodać certyfikat CA.. W tym celu wybieramy zakładkę Keys and Certificates. Mamy tu możliwość zapisywania dodatkowych kluczy prywatnych (Pre-Shared keys) oraz certyfikatów CA. Metoda zapisu jest taka sama dla obu typów zabezpieczeń i zostanie opisana na przykładzie certyfikatów CA. Jeżeli nie określiliśmy wcześniej żadnego certyfikatu CA najprawdopodobniej lista certyfikatów jest pusta. Aby dodać pierwszy certyfikat musimy najpierw kliknąć przycisk Add new. W ten sposób odblokowane zostaną pola, w których należy wpisać kolejno: identyfikator (może być dowolny, jest widoczny jedynie w konfiguracji www i ma pomóc użytkownikowi rozróżnić certyfikaty), certyfikat oraz listę wykluczeń certyfikatu (CRL). Ostatnie pole jest opcjonalne, służy do ewentualnego zablokowania dostępu części użytkowników.

WAŻNE: Po wpisaniu identyfikatora i wklejeniu certyfikatu należy zapisać zmiany poprzez kliknięcie przycisku Save settings z menu głównego. Jeżeli chcemy usunąć któryś z certyfikatów należy wybrać go z listy i kliknąć Delete, a następnie zapisać konfigurację. Możliwe jest dodanie dowolnej liczby certyfikatów.



Możliwe jest również utworzenie połączenia z urządzeniami nie posiadającymi stałego adresu IP. W tym wypadku należy przejść do zakładki Mobile clients. Ustawienia są analogiczne do zakładki Tunnels, ale jest ich mniej (przykładowo nie ma miejsca na wpisanie klucza prywatnego-dla klientów mobilnych podajemy je w zakładce Keys and certificates).

UWAGA: Przy połączeniach IPsec może zajść potrzeba zdefiniowania routingu, co zostało opisane w kolejnej sekcji.

4.2.15 Generowanie certyfikatów SSL

Aby móc korzystać z uwierzytelniania za pomocą certyfikatów należy utworzyć kilka plików, których zawartość następnie należy wkleić do odpowiednich pól w konfiguracji www w zakładkach OpenVPN lub IPsec. Do całej procedury potrzebny jest komputer z systemem operacyjnym Linux z zainstalowanym pakietem programów openssl. Istnieje też wersja pakietu pod system Windows dostępna pod adresem ***http://gnuwin32.sourceforge.net/packages/openssl.htm***.

Na początku należy przygotować katalog, w którym będą przechowywane wszystkie klucze i certyfikaty. Powiedzmy że jest to katalog ~/klucze. Należy utworzyć w nim dwa pliki: listę wystawianych certyfikatów oraz plik do numerowania certyfikatów:

```
touch index.txt
echo 00 > serial
```

Oraz podkatalogi, w których będą trzymane klucze i certyfikaty:

```
mkdir private certs newcerts crl
```

Pierwszym krokiem jest stworzenie certyfikatu własnego „urzędu'' certyfikującego. Jest to nadrzędny certyfikat, na podstawie którego tworzone są inne. Po utworzeniu klucza prywatnego CA:

```
openssl genrsa -des3 -out private/cakey.pem 1024
```

Uwaga: należy dokładnie zapamiętać hasło do klucza prywatnego!
Należy wygenerować certyfikat CA:

```
openssl req -new -x509 -days 365 -key private/cakey.pem -out cacert.pem
```

Podczas tworzenia certyfikatu należy podać dane certyfikatu: kraj, województwo, miasto, nazwę firmy, jej sekcję, nazwę certyfikatu oraz adres e-mail. Najważniejszym polem jest nazwa (Common Name), reszta danych może być dowolna. Mając już swój własny urząd certyfikujący, należy następnie wystawić oddzielne certyfikaty dla każdego z urządzeń. Po utworzeniu klucza prywatnego:

```
openssl genrsa -des3 -out private/urzadzenie1key.pem
```

Należy wygenerować wniosek o wystawienie certyfikatu:

```
openssl req -new -key private/urzadzenie1key.pem -out urzadzenie1req.pem
```

Podczas tego procesu znowu należy podać dane. Mogą być one identyczne poprzednimi oprócz pola Common Name. Urząd certyfikujący podpisuje certyfikat:

```
openssl ca -notext -in urzadzenie1req.pem -out urzadzenie1cert.pem
```

Aby móc wykorzystać certyfikat w modemie MTX należy zdjąć hasło z klucza prywatnego:

```
openssl rsa -in private/urzadzenie1key.pem -out
private/urzadzenie1key.pem_bezhasla
```

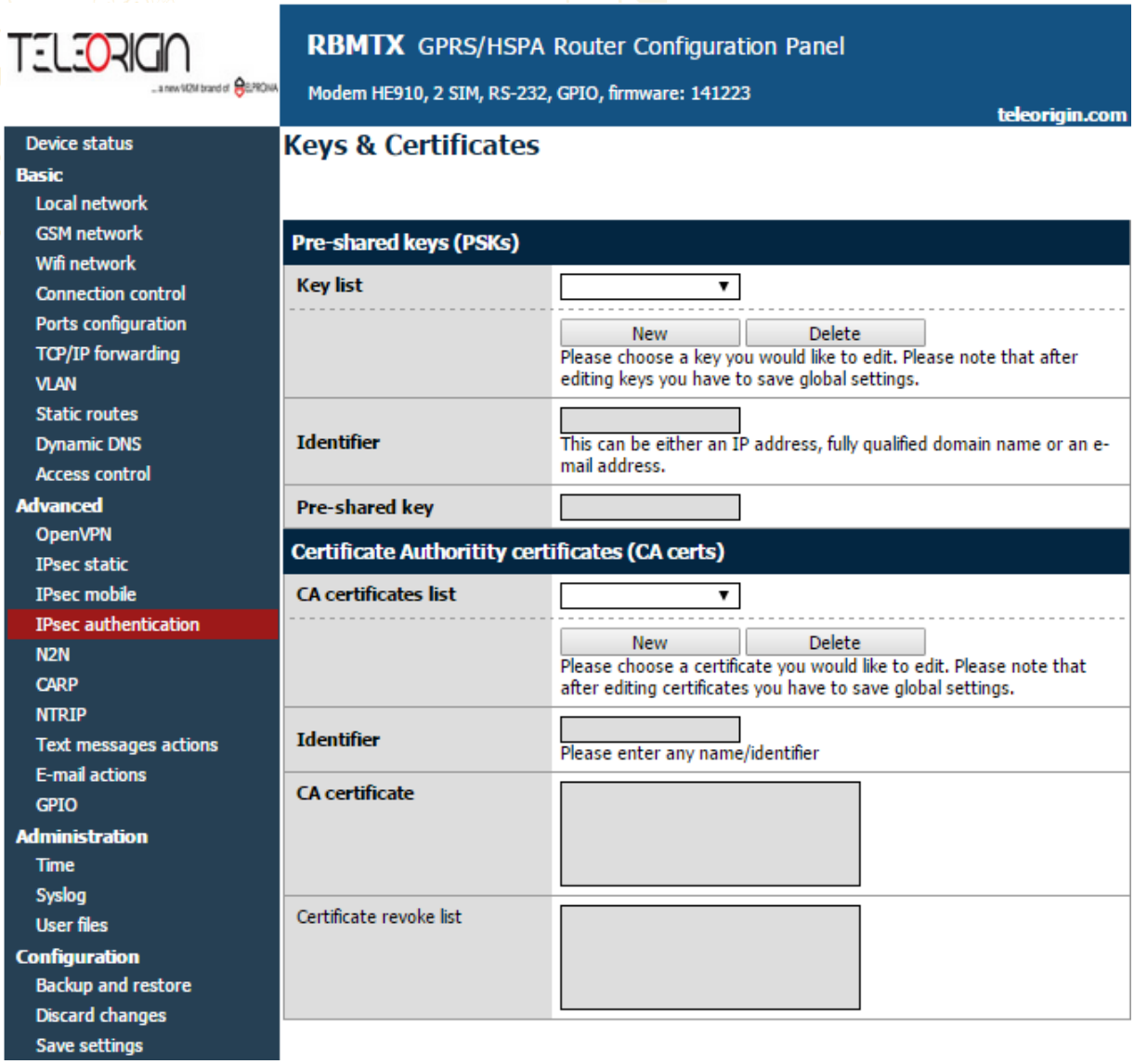
Procedurę należy powtórzyć dla każdego urządzenia (powinno się pamiętać o nadawaniu różnych Common Name i różnych nazw plików dla kolejnych urządzeń).

W konfiguracji www w zakładce IPsec/Tunnels (jeżeli ten protokół będzie wykorzystywany) w pole Certificate wklejamy zawartość pliku `urzadzenie1cert.pem`, w pole Key `urzadzenie1key.pem_bezhasla`. W pole peer certificate powinno się wkleić certyfikat drugiego urządzenia lub pozostawić je puste i wtedy w zakładce Keys and Certificates dodać nowy certyfikat CA i wkleić zawartość pliku `cacert.pem`.

Jeżeli potrzebne będzie korzystanie z protokołu OpenVPN, to konfiguracji www w zakładce OpenVPN w pole CA cert należy wkleić zawartość pliku `cacert.pem`, w pole Server/Client cert zawartość pliku `urzadzenie1cert.pem`, a w pole Server/Client private key zawartość pliku `urzadzenie1key.pem_bezhasla`. Dodatkowo dla OpenVPN powinno się wygenerować plik parametrami Diffiego-Hellmana:

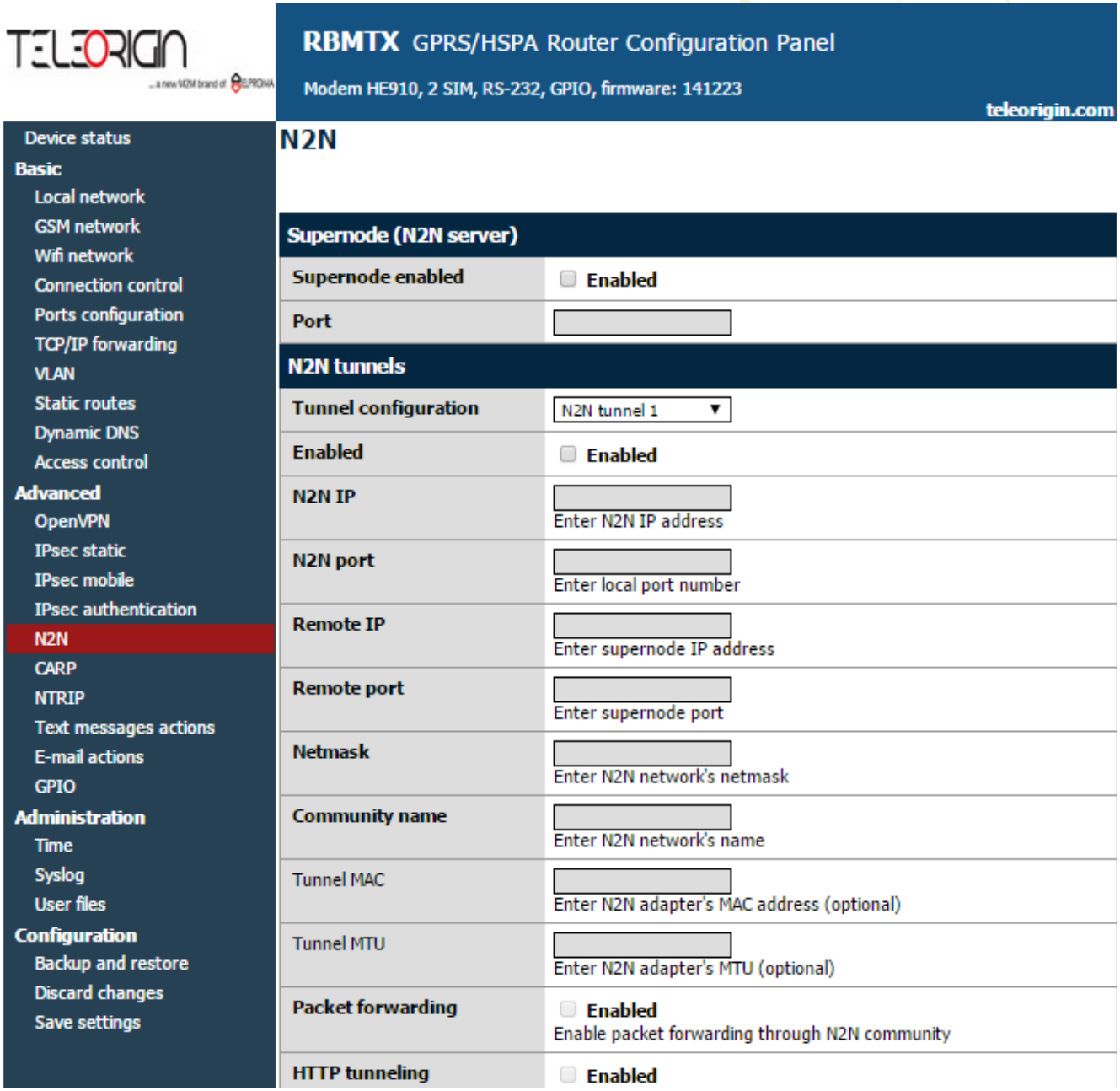
```
openssl dhparam -out dh1024.pem 1024
```

I jego zawartość wkleić w pole DH PEM. Plik ten, podobnie jak Certyfikat CA jest wspólny dla wszystkich urządzeń w sieci VPN.


RBMTX GPRS/HSPA Router Configuration Panel
Modem HE910, 2 SIM, RS-232, GPIO, firmware: 141223
teleorigin.com
Device status
Basic
Local network
GSM network
Wifi network
Connection control
Ports configuration
TCP/IP forwarding
VLAN
Static routes
Dynamic DNS
Access control
Advanced
OpenVPN
IPsec static
IPsec mobile
IPsec authentication
N2N
CARP
NTRIP
Text messages actions
E-mail actions
GPIO
Administration
Time
Syslog
User files
Configuration
Backup and restore
Discard changes
Save settings
Keys & Certificates
Pre-shared keys (PSKs)
Key list
New
Delete
Please choose a key you would like to edit. Please note that after editing keys you have to save global settings.
Identifier
This can be either an IP address, fully qualified domain name or an e-mail address.
Pre-shared key
Certificate Authoritity certificates (CA certs)
CA certificates list
New
Delete
Please choose a certificate you would like to edit. Please note that after editing certificates you have to save global settings.
Identifier
Please enter any name/identifier
CA certificate
Certificate revoke list

4.2.16 N2N

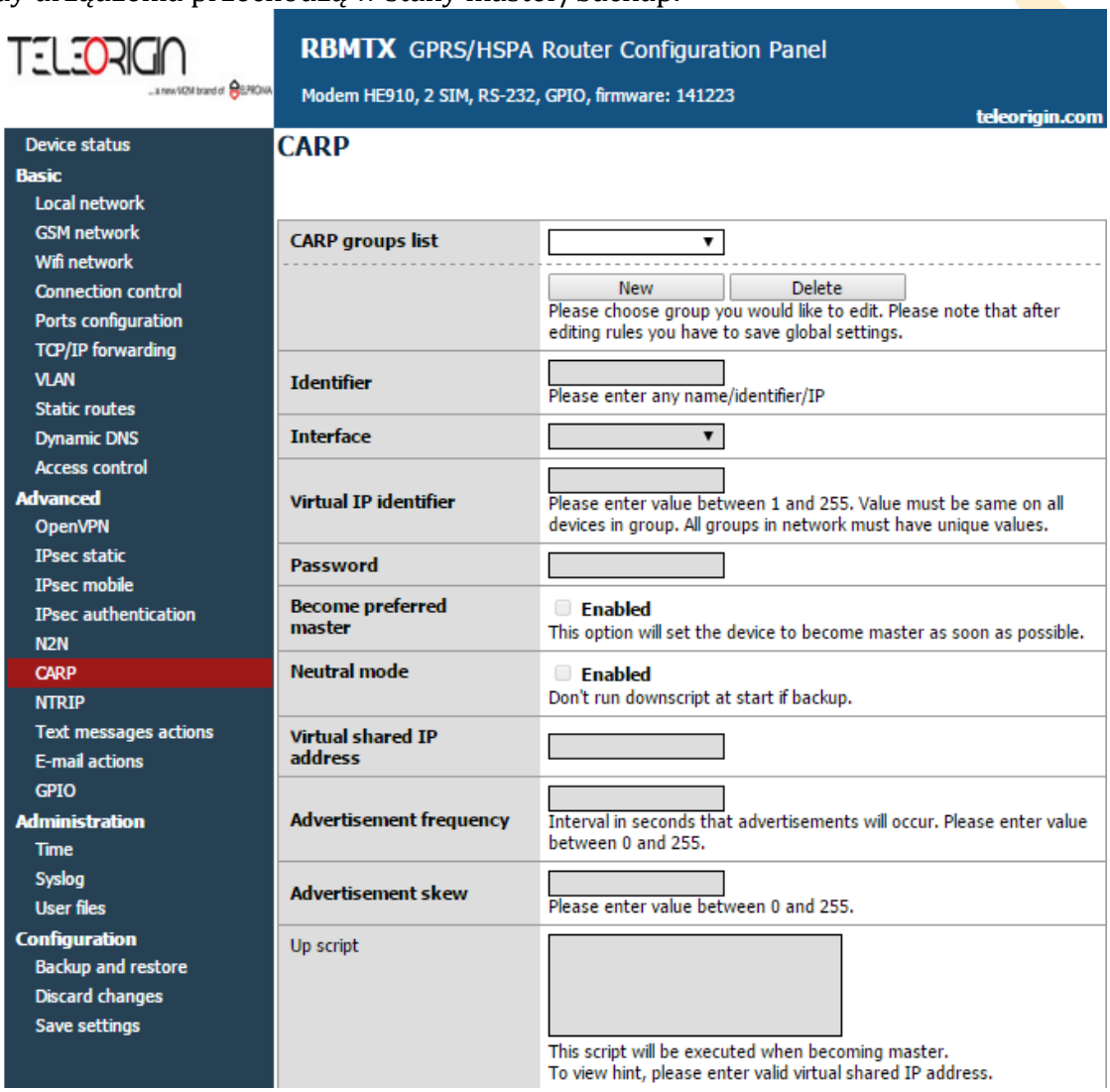
N2N to aplikacja umożliwiająca stworzenie bezpiecznej podsieci jak Open VPN i IPsec, aczkolwiek oparta jest ona na połączeniach typu P2P. Użytkownik może skonfigurować modem jako serwer N2N (wystarczy zaznaczyć opcję oraz wybrać port na którym ma być ona dostępna) oraz do czterech połączeń tunelowych. Aby skonfigurować tunel określ adres IP N2N, lokalny i zdalny port, maskę oraz zdalny adres IP. Musisz wprowadzić nazwę grupy (Community name) oraz klucz (wszyscy członkowie sieci N2N powinni mieć sprecyzowane oba parametry, pozostałe parametry powinny być wprowadzane tylko przez doświadczonych użytkowników).



4.2.17 CARP

CARP jest protokołem sieciowym umożliwiającym połączenie pomiędzy wieloma urządzeniami (redundancy group), które będą dostępne jako jedno urządzenie pod wskazanym adresem sieciowym. Przykładowo możesz wybrać urządzenia, które mają adresy IP 192.168.1.2 i 192.168.1.3 aby były dostępne pod adresem 192.168.1.115. Jeżeli jedno przestanie pracować, drugie z nich nie przestanie obsługiwać użytkowników. Urządzenie które jest aktualnie aktywne pod dzielonym adresem nazywane jest typu master, podczas gdy pozostałe nazywamy backup.

Jeżeli chcesz skonfigurować CARP, wybierz proszę interfejs sieciowy pod którym będzie dostępny klient CARP oraz wybierz identyfikator grupowy odpowiadający pozostałym urządzeniom z tej grupy – musi być to numer pomiędzy 1 a 255. Wprowadź wirtualny dzielony adres IP. Opcje Advertisement frequency oraz Advertisement skew regulują jak często urządzenia będą komunikować się między sobą. Pamiętaj aby zdefiniować skrypty up oraz down, które ustawią/skasują routing gdy urządzenia przechodzą w stany master/backup.

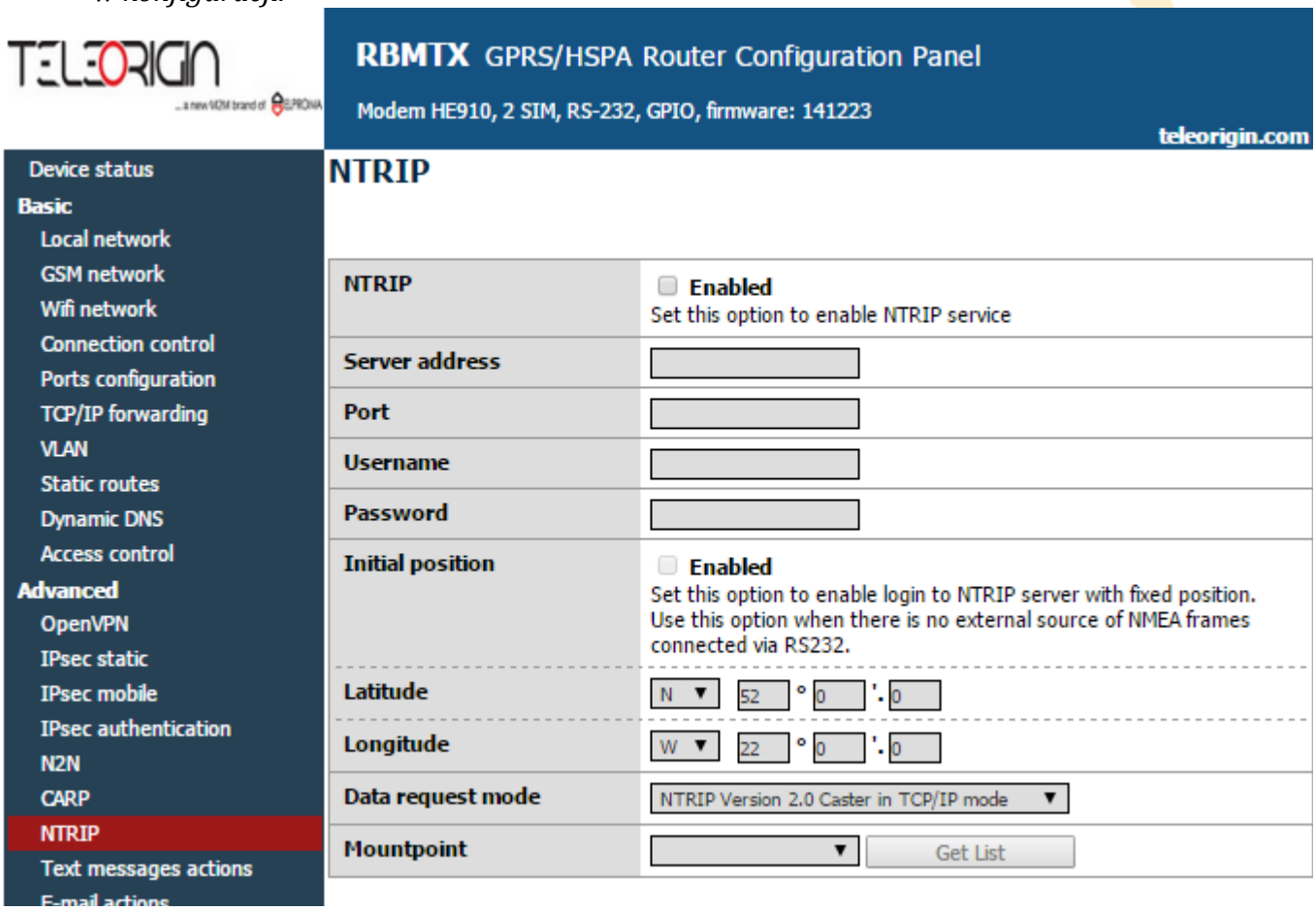


4.2.18 NTRIP configuration page

Jeden z trybów pracy portu /dev/ttyS0 jest komunikacja z urządzeniem zewnętrznym z użyciem protokołu NTRIP. Jeżeli zdecydujesz się użyć tego trybu, niezbędne będzie ustawienie tego trybu w zakładce RS232 Port. Następnie wejdź w zakładkę NTRIP. Pola adresu serwera, portu i pozycji początkowej są wymagane. Nazwa użytkownika i hasło są opcjonalne.

Możliwe jest także uruchomienie trybu Data Request. Po wprowadzeniu wymaganych danych w pola, kliknij przycisk Get List aby pobrać listę źródeł z serwera – może to zająć chwilę. Po zakończeniu pobierania wybierz jedno ze źródeł.

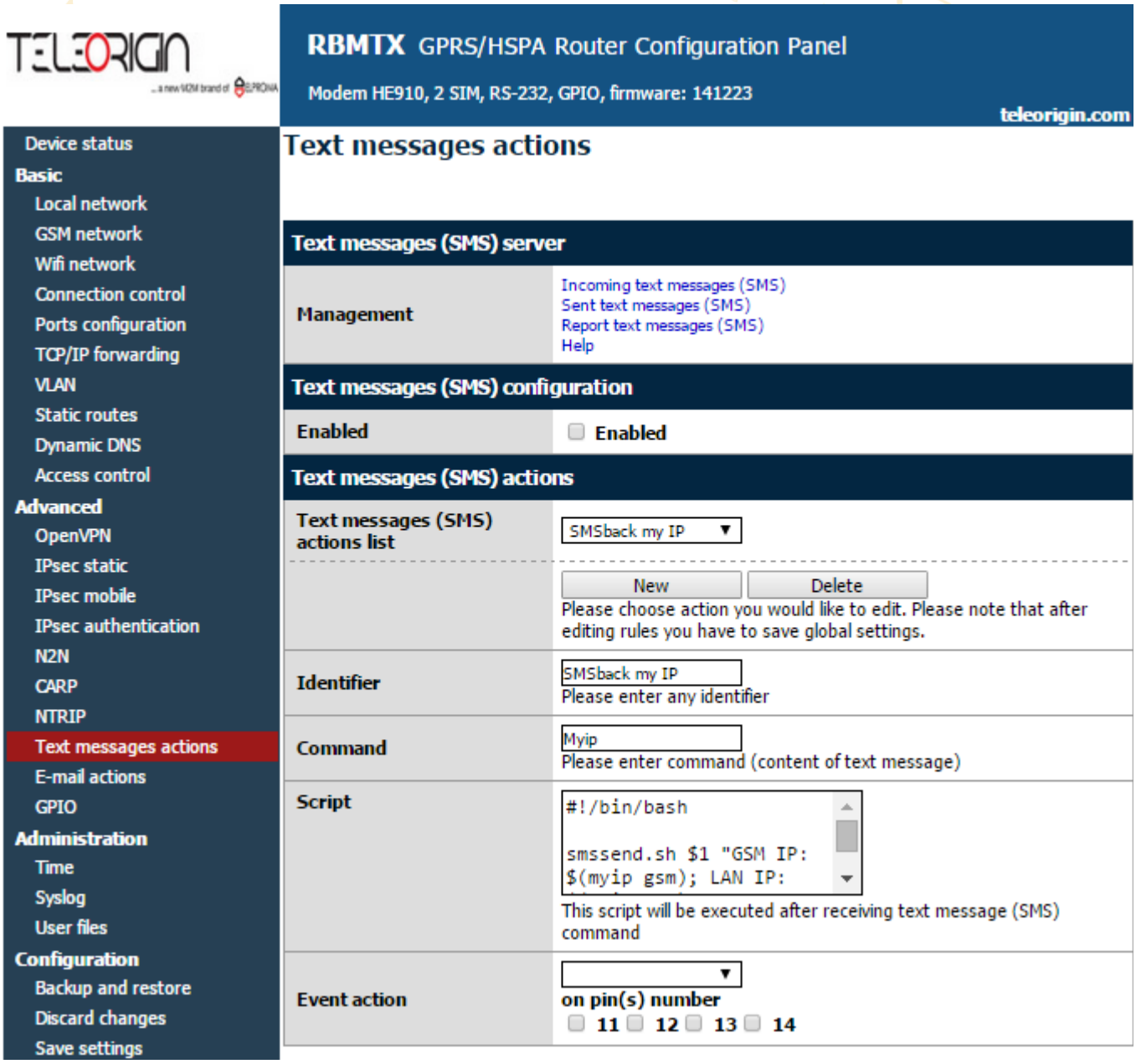
Uwaga: *Wprowadzenie pozycji początkowej jest niezbędne aby zalogować się do serwera NTRIP. Pozycja może być oszacowana w przybliżeniu, proszę wybrać pozycję która na pewno jest w zasięgu kraju użytkowania. Jeżeli podłączysz urządzenie zewnętrzne do portu S0, który wysyła ramki NMEA, zostaną one przesłane do serwera I odpowiedzi tego serwera będą dotyczyły obecnej pozycji, a nie tej zapisanej w konfiguracji.*



4.2.19 SMS Actions

Zakładka SMS Actions umożliwia użytkownikowi zdefiniowanie skryptów które zostaną uruchomione gdy modem odbierze SMS z określoną zawartością.

Aby włączyć tę opcję należy upewnić się że globalne pole SMS Actions jest zaznaczone oraz że jeden z portów jest ustawiony w tryb SMS receiving w zakładce Ports configuration. Następnie należy kliknąć w przycisk New, wprowadzić jakikolwiek identyfikator oraz komendę SMS która wywoływać będzie akcję. Możliwe jest zainicjowanie dowolnego skryptu (typu shell) i/oraz ustawienie akcji na GPIO.



4.2.20 GPIO

Dzięki ustawieniom w zakładce GPIO konfiguracji www możliwa jest obsługa zewnętrznych portów wejściowych i wyjściowych GPIO. W momencie przełączenia zakładki na GPIO automatycznie wczytuje się aktualny stan portów GPIO reprezentowany przez osiem pól w górnej części strony. W całej konfiguracji przyjęto konwencję zaznaczone pole-stan wysoki, odznaczone pole-stan niski. Poprawne wczytanie stanu sygnalizuje napis „OK'', w razie błędu wyświetlany jest napis „ERROR!''. Jeżeli użytkownik chce odświeżyć stan portów, należy kliknąć przycisk Refresh.

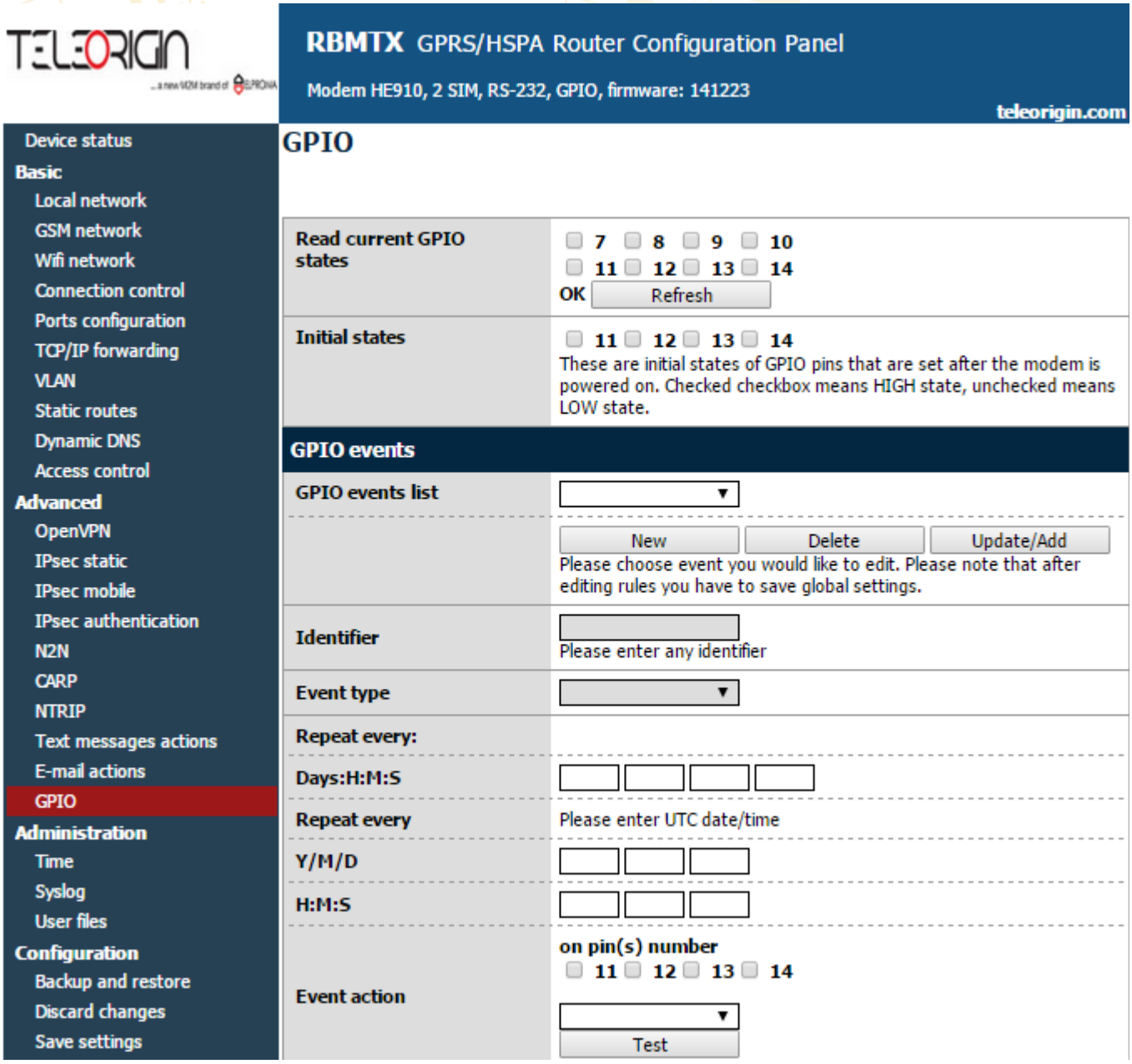
Pola 11,12,13,14 w sekcji Initial States pozwalają na ustalenie początkowego stanu wyjść. Stan początkowy jest ustalany w momencie włączania modemu oraz w przypadku zmiany i zapisania nowej konfiguracji GPIO.

W selekcji GPIO events możliwe jest dodawanie dowolnej liczby zdarzeń. Zdarzenie polega na zmianie stanu na jednym lub wielu portach GPIO. Aby dodać nowe wydarzenie należy kliknąć przycisk New, następnie wypełniamy wszystkie pola. Identyfikator (Identifier) służy jedynie rozróżnianiu wydarzeń i może być dowolnym ciągiem znaków. Event type to typ zdarzenia: może ono występować jednorazowo (One time) lub w regularnych odstępach czasu (Regular). W przypadku zdarzenia jednorazowego należy podać dokładną datę i godzinę zdarzenia (czas UTC, należy upewnić się czy na urządzeniu ustawiono poprawny czas!), w przypadku zdarzenia wielokrotnego ustalamy co jaki czas będzie ono powtarzane. Ostatnim ustawieniem jest Event action. Należy wybrać, których pinów dotyczyć będzie wydarzenie i jaką czynność na nich wykonać (zmienić stan na wysoki, zmienić stan na niski lub przełączyć stan na przeciwny). Przykładowo jeżeli zaznaczymy piny 11 i 13 oraz „Set HIGH state'' to w momencie wykonania zdarzenia na pinach 11 i 13 ustalony zostanie stan wysoki natomiast na pinach 12 i 14 stan nie zostanie zmieniony i zostanie taki jak przed wydarzeniem. Możliwe jest też przetestowanie wydarzenia za pomocą przycisku Test (po kliknięciu Test stan pinów na górze strony zostanie odświeżony automatycznie).

Możliwe jest również ręczne sterowanie portami GPIO używając skryptu php dostępnego pod adresem `<ip_urzadzenia>/actions/gpio.php`. Parametry są przekazywane do skryptu poprzez następujące argumenty:

Parametr	Dozwolone wartości
cmd	readall (czytaj wszystkie porty), read (czytaj wybrane porty), write (zmień stan na porcie)
pins	Dowolna kombinacja pinów 7-14 rozdzielonych przecinkami
state	H,L,I,S (stan wysoki, stan niski, wejście, zmiana stanu na przeciwny)

`readall` nie wymaga dodatkowych parametrów. `read` i `write` wymagają ustalenia parametru `pins`. `write` wymaga podania parametru `state`. Należy pamiętać, że nie jest możliwa zmiana stanu na pinach wejściowych. Parametry powinny być podane w polu adresu po znaku `?`. Parametr i jego wartość powinny być rozdzielone znakiem `=`. Każda para parametr-wartość powinna być rozdzielona znakiem `&` (patrz przykłady).

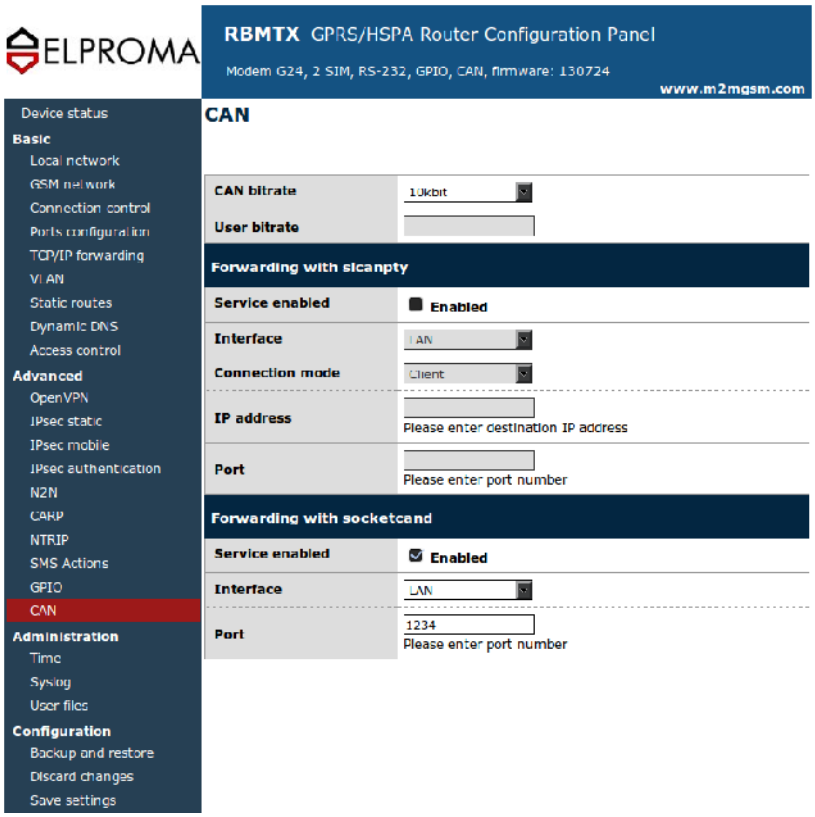


Przykłady:

- `192.168.1.234/gpio.php?cmd=readall` -Wyświetla stan wszystkich portów
- `192.168.1.234/gpio.php?cmd=read&pins=14` -Wyświetla stan wyjścia numer 14 (fizycznie)
- `192.168.1.234/gpio.php?cmd=write&pins=11,12&state=L` -Ustawia stan iniski na wyjściach numer 11 i 12 (fizycznie). Po poprawnym wykonaniu skryptu nic nie jest wyświetlane.

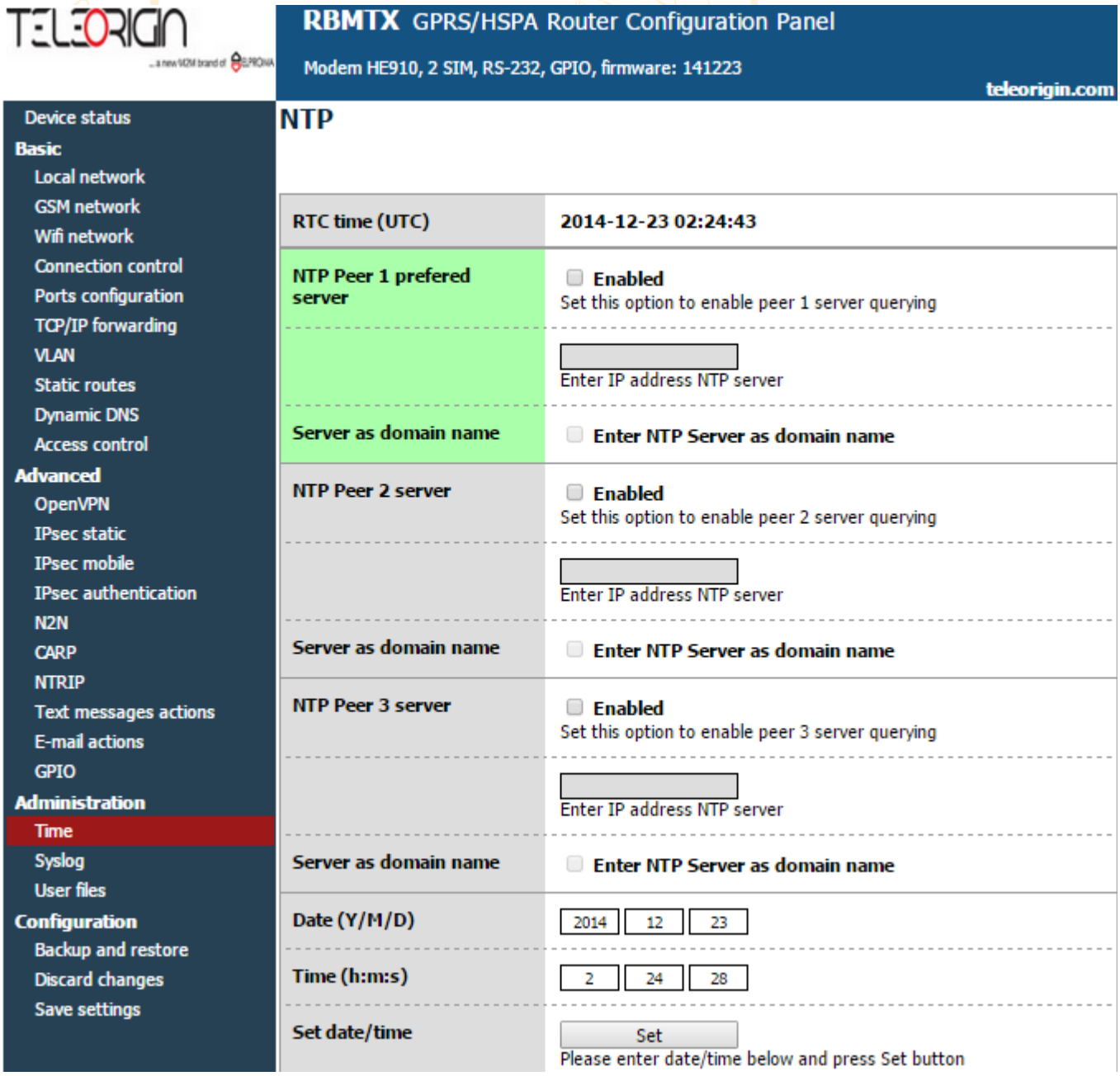
4.2.21 CAN

Jeżeli posiadasz modem wyposażony w interfejs CAN możliwe jest skonfigurowanie go w zakładce CAN. Możliwe jest ustawienie predkości pracy (baudrate) lub przekierowanie ramek CAN do TCP z użyciem slcanpty lub socketcand.



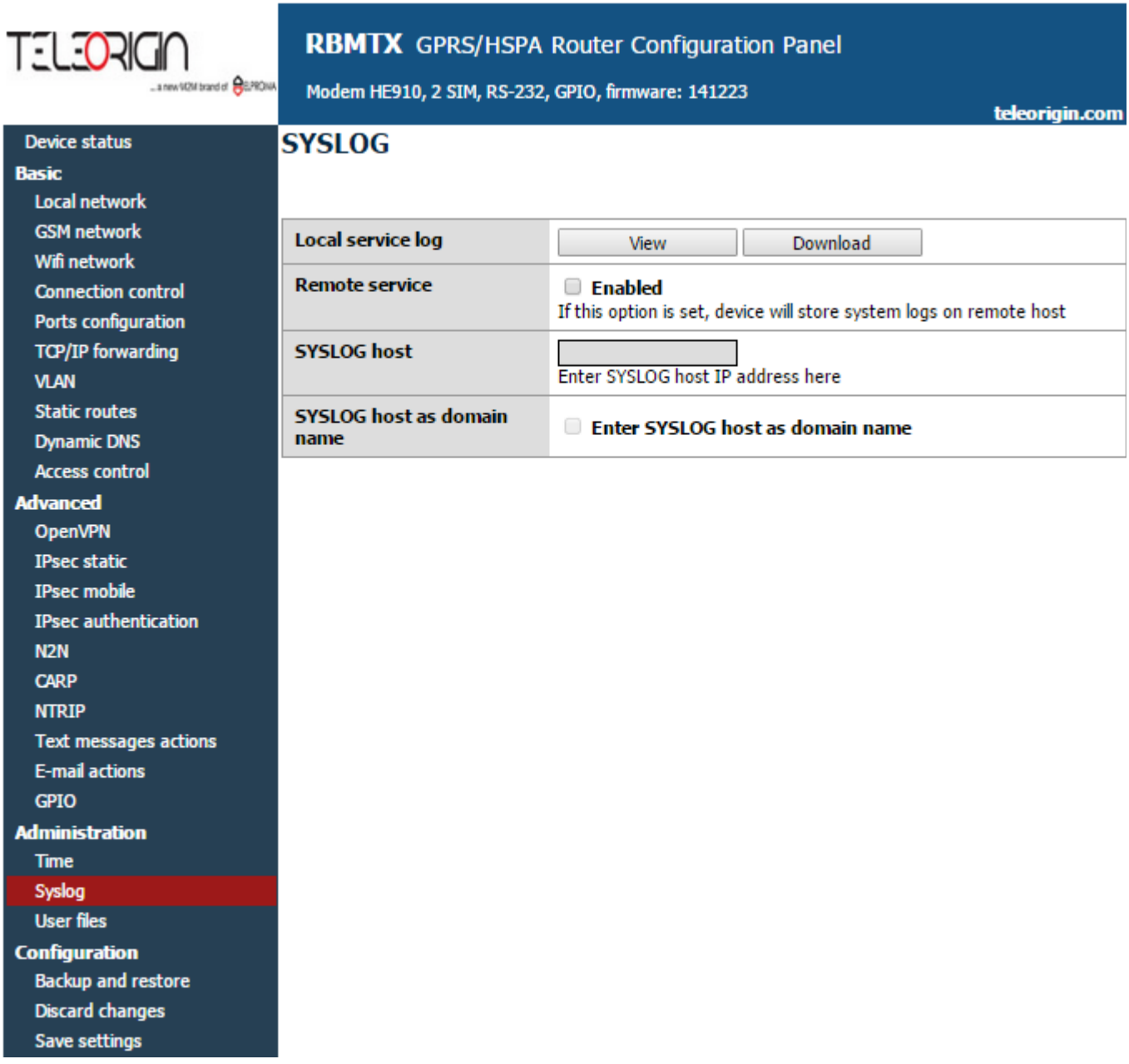
4.2.22 Time

Zakładka Time pozwala na ręczne ustawienie zegara sprzętowego lub wprowadzenie adresu IP serwera NTP w celu automatycznej synchronizacji zegara.



4.2.23 Syslog

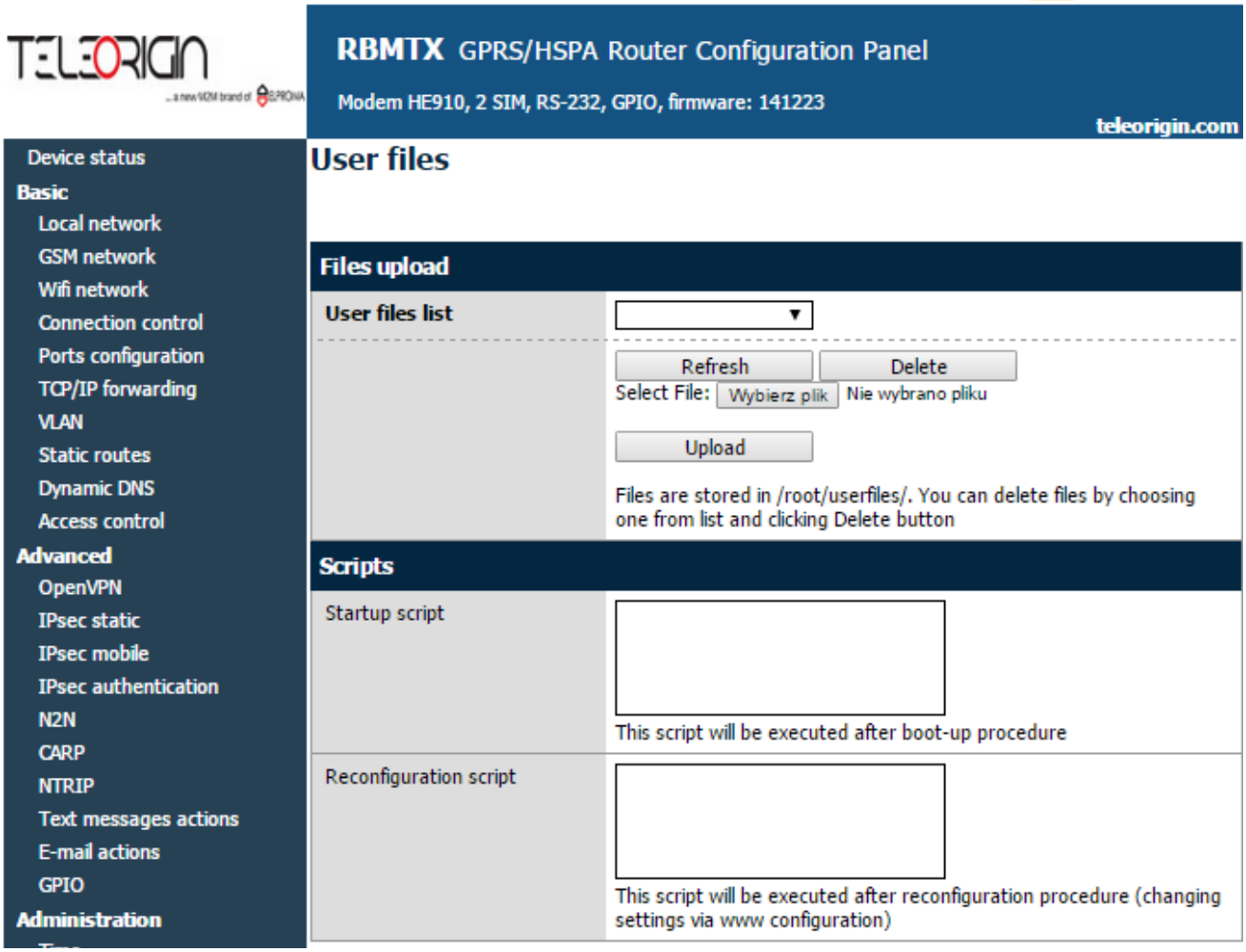
W tej zakładce definiujesz jak modem powinien zapisywać logi. Modem posiada wewnętrzną pamięć która zostaje nadpisana po przekroczeniu jej końca. Możliwe jest zapisanie logów na komputerze klikając przycisk Download. Dodatkowo istnieje możliwość zdalnego dostępu do logów włączając opcję Remote service i ustawieniu hosta SYSLOG.



4.2.24 Pliki użytkownika

Użytkownik może wgrać na modem własne skrypty i pliki wykonywalne oraz zaprogramować ich wykonywanie w określonych sytuacjach. Służy do tego zakładka **User files**.

Na samej górze zakładki znajduje się lista plików użytkownika (wczytywana automatycznie po przejściu do zakładki). Możliwe jest wybranie dowolnego pliku i jego usunięcie za pomocą przycisku Delete. Lista plików może zostać odświeżona na żądanie użytkownika przyciskiem Refresh. Do wgrywania nowych plików służy przycisk Upload new. Po jego wciśnięciu nastąpi przekierowanie do oddzielnej strony, gdzie po wciśnięciu przycisku Przeglądaj... wybieramy plik z komputera, który ma być przesłany do modemu. Po wybraniu pliku należy kliknąć przycisk Upload. Jeżeli plik zostanie przesłany poprawnie zostanie wyświetlony odpowiedni komunikat, bądź komunikat błędu oraz link pozwalający na powrót do strony głównej konfiguracji www. Wszystkim wgrywanym plikom użytkownika nadawane są prawa pliku wykonywalnego, co pozwala na ich użycie w skryptach (np. skryptach startowych modemu lub skryptach startowych VPN).



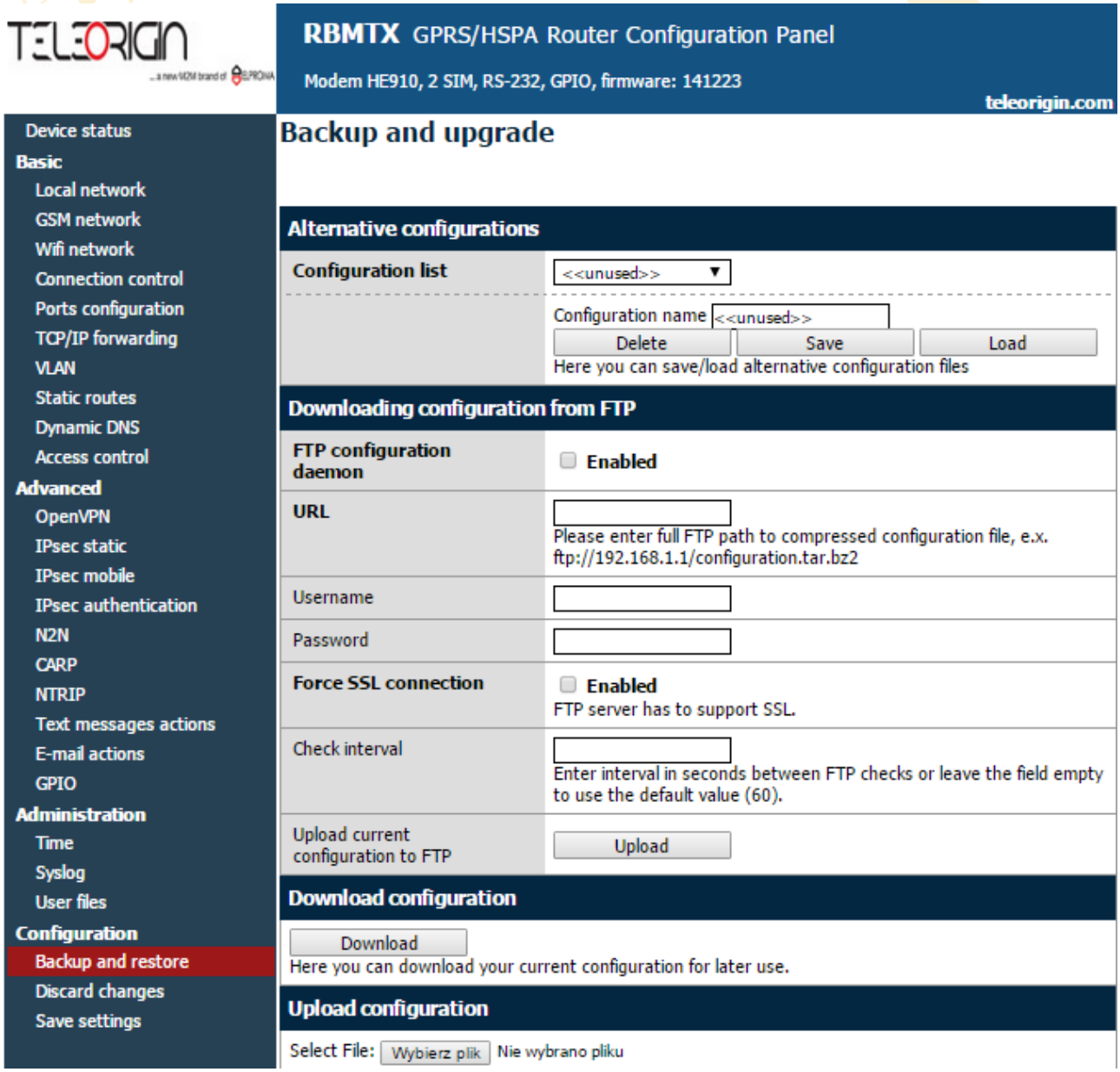
Poniżej panelu zarządzania plikami użytkownika znajdują się dwa pola, Startup script oraz Reconfiguration script. Skrypty te są wykonywane odpowiednio przy uruchamianiu modemu (po wykonaniu wszystkich czynności startowych) oraz po zapisaniu konfiguracji modemu (korzystając z przycisku Save Configuration w konfiguracji www). Skrypty mogą być napisane w języku Bash lub PHP, należy jednak pamiętać o umieszczeniu odpowiedniego nagłówka na początku skryptu (#!/bin/bash lub #!/usr/bin/php). W skryptach istnieje możliwość uruchamiania plików użytkownika, należy jedynie pamiętać, że są one przechowywane w katalogu /root/userfiles.

UWAGA: Pliki binarne wgrywane do modemu muszą być skompilowane pod procesor zainstalowany w modemie!

4.2.25 Zapisywanie/przywracanie kopii zapasowej konfiguracji modemu

Zakładka **Backup and restore** umożliwia następujące operacje:

- Zapis/Odczyt alternatywnych ustawień
- Konfiguracja klienta FTP: cykliczne sprawdzenie serwera FTP pod kątem zmian konfiguracji
- Pobranie/Wysłanie kopii zapasowej konfiguracji



4.2.26 Discard changes

Porzucenie zmian możliwe jest po wciśnięciu przycisku **Discard changes.**

4.2.27 Save settings

W celu zapisania zmian należy kliknąć przycisk **Save settings** i poczekać na wiadomość potwierdzającą wykonanie tej operacji.

4.3 Opis logów systemowych

Poniżej znajduję się przykładowy log wraz z opisem podstawowych czynności:

01/01/0000:00:30 rbmtx syslogd 1.4.1: restart.
01/01/0000:00:31 rbmtx Start: RBMTX - FIRM:140626 – **informacje o modemie i wer. firmware'u**
01/01/0000:00:35 rbmtx supervisor[560]: SIM Holder open/closed – **Kieszeń SIM zamknięta/otwara przez oprogramowanie.**
01/01/0000:00:36 rbmtx supervisor[560]: Modem init 1 – **pierwsza próba inicjalizacji**
01/01/0000:01:09 rbmtx supervisor[560]: Init /dev/ttyS1 – **inicjalizacja portu**
01/01/0000:01:10 rbmtx supervisor[560]: Init /dev/ttyACM0
01/01/0000:01:13 rbmtx supervisor[560]: Modem is not registered on the GSM network – **modem nie może zalogować się do sieci**
01/01/0000:01:13 rbmtx supervisor[560]: Entering Modem is ready
01/01/0000:01:13 rbmtx supervisor[560]: Entering PIN OK – **modem jest gotowy do połączenia**
01/01/0000:01:13 rbmtx supervisor[560]: Entering PIN error code: - **zły kod PIN**
01/01/0000:01:14 rbmtx login[811]: unable to change tty `/dev/ttyS0' for user `root'
01/01/0000:01:14 rbmtx login[811]: ROOT LOGIN on `ttyS0'
01/01/0000:01:20 rbmtx pppd[901]: pppd 2.4.5 started by root, uid 0 – **połączenie**
01/01/0000:01:21 rbmtx chat[903]: timeout set to 2 seconds
01/01/0000:01:21 rbmtx chat[903]: send (AT)
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: AT
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (ATZ0)
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: ATZ0
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (AT)
01/01/0000:01:21 rbmtx chat[903]: abort on (NO DIALTONE)
01/01/0000:01:21 rbmtx chat[903]: abort on (ERROR)
01/01/0000:01:21 rbmtx chat[903]: abort on (NO ANSWER)
01/01/0000:01:21 rbmtx chat[903]: abort on (BUSY)
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: AT
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (ATZ0)
01/01/0000:01:21 rbmtx chat[903]: abort on (NO CARRIER)
01/01/0000:01:21 rbmtx chat[903]: timeout set to 30 seconds
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: ATZ0
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (AT)
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: AT

```
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (AT+CGDCONT=1,"ip","example.apn")
01/01/0000:01:22 rbmtx chat[903]: clear abort on (ERROR)
01/01/0000:01:22 rbmtx chat[903]: send (dddATD*99#)
01/01/0000:01:23 rbmtx supervisor[560]: pppd check loop:1
01/01/0000:01:25 rbmtx chat[903]: expect (CONNECT)
01/01/0000:01:25 rbmtx chat[903]: AT+CGDCONT=1,"ip","example.apn"
```

4.4 Aktualizacja oprogramowania

Rozdział ten opisuje sposób aktualizacji oprogramowania modemu. Aktualny numer oprogramowania można znaleźć tutaj: ***http://x.x.x.x/firmware.php*** gdzie *x.x.x.x* to adres IP Twojego modemu. (fabrycznie 192.168.1.234).

Do aktualizacji potrzebne są następujące pliki:

- plink.exe (putty)
- pscp.exe (putty)
- service.key (klucz prywatny)
- servicekey.ppk (klucz prywatny wygenerowany przez putty)
- upgrade.bat (skryp aktualizujący)
- upload_img.bat (skopiuj plik .bin do scryptu)
- upgrade_20110301.bin (nazwa zależy od wersji aktualizacji)

W celu zaktualizowania oprogramowania należy poczynić następujące kroki:

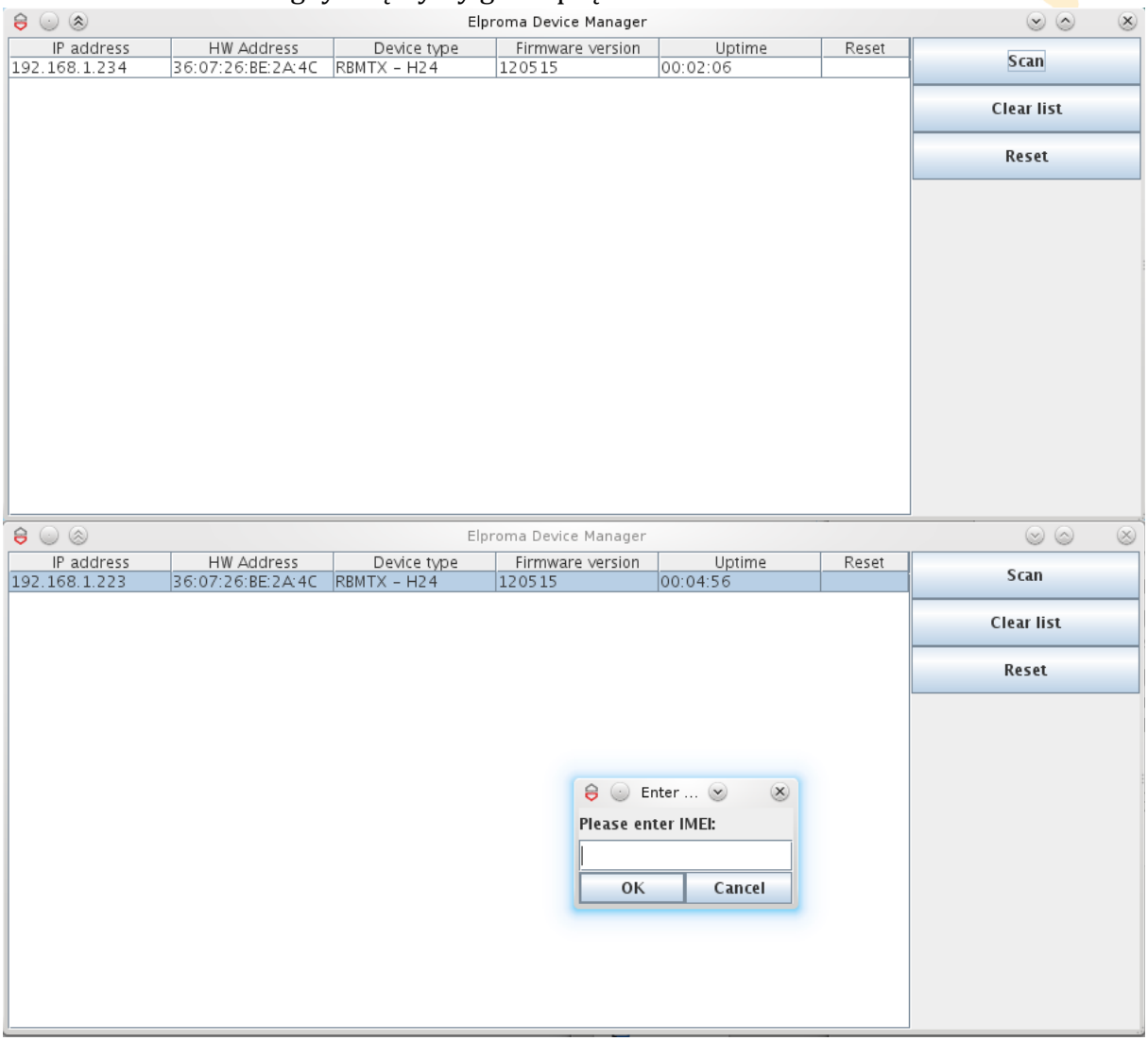
- Uruchom plik upload_img.bat z parametrami: plik i adres IP
  upload_img.bat upgrade_20101001.bin 192.168.1.234
  W systemie Windows (pamiętaj o znaku ":" na końcu wiersza):
  pscp -scp -i servicekey.ppk -P 65535 service@192.168.1.234:
  W systemie Linux:
  scp -i service.key -P 65535 upgrade.bin service@IP:
- Uruchom plik
  upgrade.bat 192.168.1.234
  Windows OS:
  plink -ssh -i servicekey.ppk -P 65535 service@192.168.1.234 upgrade
  Linux OS:
  ssh -i service.key -p 65535 service@192.168.1.234 upgrade
- Możesz użyć także komend reboot, delusblog, help, np. by zresetować:
  plink -ssh -i servicekey.ppk -P 65535 service@192.168.1.234 reboot

4.5 Elproma Device Manager

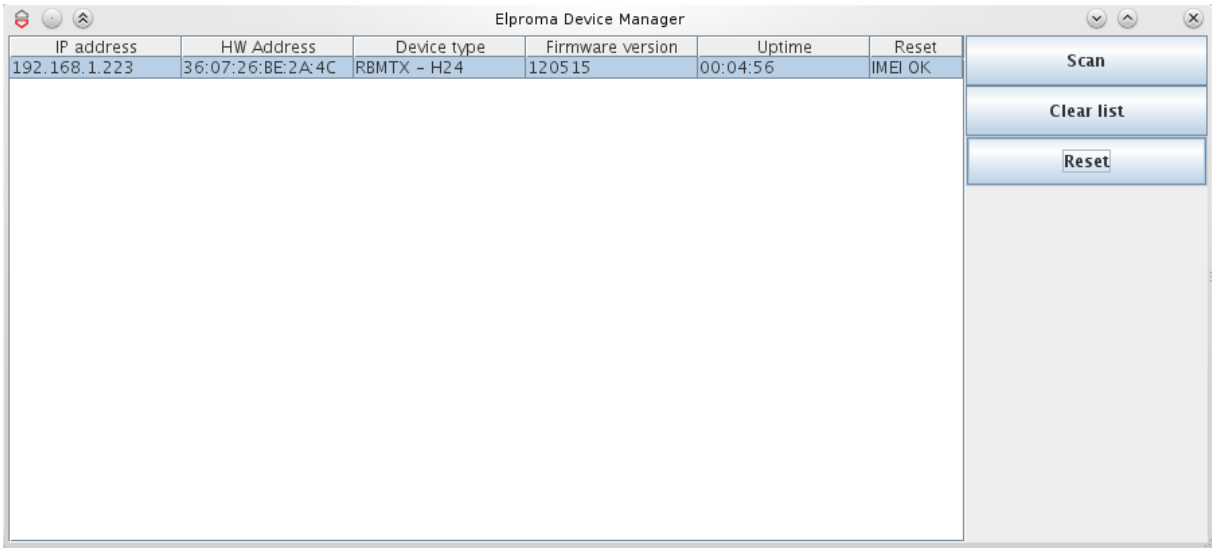
Elproma Device Manager to program pozwalający na wyszukiwanie modemów RB MTX w lokalnej sieci komputerowej (LAN). Za jego pomocą można przywracać ustawienia fabryczne urządzeń na podstawie numeru IMEI, co jest szczególnie przydatne w wypadku gdy użytkownik zapomniał numeru IP konkretnego urządzenia i nie ma możliwości kontrolowania go.

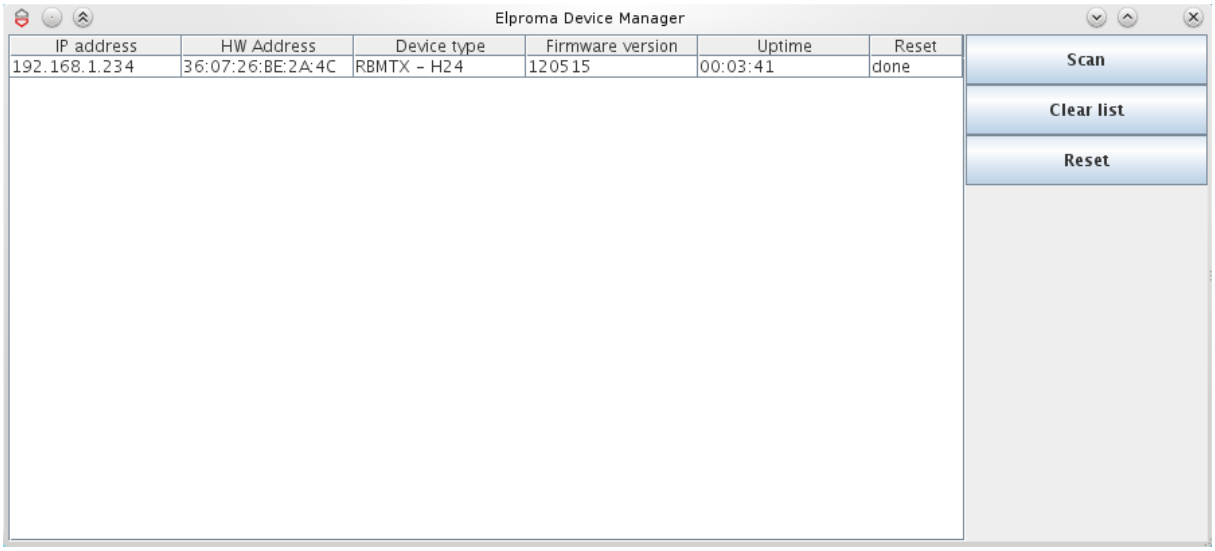
Instalacja programu jest bardzo prosta - wystarczy uruchomić plik ***.exe*** i wybrać ścieżkę, gdzie aplikacja zostanie rozpakowana. Główne okno programu składa się z tabeli, w której wyświetlane są informacje o znalezionych urządzeniach oraz przycisków: Scan (Skanuj), Clear list (Wyczyść listę), Reset (Przywróć ustawienia fabryczne) oraz About (Informacje o programie).

Na początku pracy z programem należy przeskanować lokalną sieć w poszukiwaniu modemów. Zwykle trwa to kilka sekund w zależności od natężenia ruchu w sieci. Należy pamiętać, że uruchomienie całego oprogramowania przez modem może potrwać do kilku minut, dlatego też nie będzie odpowiadał on przy skanowaniu od razu gdy włączymy go do prądu.



Po skanowaniu możemy z tabeli odczytać informacje o znalezionych urządzeniach takie jak adres IP (IP address), adres MAC (MAC address), nazwa urządzenia (Device name), wersja oprogramowania (Firmware ver.) i czas od włączenia (Uptime). Jeżeli chcemy przywrócić konfigurację fabryczną któremuś z urządzeń na liście, należy nacisnąć przycisk Reset i wpisać IMEI. Program wyśle specjalny pakiet do wszystkich urządzeń, ale konfiguracja fabryczna zostanie przywrócona tylko na tym urządzeniu, o podanym przez użytkownika numerze IMEI. Jeżeli podano prawidłowy IMEI w ostatniej kolumnie tabeli przy jednym z urządzeń wyświetli się „IMEI OK''. Urządzenie zostanie uruchomione ponownie aby załadować nową konfigurację i po około 1-2 minutach potwierdzi całą operację - napis „IMEI OK'' powinien zamienić się na „done'' (Zrobione).





5 Rozwiązywanie problemów

5.1 Brak połączenia/komunikacji z modemem

W przypadku gdy nie ma połączenia/komunikacji z modemem zrób następujące:

- Sprawdź połączenia kablowe modemu (USB, RS232 etc.)
- Sprawdź czy zasilanie podłączone jest poprawnie.
- Sprawdź parametry TCP/IP
- Sprawdź czy urządzenie nie jest blokowane przez firewall

5.2 Modem połączony, brak połączenia z internetem

W przypadku gdy nie ma połączenia z Internetem zrób następujące:

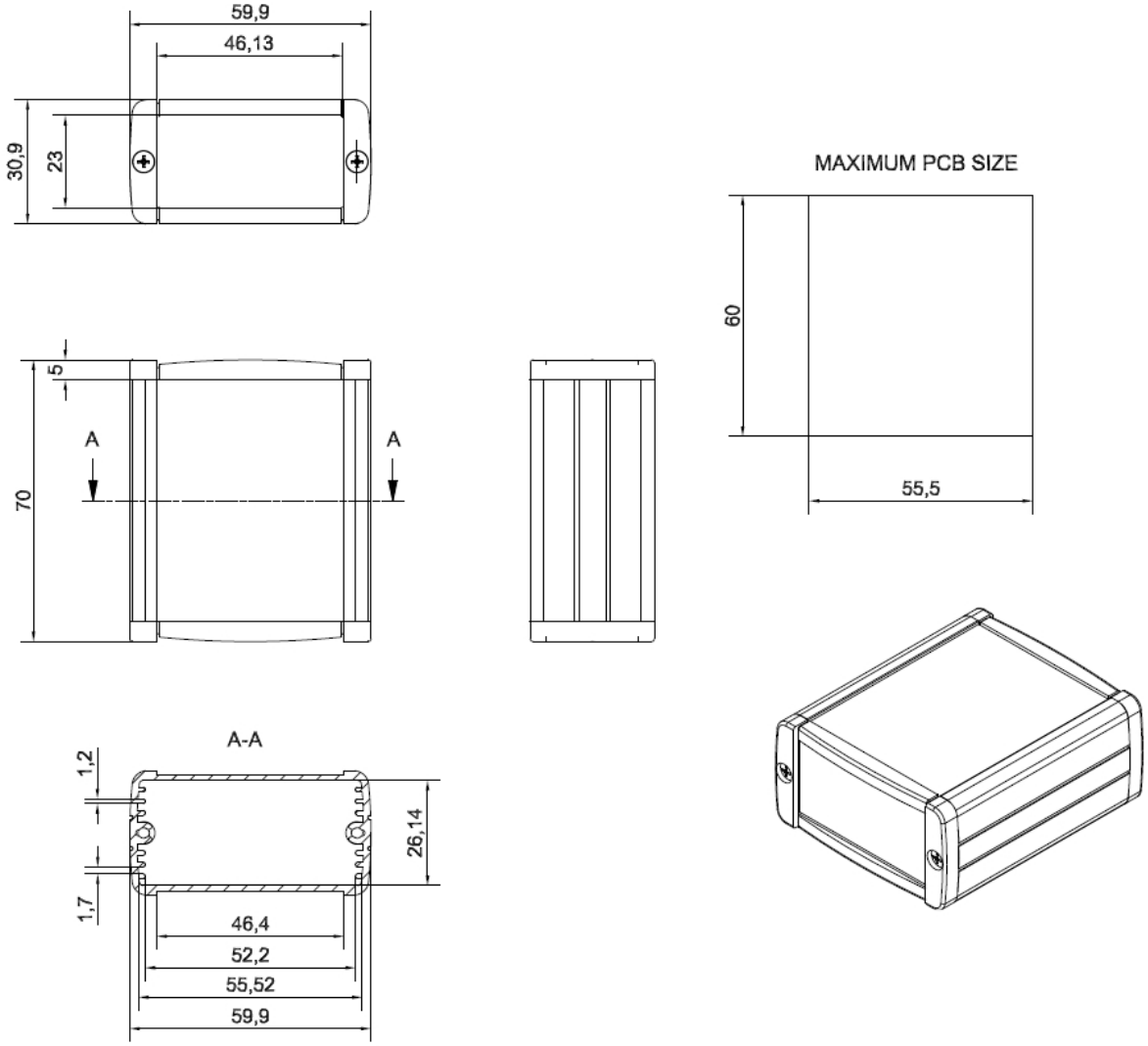
- Sprawdź podłączenie anteny
- Sprawdź zasięg sieci GSM/UMTS/LTE w miejscu użytkowania (np. na stronie operatora GSM)
- Sprawdź czy modem skonfigurowany jest poprawnie (parametry punktów dostępowych APN)
- W celu korzystania z internet mobilnego należy mieć uruchomioną usługę internetu, jeżeli Twoja karta SIM nie posiada tej usługi skontaktuj się z operatorem

6 Charakterystyka techniczna

6.1 Charakterystyka mechaniczna

Maksymalne rozmiary	70 x 59,9 x 30,9 mm (bez złącz) 80 x 59,9 x 30,9 mm (ze złączami)
Waga	≈138,3 g (tylko modem bez dodatkowych dołączeń) ≈145,7g (modem z anteną)
Objętość	≈129,56 cm3 (bez złącz)

6.2 Obudowa



6.3 Charakterystyka elektryczna

6.3.1 Zasilanie

- Nominalny zakres zasilania: 9V..30V
- Maksymalna (średnia) wartość prądu ciągłego: +800 mA max
- Pik (chwilowy), prąd: 2 A

6.3.2 Charakterystyki RF

6.3.2.1 Zakres częstotliwości dla wersji HSPA+

Mode	Freq. TX (MHz)	Freq. RX (MHz)	Channels	TX - RX offset
GSM850	824 ~ 849	869 ~ 894	128 ~ 251	45 MHz
EGSM900	890 ~ 915	935 ~ 960	0 ~ 124	45 MHz
	880 ~ 890	925 ~ 935	975 ~ 1023	45 MHz
DCS1800	1710 ~ 1785	1805 ~ 1880	512 ~ 885	95MHz
PCS1900	1850 ~ 1910	1930 ~ 1990	512 ~ 810	80MHz
WCDMA800 * (band VI)	830~840	875~885	Tx: 4162 ~ 4188 Additional: 812, 837 Rx: 4387 ~ 4413 Additional: 1037, 1062	45MHz
WCDMA800 * (band XIX)	830~845	875~890	Tx: 312~363 Additional: 387, 412, 437 Rx: 712~763 Additional: 787, 812, 837	45MHz
WCDMA850 (band V)	824 ~ 849	869 ~ 894	Tx: 4132 ~ 4233 additional 782, 787, 807, 812, 837, 862 Rx: 4357 ~ 4458 additional 1007, 1012, 1032, 1037, 1062, 1087	45MHz
WCDMA900 (band VIII)	880 ~ 915	925 ~ 960	Tx: 2712 ~ 2863 Rx: 2937 ~ 3088	45MHz

6.3.2.2 Zakres częstotliwości dla wersji UMTS

Mode	Freq. TX (MHz)	Freq. RX (MHz)	Channels	TX - RX offset
GSM850	824.2 ~ 848.8	869.2 ~ 893.8	128 ~ 251	45 MHz
EGSM900	890.0 ~ 914.8	935.0 ~ 959.8	0 ~ 124	45 MHz
	880.2 ~ 889.8	925.2 ~ 934.8	975 ~ 1023	45 MHz
DCS1800	1710.2 ~ 1784.8	1805.2 ~ 1879.8	512 ~ 885	95MHz
PCS1900	1850.2 ~ 1909.8	1930.2 ~ 1989.8	512 ~ 810	80MHz
WCDMA850 (band V)	826.4 ~ 846.6	871.4 ~ 891.6	Tx: 4132 ~ 4233 Rx: 4357 ~ 4458	45MHz
WCDMA900 (band VIII)	882.4 ~ 912.6	927.4 ~ 957.6	Tx: 2712 ~ 2863 Rx: 2937 ~ 3088	45MHz
WCDMA1900 (band II)	1852.4 ~ 1907.6	1932.4 ~ 1987.6	Tx: 9262 ~ 9538 Rx: 9662 ~ 9938	80MHz
WCDMA2100 (Band I)	1922.4 ~ 1977.6	2112.4 ~ 2167.6	Tx: 9612 ~ 9888 Rx: 10562 ~ 10838	190MHz

6.3.2.3 Charakterystyka WiFi

Standard	802.11b/g/n, 802.3, 802.3u
Częstotliwość	2.4 Ghz
Moc wyjściowa	13 dBm@11n 17 dBm@11b 15 dBm@11g tolerancja ±2 dBm.
Transfer danych	do 150Mbps

6.3.2.4 Zewnętrzna antena

Zewnętrzna antena jest dołączona do modemu przez złącze SMA. Antena musi mieć parametry jak te przedstawione w poniższej tabeli:

Zakres częstotliwości anteny	Dual-band GSM 900/DCS 1800 MHz
Impedancja	50 Ω
Impedancja DC	0 Ω
Moc	0 dBi bez kabla; 2dBi z kablem
VSWR (z kablem)	-10 dB

Antena wybrana do pracy z modemem powinna być jak najlepiej dopasowana do warunków otoczenia w którym pracuje modem. Jeżeli modem umieszczony jest w pomieszczeniu, w którym zasięg sygnału jest zbyt niski, powinna być zastosowana zewnętrzna (na zewnątrz budynku) albo specyficzna wewnętrzna (wewnątrz pomieszczenia) antena aby zwiększyć moc odbieranego sygnału.

6.4 Charakterystyka otoczenia

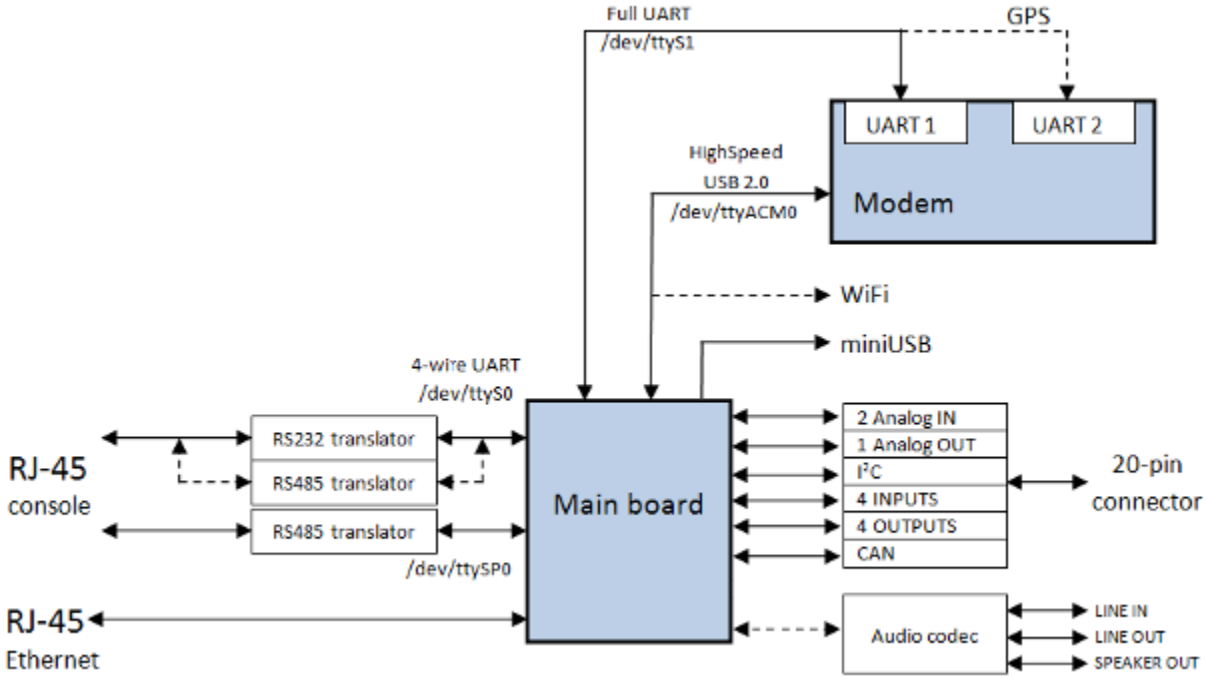
Poniższa tabela przedstawia warunki w jakich może pracować urządzenie.

Uwaga! Przekroczenie poniższych wartości może spowodować uszkodzenie modemu.

Parametr	Warunek	Min	Max	Jednostka
Temperatura pracy		0	60	°C

7 Architektura

Poniższy diagram przedstawia uproszczony schemat architektury modemu RB MTX. Dodatkowe funkcjonalności, dostępne jako opcja zaznaczono liniami przerywanymi.



8 Zalecenia dotyczące bezpieczeństwa

8.1 Ogólne bezpieczeństwo

Proszę wypełniać regulacje dotyczące bezpieczeństwa przy używaniu urządzeń radiowych zważywszy na możliwość wprowadzania zakłóceń. Przeczytaj dokładnie poniższe porady.

Wyłącz modem GSM w następujących okolicznościach:

- w samolocie – użytkowanie telefonów komórkowych w samolocie może spowodować jego błędne działanie i doprowadzić do katastrofy; używanie telefonii komórkowej w samolocie jest nielegalne i karalne.
- na wszelkiego rodzaju stacjach paliw.
- na każdym obszarze gdzie występuje zagrożenie łatwego wzniecenia pożaru lub eksplozji.
- w szpitalach i wszędzie gdzie używa się urządzeń medycznych.

Uszanuj zakazy używania urządzeń radiowych w miejscach gdzie występują znaki mówiące że używanie telefonów komórkowych jest zabronione lub niebezpieczne.

Korzystanie z modemu GSM w pobliżu innych urządzeń elektronicznych może także spowodować zaburzenie działania tych urządzeń jeżeli nie są odpowiednio zabezpieczone. Może prowadzić to do zniszczenia lub błędnego działania modemu GSM lub innych urządzeń.

8.2 Eksploatacja i konserwacja

Modem RBMTX jest urządzeniem elektronicznym które powinno być używane z ostrożnością. Proszę zastosować się do sugestii podanych poniżej aby Twój modem mógł działać przez wiele lat:

- Nie wystawiaj modemu na ekstremalne warunki jak wysoka temperatura lub wysoka wilgotność,
- Nie trzymaj modemu w brudnych i zakurzonych miejscach,
- Nie demontuj modemu RBMTX,
- Nie wystawiaj modemu na działanie wody, deszczu czy pary,
- Nie upuszczaj, trzęś lub uderzaj modemu,
- Nie umieszczaj modemu blisko urządzeń magnetycznych np. kart magnetycznych,
- Używanie urządzeń lub akcesoriów trzeciej kategorii, które nie są autoryzowane przez Elproma Elektronika może spowodować utratę gwarancji i/lub uszkodzenie modemu,
- Nie zostawiaj modemu przy dzieciach poniżej 3 roku życia.

8.3 Odpowiedzialność

Modem jest pod Twoją odpowiedzialnością. Proszę używać go zgodnie z powołaniem i zachowaniem lokalnych regulacji. Nie jest to zabawka – proszę przechowywać modem z dala od dzieci.

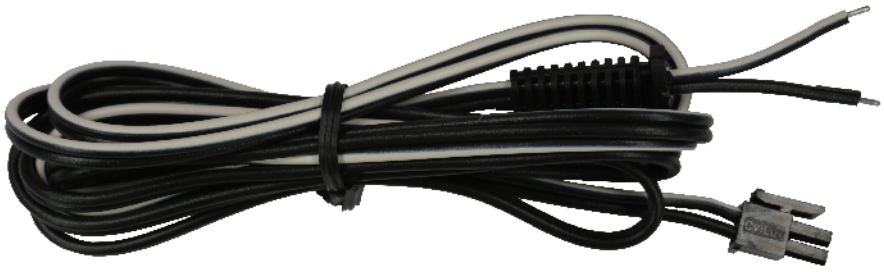
Spróbuj używać funkcji bezpieczeństwa (PIN etc.) aby zablokować nieautoryzowane użycie modemu lub kradzież.

9 Akcesoria

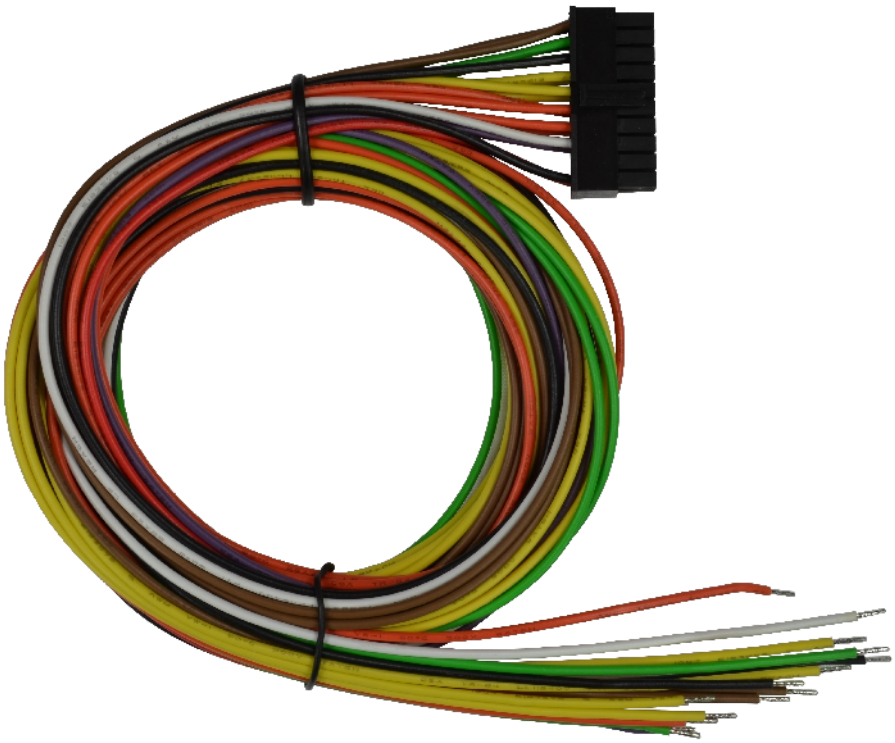
Tabela poniżej przedstawia akcesoria polecane do użycia z modemem.

RB-PS12VP2L15	zasilacz 12V	<1,5m> 2 PIN
RB-PSCP2L15	kabel zasilający	2PIN <1,5m> open end
RB-903G	kątowa antena 3G	2J010
RB-89MSH	szufladka na kartę SIM	MOLEX 0912360001
RB-MDH	mocowanie na szynę DIN	
RB-MR2R4	Kabel RS232/RS485 2in1	

Kabel zasilający open end



Kabel GPIO



Kabel RS232/485

Mocowanie na szynę DIN

Mocowanie na rzepy

10 Znak towarowy

RBMTX has been assessed in order to satisfy the essential requirements of the R&TTE Directive 1999/05/EC (Radio Equipment & Telecommunications Terminal Equipments) to demonstrate the conformity against the harmonised standards with the final involvement of a Notified Body.

CE

11 Zalecenia dotyczące bezpieczeństwa

PRZECZYTAJ UWAŻNIE

Upewnij się, że korzystanie z produktu w Twoim kraju oraz środowisku docelowym jest dozwolone. Nieprawidłowe użytkowanie tego produktu może być niebezpieczne i powinno być unikane w następujących sytuacjach:

- w miejscach, gdzie może on zakłócić pracę innych urządzeń elektronicznych, takich jak szpitale, porty lotnicze, pokład samolotu itd.
- w miejscach, w których występuje zagrożenie wybuchem, takich jak stacje benzynowe, rafinerie, itd.

Obowiązkiem użytkownika jest zapoznanie się z przepisami kraju użytkowania oraz przepisami dotyczącymi środowiska pracy urządzenia.

Nie należy rozmontowywać urządzenia: każdy ślad manipulacji może przyczynić się do utraty gwarancji.

Zalecamy stosowanie się do instrukcji dotyczących odpowiedniego podłączenia przewodów. Produkt należy zasilać stabilizowanym napięciem oraz zadbać, aby okablowanie było dostosowane do przepisów przeciwpożarowych i bezpieczeństwa.

Z produktem należy obchodzić się z uwagą, unikać kontaktu ze złączami, ponieważ elektrostatyczne wyładowania mogą uszkodzić produkt. Te same środki ostrożności należy przedsięwziąć z kartą SIM – sprawdź dokładnie instrukcję jej użytkowania. Nie wkładaj lub usuwaj karty SIM, gdy produkt jest w trybie oszczędzania energii.

Integracja systemu odpowiedzialna jest za funkcjonowanie produktu końcowego; w związku z tym należy zwrócić uwagę na zewnętrzne komponenty dołączane do modułu, jak również zastosowanie w innych projektach lub instalacjach, ponieważ istnieje ryzyko zaburzenia pracy sieci GSM i zewnętrznych urządzeń lub negatywny wpływ na zabezpieczenia. W przypadku wątpliwości odnieś się do dokumentacji technicznej i obowiązujących przepisów.

Każdy moduł musi być wyposażony w odpowiednią antenę o określonej charakterystyce. Antena musi być zamocowana z uwagą w celu uniknięcia zakłóceń pochodzących od innych urządzeń oraz w minimalnej odległości od ludzi (20cm). W przypadku gdy wymagania nie zostaną spełnione, system pracuje wbrew regulacjom SAR.

12 Lista skrótów

ACM	Accumulated Call Meter
ASCII	American Standard Code for Information Interchange
AT	Attention commands
CB	Cell Broadcast
CBS	Cell Broadcasting Service
CCM	Call Control Meter
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CMOS	Complementary Metal-Oxide Semiconductor
CR	Carriage Return
CSD	Circuit Switched Data
CTS	Clear To Send
DAI	Digital Audio Interface
DCD	Data Carrier Detected
DCE	Data Communications Equipment
DRX	Data Receive
DSR	Data Set Ready
DTA	Data Terminal Adaptor
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi Frequency
DTR	Data Terminal Ready
EMC	Electromagnetic Compatibility
ETSI	European Telecommunications Equipment Institute
FTA	Full Type Approval (ETSI)
GPRS	General Radio Packet Service
GSM	Global System for Mobile communication
HF	Hands Free
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IRA	Internationale Reference Alphabet
ITU	International Telecommunications Union
IWF	Inter-Working Function
LCD	Liquid Crystal Display

LED	Light Emitting Diode
LF	Linefeed
ME	Mobile Equipment
MMI	Man Machine Interface
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OEM	Other Equipment Manufacturer
PB	Phone Book
PDU	Protocol Data Unit
PH	Packet Handler
PIN	Personal Identity Number
PLMN	Public Land Mobile Network
PUCT	Price per Unit Currency Table
PUK	PIN Unblocking Code
RACH	Random Access Channel
RLP	Radio Link Protocol
RMS	Root Mean Square
RTS	Ready To Send
RI	Ring Indicator
SAR	Specific Absorption Rate (e.g. of the body of a person in an electromagnetic field)
SCA	Service Center Address
SIM	Subscriber Identity Module
SMD	Surface Mounted Device
SMS	Short Message Service
SMSC	Short Message Service Center
SPI	Serial Protocol Interface
SS	Supplementary Service
TIA	Telecommunications Industry Association
UDUB	User Determined User Busy
USSD	Unstructured Supplementary Service Data

13 Wsparcie online

Elproma zapewnia wsparcie online, dzięki któremu otrzymasz:

- Najnowszą wersję tego dokumentu
- Najnowsze sterowniki dla routera RBMTX
- Wsparcie techniczne

Te i inne informacje mogą państwo znaleźć na stronach:
www.elproma.com.pl or www.teleorigin.com.
Aby uzyskać więcej informacji skontaktuj się z nami:
email: office@elproma.com.pl lub info@elproma.com.pl
tel.: +48 (22) 751 76 80
fax.: +48 (22) 751 76 81
skype: elproma.elektronika