RBMTX-Lite

Podręcznik Użytkownika

GSM/UMTS/LTE

TELEORIGIN
UNIQUE TECHNOLOGY FOR TELEMETRY

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

e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

Spis treści

1. Historia dokumentu 4
2. Opakowanie 5
2.1 Pudełko 5
2.2 Zawartość opakowania 5
2.3 Wersje routera 6
3. Opis ogólny 7
3.1 Panel przedni 7
3.2 Panel tylny 7
3.3 Interfejsy zewnętrzne 8
3.3.1 Złącze anteny GSM/UMTS/LTE 8
3.3.2 Port szeregowy routera (RS232/RS485) 8
3.3.3 Złącze LAN 8
3.3.4 Złącze zasilania 9
3.3.5 Złącze karty SIM 10
3.4 Etykieta produktu 10
3.5 Działanie kontrolek LED 11
4. Podstawowe funkcje i usługi 12
5. Korzystanie z routera 13
5.1 Konfiguracja 13
5.1.1 Wkładanie karty SIM 13
5.1.2 Podłączanie anteny 14
5.1.3 Podłączanie kabla zasilającego 15
5.1.4 Podłączanie kabla LAN do gniazda RJ-45 15
5.2 Konfiguracja routera 16
5.2.1 Konfiguracja połączenia 16
5.2.2 Ekran statusu routera 17
5.2.3 Ustawienia podstawowe: WAN config 19
5.2.4 Ustawienia podstawowe: Local network 20
5.2.5 Ustawienia podstawowe: Modem settings 21
5.2.6 Ustawienia podstawowe: Connection control 22
5.2.7 Ustawienia podstawowe: Ports configuration 23
5.2.8 Ustawienia podstawowe: TCP/IP forwarding 24
5.2.9 Ustawienia podstawowe: VLAN 25
5.2.10 Ustawienia podstawowe: Static routes 26
5.2.11 Ustawienia podstawowe: Dynamic DNS 27
5.2.12 Ustawienia podstawowe: Access control 28
5.2.13 Ustawienia zaawansowane: OpenVPN 30
5.2.14 Ustawienia zaawansowane: Ipsec static/Ipsec mobile 32
5.2.15 Generowanie certyfikatów SSL 35
5.2.16 Ustawienia zaawansowane: NTRIP 37
5.2.17 Ustawienia zaawansowane: Text messages actions 38
5.2.18 Ustawienia zaawansowane: E-mail actions 39
5.2.19 Ustawienia zaawansowane: SNMP 40
5.2.20 Ustawienia administracyjne: Time 41
5.2.21 Ustawienia administracyjne: Syslog 42
5.2.22 Ustawienia administracyjne: User files 43

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.2.23 Ustawienia konfiguracyjne: Backup and restore 44
5.2.24 Ustawienia konfiguracyjne: Discard changes 44
5.2.25 Przycisk Save settings 44
5.3 Opis logów systemowych 45
5.4 Elproma Device Manager....46

6. Rozwiązywanie problemów 48

6.1 Brak komunikacji z routerem 48
6.2 Router odpowiada, lecz brak połączenia internetowego 48

7. Charakterystyka techniczna....49

7.1 Charakterystyka mechaniczna 49
7.2 Obudowa (schemat z wymiarami) 49
7.3 Charakterystyka elektryczna....49
7.3.1 Zasilanie 49
7.3.2 Charakterystyka RF 50
7.3.2.1 Zakresy częstotliwości – wersja UMTS/HSPA 50
7.3.2.2 Zakresy częstotliwości – wersja LTE....51
7.3.2.3 Charakterystyka Wi-Fi....52
7.3.2.4 Antena zewnętrzna 52
7.4 Charakterystyka środowiskowa 53

8. Architektura routera....54

9. Zalecenia dotyczące bezpieczeństwa 55

9.1 Bezpieczeństwo ogólne 55
9.2 Eksploatacja i konserwacja 55
9.3 Odpowiedzialność....55

10. Akcesoria 56

Kabel zasilający typu "open-end" 56
Kabel RS232/485....56

11. Zalecenia dotyczące bezpieczeństwa 57

12. Certyfikaty 58

12.1 Zagadnienia dotyczące oceny zgodności 58
12.2 Deklaracje zgodności 58
12.3 Ograniczenia krajowe 58

13. Lista skrótów....59

14. Wsparcie online 61

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

e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

1. Historia dokumentu

Wersja	Data	Zmiany
#0.6	8.03.2018	Wersja wstępna
#0.8	21.05.2018	Nowe zrzuty ekranu
#0.9	13.09.2018	Opis kontrolek LED
#1.0	18.01.2018	Nowe wersje routera, skorygowane zrzuty ekranu
#1.1	17.04.2019	Dodano instrukcję generowania certyfikatów OpenVPN

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

2. Opakowanie

2.1 Pudełko

Na pudełku znajduje się naklejka, odpowiadającą naklejce umieszczonej na urządzeniu, potwierdzająca jednoznacznie, że router jest produktem oryginalnym. Po informacje dodatkowe dotyczące naklejek patrz pkt "Etykieta produktu".

2.2 Zawartość opakowania

Opakowanie zawiera:
1) router RBMTX-Lite,
2) antenę GSM (ze złączem SMA),
3) zasilacz,
4) uchwyt naścienny.

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

2.3 Wersje routera

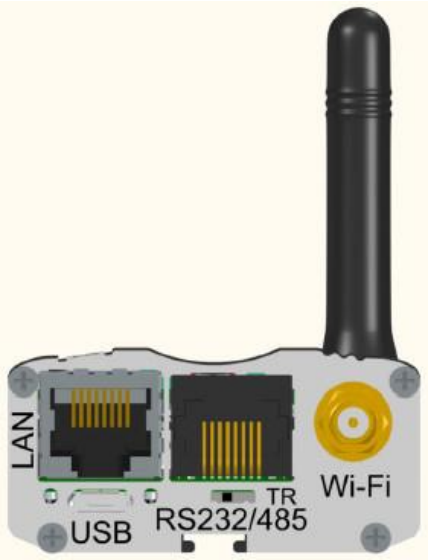
W tabeli poniżej przedstawiono standardowe konfiguracje (warianty) urządzenia.

Opcja	Standard	Opcja
Zasilanie	9-30 V	-
Pamięć	256 MB RAM, 512 MB MicroSD (część wykorzystana w systemie Linux; w przyszłości pojemność karty może ulec zmianie)	-
Procesor	Cortex A7, maks. 528 MHz, I.MX6UL(L)	-
RS232	Konsola systemowa	-
RS485	1	-
Połączenie	UMTS/LTE kat. 1	LTE kat. 4
Dual SIM	Dostępne	-
LAN	Ethernet 10/100 Mbps	-
Wi-Fi	-	Dostępne
Bluetooth	-	Dostępne

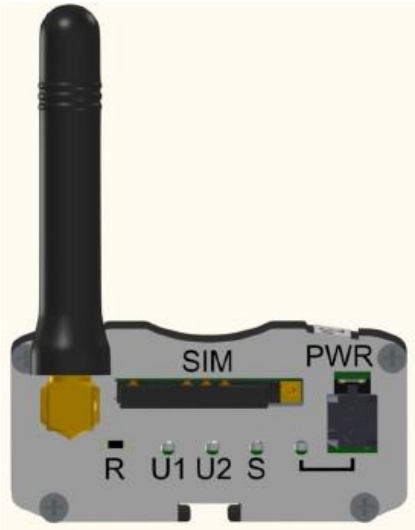
Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

3. Opis ogólny

3.1 Panel przedni



3.2 Panel tylny



Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

3.3 Interfejsy zewnętrzne

3.3.1 Złącze anteny GSM/UMTS/LTE

Złącze anteny SMA znajdujące się na panelu przednim służy do łączenia się z siecią GSM/UMTS/LTE. Aby nawiązać połączenie z siecią GSM/UMTS/LTE należy podłączyć antenę. W dobrych warunkach (duży zasięg, wysoki poziom odbieranego sygnału, itp.) należy skorzystać z anteny załączonej w opakowaniu. Jeśli poziom sygnału jest niski należy użyć zewnętrznej anteny kierunkowej/dookólnej lub anteny wewnętrznej.

Uwaga: *W przypadku niepodłączenia anteny nawiązanie połączenia z siecią GSM/UMTS/LTE nie będzie możliwe.*

3.3.2 Port szeregowy routera (RS232/RS485)

Port szeregowy RS232/RS485 (złącze RJ-45 oznakowane jako RS232/485) znajduje się na przednim panelu routera. Opis jego styków opisano w tabelach poniżej.

Wersja		
RS232 RS485	2 x 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

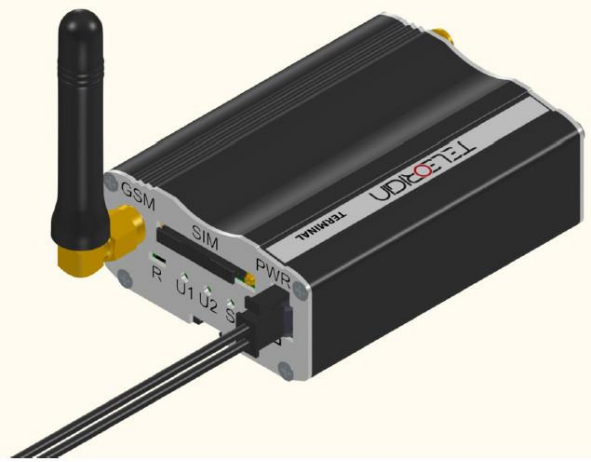
	Rb-MTX	RS232	RS485
	RJ45	DB9F	DB9F
A	1	nc	1
5V	2	2	2
B	3	3	nc
GND	4	nc	nc
TX	5	5	5
RX	6	ns	6
RTS	7	7	nc
CTS	8	8	nc

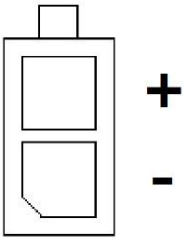
3.3.3 Złącze LAN

Drugie złącze RJ-45 (oznakowane jako LAN) znajduje się przy złączu szeregowym i służy do komunikowania się z komputerem PC lub laptopem za pośrednictwem interfejsu sieci Ethernet. Konfiguracja WWW jest dostępna w przeglądarce (domyślny adres IP: 192.168.1.234). Adres można zmienić w zakładce "Local Network".

3.3.4 Złącze zasilania

W celu zasilenia urządzenia należy zastosować oryginalny zasilacz dołączony do opakowania. Zapewnia on "czyste” zasilanie urządzenia i zapobiega stanom nieustalonym występującym w liniach zasilania i generowanych przez obwody indukcyjne. Zakres zasilania routera wynosi 9 – 30 V.





Układ styków zasilacza

UWAGA: Urządzenie wyłącza się poprzez wyjęcie wtyczki zasilacza zewnętrznego z gniazda elektrycznego. Gniazdo musi być usytuowane w pobliżu urządzenia i łatwo dostępne.

3.3.5 Złącze karty SIM

Pierwsze złącze karty SIM znajduje się na przednim panelu routera RBMTX-Lite, drugie zaś w jego wnętrzu. Aby włożyć kartę SIM należy **wcisnąć żółty przycisk i wyjąć czarną szufladkę na kartę** (patrz ilustracja). Aby możliwe było korzystanie z usług sieci GSM, do routera należy włożyć przynajmniej jedną kartę SIM.

3.4 Etykieta produktu

Etykieta produktu zawiera następujące informacje:

- numer seryjny produktu,
- oznakowanie CE,
- 15-cyfrowy kod kreskowy,
- nazwę modelu (RBMTX-Lite).

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

3.5 Działanie kontrolek LED

Router jest wyposażony w cztery kontrolki LED wskazujące tryb pracy urządzenia. Opis kontrolek zamieszczono w tabeli poniżej.

Kontrolka	Kolor	Opis
U1	Czerwony	Obsługa przez użytkownika
U2	Niebieski	Router jest aktywny
S	Żółty	Wskazanie sieci: RBMTX-Lite 3G: • Miga rzadko (200 ms wł., 1800 ms wył.) – wyszukiwanie sieci, • Miga rzadko (1800 ms wł., 200 ms wył.) – w oczekiwaniu/transfer danych, • Świeci ciągle – transmisja głosowa/CSD. RBMTX-Lite 4G: • Miga rzadko (200 ms wł., 1800 ms wył.) – wyszukiwanie sieci, • Miga rzadko (1800 ms wł., 200 ms wył.) – w oczekiwaniu, • Miga często (125 ms wł., 125 ms wył.) – transfer danych, • Świeci ciągle – transmisja głosowa
PWR	Zielony	Zasilanie

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

4. Podstawowe funkcje i usługi

Podstawowe funkcje i usługi przedstawiono w tabeli poniżej.

Funkcja / Usługa	Opis
Obsługiwane pasma	Wersja UMTS/HSPA: • GSM 900/1800 MHz • UMTS 900/2100 MHz Wersja LTE: • GSM 900/1800 MHz • WCDMA FDD B1, B8 Class 3 • LTE FDD B1, B3, B7, B8, B20 Cat. 1 i Cat. 4
Transfer danych	• LTE Cat. 1 (downlink 10 Mbit/s, uplink 5 Mbit/s) • LTE Cat. 4 (donwlink 150 Mbit/s, uplink 50 Mbit/s) • UMTS (downlink 7.2 Mbit/s) • GPRS (Multi-slot class 10, max BR downlink 85,6 Kb/s) • Protokoły wbudowane: PPP, TCP/IP, UDP/IP, MMS, HTTP, HTTPS, SSL, FTP, FTPS, SMTP, SMTPS, NTP, NITZ, PING • Przekierowanie portów, Ipsec, OpenVPN • Protokół Class B GSM 07.10 multiplexing
Wi-Fi*	Standard: • 802.11b/g/n Transfer danych: • maks. 150 Mbps
Bluetooth*	V4.1+EDR
Zasilanie	• Zakres napięcia nominalnego: 9 – 30 V • Maksymalne zasilanie ciągłe (średnie): 5 W • Szczytowa (chwilowa) wartość prądu: 1 A
Interfejsy (wersja podstawowa)	• Złącze anteny GSM/UMTS/LTE: SMA • 2 x SIM (drugi SIM jest wewnętrzny): standard 1,8 V/3 V • RS232 i RS485 przez RJ-45 • RJ-45 (x2) • microUSB (OTG) • Złącze zasilania • Montowany fabrycznie przycisk resetujący • 4 x LED
Opcje	• Złącze anteny Wi-Fi: SMA (męskie) • Złącze anteny Bluetooth: SMA
Inne	Rozmiar fizyczny: • Wymiary maksymalne: 83 x 53,5 x 26 mm (ze złączami) Zakres temperatury pracy: • -20 °C/60 °C

* Opcjonalnie

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5. Korzystanie z routera

5.1 Konfiguracja

Aby skonfigurować router należy wykonać następujące kroki:

5.1.1 Wkładanie karty SIM

- Wciśnij żółty przycisk znajdujący się na panelu przednim i wyciągnij szufladkę na kartę SIM.
- Umieść kartę SIM w adapterze w sposób przedstawiony na ilustracji poniżej.

Routery są dostępne w wersjach z jednym lub dwoma gniazdami na karty SIM. Aby włożyć drugą kartę SIM należy odkręcić jeden z paneli routera, wysunąć płytkę PCB i umieścić kartę SIM w adapterze wewnętrznym.

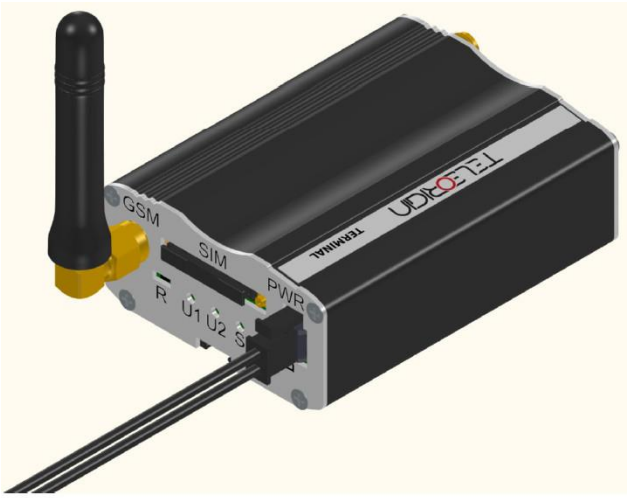
Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.1.2 Podłączanie anteny

- Podłącz antenę GSM/UMTS/LTE do złącza SMA.

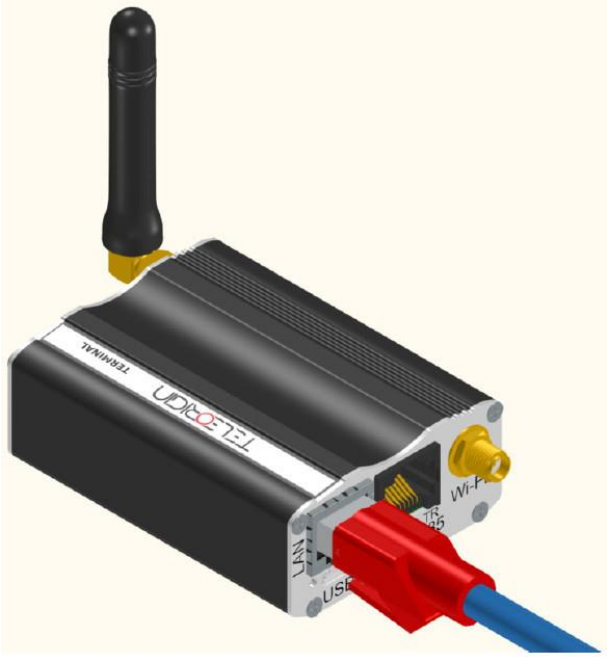
5.1.3 Podłączanie kabla zasilającego

- Podłącz kabel zasilający do złącza zasilacza (PWR).



5.1.4 Podłączanie kabla LAN do gniazda RJ-45

Podłącz kabel LAN do gniazda RJ-45.



Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.2 Konfiguracja routera

Router konfiguruje się za pośrednictwem przeglądarki internetowej. Ustawienia są podzielone na sekcje, umożliwiając w ten sposób użytkownikowi łatwe odnalezienie potrzebnej opcji. Aby zapisać nową konfigurację, należy skorzystać z opcji "Save settings". Użytkownik może również anulować zmiany, wybierając odpowiednią opcję w menu.

OSTRZEŻENIE: Zawartość pamięci podręcznej (cache) jest usuwana podczas resetowania urządzenia.
UWAGA: Dostępność zakładek jest uzależniona od wersji routera.

5.2.1 Konfiguracja połączenia

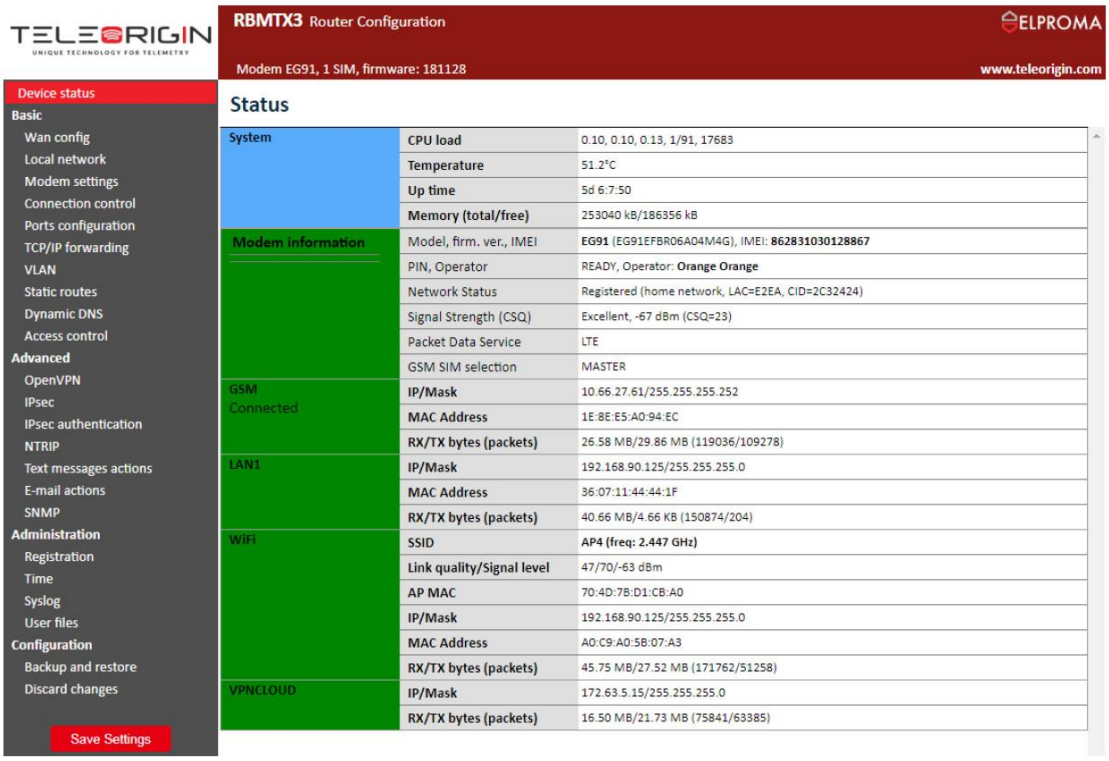
Po podłączeniu wszystkich niezbędnych kabli (patrz pkt "Konfiguracja routera") możesz skonfigurować połączenie sieciowe. Podłącz kabel LAN do komputera, przejdź do właściwości protokołu TCP/IP (***Połączenia sieciowe*** → ***Połączenie lokalne*** → ***Protokół internetowy TCP/IP*** → ***Właściwości***) i ustaw swój adres IP jako: 192.168.1.x. Zapoznaj się z instrukcją zmiany ustawień TCP/IP Twojej karty sieciowej (przykład dotyczy systemu Windows 7) tutaj: http://windows.microsoft.com/en-us/windows/change-tcp-ip-settings#1TC=windows-7.

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.2.2 Ekran statusu routera

Otwórz przeglądarkę internetową i wpisz adres **192.168.1.234**. Następnie wpisz nazwę użytkownika i hasło. Dane domyślne to:
Nazwa użytkownika: **admin**
Hasło: **12345**

Jeśli wszystkie ustawienia skonfigurowano poprawnie, system wyświetli następującą stronę:



Możesz tutaj sprawdzić czy router jest podłączony do sieci oraz parametry i dane połączenia PPP. Ekran statusu urządzenia odświeża się automatycznie.

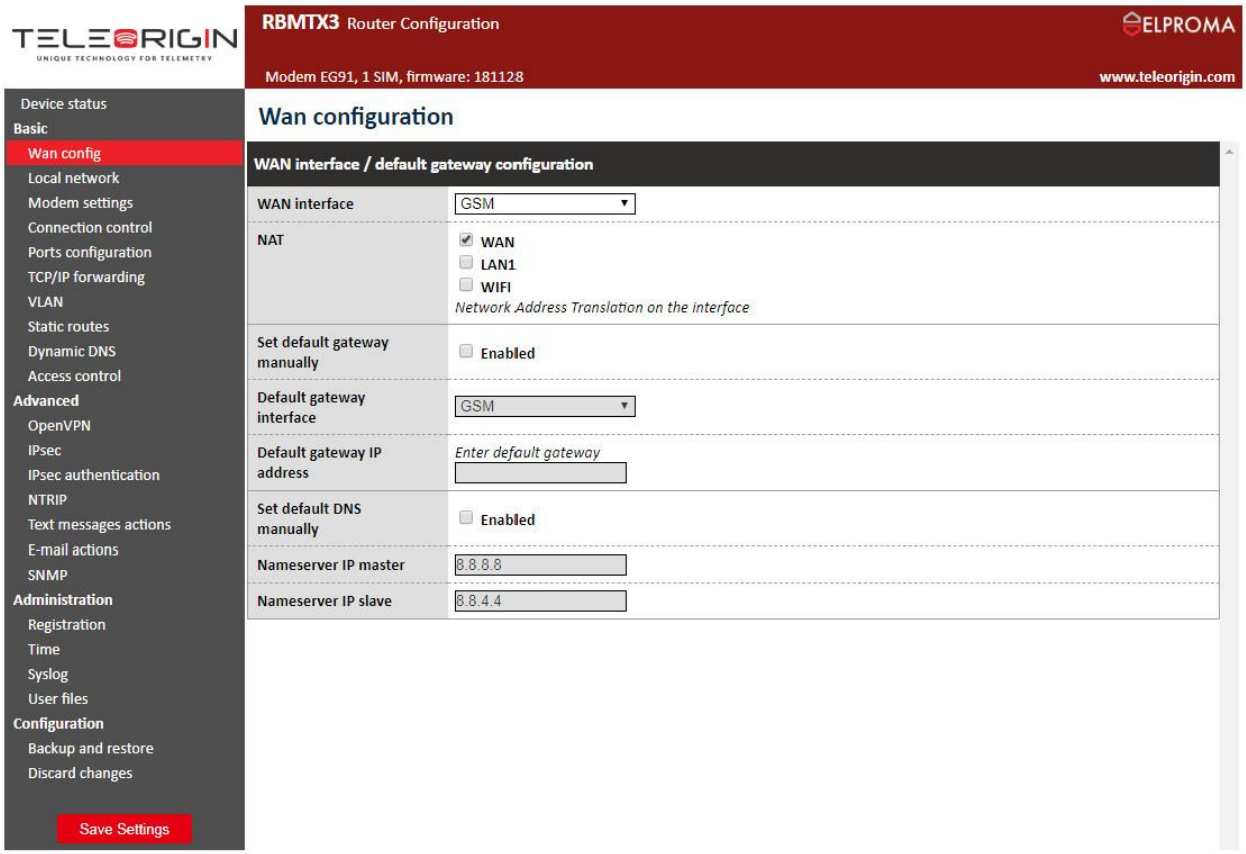
W tabeli poniżej zamieszczono opisy wszystkich pól zawartych w zakładce statusu urządzenia (Device status):

Pole	Przykład	Opis
CPU Load	0.67, 0.22, 0.16, 1/85, 9732	Parametry obciążenia procesora
Temperature	51,2 C	Temperatura procesora
Uptime	20d 19:22:21	Całkowity czas od włączenia
Memory (total/free)	253040 kB/192532 kB	Ilość dostępnej pamięci
Model, firmware ver., IMEI	GMM: UG95 lub EG9x	Dane modułu GSM
IMEI	359852050093104	Numer seryjny urządzenia
PIN, Operator	READY, Operator: Orange	Dostępne statusy karty SIM: SIM PIN – blokada PIN (ustaw prawidłowy kod PIN w zakładce "GSM network") READY – odblokowanie karty SIM SIM PUK – blokada PUK
Network Status	Registered (Home, LAC=2B21, CID-028FC03)	Status rejestracji (parametr 1), kod regionu (parametr 2), Cell ID (parametr 3). Możliwe statusy: - not registered: w chwili obecnej router nie wyszukuje nowego operatora do rejestracji, - registered: Home, - not registered, searching - niezarejestrowany, lecz router wyszukuje w chwili obecnej nowego operatora do rejestracji, - Registration denied – rejestracja odrzucona - unknown - nieznany - registered, roaming – zarejestrowany w roamingu
Signal strength (CSQ)	Excellent, - 73 dBm (CSQ = 20)	-
Packet Data Service	LTE	Typ pakietu danych usługi
GSM selection	MASTER	Wybór karty SIM
LAN1 IP/Mask	192.168.90.125/255.255.255.0	-
LAN1 MAC address	36:07:11:44:44:1F	-
RX/TX bytes (packets)	40.66 MB/4.66 KB (150885/204)	Ilość użytych pakietów RX/TX
VPNCLOUD IP/Mask	172.63.5.15/255.255.255.0	Routery z opcją TACS
VPNCLOUD RX/TX bytes (packets)	10.11 MB/7.05 MB (41778/29863)	

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.2.3 Ustawienia podstawowe: WAN config

Stronę konfiguracyjną sieci WAN przedstawiono na ilustracji poniżej.

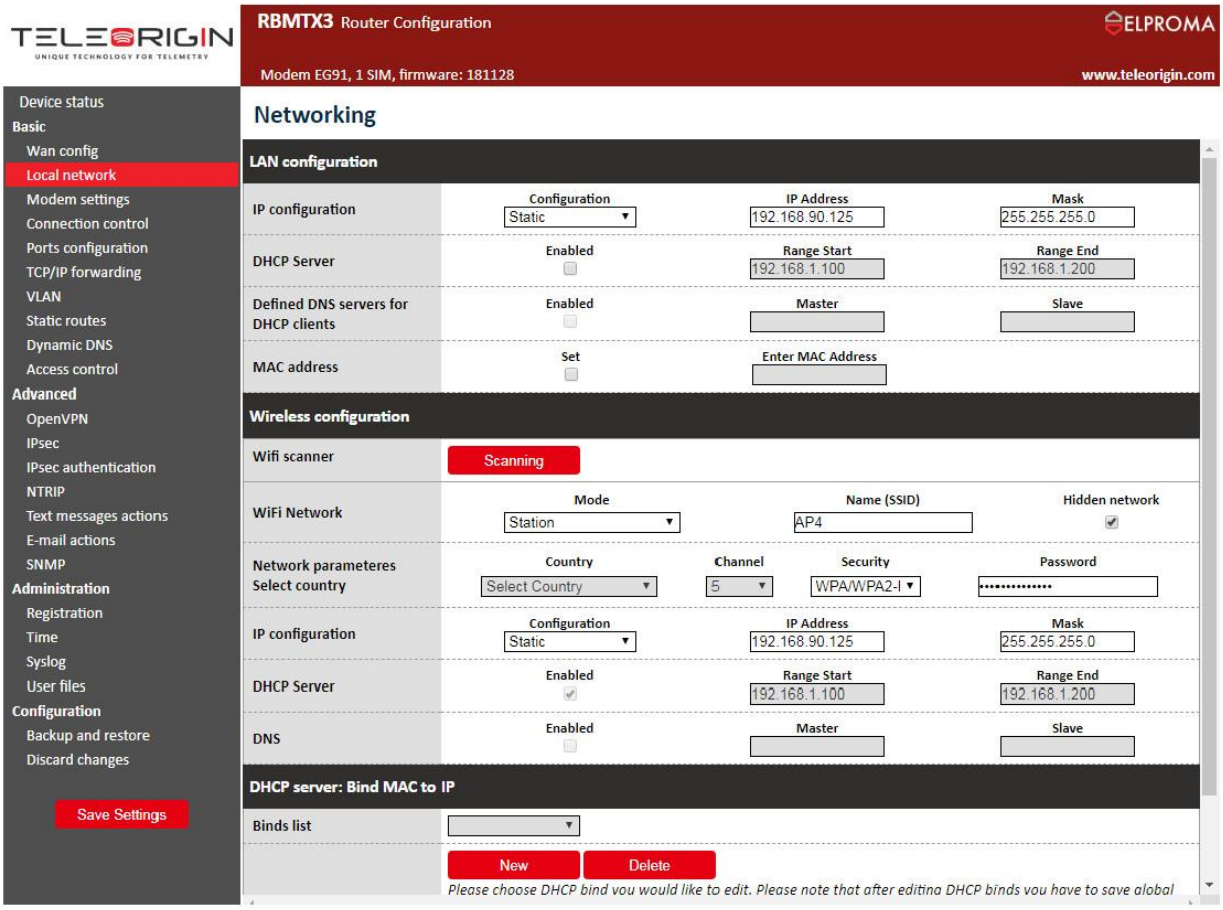


Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.2.4 Ustawienia podstawowe: Local network

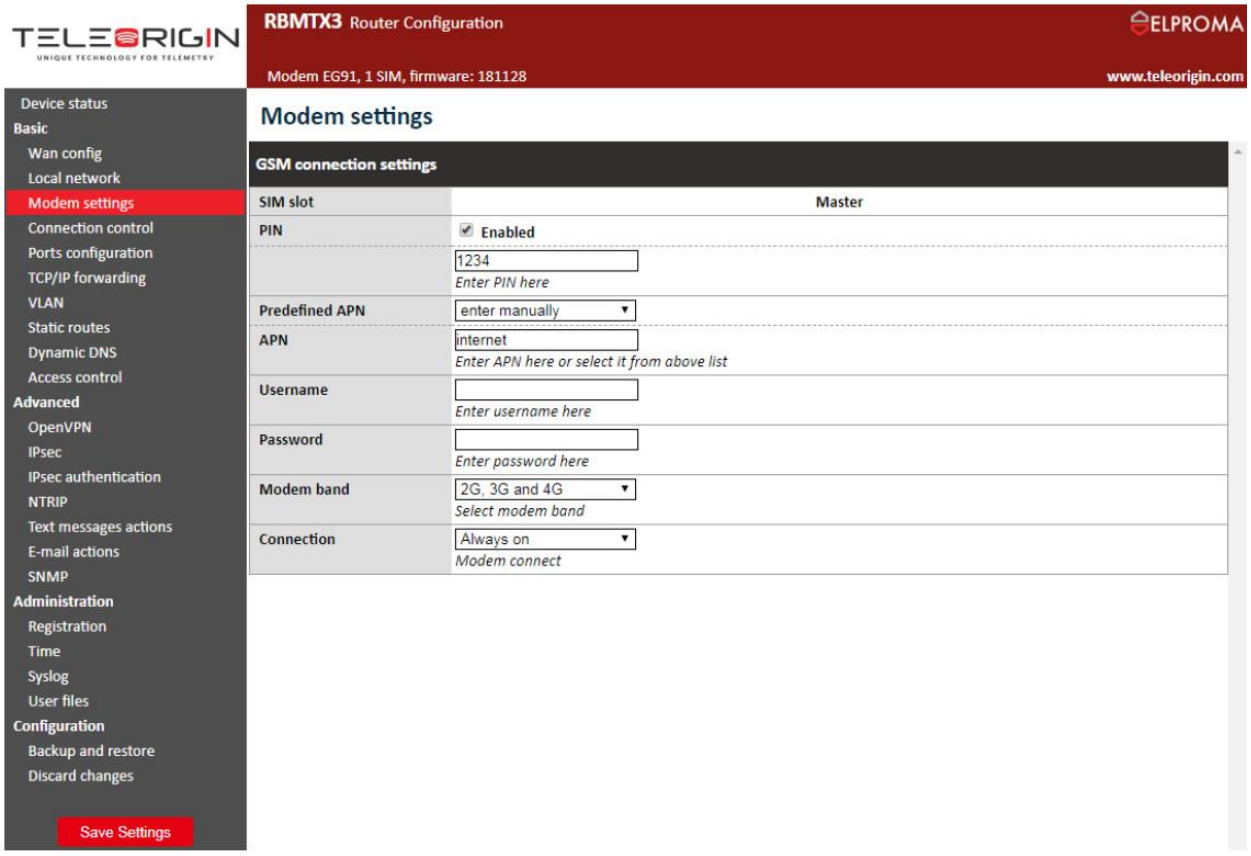
Na stronie konfiguracyjnej sieci lokalnej (Local network) dostępne są niezbędne parametry połączenia. Możesz tutaj ustawić adres IP (lub wybrać opcję automatycznego wyboru IP z użyciem DHCP), maskę podsieci, domyślną bramkę czy też adres DNS. Ostatnie dwie opcje można ustawić ręcznie bądź pobrać automatycznie z sieci GSM lub DHCP. Router może również pracować jako serwer DHCP. Możesz skonfigurować jego zakres pracy lub zestaw powiązań IP-MAC (binds).

Zakładka “Wireless configuration” jest dostępna wyłącznie w routerze RBMTX-Lite z opcją Wi-Fi. W zakładce tej użytkownik może ustawić parametry połączenia Wi-Fi. Aby wyszukać wszystkie dostępne sieci Wi-Fi, należy użyć przycisku “Scanning”. Spowoduje to przejście do strony zawierającej listę dostępnych sieci. Możesz ustawić tryb Wi-Fi (Access point lub Station), podać nazwę i hasło danej sieci, a także wybrać opcję uruchomienia serwera DHCP i klientów AP.



5.2.5 Ustawienia podstawowe: Modem settings

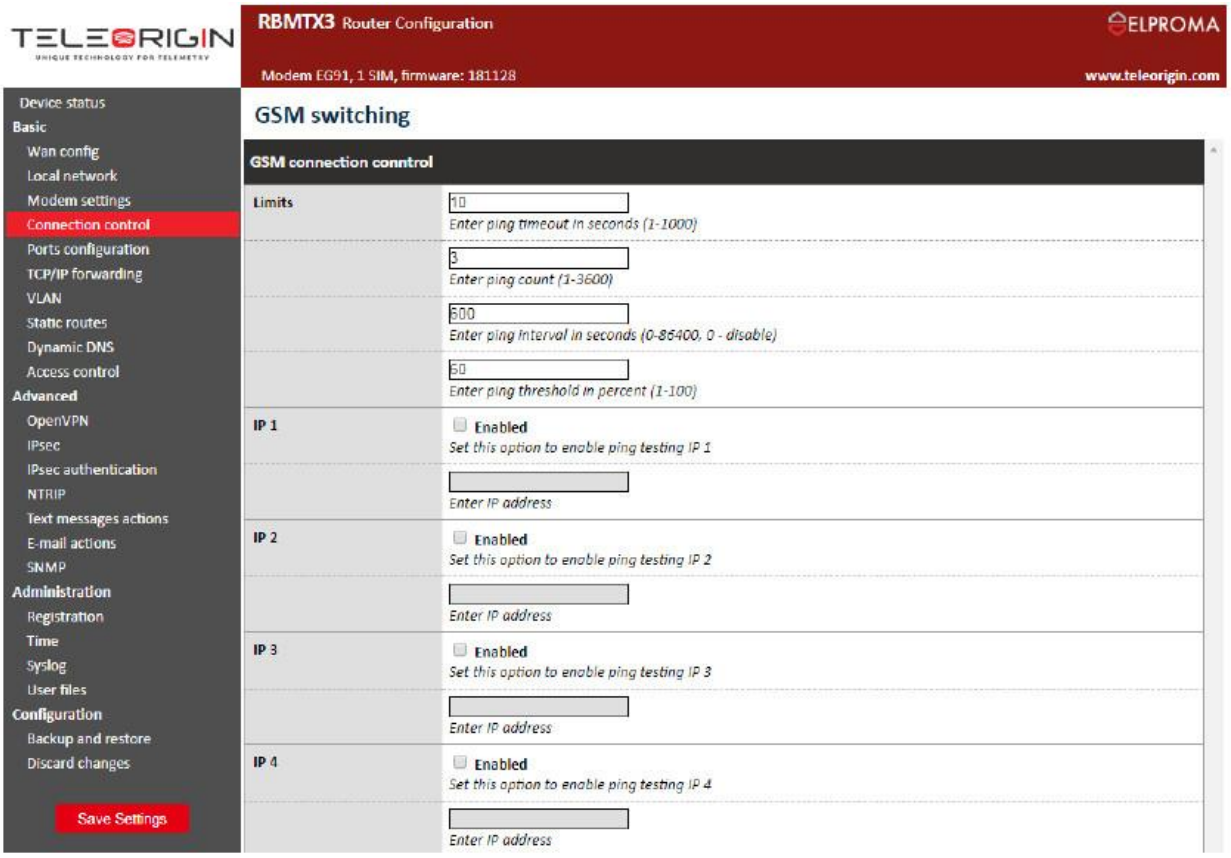
Na stronie "Modem settings" można zdefiniować parametry połączenia internetowego (APN, Username, Password, CSD, ISP IP i Modem band) dla jednego lub dwóch kart SIM (w zależności od wersji routera). Należy zapoznać się z tymi parametrami, gdyż stanowią one istotny element procesu ustanawiania dostępu do sieci internetowej. Parametry te powinny być zapewnione przez Twojego dostawcę sieci komórkowej.



Aby wprowadzić numer PIN karty SIM, zaznacz pole "Enabled", następnie wpisz prawidłowy PIN w polu poniżej. Należy pamiętać, że rozmowy wychodzące są wykonywane zawsze z użyciem głównej karty SIM (MASTER SIM).

5.2.6 Ustawienia podstawowe: Connection control

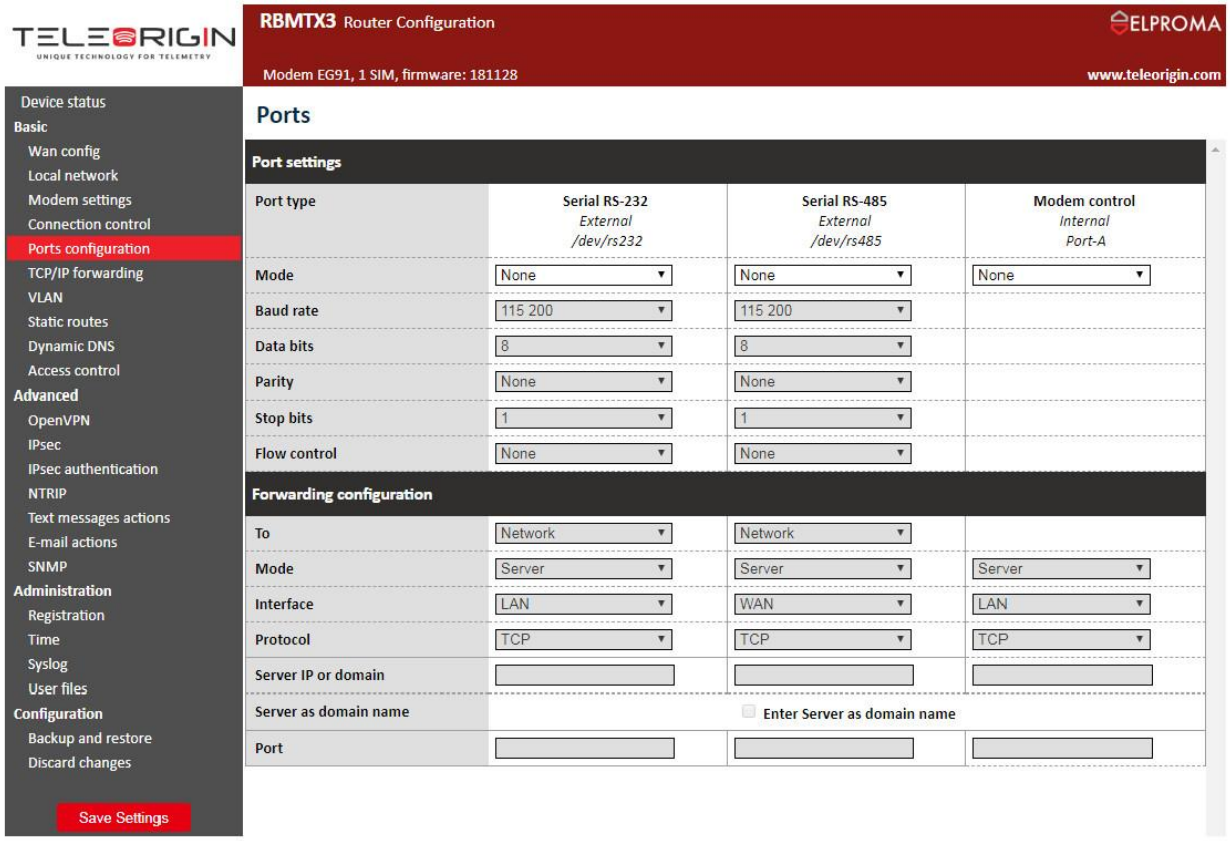
Na stronie "Connection control" użytkownik może skonfigurować parametry przełączania pomiędzy kartami SIM. Możliwe jest również zdefiniowanie czasu operacji testowania połączenia (ping) oraz ustawienie liczby prób dla wybranych 4 adresów IP. W przykładzie poniżej (patrz ilustracja) przełączenie kart z Master na Slave (bądź odwrotnie) nastąpi po trzech próbach 10-sekundowych.



5.2.7 Ustawienia podstawowe: Ports configuration

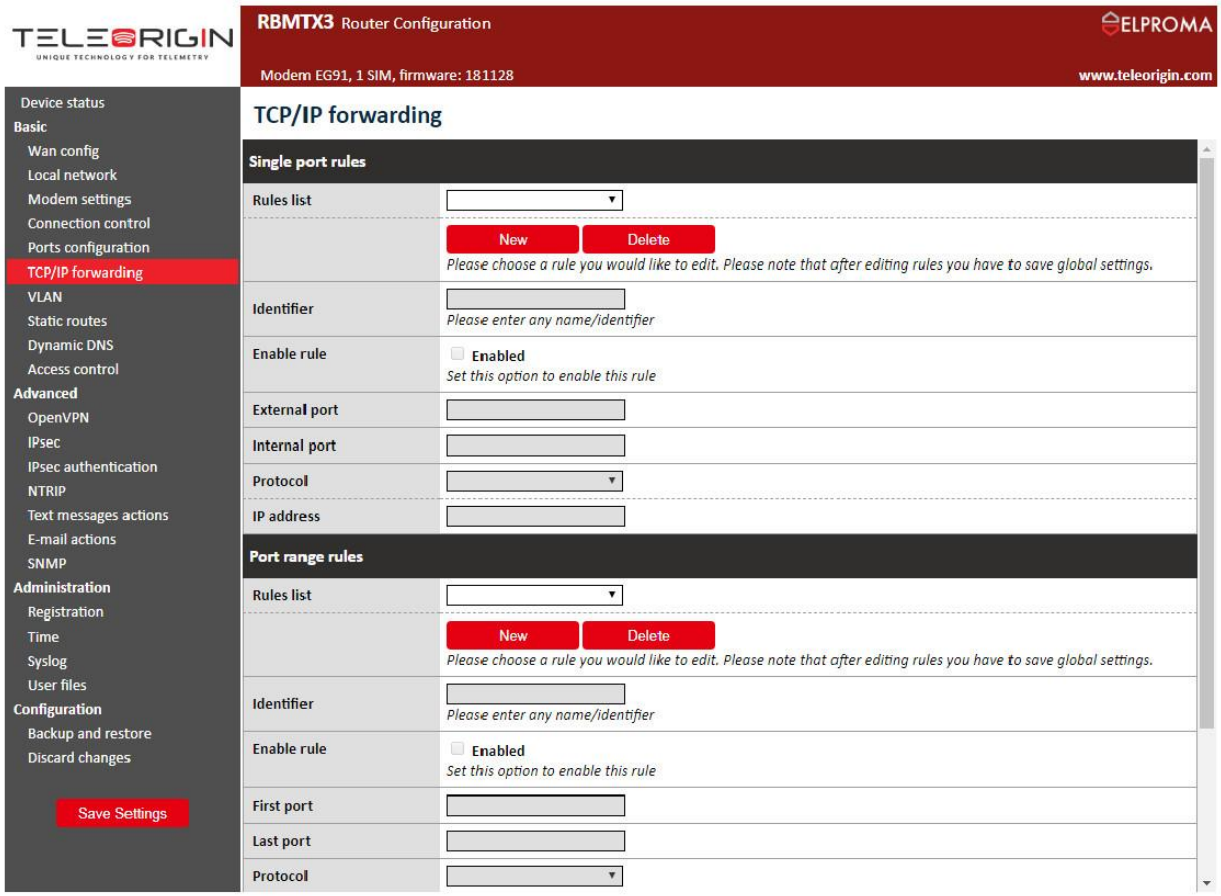
Na stronie "Ports configuration" użytkownik może skonfigurować parametry portu szeregowego RS232/RS485. Dostępne są trzy porty konfigurowalne: /dev/ttyS0, /dev/ttyACM0 oraz /dev/ttyS1 lub /dev/ttyUSB0 (w zależności od wersji routera). Każdy port może być skonfigurowany do pracy w innym trybie. Port /dev/ttyS0 można skonfigurować do pracy w trybie Router, ModBus lub NTRIP. Pozostałe dwa porty mogą także pracować jako port routera (sterowanie i dane) lub jako port odbierający wiadomości SMS (patrz pkt "Czynności dotyczące widomości SMS").

Każdy port można skonfigurować do pracy w trybie Forwarding, aby umożliwić użytkownikowi ich przekierowywanie na port TCP/UDP (jako serwer lub klient). Port /dev/ttyS0 można również przekierować na sterowanie routerem lub jego danymi. W takim przypadku nie jest możliwe uruchomienie żadnego innego trybu na tym porcie. Ustawienie niektórych trybów na portach dev/ttyS0 i /dev/ttyS1 (dotyczy wyłącznie wersji LTE) umożliwia skonfigurowanie parametrów takich jak: szybkość transmisji (Baud rate), bity danych (Data bits), parzystość (Parity checking) i protokół (Protocol). W przypadku nieaktywności któregoś parametru użytkownik nie ma możliwości jego zmiany.



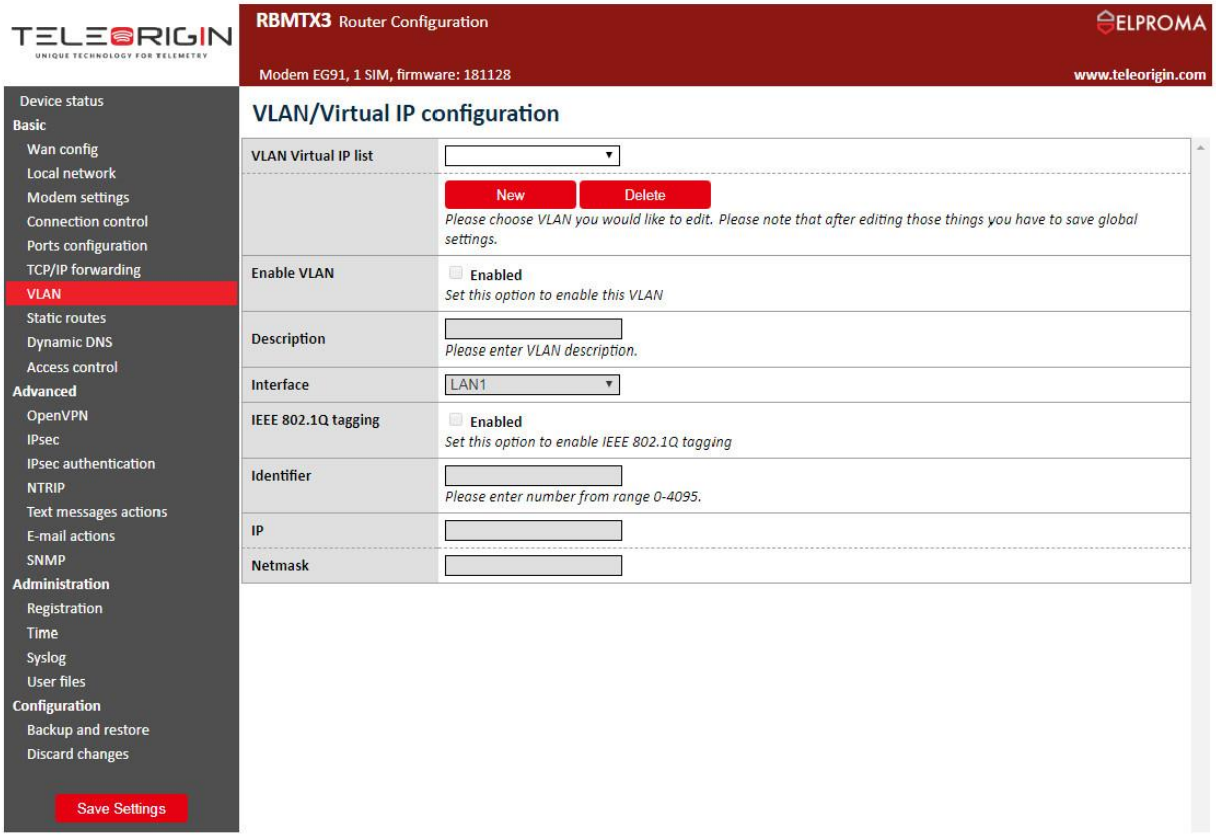
5.2.8 Ustawienia podstawowe: TCP/IP forwarding

Na tej stronie użytkownik może konfigurować pojedyncze porty lub zakresy portów, które będą przekierowane na dany adres IP. Aby dodać nową regułę dla pojedynczego portu, należy przejść do zakładki TCP/IP Forwarding i w sekcji "Single port rules" kliknąć przycisk "New". Następnie należy wpisać wszystkie wymagane informacje: identyfikator, zaznaczyć pole "Enabled", wpisać port zewnętrzny i wewnętrzny, wybrać protokół (TCP lub UDP) oraz wprowadzić adres IP. Podczas dodawania nowej reguły lub przechodzenia do innej zakładki wprowadzane dane zostaną zapisane automatycznie. Dane te (lub dowolną inną regułę) można usunąć, wciskając przycisk "Delete". Po wprowadzeniu zmian należy dodatkowo kliknąć przycisk "Save Settings", aby zapisać całą konfigurację. W takim sam sposób użytkownik może dodawać reguły dotyczące zakresów portów w sekcji "Port range rules", a także określić adres IP dla sieci niezaufanej w sekcji DMZ.



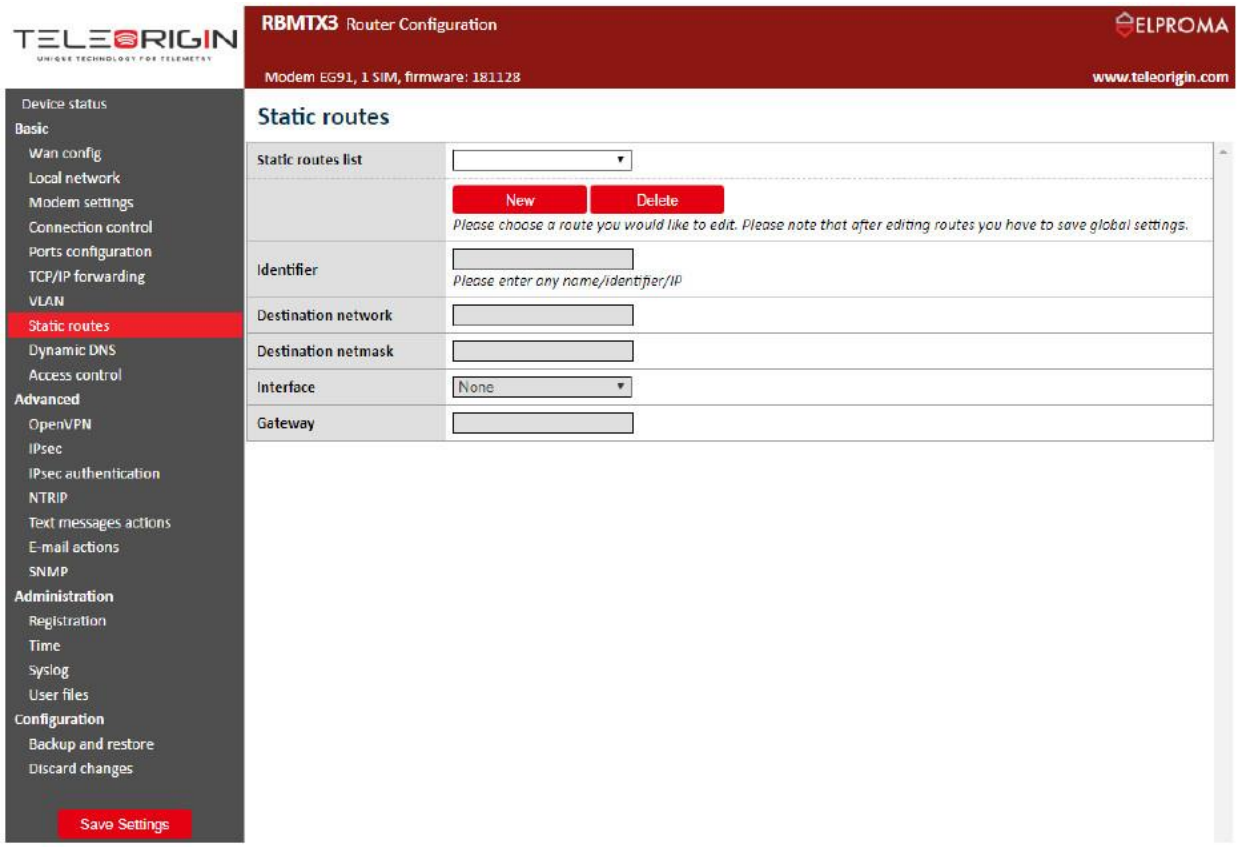
5.2.9 Ustawienia podstawowe: VLAN

Strona "VLAN" umożliwia użytkownikowi tworzenie wirtualnych adresów IP. Można tu zdefiniować adres IP, maskę podsieci oraz identyfikator w zakresie 0 – 4095. Poprzez zaznaczenie opcji "IEEE 802.1Q tagging" wirtualny adres IP stanie się częścią VLAN.



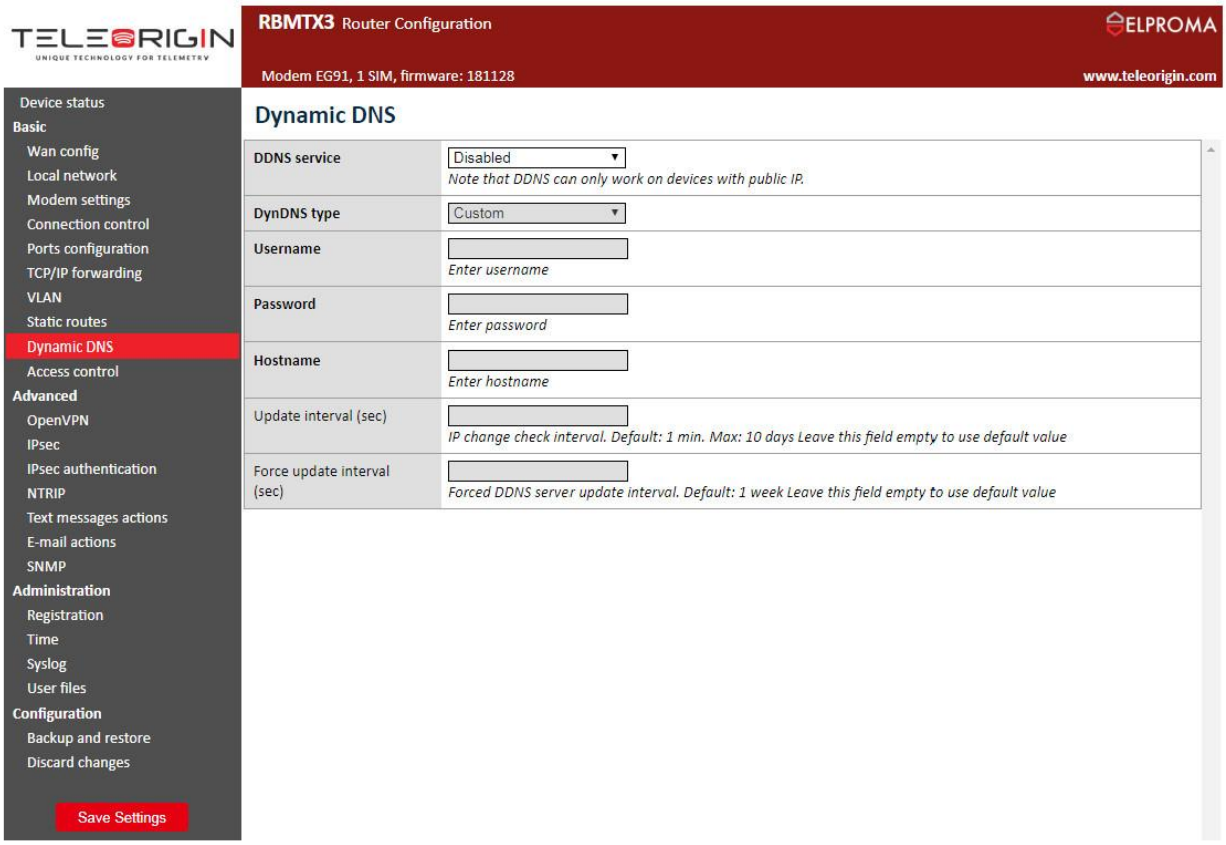
5.2.10 Ustawienia podstawowe: Static routes

Na stronie "Static routes" użytkownik może definiować połączenia (routings) według własnych preferencji. Aby dodać nowe połączenie, należy kliknąć przycisk "Add new". Następnie wpisać identyfikator (na potrzeby rozróżniania połączeń w konfiguracji internetowej), wybrać interfejs, wprowadzić sieć docelową (Destination network), maskę podsieci (Destinataion netmask) i bramkę (Gateway).



5.2.11 Ustawienia podstawowe: Dynamic DNS

Dynamic DNS to usługa umożliwiająca użytkownikowi udostępnianie urządzenia pod określonym adresem internetowym, niezależnie od zmian adresu IP. Aby tego dokonać, należy stworzyć konto na jednym z serwisów internetowych obsługujących router RBMTX-Lite (np. DynDNS.org lub No-IP.com). Po stworzeniu konta w zakładce Dynamic DNS należy wprowadzić wymagane dane konfiguracji WWW, tj. usługodawcę, rodzaj usługi (w przypadku DynDNS.org), nazwę użytkownika, hasło, nazwę hosta oraz dwa parametry: "Update interval" i "Force update interval". Pierwszy z nich określa czas między dwiema kontrolami, mającymi na celu wykrycie czy adres IP uległ zmianie. Parametr "Force update interval" określa czas między wymuszonymi aktualizacjami danych IP, niezależnie od tego czy adres IP uległ zmianie, czy nie. W razie wątpliwości pola te można pozostawić puste – w takim przypadku system uzupełni je wartościami domyślnymi.



5.2.12 Ustawienia podstawowe: Access control

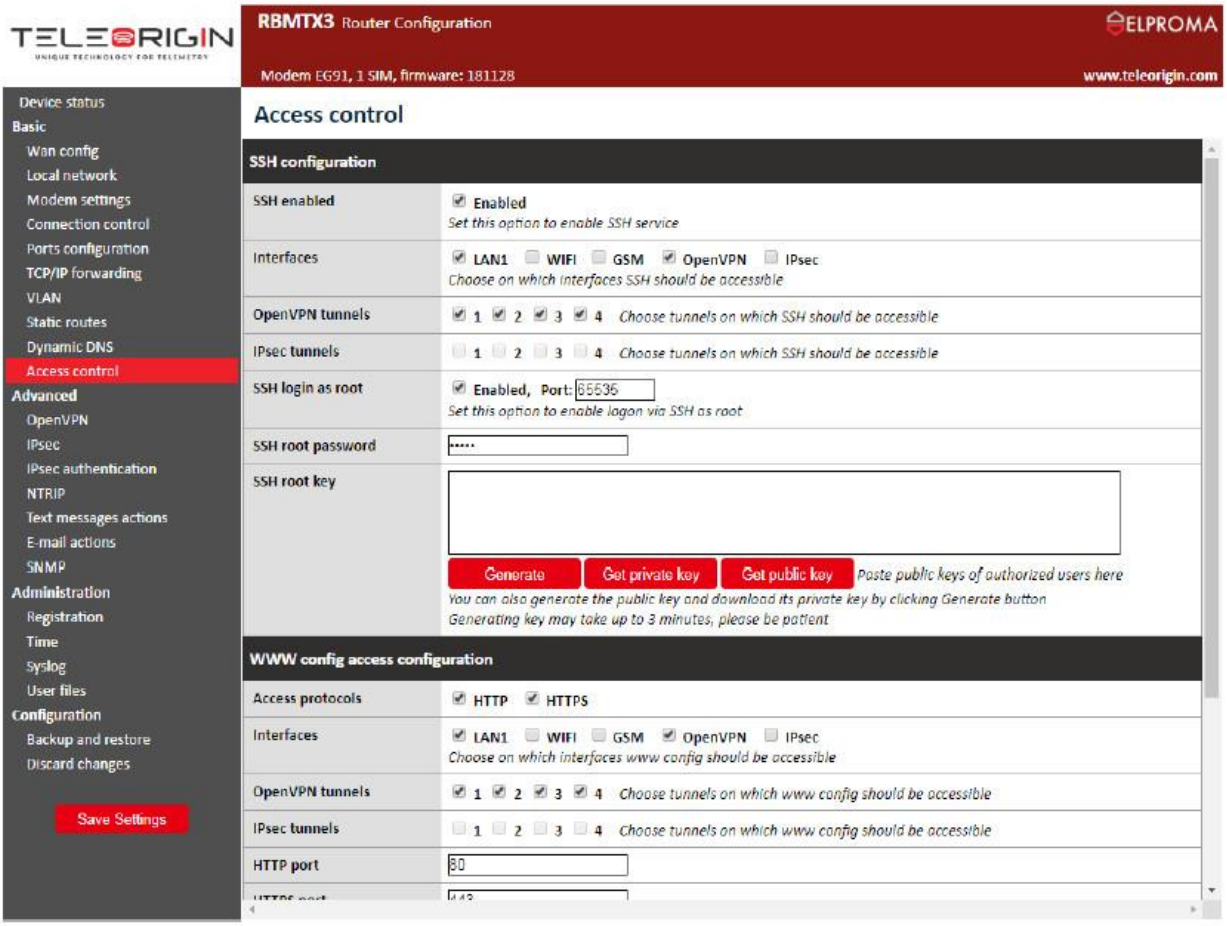
Pierwsza sekcja strony "Access control" pozwala użytkownikowi na konfigurację protokołu SSH, tj. jego włączenie/wyłączenie, wybranie portów i interfejsów, w których będzie on dostępny (dotyczy to także tuneli OpenVPN i IPsec). Możliwe jest również zablokowanie funkcji logowania przez SSH jako root oraz zmiana/usuwanie haseł/kluczy dla użytkowników root i service. Po zmianie hasła należy pamiętać o zapisaniu całej konfiguracji, wciskając przycisk "Save settings" w menu głównym. Usunięcie hasła oznacza, że nie będzie ono wymagane przy logowaniu. Podczas logowania za pośrednictwem protokołu SSH wyższy od hasła priorytet ma uwierzytelnienie kluczem, tzn. system nie poprosi użytkownika z kluczem zaufanym o podanie hasła, a klient nieposiadający takiego klucza będzie mógł zalogować się za pomocą hasła. W pola "SSH root key" i "SSH service key" można wkleić wiele kluczy.

UWAGA: Konto "Service" służy do aktualizowania oprogramowania. Wyłączenie protokołu SSH spowoduje dezaktywację aktualizacji.

Użytkownik może generować wymagane klucze bezpośrednio w routerze. W tym celu należy kliknąć przycisk "Generate" i odczekać do zakończenia procesu (co może zająć kilka minut). Nie należy w tym czasie zmieniać ustawień lub przełączać zakładek. Po wygenerowaniu klucza system wyświetli komunikat potwierdzający wykonanie operacji. Klucz publiczny zostanie automatycznie wklejony do pola kluczy (jeżeli pole to nie było puste przed wciśnięciem przycisku, jego zawartość zostanie zapisana, a wygenerowany klucz będzie widoczny na liście jako pierwszy). Od tej chwili możliwe będzie ściąganie kluczy prywatnego i publicznego za pomocą przycisków "Get private key" i "Get public key". Aby zalogować się przy pomocy klucza w systemie Linux, należy pobrać klucz prywatny, zmienić jego nazwę na "id_rsa" i umieścić go w katalogu /home/user/.ssh/.

W sekcji "WWW config access" możliwy jest również wybór protokołów HTTP/HTTPS, a także portów i interfejsów (dotyczy to również tuneli OpenVPN i IPsec), w których będą one dostępne. System umożliwia również zmianę hasła do konfiguracji ustawień internetowych (zmiana ta następuje niezwłocznie i nie wymaga zapisywania konfiguracji). Na potrzeby bezpieczeństwa jednoczesne odznaczenie protokołów HTTP i HTTPS jest niemożliwe.

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81



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

e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.2.13 Ustawienia zaawansowane: OpenVPN

Użytkownik może podłączyć router do sieci VPN lub stworzyć własną sieć z użyciem oprogramowania OpenVPN. Strona OpenVPN umożliwia stworzenie czterech połączeń VPN (tuneli). Aby wyświetlić i zmienić ustawienia dowolnego tunelu, należy go wybrać z listy rozwijalnej "Tunnel configuration". Następnie należy wybrać typ routera (serwer lub klient) oraz jeden z dostępnych typów połączenia (tun lub tap). Połączenie typu tun może być realizowane pomiędzy jednym lub kilkoma urządzeniami. W zależności od wybranych ustawień na tej stronie, w dalszej części konfiguracji należy podać adresy IP sieci/klienta lub sieć i maskę podsieci.

Jeśli urządzenie ma pracować jako serwer, należy wprowadzić port, na którym urządzenie ma nasłuchiwać na połączenie (domyślny port VPN to 1194; należy pamiętać o odblokowaniu tego portu w zakładce "Firewall"). Następnie należy wybrać urządzenie, które ma realizować połączenie: eth (zewnętrzny port RJ-45) lub ppp (połączenie przez sieć komórkową). Istotne znaczenie ma również wybór właściwego protokołu: TCP lub UDP (w przypadku wątpliwości wybierz opcję drugą). W przypadku połączenia typu tun niezbędne jest podanie adresów IP serwera i klienta (zaleca się stosowanie adresów z puli: 10.x.x.x). Dla połączenia tap należy wprowadzić adres podsieci VPN oraz maskę podsieci (np. 10.1.0.0 i 255.255.255.0). W większości przypadków Twoje urządzenie zarezerwuje pierwszy adres IP z puli dostępnych adresów (tj. 10.1.0.1 w przypadku użycia sieci 10.1.0.0).

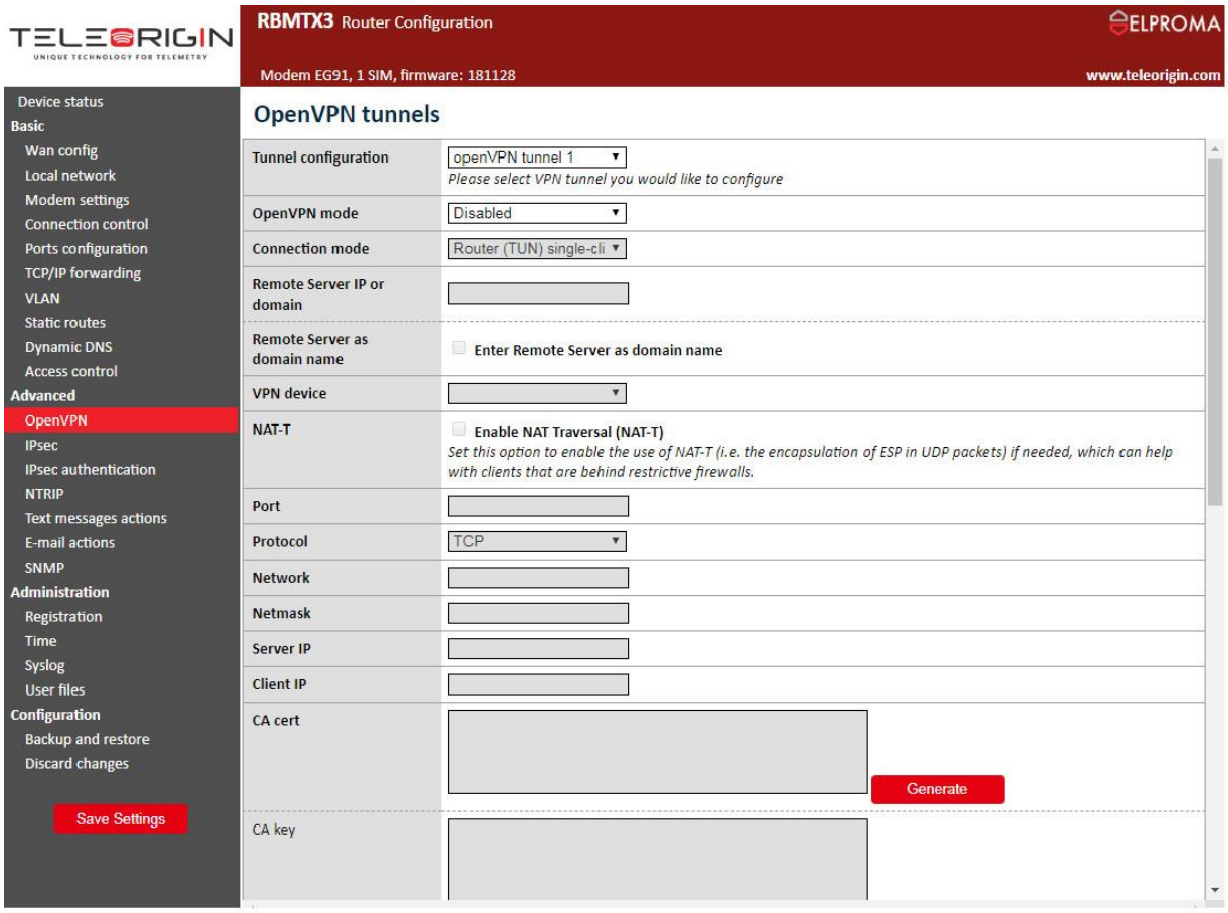
W przypadku gdy urządzenie ustawiono jako klient, oprócz ustawień serwera należy wprowadzić adres IP serwera VPN w polu "Remote Server IP" oraz port nasłuchiwania w polu "Port".

Po wprowadzeniu wszystkich wymaganych informacji użytkownik powinien wypełnić cztery pola certyfikatów, które powinny być generowane na każdym komputerze (więcej informacji znajdziesz na stronie internetowej OpenVPN w zakładce „Pomoc”). Zawartość plików należy wkleić w odpowiednie pola konfiguracyjne. System umożliwia zwiększenie poziomu zabezpieczenia połączenia VPN poprzez wprowadzenie klucza TLS w pole "TLS key" dla wszystkich urządzeń w sieci VPN. Ostatnią opcją jest przełączanie kompresji LZO (zaleca się aktywację tej opcji w celu ulepszenia komunikacji sieciowej) oraz dodawanie parametrów w polu "Additional configuration".

Generowanie certyfikatów:

1. Przyjmujemy, że RBMTX będzie zarówno serwerem, jak i CA (Centrum autoryzującym certyfikaty).
2. Na routerze, który będzie działał jako CA i serwer wybieramy „OpenVPN mode” -> „Client”
3. Następnie wybieramy „Connection mode” -> „Router (TUN) multi-client” oraz port (np. 1194)
4. Generujemy certyfikat i klucz prywatny CA (przyciski „Generate”), a następnie certyfikat CA kopiujemy na właściwe urządzenie klienta
5. Generujemy certyfikat i klucz prywatny dla klienta („Server/client cert” oraz „Server/client private key”). Ponieważ wyżej wybrano „OpenVPN mode client”, to wygenerowana będzie para dla klienta.
6. Parę certyfikatów klienta również kopiujemy na właściwe urządzenie klienta, a następnie usuwamy z formularza.
7. Zmieniamy „OpenVPN mode” -> „Server”
8. Ustawiamy adres i maskę sieci (lokalne dla połączenia VPN, np. 10.0.0.0/255.255.255.0)
9. Generujemy certyfikat i klucz prywatny serwera
10. Generujemy DH PEM
11. Zapisujemy ustawienia na RBMTX poprzez „Save settings”

Na kliencie konfigurujemy port i protokół, a następnie podajemy publiczny adres serwera i z wygenerowanymi na serwerze certyfikatami CA i pary certyfikat/klucz klienta wszystko powinno działać. Trzeba pamiętać o tym, aby certyfikat serwera był wygenerowany dla serwera, a certyfikat klienta dla klienta . Obydwa muszą być potwierdzone przez to samo (wspólne dla serwera i klienta) CA. Jeżeli wszystkie certyfikaty będą generowane na RBMTX, to będzie on jednocześnie autoryzował certyfikaty zarówno klienta, jak i serwera.



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

e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.2.14 Ustawienia zaawansowane: Ipsec static/Ipsec mobile

IPsec to zbiór protokołów internetowych umożliwiający tworzenie bezpiecznego połączenia między urządzeniami. Aby skonfigurować takie połączenie w routerze RBMTX-Lite, należy skorzystać z trzech zakładek konfiguracyjnych: Tunnels, Mobile Clients i Keys and Certificates. Najpierw należy aktywować Ipsec w zakładce Tunnels. Pod tą opcją znajduje się pole wyboru umożliwiające przełączanie pomiędzy konfiguracjami różnych tuneli. Aby aktywować konkretny tunel, należy zaznaczyć pole wyboru "Enable tunnel". Następnie należy wybrać interfejs sieciowy, za pośrednictwem którego będzie realizowane połączenie. Nie sposób omówić tutaj wszystkich możliwości nawiązywania połączenia za pomocą protokołu IPsec, dlatego też poniżej opisano konfigurację przykładową.

Załóżmy, że chcemy połączyć ze sobą dwa routery RBMTX-Lite o następujących adresach IP: 123.45.67.1 i 123.45.67.2. Pierwsza opcja, tj. "DPD interval" określa czas, po którym połączenie zostanie zamknięte, jeżeli drugie urządzenie nie odpowie. W pole to można wpisać dowolną wartość. My wpisaliśmy 3600 sekund. Następnie użytkownik musi wybrać lokalną podsieć, która będzie dostępna po zdalnej stronie połączenia. Może to być Single host (router), Network (sieć kilku urządzeń) lub LAN subnet (podsieć sieci lokalnej). Załóżmy, że planujemy dodać więcej urządzeń – musimy zatem wybrać sieć. Dla pierwszego routera wpisujemy następujące ustawienia: IP = 192.168.36.1, Network = 192.168.36.0, a Netmask = 255.255.255.0. Adres IP musi być zgodny z wybraną siecią i jej maską. Kolejnym krokiem jest uzupełnienie sekcji "Remote subnet". Podsieć lokalna pierwszego urządzenia musi odpowiadać podsieci zdalnej drugiego urządzenia i odwrotnie. W sekcji "Local subnet" drugiego routera wpisaliśmy następujące ustawienia: IP = 192.168.35.1, Network = 192.168.35.0 i Netmask = 255.255.255.0; dla podsieci zdalnej pierwszego routera należy wpisać: Address = 192.168.35.0, Netmask = 255.255.255.0. Po określeniu podsieci lokalnej i zdalnej należy wypełnić pole "Remote gateway", w którym wpisujemy adres IP urządzenia drugiego. W naszym konkretnym przypadku będzie to 123.45.67.2 dla routera pierwszego i 123.45.67.1 dla routera drugiego.

W kolejnym kroku należy zdefiniować pierwszą fazę negocjacji połączenia. Wybieramy tryb "Negotiation" (tryb "Aggressive" jest mniej bezpieczny, lecz szybszy od trybu "Main"). Kolejnym ustawieniem jest identyfikator urządzenia. Najczęściej używanym ustawieniem jest "My IP address" dla uwierzytelnienia PSK i "RSA Cert subject" dla certyfikatów RSA. Wybierz następnie metodę szyfrowania (Encryption), algorytm funkcji skrótu (Hash algorithm) i zbiór kluczy DH (DH key group) – ustawienia te muszą być jednakowe po obu stronach połączenia. Szyfrowanie typu Blowfish jest z reguły najszybsze, a AES najwolniejsze, lecz najbezpieczniejsze. Możesz dodatkowo ustawić czas fazy 1 lub pozostawić to pole puste (system zastosuje wartość domyślną). Najważniejszym parametrem fazy 1 jest metoda uwierzytelniania: "Pre-shared key" jest metodą podobną do metody "Password" (musisz wpisać jednakowy klucz po obu stronach). O wiele skuteczniejszą metodą jest zastosowanie certyfikatów RSA, lecz wymaga ona wygenerowania certyfikatu i klucza dla każdego urządzenia. Użytkownik ma do wyboru dwie opcje: wpisanie certyfikatu drugiego urządzenia w polu "Peer certificate" lub dodanie certyfikatu CA (opis w dalszej części instrukcji).

W drugiej fazie negocjacji połączenia należy określić protokół (ESP to uwierzytelnienie z szyfrowaniem, AH zaś jest samym uwierzytelnieniem), algorytm szyfrowania (Encryption algoritym), algorytm funkcji skrótu (Hash algorithm) oraz zbiór kluczy PFS (PFS key group). Należy zauważyć, że użytkownik może wybrać kilka algorytmów, lecz przynajmniej jeden z nich musi być zgodny po obu stronach połączenia. Ostatnim parametrem jest "Phase 2 lifetime" (pozostawiając to pole puste system zastosuje wartość domyślną).

Po skonfigurowaniu wszystkich parametrów należy pamiętać o zapisaniu konfiguracji. Proces konfiguracji połączenia IPsec zakończy się, chyba że użytkownik wybierze metodę uwierzytelniania za pomocą certyfikatów RSA i CA. W takim przypadku należy kliknąć zakładkę "Keys and Certificates", w której można dodać kilka kluczy PSK i certyfikaty CA. Ponieważ procedura dodawania obydwu elementów jest podobna, opiszemy jedynie dodawanie certyfikatów CA.

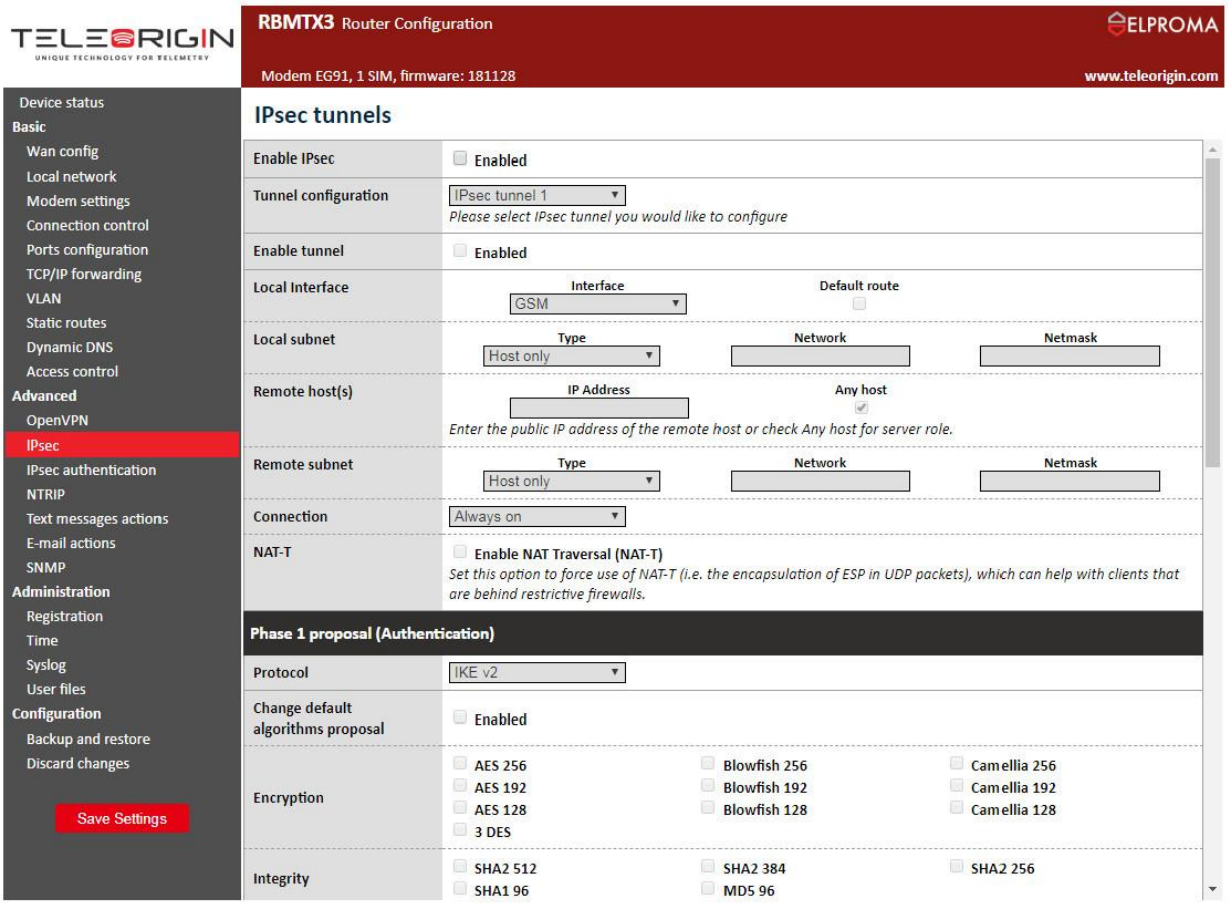
Aby dodać nowy certyfikat należy kliknąć na przycisk "Add new", wybrać identyfikator (służący do rozróżniania certyfikatów w konfiguracji sieciowej), wkleić certyfikat CA i listę certyfikatów nieważnych. Ostatnie pole jest polem opcjonalnym umożliwiającym blokowanie użytkowników, którzy nie powinni mieć możliwości przyłączenia się do Twojej sieci.

WAŻNE: Po wypełnieniu niezbędnych pól kliknij przycisk "Save", a następnie zapisz całą konfigurację, klikając przycisk "Save settings". Aby usunąć certyfikat, należy wybrać go na liście, kliknąć przycisk "Delete", a następnie zapisać całą konfigurację.

System umożliwia tworzenie połączenia IPsec z urządzeniami bez stałych adresów IP. Aby tego dokonać, należy kliknąć zakładkę "Mobile clients". Proces konfiguracyjny jest analogiczny do konfiguracji tuneli z tą różnicą, że zawiera mniej parametrów (np. nie ma pola PSK – klucze Pre-shared należy dodać do klientów w zakładce "Keys and Certificates").

***WAŻNE*:** Podczas konfigurowania połączenia IPsec użytkownik może zdecydować się na dodanie połączenia niestandardowego. Zagadnienie to opisano w kolejnym punkcie.

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81



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

e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.2.15 Generowanie certyfikatów SSL

Aby móc korzystać z uwierzytelniania za pomocą certyfikatów SSL, należy stworzyć kilka plików, których zawartość należy przekopiować do odpowiednich pól w zakładkach "OpenVPN" lub "IPsec". Można tego dokonać za pomocą komputera z systemem operacyjnym Linux i zainstalowanym pakietem programów OpenSSL. Istnieje też wersja pakietu dla systemu Windows, dostępna pod adresem http://gnuwin32.sourceforge.net/packages/openssl.htm.

Najpierw należy przygotować katalog, w którym będą przechowywane wszystkie klucze i certyfikaty. Załóżmy, że jest to katalog *~/klucze*. Należy utworzyć w nim dwa pliki: listę certyfikatów oraz plik służący do ich numerowania:

touch index.txt
echo 00 > serial,

a także podkatalogi do przechowywania kluczy i certyfikatów:

mkdir private certs newcerts crl.

Do tworzenia certyfikatów wymagane jest stworzenie certificate authority (CA). Jest to certyfikat nadrzędny, na podstawie którego tworzone są pozostałe certyfikaty. Po utworzeniu klucza prywatnego CA:

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

Ostrzeżenie: Zapamiętaj hasło do prywatnego klucza CA!
Należy wygenerować certyfikat CA:

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

Podczas tworzenia certyfikatu jego użytkownik musi podać określone dane, takie jak kraj, województwo, miasto, nazwa firmy, adres e-mail i nazwa wspólna. Ostatnie pole, tj. nazwa wspólna (Common name) jest polem najważniejszym i musi być niepowtarzalne dla każdego urządzenia.

Po stworzeniu certyfikatu CA należy wygenerować oddzielne certyfikaty dla każdego urządzenia.

Najpierw należy stworzyć klucz prywatny:

openssl genrsa -des3 -out private/device1key.pem

Następnie należy wygenerować żądanie wygenerowania certyfikatu:

openssl req -new -key private/device1key.pem -out device1req.pem

Użytkownik musi tutaj podać powtórnie dane, takie jak kraj, województwo, itp. Mogą to być dane identyczne jak poprzednie, z wyjątkiem pola "Common Name".

CA podpisuje certyfikat:

openssl ca -notext -in device1req.pem -out device1cert.pem

Aby móc wykorzystać dany certyfikat w routerze RBMTX-Lite, należy dezaktywować hasło do klucza prywatnego:

openssl rsa -in private/device1key.pem -out private/device1key.pem_nopass

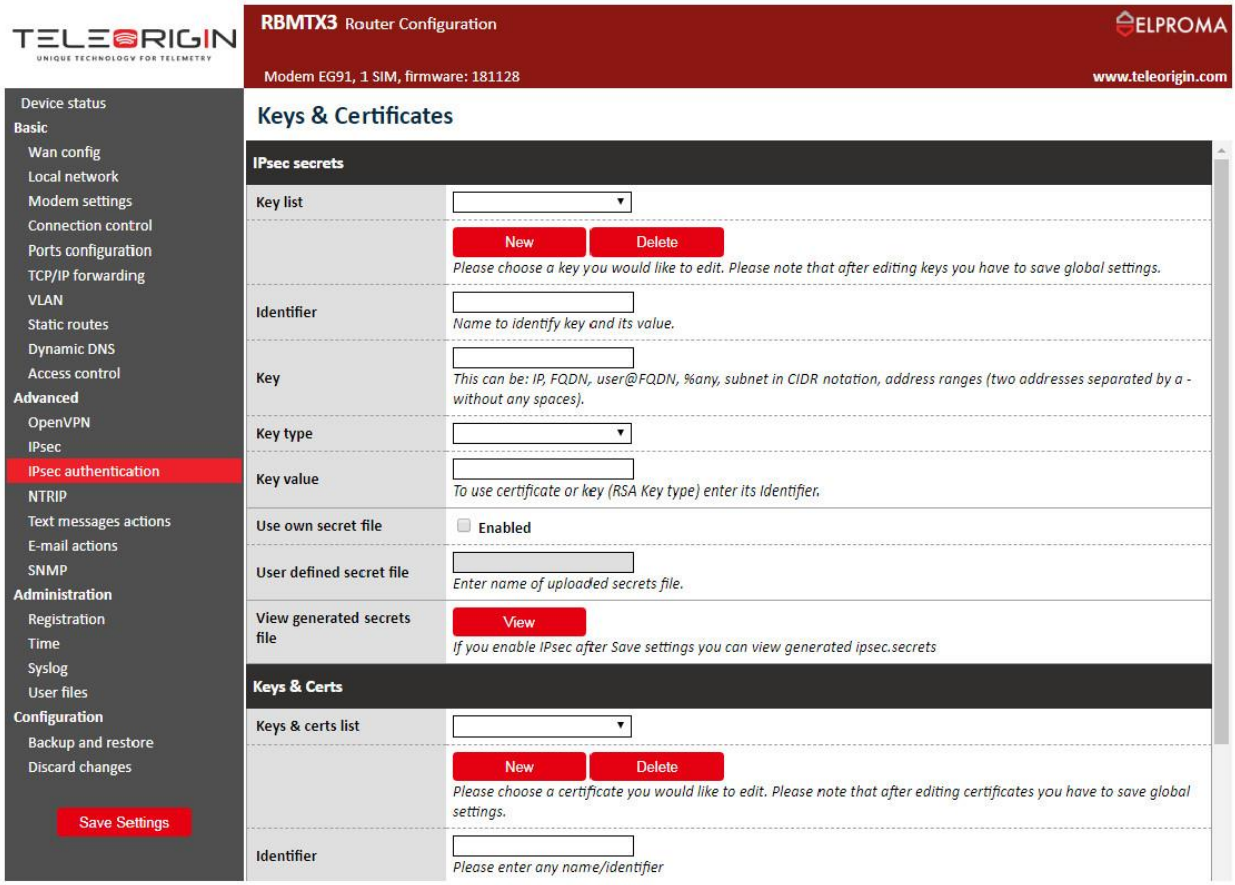
Całą procedurę należy powtórzyć dla każdego urządzenia (należy pamiętać o przedzieleniu różnych nazw wspólnych (Common Name) i nazw plików do poszczególnych urządzeń!).

W przypadku użycia protokołu IPsec w konfiguracji parametrów internetowych – w zakładce IPsec/Tunnels należy wypełnić określone pola, tj. w pole "Certificate" należy wkleić zawartość pliku *device1cert.pem*, a w pole Key – pliku *device1key.pem_nopass*. W pole "Peer certificate" należy wkleić certyfikat innego urządzenia lub pozostawić je puste. W takim przypadku, w zakładce "Keys" and Certificates" należy dodać certyfikat CA i wkleić zawartość pliku *cacert.pem.*

Jeżeli konieczne okaże się skorzystanie z protokołu OpenVPN, wówczas w pole "CA cert" w zakładce "OpenVPN" należy wkleić zawartość pliku *cacert.pem*, w pole "Server/Client cert" – zawartość pliku *device1cert.pem*, w pole "Server/Client private key" zaś – zawartość pliku *device1key.pem_nopass*. Dla połączenia VPN należy wygenerować plik z parametrami Diffie'go-Hellmana:

openssl dhparam -out dh1024.pem 1024,

a jego zawartość wkleić w pole "DH PEM". Plik ten jest wspólny dla wszystkich urządzeń w sieci VPN.

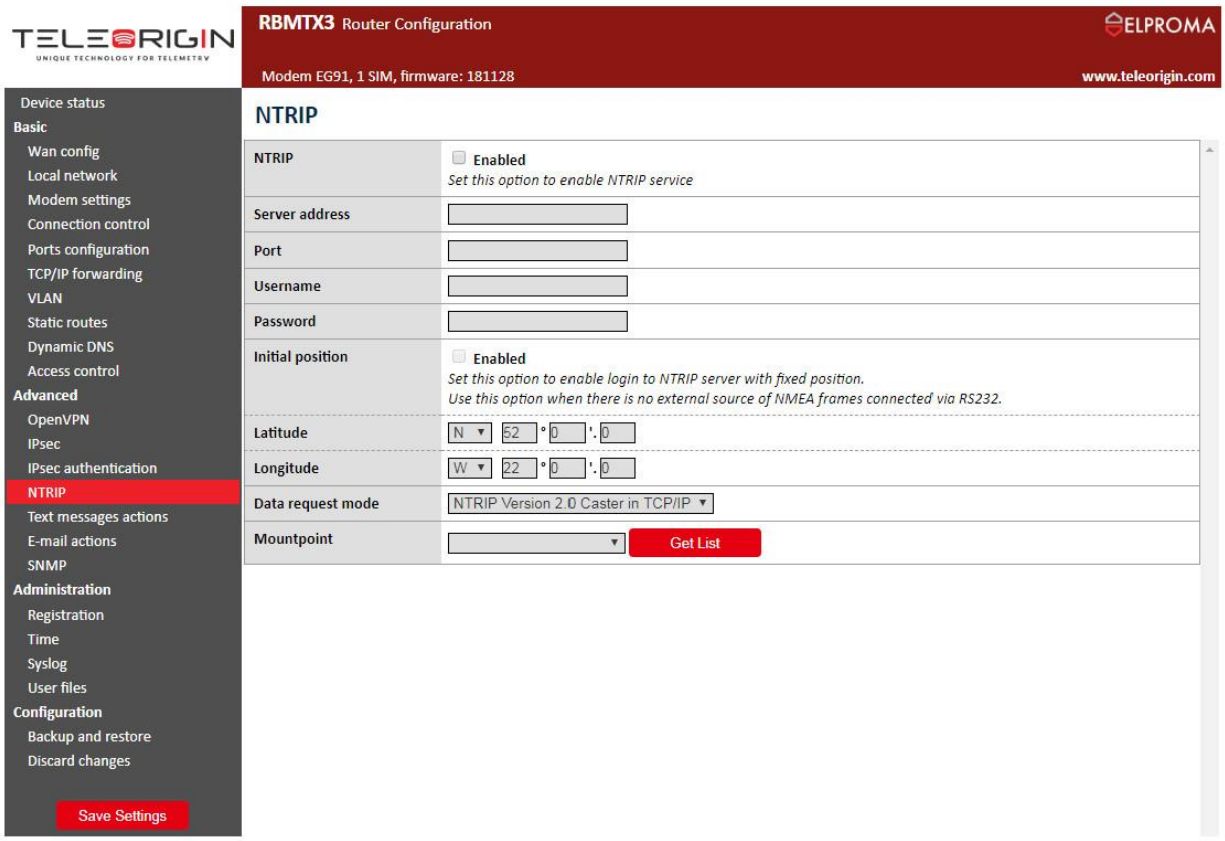


5.2.16 Ustawienia zaawansowane: NTRIP

Jednym z trybów portu /dev/ttyS0 jest komunikacja z urządzeniem zewnętrznym z użyciem protokołu NTRIP. Jeżeli zdecydujesz się na skorzystanie z tego trybu, konieczne będzie ustawienie go w zakładce "RS232 Port configuration". Następnie należy przejść do strony "NTRIP". Pola adresu serwera, portu i pozycji początkowej są wymagane. Nazwa użytkownika i hasło są opcjonalne.

System umożliwia również wybranie trybu "Data Request". Po wprowadzeniu wymaganych danych w pola należy kliknąć przycisk "Get list", aby pobrać listę źródeł z serwera – może to zająć chwilę. Po zakończeniu pobierania należy wybrać jedno ze źródeł.

Uwaga: W przypadku, gdy do portu S0 nie jest przyłączone żadne urządzenie zewnętrzne wysyłające ramki NMEA, aby móc zalogować się do serwera NTRIP należy wprowadzić pozycję początkową.

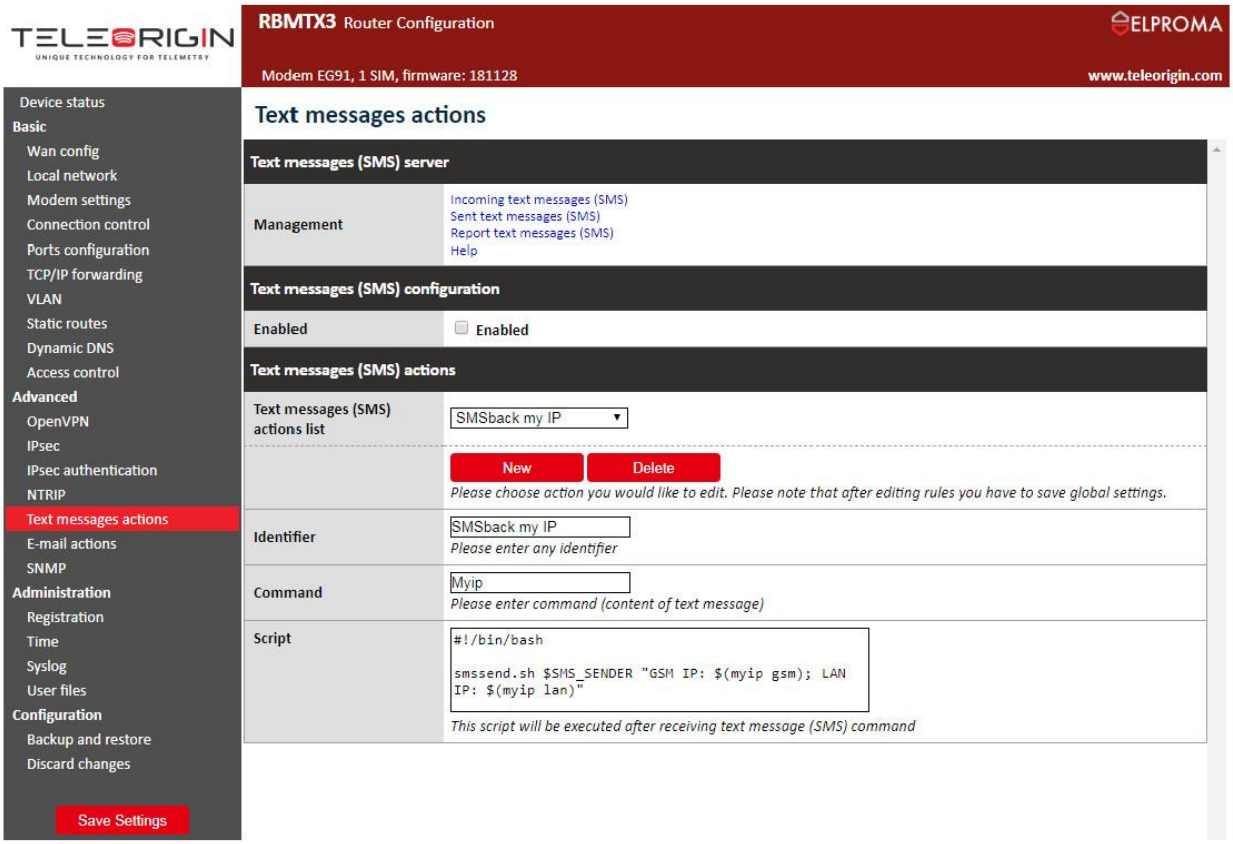


Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

5.2.17 Ustawienia zaawansowane: Text messages actions

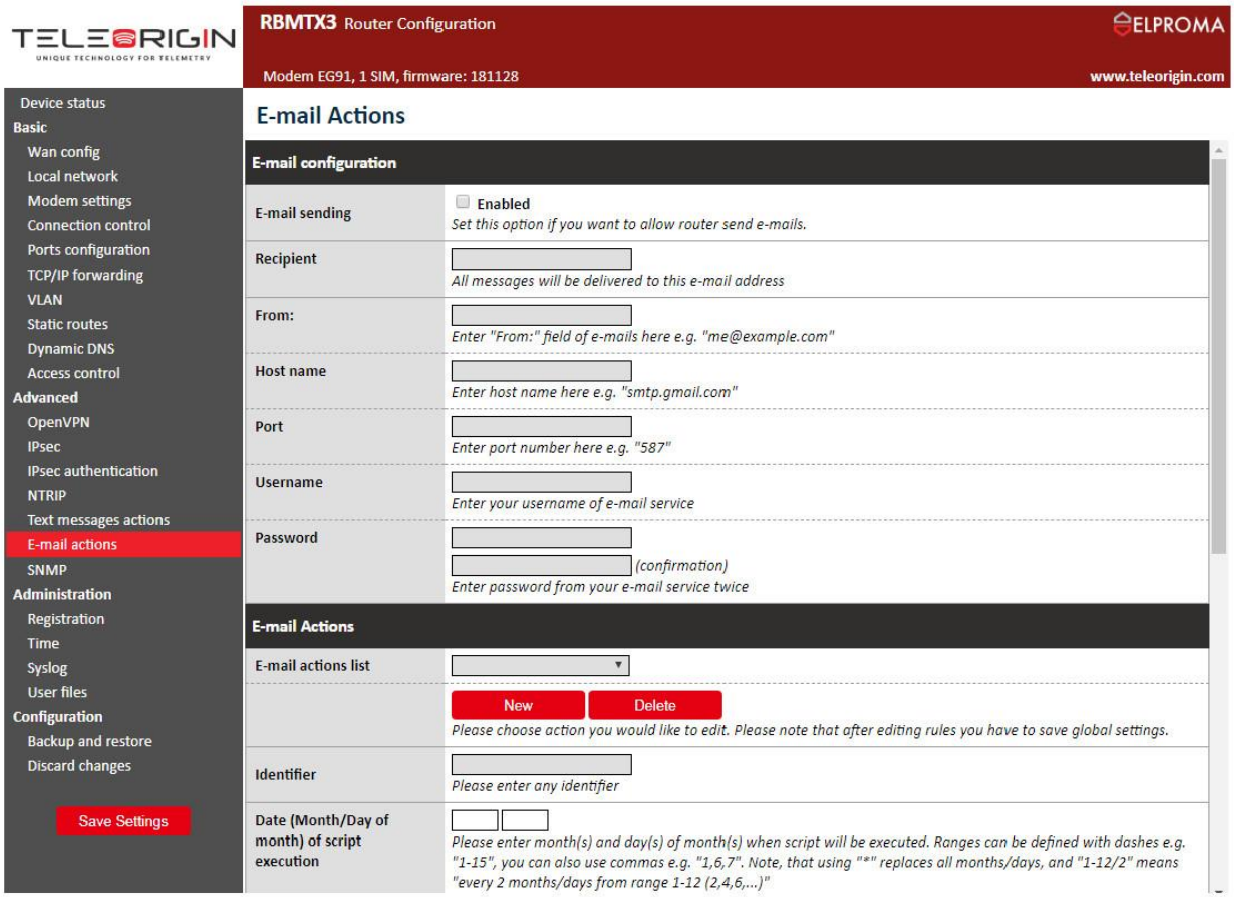
Zakładka "Text Messages Actions" umożliwia użytkownikowi definiowanie skryptów, które będą wykonywane każdorazowo, gdy router odbierze widomość SMS z określoną zawartością.

Aby włączyć tę opcję, należy upewnić się że pole wyboru "SMS Actions" jest zaznaczone oraz że jeden z portów w zakładce "Ports configuration" został ustawiony w tryb otrzymywania wiadomości SMS (SMS receiving). Następnie należy kliknąć przycisk "New", wprowadzić dowolny identyfikator oraz polecenie SMS, które wywoływać będzie daną czynność. Użytkownik może napisać dowolny skrypt typu shell i/lub ustawić realizację czynności GPIO.

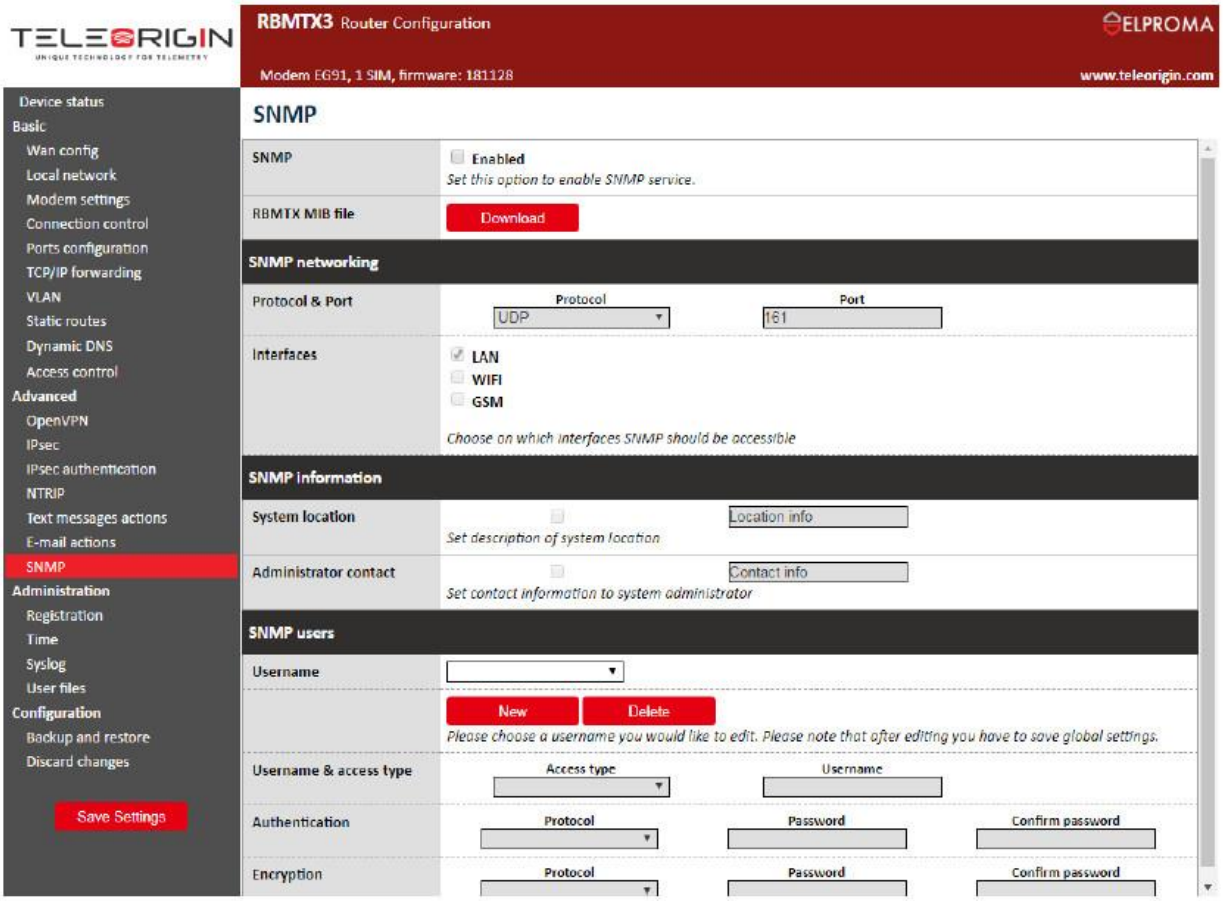


5.2.18 Ustawienia zaawansowane: E-mail actions

W sekcji "E-mail actions" użytkownik może konfigurować parametry wysyłania wiadomości na koncie poczty elektronicznej (konfiguracja obejmuje następujące parametry: odbiorca (Recipient), nadawca (Sender), adres serwera (Server address), użytkownik (User) i hasło (Password). System umożliwia również konfigurację skryptu uruchamianego automatycznie (wiadomości mogą być wysyłane z załącznikami i dostępna jest opcja kompresji pliku przed wysyłką).

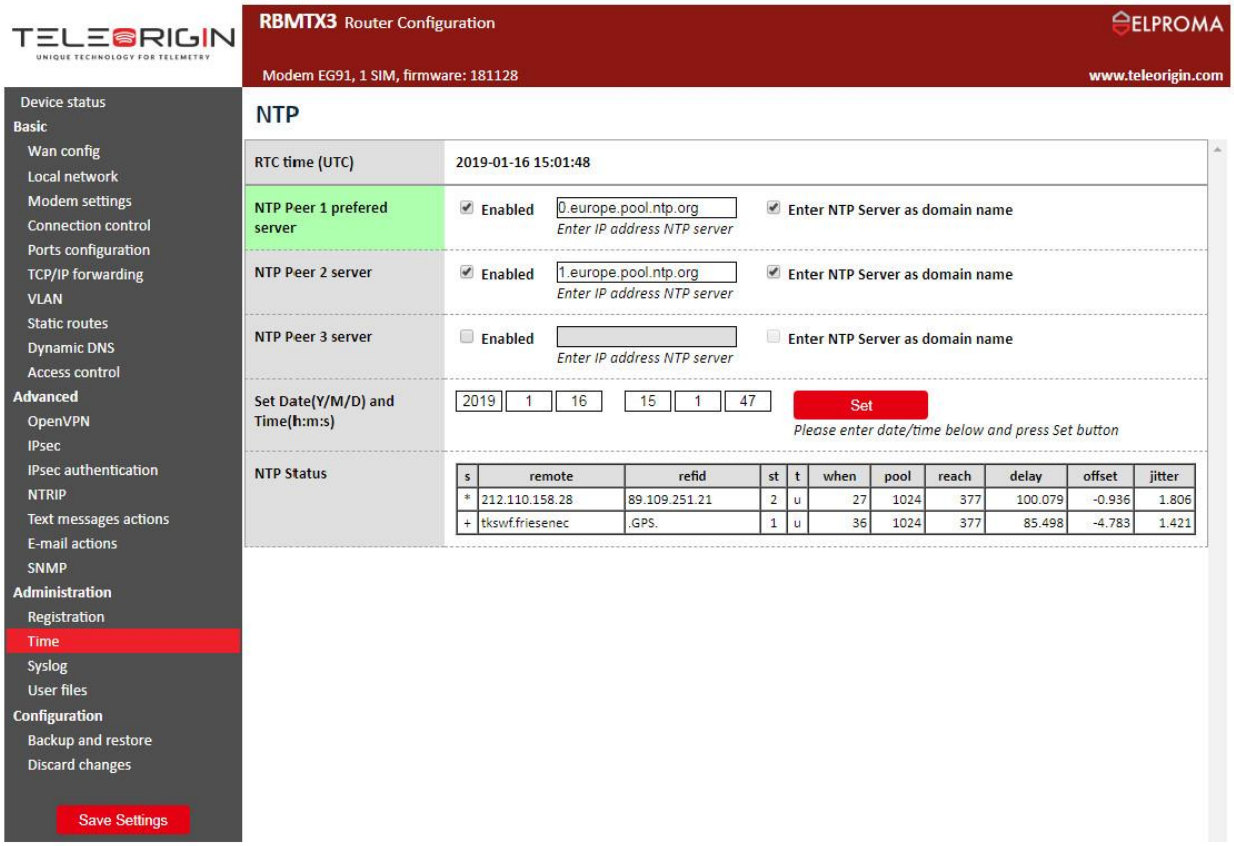


5.2.19 Ustawienia zaawansowane: SNMP



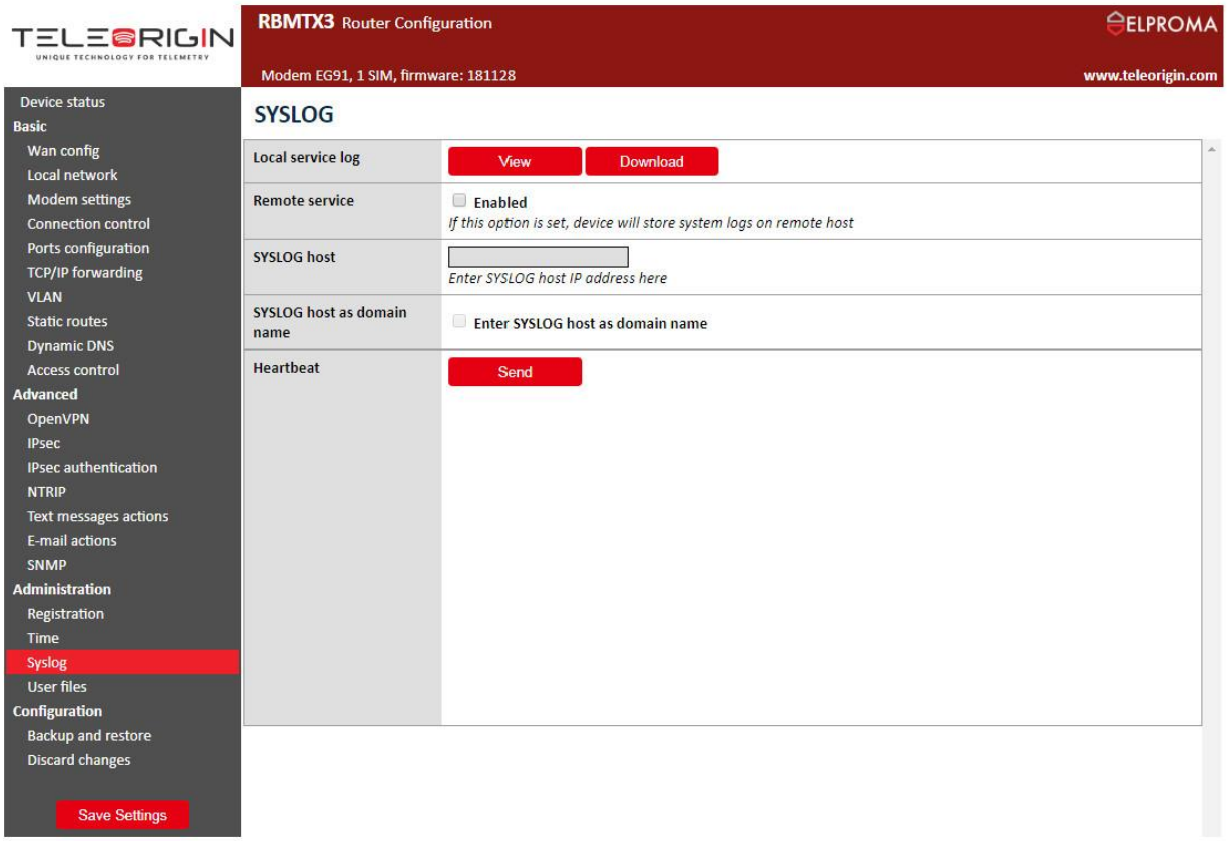
5.2.20 Ustawienia administracyjne: Time

Na tej stronie użytkownik może ręczne skonfigurować zegar sprzętowy lub wpisać adres IP serwera NTP, aby zsynchronizować czas automatycznie.



5.2.21 Ustawienia administracyjne: Syslog

Na tej stronie użytkownik może definiować sposób, w jaki router ma zapisywać logi. Router posiada pamięć wewnętrzną, która jest nadpisywana po osiągnięciu limitu pojemności. Użytkownik może również zapisać logi na komputerze klikając opcję "Download". Można również ustawić zdalny dostęp do logów zaznaczając „Remote service" i konfigurując hosta SYSLOG.

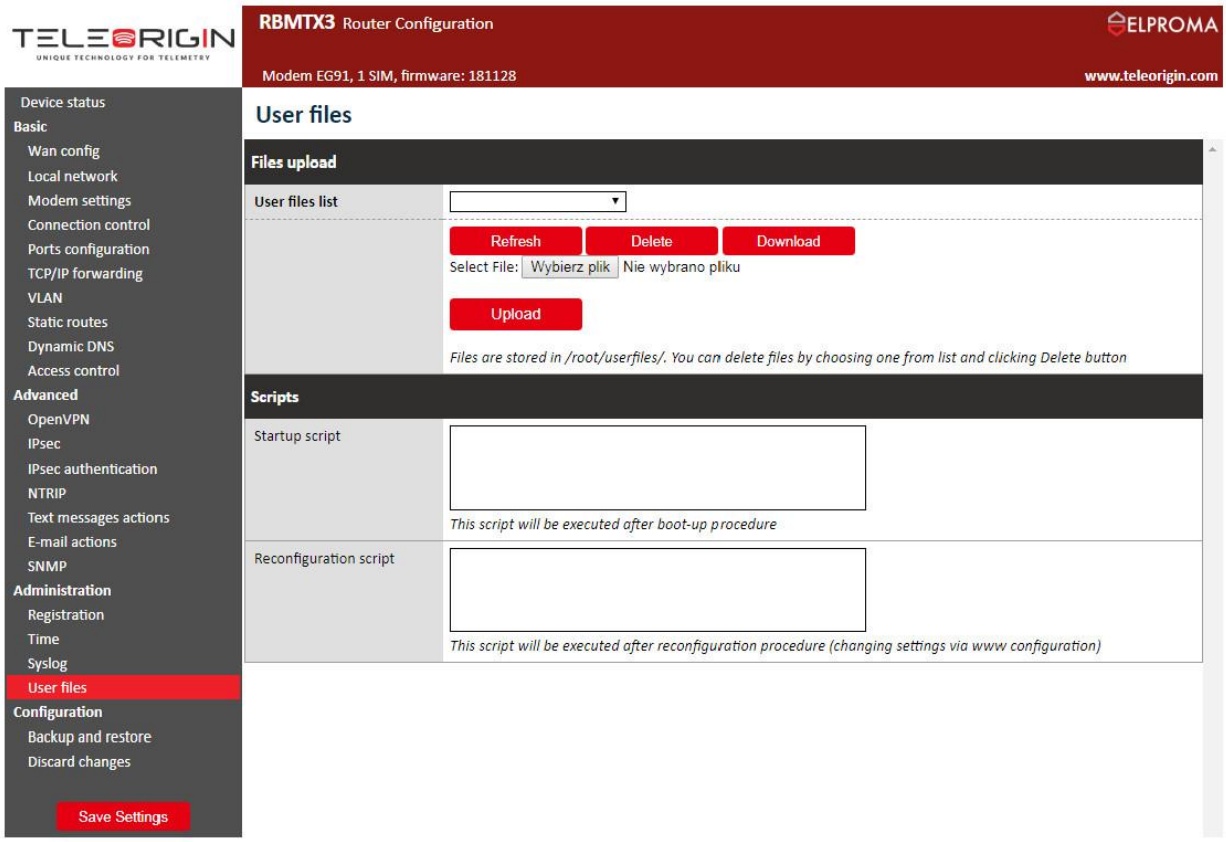


5.2.22 Ustawienia administracyjne: User files

Użytkownik może wgrywać do routera własne skrypty i programy, a także programować ich wykonywanie w konkretnych sytuacjach (np. po połączeniu się z siecią VPN lub po pierwszym uruchomieniu routera). W zakładce "User files" znajduje się lista użytkowników aktualizowana automatycznie po przejściu do zakładki i odświeżana po wciśnięciu przycisku "Refresh". Aby usunąć plik, należy go wybrać z listy i wcisnąć przycisk "Delete". Aby wgrać nowy plik należy wybrać go (po wciśnięciu przycisku "Browse..."), a następnie wcisnąć przycisk "Upload". Po zakończeniu pobierania system wyświetli komunikat o pomyślnym zakończeniu operacji lub o błędzie. Wszystkie pliki są przechowywane z prawami plików wykonywalnych, co pozwala na ich użycie w skryptach.

Pod panelem przesyłania plików znajdują się dwa pola "Startup script" i "Reconfiguration script" , w których użytkownik może pisać skrypty. Skrypt *Startup* jest wykonywany po procedurze uruchomienia routera, skrypt *Reconfiguration* zaś – każdorazowo po kliknięciu przycisku "Save Configuration" na stornie konfiguracji WWW. Użytkownik może pisać skrypty w języku Bash lub PHP. Należy jednak pamiętać o umieszczeniu odpowiedniego nagłówka na początku skryptu (#!/bin/bash lub #!/usr/bin/php). System umożliwia uruchamianie plików użytkownika przechowywanych w katalogu /root/userfiles.

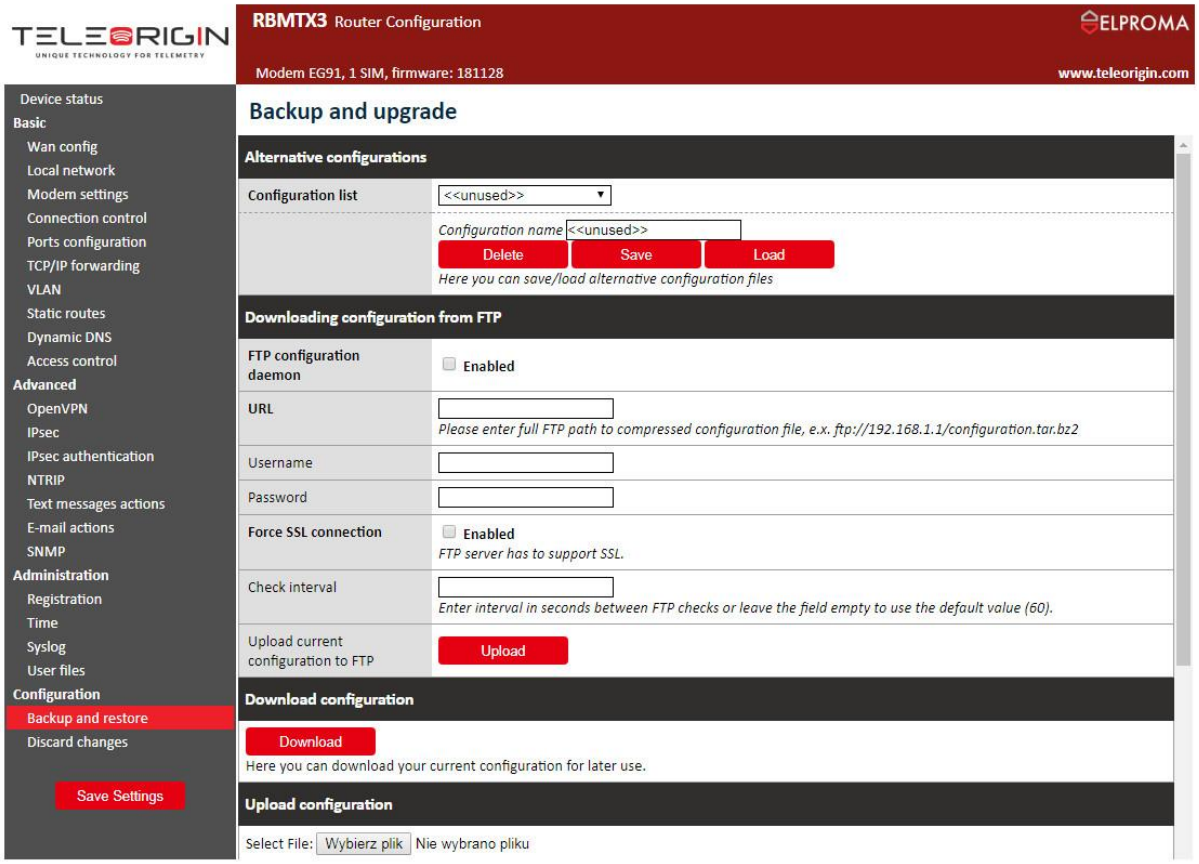
OSTRZEŻENIE: Pliki binarne wgrywane do routera powinny być skompilowane dla procesora użytego w routerze (patrz tebela w pkt 2.3)!



5.2.23 Ustawienia konfiguracyjne: Backup and restore

W zakładce "Backup and restore" użytkownik może:

- zapisywać/wgrywać konfiguracje alternatywne,
- skonfigurować klienta FTP, aby sprawdzał czy na serwerze FTP jest najnowsza konfiguracja,
- pobierać/wysyłać kopie zapasowe konfiguracji.



5.2.24 Ustawienia konfiguracyjne: Discard changes

Dzięki tej opcji użytkownik może anulować bieżące, niezapisane dotychczas zmiany konfiguracyjne.

5.2.25 Przycisk Save settings

Aby zapisać zmiany, należy kliknąć przycisk "Save setting" i odczekać do pojawienia się komunikatu potwierdzającego zapisanie danych konfiguracyjnych.

5.3 Opis logów systemowych

Poniżej przedstawiono strukturę standardowego logu systemowego z niektórymi błędami podstawowymi:

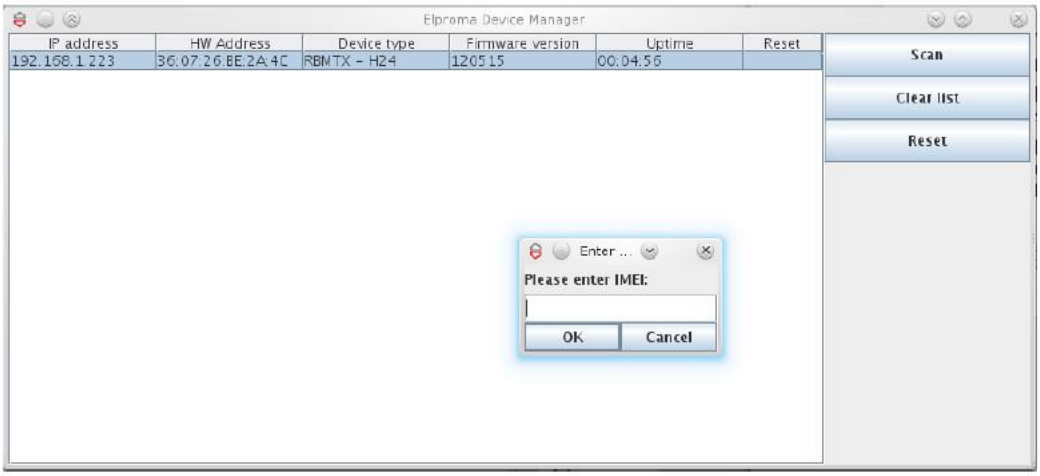
01/01/0000:00:30 rbmtx syslogd 1.4.1: restart.
01/01/0000:00:31 rbmtx Start: RBMTX-Lite - FIRM:171026 – **informacje o modemie i wersji oprogramowania sprzętowego**
01/01/0000:00:35 rbmtx supervisor[560]: SIM Holder open/closed – **adapter SIM zamknięty/otwarty przez oprogramowanie**
01/01/0000:00:36 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 nawiązania 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"

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

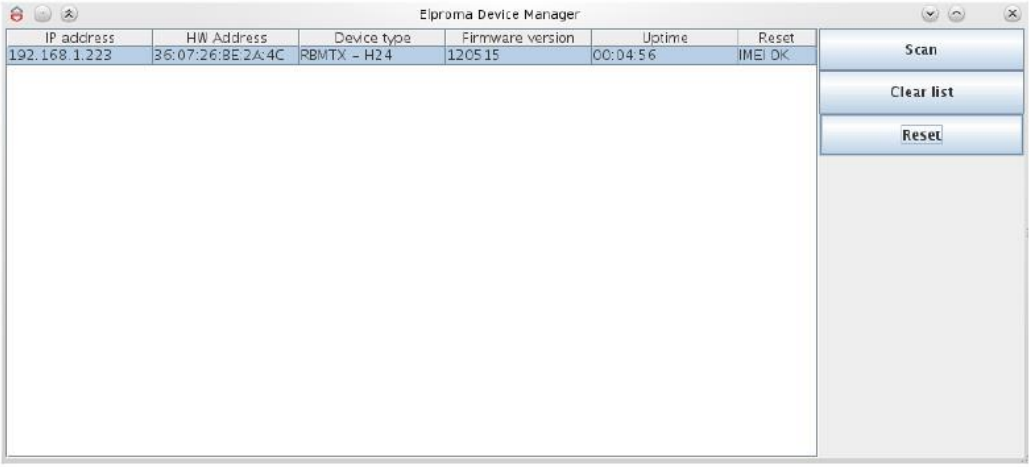
5.4 Elproma Device Manager

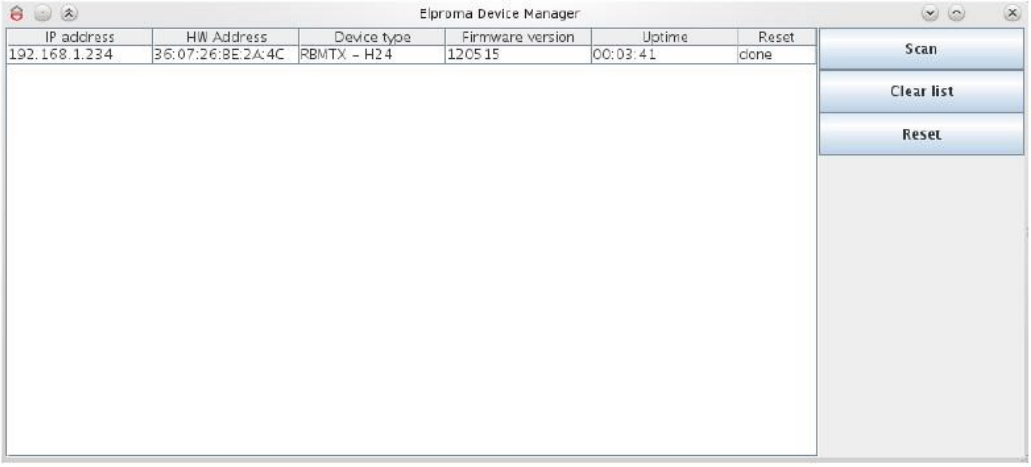
Elproma Device Manager jest aplikacją umożliwiającą użytkownikowi wyszukiwanie routerów RBMTX-Lite w sieci lokalnej (LAN), a następnie przywracanie ustawień fabrycznych poprzez wprowadzanie numeru IMEI urządzeń. Jest to szczególnie przydatne, w wypadku gdy użytkownik nie pamięta numeru IP urządzenia i nie może uzyskać do niego dostępu za pośrednictwem portu szeregowego.

Instalacja aplikacji jest bardzo prosta. W systemie Windows należy rozpakować plik pobrany z serwisu EDM-native, a następnie uruchomić plik EDM.exe. Wersja dla systemu Linux jest dostępna tutaj: edm. Główne okno programu składa się z tabeli, w której wyświetlane są informacje o urządzeniach dostępnych w Twojej sieci oraz przyciski: Scan (skanuj), Clear list (wyczyść listę), Reset (przywróć ustawienia fabryczne). Na początku pracy z aplikacją należy przeskanować lokalną sieć w poszukiwaniu routerów. Wyświetlenie listy wszystkich urządzeń zajmuje z reguły kilka sekund. Należy pamiętać, że uruchomienie routera może potrwać kilka minut i spowodować brak reakcji urządzenia tuż po jego włączeniu.



Po zakończeniu procedury skanowania użytkownik może odczytać w tabeli informacje o znalezionych urządzeniach - adres IP (IP address), adres MAC (MAC address), nazwa urządzenia (Device name), wersja oprogramowania sprzętowego (Firmware ver.) oraz czas od włączenia (Uptime). Jeżeli chcesz przywrócić konfigurację fabryczną w dowolnym urządzeniu widocznym na liście, kliknij przycisk "Reset" i wpisz IMEI. Program wyśle specjalny pakiet do wszystkich urządzeń, lecz konfiguracja fabryczna zostanie przywrócona tylko na urządzeniu z podanym przez użytkownika numerze IMEI. Jeżeli numer ten jest prawidłowy, konfiguracja zostanie przywrócona, co zostanie potwierdzone wyświetleniem się tekstu "IMEI OK" w jednym z pól ostatniej kolumny tabeli. Urządzenie uruchomi się powtórnie, aby załadować nową konfigurację i po około 1-2 minutach potwierdzi pomyślne zakończenie całej operacji (komunikat "IMEI OK" zmieni się na "Done" jak na rysunkach poniżej).





Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

6. Rozwiązywanie problemów

6.1 Brak komunikacji z routerem

W przypadku braku komunikacji z routerem:

- sprawdź wszystkie zewnętrzne połączenia i kable routera,
- sprawdź czy zasilanie podłączone jest poprawnie,
- sprawdź parametry komunikacji TCP/IP,
- sprawdź czy urządzenie nie jest blokowane przez zaporę sieciową (Firewall).

6.2 Router odpowiada, lecz brak połączenia internetowego

W przypadku braku połączenia internetowego:

- sprawdź czy antena jest podłączona prawidłowo,
- sprawdź zasięg sieci GSM/UMTS/LTE w strefie użytkowania (np. na stronie operatora GSM),
- sprawdź czy modem jest skonfigurowany z użyciem parametrów dostarczonych przez dostawcę usług sieciowych (APN, użytkownik GSM, hasło itp.)
- jeśli po wykonaniu powyższych czynności nadal nie masz dostępu do internetu, skontaktuj się z operatorem.

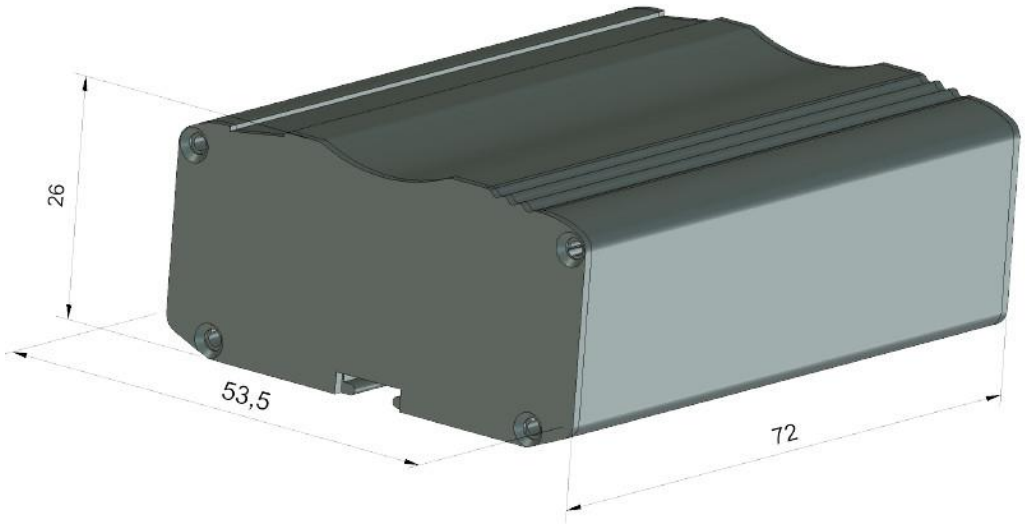
Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

7. Charakterystyka techniczna

7.1 Charakterystyka mechaniczna

Wymiary maksymalne	72 x 53,5 x 26 mm (bez złączy)
Masa	≈ 90 g (dotyczy routera bez złączy zewnętrznych)
Objętość	≈ 100 cm^3 (bez złączy)

7.2 Obudowa (schemat z wymiarami)



7.3 Charakterystyka elektryczna

7.3.1 Zasilanie

- Nominalny zakres zasilania: 9 – 30 V.
- Moc maksymalna (średnia): 5 W.
- Szczytowa (chwilowa) wartość prądu: 1 A.

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

7.3.2 Charakterystyka RF

7.3.2.1 Zakresy częstotliwości – wersja UMTS/HSPA

Pasmo	Odbiór	Transmisja	Jednostka
EGSM900	925 – 960	880 – 915	MHz
DCS1800	1805 – 1880	1710 – 1785	MHz
UMTS2100	2110 – 2170	1920 – 1980	MHz
UMTS1900	1930 – 1990	1850 – 1910	MHz
UMTS900	925 – 960	880 – 915	MHz
UMTS850	869 – 894	824 – 849	MHz

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

7.3.2.2 Zakresy częstotliwości – wersja LTE

Pasmo	Odbiór	Transmisja	Jednostka
EGSM900	880 – 915	925 – 960	MHz
DCS1800	1710 – 1785	1805 – 1880	MHz
WCDMA B1	1920 – 1980	2110 – 2170	MHz
WCDMA B2	1850 – 1910	1930 – 1990	MHz
WCDMA B4	1710 – 1755	2110 – 2155	MHz
WCDMA B5	824 – 849	869 – 894	MHz
WCDMA B8	880 – 915	925 – 960	MHz
LTE-FDD B1	1920 – 1980	2110 – 2170	MHz
LTE-FDD B2	1850 – 1910	1930 – 1990	MHz
LTE-FDD B3	1710 – 1785	1805 – 1880	MHz
LTE-FDD B4	1710 – 1775	2110 – 2155	MHz
LTE-FDD B5	825 – 849	869 – 894	MHz
LTE-FDD B7	2500 – 2570	2620 – 2690	MHz
LTE-FDD B8	880 – 915	925 – 960	MHz
LTE-FDD B12	699 – 716	729 – 746	MHz
LTE-FDD B13	777 – 787	746 – 756	MHz
LTE-FDD B20	832 – 862	791 – 821	MHz
LTE-FDD B28A	703 – 733	758 – 788	MHz

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

7.3.2.3 Charakterystyka Wi-Fi

Standard:	802.11b/g/n
Częstotliwość:	2.4 Ghz
Moc wyjściowa:	13 dBm@11n 17 dBm@11b 15 dBm@11g Tolerancja ±2 dBm
Transfer danych:	Maks. 150 Mbps

7.3.2.4 Antena zewnętrzna

Antena zewnętrzna jest przyłączona do routera za pośrednictwem złącza SMA.
Antena musi mieć parametry przedstawione w tabeli poniżej.

Zakres częstotliwości anteny:	GSM, UMTS lub LTE dla GSM lub ISM 2,4 GHz dla Wi-Fi
Impedancja:	50 Ω
Impedancja DC:	0 Ω
Zysk:	0 dBi
VSWR (z kablem)	-10 dB

Antena wybrana do pracy z routerem powinna być dopasowana optymalnie do warunków roboczych routera. Jeżeli router znajduje się w pomieszczeniu, w którym zasięg sieci jest zbyt niski, należy zastosować antenę zewnętrzną lub specjalną antenę wewnętrzna, aby zwiększyć moc odbieranego sygnału.

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

7.4 Charakterystyka środowiskowa

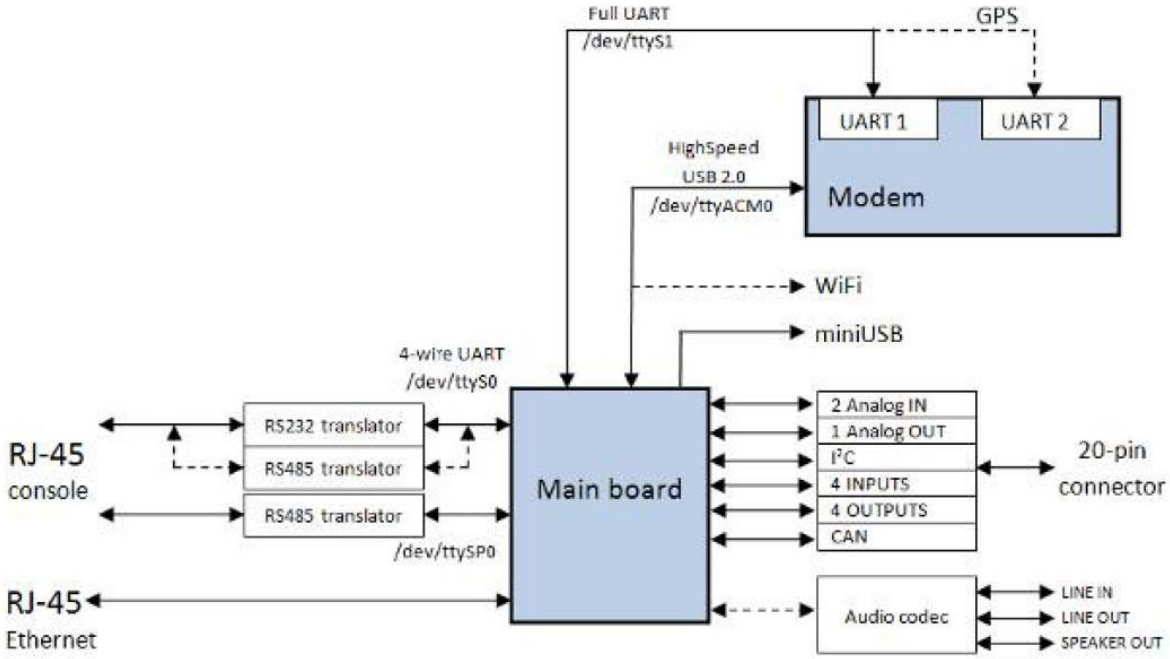
Uwaga! Przekroczenie poniższych wartości może spowodować trwałe uszkodzenie routera.

Parametr	Min.	Maks.	Jednostka
Temperatura pracy	-20	60	°C

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

8. Architektura routera

Schemat poniżej przedstawia uproszczoną architekturę routera RBMTX-Lite. Funkcje oznaczone liniami kropkowanymi są funkcjami opcjonalnymi.



Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

9. Zalecenia dotyczące bezpieczeństwa

9.1 Bezpieczeństwo ogólne

Ze względu na możliwość generowania zakłóceń, podczas używania urządzeń radiowych należy przestrzegać przepisów bezpieczeństwa. Zapoznaj się szczegółowo z zaleceniami poniżej.

Router GSM należy **wyłączać**:

- 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 stacjach paliw,
- w każdym środowisku, które może spowodować wybuch lub wzniecenie pożaru,
- w szpitalach oraz w każdym miejscu, w którym używa się urządzeń medycznych.

Przestrzegaj zakazów używania urządzeń radiowych w miejscach, w których znajdują się znaki informujące o tym, że korzystanie z telefonów komórkowych jest zakazane lub niebezpieczne.

Korzystanie z routera GSM w pobliżu innych urządzeń elektronicznych może również zakłócać prawidłowe działanie tych urządzeń w przypadku ich nienależytego zabezpieczenia. Może to spowodować zniszczenie lub awarię routera GSM bądź innych urządzeń.

9.2 Eksploatacja i konserwacja

Router RBMTX-Lite jest urządzeniem elektronicznym, z którym należy obchodzić się z należytą ostrożnością. Postępuj zgodnie z zaleceniami zamieszczonymi poniżej, aby zapewnić długoletnie działanie Twojego routera.

- Nie wystawiaj modemu na działanie ekstremalnych warunków, takich jak wysoka temperatura lub wilgotność.
- Nie przechowuj routera w miejscach zanieczyszczonych lub zapylonych.
- Nie demontuj routera.
- Nie wystawiaj routera na działanie wody, deszczu lub pary.
- Nie upuszczaj, nie wstrząsaj i nie uderzaj routera.
- Nie umieszczaj routera w pobliżu urządzeń magnetycznych (np. kart kredytowych, itp.).
- Eksploatacja urządzeń lub akcesoriów stron trzecich, które nie są autoryzowane przez Elproma Elektronika Sp. z o.o., może spowodować utratę gwarancji i/lub trwałe uszkodzenie routera.
- Chroń router przed dostępem dzieci poniżej 3 roku życia.

9.3 Odpowiedzialność

Jako użytkownik, ponosisz pełną odpowiedzialność za router. Używaj go z należytą dbałością oraz przestrzegając lokalnych przepisów. Niniejsze urządzenie nie jest zabawką – przechowuj je z dala od dzieci.

Aby zapobiec nieuprawnionemu użyciu routera lub jego kradzieży, stosuj funkcje zabezpieczające (PIN, itp.).

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

10. Akcesoria

W tabeli poniżej przedstawiono zalecane akcesoria routera RBMTX-Lite.

Nr części	Nazwa	Opis
RB-PS12VL2L15	Zasilacz 12 V	< 1,5 m > 2 PIN
RB-PSCP2L15	Kabel zasilający	2PIN < 1,5 m > open end
RB-904G	Antena GSM/UMTS/LTE	2J011
RB-89MSH	Szufladka na kartę SIM	MOLEX 0912360001
RB-MDH	Mocowanie szyny DIN	
RB-MR2R4	Kabel RS232/RS485 2in1	

Kabel zasilający typu "open-end"

Kabel RS232/485

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

11. Zalecenia dotyczące bezpieczeństwa

PRZECZYTAJ UWAŻNIE

Upewnij się, że korzystanie z produktu jest dozwolone w Twoim kraju i w wymaganym środowisku. Użytkowanie niniejszego produktu może być niebezpieczne i należy go unikać:

- w miejscach takich jak szpitale, porty lotnicze, statki powietrzne, itp., w których produkt może zakłócać pracę innych urządzeń elektronicznych,
- w miejscach, w których występuje zagrożenie wybuchem takich jak stacje benzynowe, rafinerie, itp.

Obowiązkiem użytkownika jest egzekwowanie przepisów dotyczących kraju użytkowania i środowiska pracy urządzenia.

Nie należy demontować urządzenia, gdyż każdy ślad manipulowania może przyczynić się do unieważnienia gwarancji.

Zaleca się postępowanie zgodnie z instrukcją użytkowania w zakresie prawidłowego przyłączenia przewodów. Produkt należy zasilać ze źródła stabilizowanego napięcia, okablowanie zaś musi spełniać wymagania przepisów przeciwpożarowych i bezpieczeństwa.

Z produktem należy obchodzić się z ostrożnie, unikać kontaktu ze stykami, gdyż wyładowania elektrostatyczne mogą uszkodzić produkt. Stosowanie analogicznych środków ostrożności dotyczy również postepowania z kartą SIM – należy zapoznać się szczegółowo z instrukcją jej użytkowania. Nie wkładaj lub nie usuwaj karty SIM, gdy produkt jest w trybie oszczędzania energii.

Integrator systemów ponosi odpowiedzialność za funkcjonowanie produktu końcowego. W związku z tym, ze względu na ryzyko zakłócenia pracy sieci GSM i zewnętrznych urządzeń lub negatywny wpływ na zabezpieczenia, należy postępować ostrożnie z zewnętrznymi komponentami routera, a także z komponentami zastosowanymi w innych projektach lub instalacjach. W przypadku jakichkolwiek wątpliwości należy odnieść się do dokumentacji technicznej i obowiązujących przepisów.

Każde urządzenie musi być wyposażone w odpowiednią antenę o określonej charakterystyce. Antenę należy zamontować z zachowaniem należytej staranności, w sposób zapobiegający zakłóceniom generowanym przez inne urządzenia oraz w minimalnej odległości od ludzi (20 cm). W przypadku niespełnienia powyższych wymagań integrator systemów musi ocenić produkt końcowy pod kątem przepisów SAR.

1. Urządzenie nie zapewnia ochrony przed wyładowaniami atmosferycznymi i przepięciami. W przypadku montażu na zewnątrz budynku należy zastosować zabezpieczenie w postaci obudowy niemetalicznej zgodnie z normą UL 50. Oprócz tego użytkownik powinien zapewnić zabezpieczenie przed wyładowaniami atmosferycznymi i nadmiernym napięciem zgodnie z Krajowymi Normami Elektrycznymi.
2. Należy upewnić się, że korzystanie z produktu jest dozwolone w danym kraju oraz w wymaganym środowisku. Niektóre dyrektywy wydane przez Wspólnotę Europejską dotyczą sprzętu elektronicznego wprowadzonego na rynek. Wszystkie stosowne informacje oraz treść dyrektywy 2014/53/UE (RED) dotyczące sprzętu komunikacyjnego są dostępne na witrynie Komisji Europejskiej: http://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en.

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

12. Certyfikaty

12.1 Zagadnienia dotyczące oceny zgodności

Produkt RBMTX-Lite oceniono z udziałem jednostki notyfikowanej pod kątem spełniania istotnych wymagań dyrektywy nr 2014/53/UE (RED) dotyczącej urządzeń radiowych, aby wykazać zgodność z normami zharmonizowanymi.

12.2 Deklaracje zgodności

Produkt RBMTX-Lite jest zgodny z następującymi normami lub z pozostałymi dokumentami normatywnymi:

12.3 Ograniczenia krajowe

Niniejsze urządzenie jest przeznaczone do użycia we wszystkich państwach członkowskich UE (oraz w innych krajach przestrzegających postanowień dyrektywy 2014/53/UE) bez ograniczeń, z wyłączeniem krajów wymienionych poniżej:

Norwegia	Niniejszy podpunkt nie dotyczy obszaru geograficznego zlokalizowanego w promieniu 20 km od geograficznego środka miejscowości Ny-Ålesund.

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

13. 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	International 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

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

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
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

Elproma Elektronika Sp. z o.o.
Ul. Szymanowskiego 13
05-092 Łomianki k/Warszawy
e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81

14. Wsparcie online

Elproma zapewnia kompleksową obsługę klienta w trybie online, obejmującą:

- najnowszą wersję niniejszego dokumentu,
- najnowsze sterowniki do routera RBMTX-Lite,
- wsparcie techniczne.

Stosowne informacje są dostępne na stronie www.elproma.com.pl lub www.teleorigin.com.

W sprawie informacji dodatkowych skontaktuj się z nami:

Email: info@teleorigin.com lub info@elpromaelectronics.com
Tel.: +48 (22) 751 76 80
Faks: +48 (22) 751 76 81

TELEORIGIN
UNIQUE TECHNOLOGY FOR TELEMETRY

D Z I Ę K U J E M Y

TELEORIGIN
UNIQUE TECHNOLOGY FOR TELEMETRY

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

e-mail: info@teleorigin.com
tel. +48 (22) 751 76 80
fax +48 (22) 751 76 81