



Wszelkie prawa do niniejszej instrukcji są własnością firmy ASTOR Sp. z o.o.  
(określanej w dalszej części jako ASTOR).

Wszelkie prawa zastrzeżone. Kopiowanie niniejszej instrukcji lub jej fragmentów  
bez pisemnej zgody firmy ASTOR jest zakazane.

Firma ASTOR zastrzega sobie prawo do dokonywania zmian technicznych bądź modyfikacji  
zawartości niniejszego dokumentu bez uprzedniego powiadomienia.

## 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  |
| 3.3    | Interfejsy zewnętrzne .....                             | 7  |
| 3.3.1  | Złącze anteny GSM/UMTS/LTE .....                        | 7  |
| 3.3.2  | Port szeregowy routera (RS232/RS485) .....              | 8  |
| 3.3.3  | Złącze IO .....   | 10 |
| 3.3.4  | Złącze LAN .....  | 11 |
| 3.3.5  | Złącze zasilania .....                                  | 12 |
| 3.3.6  | Złącza kart SIM .....                                   | 13 |
| 3.4    | Etykieta produktu.....                                  | 13 |
| 3.5    | Diody LED .....   | 13 |
| 4.     | Podstawowe funkcje i usługi.....                        | 14 |
| 5.     | Korzystanie z routera .....                             | 16 |
| 5.1    | Konfiguracja .....                                      | 16 |
| 5.1.1  | Wkładanie kart SIM .....                                | 16 |
| 5.1.2  | Podłączanie anteny .....                                | 16 |
| 5.1.3  | Podłączanie kabla zasilającego .....                    | 17 |
| 5.1.4  | Podłączanie kabla LAN do gniazda RJ-45 .....            | 17 |
| 5.2    | Konfiguracja routera .....                              | 17 |
| 5.2.1  | Konfiguracja połączenia .....                           | 17 |
| 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.....          | 21 |
| 5.2.7  | Ustawienia podstawowe: Ports configuration.....         | 22 |
| 5.2.8  | Ustawienia podstawowe: TCP/IP forwarding .....          | 23 |
| 5.2.9  | Ustawienia podstawowe: VLAN .....                       | 24 |
| 5.2.10 | Ustawienia podstawowe: Static routes .....              | 25 |
| 5.2.11 | Ustawienia podstawowe: Dynamic DNS.....                 | 26 |
| 5.2.12 | Ustawienia podstawowe: Access control .....             | 27 |
| 5.2.13 | Ustawienia zaawansowane: OpenVPN .....                  | 29 |
| 5.2.14 | Ustawienia zaawansowane: Ipsec static/Ipsec mobile..... | 32 |
| 5.2.15 | Generowanie certyfikatów SSL .....                      | 34 |
| 5.2.16 | Ustawienia zaawansowane: NTRIP .....                    | 36 |
| 5.2.17 | Ustawienia zaawansowane: Text messages actions.....     | 37 |

|         |  |    |
|---------|--|----|
| 5.2.18  | Ustawienia zaawansowane: E-mail actions .....              | 38 |
| 5.2.19  | Ustawienia zaawansowane: SNMP .....                        | 39 |
| 5.2.20  | Ustawienia administracyjne: Time .....                     | 40 |
| 5.2.21  | Ustawienia administracyjne: Syslog .....                   | 41 |
| 5.2.22  | Ustawienia administracyjne: User files .....               | 43 |
| 5.2.23  | Ustawienia konfiguracyjne: Backup and restore .....        | 43 |
| 5.2.24  | Ustawienia konfiguracyjne: Discard changes .....           | 44 |
| 5.2.25  | Przycisk Save settings .....                               | 44 |
| 5.3     | Opis logów systemowych .....                               | 44 |
| 5.4     | Astraada Device Manager .....                              | 45 |
| 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     | Charakterystyka elektryczna .....                          | 49 |
| 7.2.1   | Zasilanie .....  | 49 |
| 7.2.2   | Charakterystyka RF .....                                   | 49 |
| 7.2.2.1 | Zakresy częstotliwości – wersja UMTS/HSPA .....            | 49 |
| 7.2.2.2 | Zakresy częstotliwości – wersja LTE .....                  | 50 |
| 7.2.2.3 | Charakterystyka Wi-Fi .....                                | 51 |
| 7.2.2.4 | Antena zewnętrzna .....                                    | 51 |
| 7.4     | Charakterystyka środowiskowa .....                         | 51 |
| 8.      | Architektura routera .....                                 | 52 |
| 9.      | Zalecenia dotyczące bezpieczeństwa .....                   | 53 |
| 9.1     | Bezpieczeństwo ogólne .....                                | 53 |
| 9.2     | Eksploatacja i konserwacja .....                           | 53 |
| 9.3     | Odpowiedzialność .....                                     | 53 |
| 10.     | Zalecenia dotyczące bezpieczeństwa .....                   | 55 |
| 11.     | Certyfikaty .....  | 56 |
| 11.1    | Zagadnienia dotyczące oceny zgodności .....                | 56 |
| 11.2    | Deklaracje zgodności .....                                 | 56 |
| 11.3    | Ograniczenia krajowe .....                                 | 56 |
| 12.     | Lista skrótów .....  | 57 |
| 13.     | Wsparcie online .....                                      | 59 |

## 1. Historia dokumentu

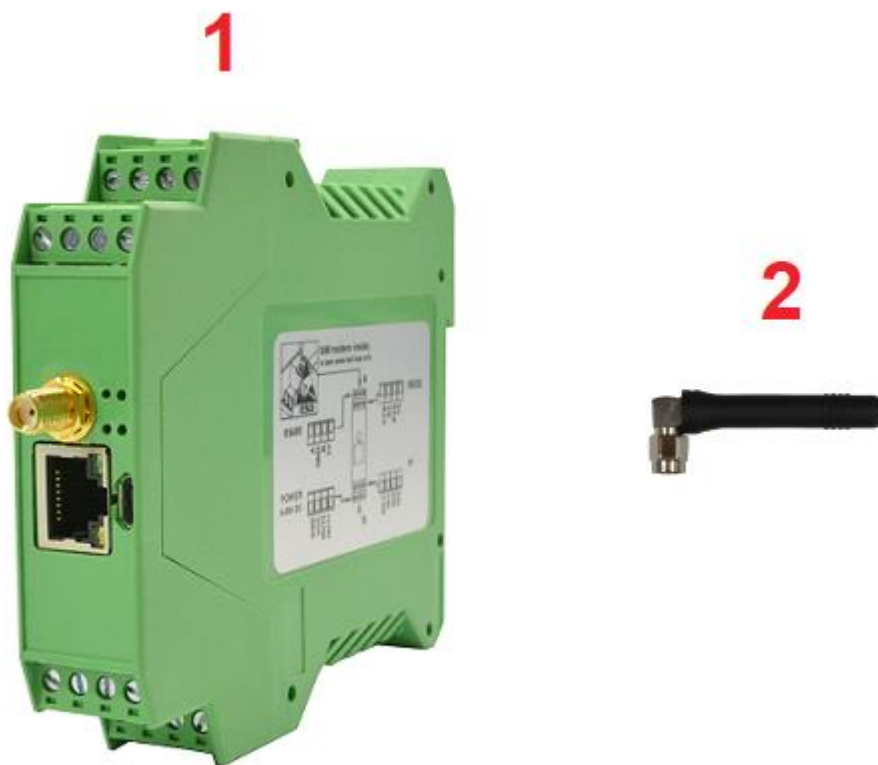
| <b>Wersja</b> | <b>Data</b> | <b>Zmiany</b>  |
|---------------|-------------|----------------|
| #1.0          | 29.11.2019  | Wersja wstępna |

## 2. Opakowanie

### 2.1 Pudełko

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

### 2.2 Zawartość opakowania



Opakowanie zawiera:

- 1) router AS30GSM420P-IO,
- 2) antenę GSM (ze złączem SMA)

## 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   |

## 3. Opis ogólny

### 3.1 Panel przedni

---



### 3.3 Interfejsy zewnętrzne

---

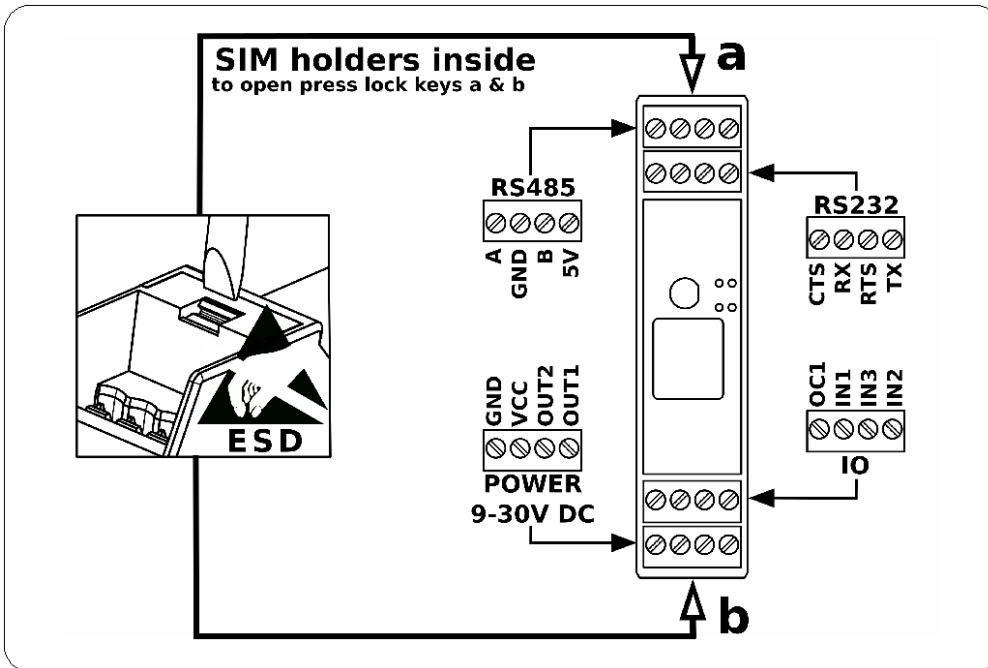
#### 3.3.1 Złącze anteny GSM/UMTS/LTE

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.

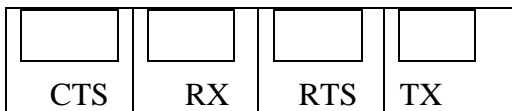
### 3.3.2 Port szeregowy routera (RS232/RS485)

Porty szeregowy RS232 i RS485 (złącze 4-pinowe, oznakowane na poniższym obrazku jako „RS232” i „RS485”) znajdują się po bokach routera. Opis styków znajduje się na rysunku i w tabelach poniżej.





RS232:



RS485:



**RS485**

**RS232**

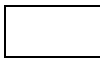
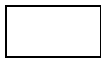
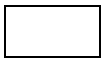
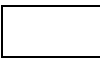
**IO**

**POWER**

### 3.3.3 Złącze IO

Na złączu IO są 3 cyfrowe wejścia i 1 wyjście typu open collector. Poniżej znajduje się opis wyprowadzeń złącza IO.

IO

| OC1   | IN1   | IN3   | IN2   |
|---|---|---|---|
|  |  |  |  |



### 3.3.4 Złącze LAN

Złącze Ethernet znajduje się przy złączu antenowym 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".

**Ethernet**



### 3.3.5 Złącze zasilania

Zakres zasilania routera wynosi 9 – 30 V.

Power:

| GND | VCC | OUT2 | OUT1 |
|-----|-----|------|------|
| □   | □   | □    | □    |



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

### 3.3.6 Złącza kart SIM

Oba złącza na karty SIM są umieszczone w środku urządzenia. Aby możliwe było korzystanie z usług sieci GSM/LTE, do routera należy włożyć przynajmniej jedną kartę SIM.

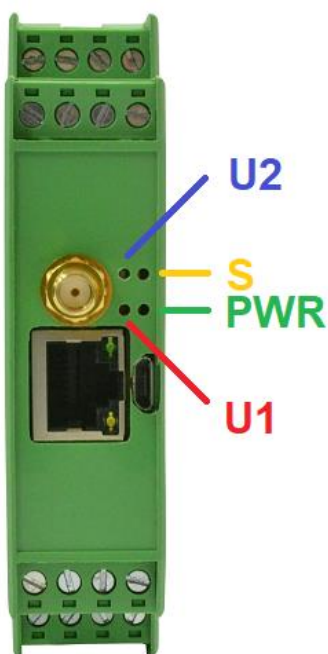
### 3.4 Etykieta produktu

Etykieta produktu zawiera następujące informacje:

- numer seryjny produktu,
- oznakowanie CE,
- 15-cyfrowy kod kreskowy,
- nazwę modelu (AS30GSM420P-IO),
- domyślny adres IP, nazwę użytkownika i hasło do logowania do panelu konfiguracyjnego.

### 3.5 Diody LED

Router jest wyposażony w cztery diody LED wskazujące tryb pracy urządzenia. Opis kontroltek zamieszczono w tabeli poniżej.



| Kontrolka | Kolor     | Opis                      |
|-----------|-----------|---------------------------|
| U1        | Czerwony  | Obsługa przez użytkownika |
| U2        | Niebieski | Router jest aktywny       |

|     |         |  |
|-----|---------|--|
| S   | Żółty   | Wskazanie sieci:<br>AS30GSM420P-IO 3G: <ul style="list-style-type: none"> <li>• Miga rzadko (200 ms wł., 1800 ms wył.) – wyszukiwanie sieci,</li> <li>• Miga rzadko (1800 ms wł., 200 ms wył.) – w oczekiwaniu/transfer danych,</li> <li>• Świeci ciągle – transmisja głosowa/CSD.</li> </ul> AS30GSM420P-IO 4G: <ul style="list-style-type: none"> <li>• Miga rzadko (200 ms wł., 1800 ms wył.) – wyszukiwanie sieci,</li> <li>• Miga rzadko (1800 ms wł., 200 ms wył.) – w oczekiwaniu,</li> <li>• Miga często (125 ms wł., 125 ms wył.) – transfer danych,</li> <li>• Świeci ciągle – transmisja głosowa</li> </ul> |
| PWR | Zielony | Zasilanie  |

## 4. Podstawowe funkcje i usługi

Podstawowe funkcje i usługi przedstawiono w tabeli poniżej.

| Funkcja / Usługa  | Opis  |
|-------------------|---|
| Obsługiwane pasma | Wersja UMTS/HSPA: <ul style="list-style-type: none"> <li>• GSM 900/1800 MHz</li> <li>• UMTS 900/2100 MHz</li> </ul> Wersja LTE: <ul style="list-style-type: none"> <li>• GSM 900/1800 MHz</li> <li>• WCDMA FDD B1, B8 Class 3</li> <li>• LTE FDD B1, B3, B7, B8, B20 Cat. 1 i Cat. 4</li> </ul>   |
| Transfer danych   | <ul style="list-style-type: none"> <li>• LTE Cat. 1 (downlink 10 Mbit/s, uplink 5 Mbit/s)</li> <li>• LTE Cat. 4 (downlink 150 Mbit/s, uplink 50 Mbit/s)</li> <li>• UMTS (downlink 7.2 Mbit/s)</li> <li>• GPRS (Multi-slot class 10, max BR downlink 85,6 Kb/s)</li> <li>• Protokoły wbudowane: PPP, TCP/IP, UDP/IP, MMS, HTTP, HTTPS, SSL, FTP, FTPS, SMTP, SMTPS, NTP, NITZ, PING</li> <li>• Przekierowanie portów, Ipsec, OpenVPN</li> <li>• Protokół Class B GSM 07.10 multiplexing</li> </ul> |
| Wi-Fi*            | Standard: <ul style="list-style-type: none"> <li>• 802.11b/g/n</li> </ul> Transfer danych: <ul style="list-style-type: none"> <li>• maks. 150 Mbps</li> </ul>   |
| Bluetooth*        | V4.1+EDR  |
| Zasilanie         | <ul style="list-style-type: none"> <li>• Zakres napięcia nominalnego: 9 – 30 V</li> <li>• Maksymalne zasilanie ciągłe (średnie): 5 W</li> </ul>   |

|                                |  |
|--------------------------------|--|
|                                | <ul style="list-style-type: none"> <li>• Szczytowa (chwilowa) wartość prądu: 1 A</li> </ul>  |
| Interfejsy (wersja podstawowa) | <ul style="list-style-type: none"> <li>• Złącze anteny GSM/UMTS/LTE: SMA</li> <li>• 2 x SIM (wewnętrzne): standard 1,8 V/3 V</li> <li>• RS232 i RS485, złącze zasilania i I/O na złączach 4-pinowych</li> <li>• Złącze Ethernet (RJ45)</li> <li>• microUSB (OTG)</li> <li>• 4 x LED</li> </ul> |
| Opcje                          | <ul style="list-style-type: none"> <li>• Złącze anteny Wi-Fi: SMA (męskie)</li> <li>• Złącze anteny Bluetooth: SMA</li> </ul>  |
| Inne                           | Rozmiar fizyczny: <ul style="list-style-type: none"> <li>• Wymiary maksymalne: 116 x 100 x 23 mm (bez złącz)</li> </ul> Zakres temperatury pracy: <ul style="list-style-type: none"> <li>• -20 °C/60 °C</li> </ul>   |

\* Opcjonalnie

## 5. Korzystanie z routera

### 5.1 Konfiguracja

Aby skonfigurować router należy wykonać następujące kroki:

#### 5.1.1 Wkładanie kart SIM

Routery są z dwoma gniazdami na karty SIM. Aby włożyć karty SIM należy otworzyć obudowę urządzenia.

#### 5.1.2 Podłączanie anteny

- Podłącz antenę GSM/UMTS/LTE do złącza SMA





### 5.1.3 Podłączanie kabla zasilającego

Podłącz kabel zasilający do złącza zasilania POWER (piny GND i VCC)

### 5.1.4 Podłączanie kabla LAN do gniazda RJ-45

Podłącz kabel LAN do gniazda RJ-45.

## 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>.

### 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:

Device status

**Basic**

- Wan config
- Local network
- Modem settings
- Connection control
- Ports configuration
- TCP/IP forwarding
- VLAN
- Static routes
- Dynamic DNS
- Access control

**Advanced**

- OpenVPN
- IPsec
- IPsec authentication
- NTRIP
- Text messages actions
- E-mail actions
- SNMP

**Administration**

- Registration
- Time
- Syslog
- User files

**Configuration**

- Backup and restore
- Discard changes

Save Settings

### Status

| System            | CPU load                  | 0.10, 0.10, 0.13, 1/91, 17683                    |
|-------------------|---------------------------|--|
|                   | Temperature               | 51.2°C   |
|                   | Up time                   | 5d 6:7:50  |
|                   | Memory (total/free)       | 253040 kB/186356 kB                              |
| Modem information |                           |  |
|                   | Model, firm. ver., IMEI   | EG91 (EG91EFBR06A04M4G), IMEI: 862831030128867   |
|                   | PIN, Operator             | READY, Operator: Orange Orange                   |
|                   | Network Status            | Registered (home network, LAC=E2EA, CID=2C32424) |
|                   | Signal Strength (CSQ)     | Excellent, -67 dBm (CSQ=23)                      |
|                   | Packet Data Service       | LTE  |
|                   | GSM SIM selection         | MASTER   |
| GSM Connected     |                           |  |
|                   | IP/Mask                   | 10.66.27.61/255.255.255.252                      |
|                   | MAC Address               | 1E:8E:E5:A0:94:EC                                |
|                   | RX/TX bytes (packets)     | 26.58 MB/29.86 MB (119036/109278)                |
| LAN1              |                           |  |
|                   | IP/Mask                   | 192.168.90.125/255.255.255.0                     |
|                   | MAC Address               | 36:07:11:44:44:1F                                |
|                   | RX/TX bytes (packets)     | 40.66 MB/4.66 KB (150874/204)                    |
| WiFi              |                           |  |
|                   | SSID                      | AP4 (freq: 2.447 GHz)                            |
|                   | Link quality/Signal level | 47/70/-63 dBm                                    |
|                   | AP MAC                    | 70:4D:7B:D1:CB:A0                                |
|                   | IP/Mask                   | 192.168.90.125/255.255.255.0                     |
|                   | MAC Address               | A0:C9:A0:5B:07:A3                                |
|                   | RX/TX bytes (packets)     | 45.75 MB/27.52 MB (171762/51258)                 |
| VPN/CLOUD         |                           |  |
|                   | IP/Mask                   | 172.63.5.15/255.255.255.0                        |
|                   | RX/TX bytes (packets)     | 16.50 MB/21.73 MB (75841/63385)                  |

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

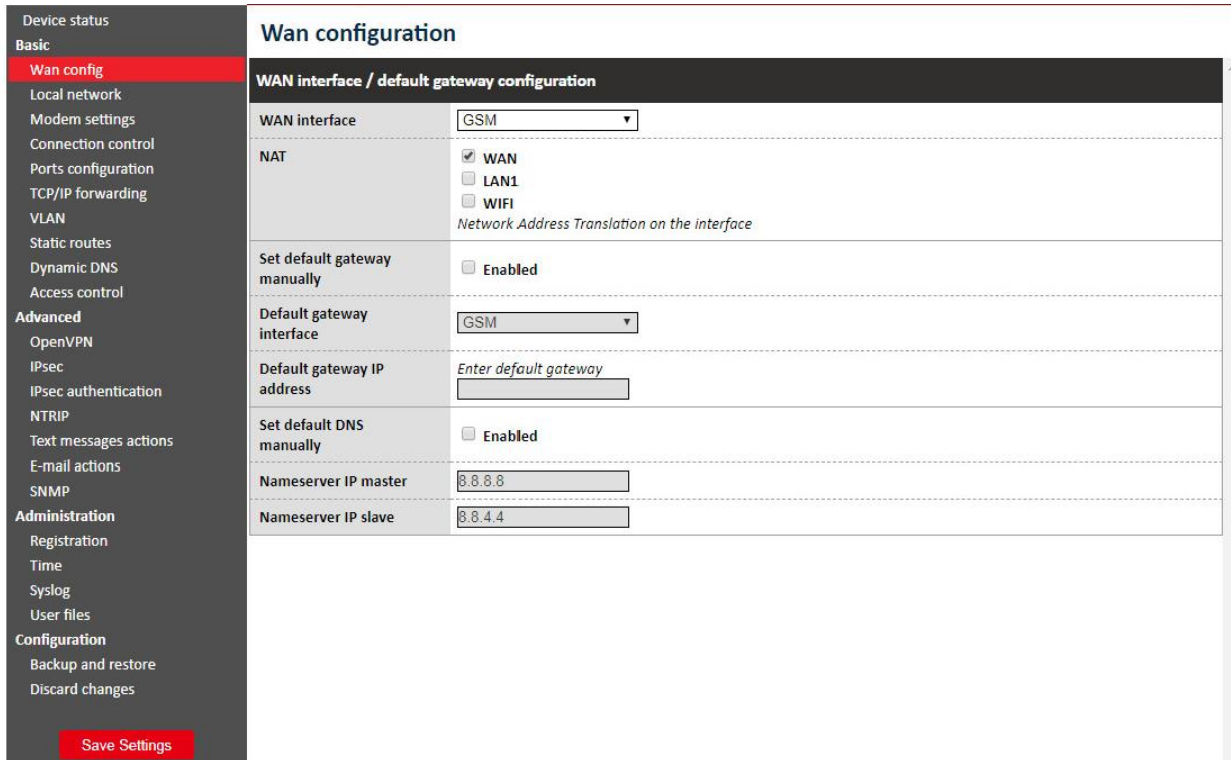
W tabeli poniżej zamieszczono opisy wszystkich pól zawartych w zakładce statusu urządzenia (Device status):

| 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:<br>SIM PIN – blokada PIN (ustaw prawidłowy kod PIN w zakładce "GSM network")<br>READY – odblokowanie karty SIM<br>SIM PUK – blokada PUK   |
| Network Status             | Registered (Home, LAC=2B21, CID=028FC03) | Status rejestracji (parametr 1), kod regionu (parametr 2), Cell ID (parametr 3).<br>Możliwe statusy:<br>- not registered: w chwili obecnej router nie wyszukuje nowego operatora do rejestracji,<br>- registered: Home,<br>- not registered, searching - niezarejestrowany, lecz router wyszukuje w chwili obecnej nowego operatora do rejestracji, |

|                                 |                                |   |
|---------------------------------|--------------------------------|---|
|                                 |                                | - Registration denied – rejestracja odrzucona<br>- unknown - niezany<br>- 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  |
| VPNCLLOUD IP/Mask               | 172.63.5.15/255.255.255.0      | Routery z opcją TACS  |
| VPNCLLOUD RX/TX bytes (packets) | 10.11 MB/7.05 MB (41778/29863) |   |

## 5.2.3 Ustawienia podstawowe: WAN config

Stronę konfiguracyjną sieci WAN przedstawiono na ilustracji poniżej.



**Wan configuration**

**WAN interface / default gateway configuration**

WAN interface: GSM

NAT:
 

- WAN
- LAN1
- WIFI

 Network Address Translation on the interface

Set default gateway manually:  Enabled

Default gateway interface: GSM

Default gateway IP address: Enter default gateway

Set default DNS manually:  Enabled

Nameserver IP master: 8.8.8.8

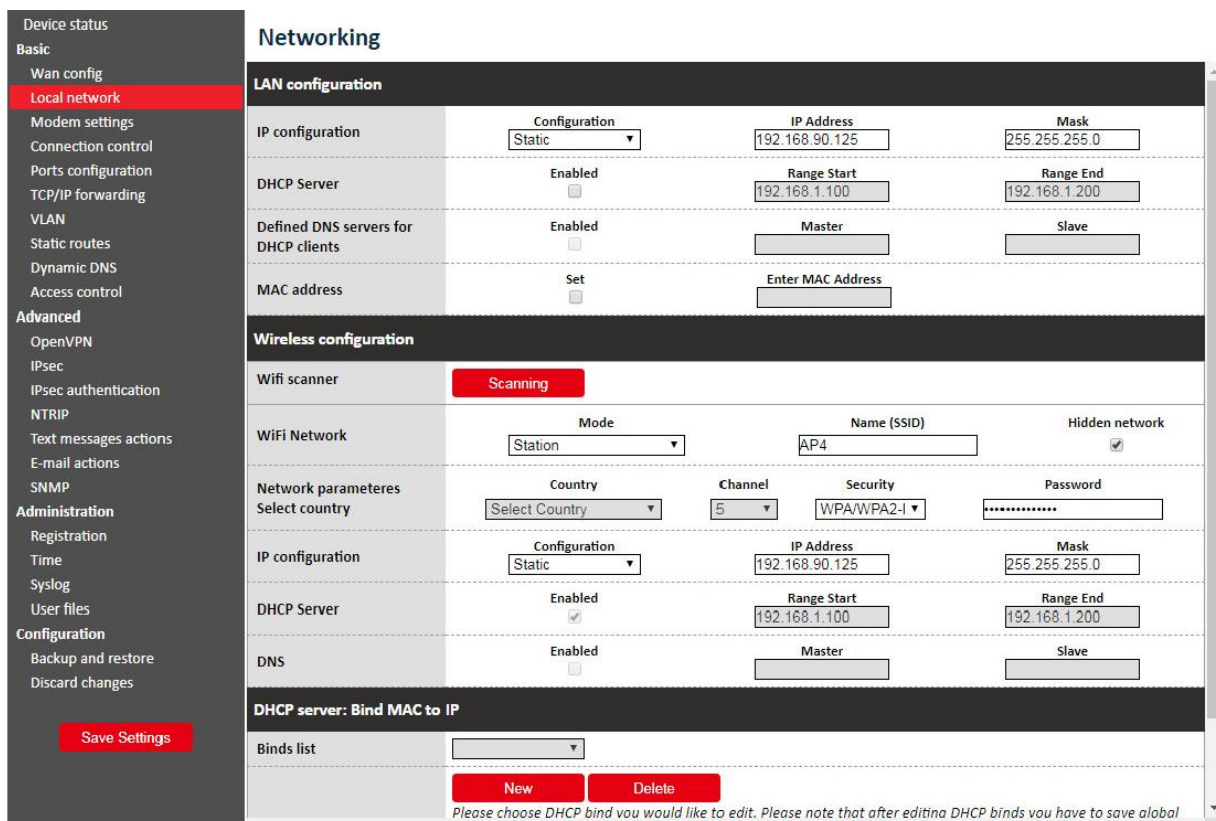
Nameserver IP slave: 8.8.4.4

Save Settings

## 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 AS30GSM420P-IO 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.



The screenshot displays the 'Networking' configuration page. On the left is a sidebar menu with categories: Device status, Basic, Advanced, Administration, and Configuration. The 'Local network' option is highlighted in red. The main content area is divided into two sections: 'LAN configuration' and 'Wireless configuration'.

**LAN configuration:**

- IP configuration:** Configuration: Static, IP Address: 192.168.90.125, Mask: 255.255.255.0
- DHCP Server:** Enabled (checkbox), Range Start: 192.168.1.100, Range End: 192.168.1.200
- Defined DNS servers for DHCP clients:** Enabled (checkbox), Master: [input], Slave: [input]
- MAC address:** Set (checkbox), Enter MAC Address: [input]

**Wireless configuration:**

- Wifi scanner:** Scanning (button)
- WiFi Network:** Mode: Station, Name (SSID): AP4, Hidden network: [checked]
- Network parameters:** Country: Select Country, Channel: 5, Security: WPA/WPA2-I, Password: [input]
- IP configuration:** Configuration: Static, IP Address: 192.168.90.125, Mask: 255.255.255.0
- DHCP Server:** Enabled (checkbox checked), Range Start: 192.168.1.100, Range End: 192.168.1.200
- DNS:** Enabled (checkbox), Master: [input], Slave: [input]

**DHCP server: Bind MAC to IP**

- Binds list:** [dropdown menu]
- New** (button) **Delete** (button)

At the bottom, a note reads: "Please choose DHCP bind you would like to edit. Please note that after editina DHCP binds you have to save alabal". A red 'Save Settings' button is located at the bottom left of the configuration area.

## 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.

| GSM connection settings |  |
|-------------------------|--|
| SIM slot                | Master   |
| PIN                     | <input checked="" type="checkbox"/> Enabled<br><input type="text" value="1234"/><br>Enter PIN here |
| Predefined APN          | <input type="text" value="enter manually"/>  |
| APN                     | <input type="text" value="internet"/><br>Enter APN here or select it from above list               |
| Username                | <input type="text"/><br>Enter username here  |
| Password                | <input type="text"/><br>Enter password here  |
| Modem band              | <input type="text" value="2G, 3G and 4G"/><br>Select modem band                                    |
| Connection              | <input type="text" value="Always on"/><br>Modem connect  |

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.

| GSM switching                 |  |
|-------------------------------|--|
| <b>GSM connection control</b> |  |
| Limits                        | <input type="text" value="10"/><br>Enter ping timeout in seconds (1-1000)  |
|                               | <input type="text" value="3"/><br>Enter ping count (1-3600)  |
|                               | <input type="text" value="600"/><br>Enter ping interval in seconds (0-86400, 0 - disable)  |
|                               | <input type="text" value="50"/><br>Enter ping threshold in percent (1-100)   |
| IP 1                          | <input checked="" type="checkbox"/> Enabled<br>Set this option to enable ping testing IP 1<br><input type="text"/><br>Enter IP address |
| IP 2                          | <input checked="" type="checkbox"/> Enabled<br>Set this option to enable ping testing IP 2<br><input type="text"/><br>Enter IP address |
| IP 3                          | <input checked="" type="checkbox"/> Enabled<br>Set this option to enable ping testing IP 3<br><input type="text"/><br>Enter IP address |
| IP 4                          | <input checked="" type="checkbox"/> Enabled<br>Set this option to enable ping testing IP 4<br><input type="text"/><br>Enter IP address |

## 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 wiadomości 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.

Device status

Basic

- Wan config
- Local network
- Modem settings
- Connection control
- Ports configuration
- TCP/IP forwarding
- VLAN
- Static routes
- Dynamic DNS
- Access control

Advanced

- OpenVPN
- IPsec
- IPsec authentication
- NTRIP
- Text messages actions
- E-mail actions
- SNMP

Administration

- Registration
- Time
- Syslog
- User files

Configuration

- Backup and restore
- Discard changes

Save Settings

### Ports

Port settings

| Port type    | Serial RS-232<br><small>External<br/>/dev/rs232</small> | Serial RS-485<br><small>External<br/>/dev/rs485</small> | Modem control<br><small>Internal<br/>Port-A</small> |
|--------------|---|---|---|
| Mode         | None  | None  | None  |
| Baud rate    | 115 200   | 115 200   |   |
| Data bits    | 8   | 8   |   |
| Parity       | None  | None  |   |
| Stop bits    | 1   | 1   |   |
| Flow control | None  | None  |   |

Forwarding configuration

|                       |  |         |        |
|-----------------------|--|---------|--------|
| To                    | Network  | Network |        |
| Mode                  | Server   | Server  | Server |
| Interface             | LAN  | WAN     | LAN    |
| Protocol              | TCP  | TCP     | TCP    |
| Server IP or domain   |  |         |        |
| Server as domain name | <input type="checkbox"/> Enter Server as domain name |         |        |
| Port                  |  |         |        |

## 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.

Device status

**Basic**

Wan config

Local network

Modem settings

Connection control

Ports configuration

TCP/IP forwarding

VLAN

Static routes

Dynamic DNS

Access control

**Advanced**

OpenVPN

IPsec

IPsec authentication

NTRIP

Text messages actions

E-mail actions

SNMP

**Administration**

Registration

Time

Syslog

User files

**Configuration**

Backup and restore

Discard changes

Save Settings

## TCP/IP forwarding

**Single port rules**

|               |   |
|---------------|---|
| Rules list    | <input style="width: 90%;" type="text"/>  |
|               | <input type="button" value="New"/> <input type="button" value="Delete"/>  |
|               | Please choose a rule you would like to edit. Please note that after editing rules you have to save global settings. |
| Identifier    | <input style="width: 90%;" type="text"/>  |
|               | Please enter any name/identifier  |
| Enable rule   | <input type="checkbox"/> <b>Enabled</b><br>Set this option to enable this rule                                      |
| External port | <input style="width: 90%;" type="text"/>  |
| Internal port | <input style="width: 90%;" type="text"/>  |
| Protocol      | <input style="width: 90%;" type="text"/>  |
| IP address    | <input style="width: 90%;" type="text"/>  |

**Port range rules**

|             |   |
|-------------|---|
| Rules list  | <input style="width: 90%;" type="text"/>  |
|             | <input type="button" value="New"/> <input type="button" value="Delete"/>  |
|             | Please choose a rule you would like to edit. Please note that after editing rules you have to save global settings. |
| Identifier  | <input style="width: 90%;" type="text"/>  |
|             | Please enter any name/identifier  |
| Enable rule | <input type="checkbox"/> <b>Enabled</b><br>Set this option to enable this rule                                      |
| First port  | <input style="width: 90%;" type="text"/>  |
| Last port   | <input style="width: 90%;" type="text"/>  |
| Protocol    | <input style="width: 90%;" type="text"/>  |

## 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.



Device status

**Basic**

Wan config

Local network

Modem settings

Connection control

Ports configuration

TCP/IP forwarding

**VLAN**

Static routes

Dynamic DNS

Access control

**Advanced**

OpenVPN

IPsec

IPsec authentication

NTRIP

Text messages actions

E-mail actions

SNMP

**Administration**

Registration

Time

Syslog

User files

**Configuration**

Backup and restore

Discard changes

Save Settings

### VLAN/Virtual IP configuration

|                      |   |
|----------------------|---|
| VLAN Virtual IP list | <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <span style="border: 1px solid #ccc; padding: 2px 10px;">▼</span> </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span style="background-color: red; color: white; padding: 2px 5px; border-radius: 3px;">New</span> <span style="background-color: red; color: white; padding: 2px 5px; border-radius: 3px;">Delete</span> </div> <p style="font-size: 0.8em; margin-top: 5px;"><i>Please choose VLAN you would like to edit. Please note that after editing those things you have to save global settings.</i></p> |
| Enable VLAN          | <input type="checkbox"/> <b>Enabled</b><br><i>Set this option to enable this VLAN</i>   |
| Description          | <input style="width: 100%;" type="text"/><br><i>Please enter VLAN description.</i>  |
| Interface            | <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <span style="border: 1px solid #ccc; padding: 2px 10px;">▼</span> </div>  |
| IEEE 802.1Q tagging  | <input type="checkbox"/> <b>Enabled</b><br><i>Set this option to enable IEEE 802.1Q tagging</i>   |
| Identifier           | <input style="width: 100%;" type="text"/><br><i>Please enter number from range 0-4095.</i>  |
| IP                   | <input style="width: 100%;" type="text"/>   |
| Netmask              | <input style="width: 100%;" type="text"/>   |

## 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 (Destination netmask) i bramkę (Gateway).

Device status

**Basic**

Wan config

Local network

Modem settings

Connection control

Ports configuration

TCP/IP forwarding

VLAN

**Static routes**

Dynamic DNS

Access control

**Advanced**

OpenVPN

IPsec

IPsec authentication

NTRIP

Text messages actions

E-mail actions

SNMP

**Administration**

Registration

Time

Syslog

User files

**Configuration**

Backup and restore

Discard changes

Save Settings

### Static routes

|                     |   |
|---------------------|---|
| Static routes list  | <input type="text"/>  |
|                     | <span style="background-color: red; color: white; padding: 2px 10px; border-radius: 3px;">New</span> <span style="background-color: red; color: white; padding: 2px 10px; border-radius: 3px; margin-left: 10px;">Delete</span> |
|                     | Please choose a route you would like to edit. Please note that after editing routes you have to save global settings.   |
| Identifier          | <input type="text"/><br><small>Please enter any name/identifier/IP</small>  |
| Destination network | <input type="text"/>  |
| Destination netmask | <input type="text"/>  |
| Interface           | <input type="text" value="None"/>   |
| Gateway             | <input type="text"/>  |

## 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 AS30GSM420P-IO (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.

| Dynamic DNS                 |   |
|-----------------------------|---|
| DDNS service                | <input type="text" value="Disabled"/><br><small>Note that DDNS can only work on devices with public IP.</small>                           |
| DynDNS type                 | <input type="text" value="Custom"/>   |
| Username                    | <input type="text"/><br><small>Enter username</small>   |
| Password                    | <input type="text"/><br><small>Enter password</small>   |
| Hostname                    | <input type="text"/><br><small>Enter hostname</small>   |
| Update interval (sec)       | <input type="text"/><br><small>IP change check interval. Default: 1 min. Max: 10 days Leave this field empty to use default value</small> |
| Force update interval (sec) | <input type="text"/><br><small>Forced DDNS server update interval. Default: 1 week Leave this field empty to use default value</small>    |

## 5.2.12 Ustawienia podstawowe: Access control

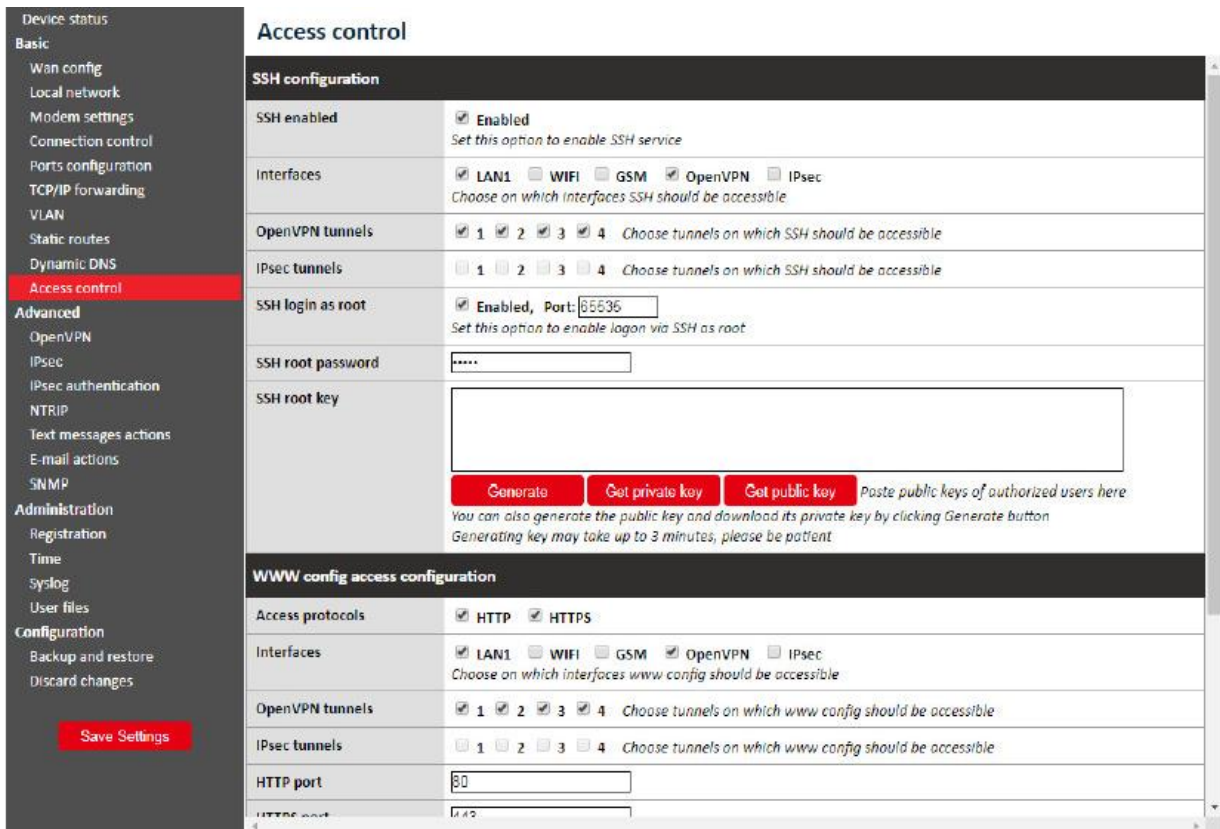
Pierwsza sekcja strony "Access control" pozwala użytkownikowi na konfigurację protokołu SSH, tj. jego włączenie/wyłączenie, wybranie portów i interfejsów, w których będzie on dostępny (dotyczy to także tuneli OpenVPN i IPsec). Możliwe jest również zablokowanie funkcji logowania przez SSH jako root oraz 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.



The screenshot shows the 'Access control' configuration page. On the left is a navigation menu with categories: Device status, Basic, Advanced, Administration, and Configuration. The 'Access control' section is highlighted in red. The main content area is titled 'Access control' and contains two main sections: 'SSH configuration' and 'WWW config access configuration'.

**SSH configuration**

- SSH enabled:**  Enabled. Set this option to enable SSH service.
- Interfaces:**  LAN1  WIFI  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.
- SSH login as root:**  Enabled, Port: . Set this option to enable login via SSH as root.
- SSH root password:**
- SSH root key:** . Below the input are three buttons: 'Generate', 'Get private key', and 'Get public key'. A note says: '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:**  LAN1  WIFI  GSM  OpenVPN  IPsec. Choose on which interfaces www config should be accessible.
- OpenVPN tunnels:**  1  2  3  4. Choose tunnels on which www config should be accessible.
- IPsec tunnels:**  1  2  3  4. Choose tunnels on which www config should be accessible.
- HTTP port:**
- HTTPS port:**

At the bottom left of the configuration area is a red 'Save Settings' button.

### 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.

Device status

**Basic**

Wan config

Local network

Modem settings

Connection control

Ports configuration

TCP/IP forwarding

VLAN

Static routes

Dynamic DNS

Access control

**Advanced**

OpenVPN

IPsec

IPsec authentication

NTRIP

Text messages actions

E-mail actions

SNMP

**Administration**

Registration

Time

Syslog

User files

**Configuration**

Backup and restore

Discard changes

Save Settings

### OpenVPN tunnels

|                              |  |
|------------------------------|--|
| Tunnel configuration         | openVPN tunnel 1 <span style="float: right;">▼</span><br><small>Please select VPN tunnel you would like to configure</small>   |
| OpenVPN mode                 | Disabled <span style="float: right;">▼</span>  |
| Connection mode              | Router (TUN) single-cli <span style="float: right;">▼</span>   |
| Remote Server IP or domain   | <input style="width: 100%;" type="text"/>  |
| Remote Server as domain name | <input type="checkbox"/> Enter Remote Server as domain name  |
| VPN device                   | <input style="width: 100%;" type="text"/>  |
| NAT-T                        | <input type="checkbox"/> <b>Enable NAT Traversal (NAT-T)</b><br><small>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.</small> |
| Port                         | <input style="width: 100%;" type="text"/>  |
| Protocol                     | TCP <span style="float: right;">▼</span>   |
| Network                      | <input style="width: 100%;" type="text"/>  |
| Netmask                      | <input style="width: 100%;" type="text"/>  |
| Server IP                    | <input style="width: 100%;" type="text"/>  |
| Client IP                    | <input style="width: 100%;" type="text"/>  |
| CA cert                      | <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: right; margin-top: 5px;"> <input style="background-color: red; color: white; padding: 2px 10px;" type="button" value="Generate"/> </div>                |
| CA key                       | <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>   |



## 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 AS30GSM420P-IO, należy skorzystać z trzech zakładki 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.

Założmy, że chcemy połączyć ze sobą dwa routery AS30GSM420P-IO 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). Założmy, 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 algorithm), 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.

|  |  |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
|--|--|---|---|--|--|----------------------|---|--|--|---------------|----------------------------------|--|--|-----------------|--------------------|---|--|--------------|---------------------|---------------------------------|---------------------------------|----------------|--|--|--|---------------|---------------------|---------------------------------|---------------------------------|------------|-------------|--|--|-------|---|--|--|--|--|--|--|----------|----------|--|--|------------------------------------|----------------------------------|--|--|------------|--|---|---|-----------|---|--|-----------------------------------|
| Device status<br>Basic<br>Wan config<br>Local network<br>Modem settings<br>Connection control<br>Ports configuration<br>TCP/IP forwarding<br>VLAN<br>Static routes<br>Dynamic DNS<br>Access control<br>Advanced<br>OpenVPN<br><b>IPsec</b><br>IPsec authentication<br>NTRIP<br>Text messages actions<br>E-mail actions<br>SNMP<br>Administration<br>Registration<br>Time<br>Syslog<br>User files<br>Configuration<br>Backup and restore<br>Discard changes<br><br><div style="text-align: center; background-color: #f00; color: white; padding: 2px; width: fit-content; margin: 0 auto;">Save Settings</div> | <h3 style="margin: 0;">IPsec tunnels</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #eee;">Enable IPsec</td> <td colspan="3"><input type="checkbox"/> Enabled</td> </tr> <tr> <td style="background-color: #eee;">Tunnel configuration</td> <td colspan="3">                 [IPsec tunnel 1] <br/> <small>Please select IPsec tunnel you would like to configure</small> </td> </tr> <tr> <td style="background-color: #eee;">Enable tunnel</td> <td colspan="3"><input type="checkbox"/> Enabled</td> </tr> <tr> <td style="background-color: #eee;">Local Interface</td> <td>                 Interface<br/>                 [GSM]             </td> <td colspan="2">                 Default route<br/> <input type="checkbox"/> </td> </tr> <tr> <td style="background-color: #eee;">Local subnet</td> <td>                 Type<br/>                 [Host only]             </td> <td>                 Network<br/> <input type="text"/> </td> <td>                 Netmask<br/> <input type="text"/> </td> </tr> <tr> <td style="background-color: #eee;">Remote host(s)</td> <td colspan="3">                 IP Address<br/> <input type="text"/>                 Any host<br/> <input checked="" type="checkbox"/> <br/> <small>Enter the public IP address of the remote host or check Any host for server role.</small> </td> </tr> <tr> <td style="background-color: #eee;">Remote subnet</td> <td>                 Type<br/>                 [Host only]             </td> <td>                 Network<br/> <input type="text"/> </td> <td>                 Netmask<br/> <input type="text"/> </td> </tr> <tr> <td style="background-color: #eee;">Connection</td> <td colspan="3">[Always on]</td> </tr> <tr> <td style="background-color: #eee;">NAT-T</td> <td colspan="3"> <input type="checkbox"/> <b>Enable NAT Traversal (NAT-T)</b><br/> <small>Set this option to force use of NAT-T (i.e. the encapsulation of ESP in UDP packets), which can help with clients that are behind restrictive firewalls.</small> </td> </tr> <tr style="background-color: #333; color: white;"> <td colspan="4" style="text-align: center;"><b>Phase 1 proposal (Authentication)</b></td> </tr> <tr> <td style="background-color: #eee;">Protocol</td> <td colspan="3">[IKE v2]</td> </tr> <tr> <td style="background-color: #eee;">Change default algorithms proposal</td> <td colspan="3"><input type="checkbox"/> Enabled</td> </tr> <tr> <td style="background-color: #eee;">Encryption</td> <td> <input type="checkbox"/> AES 256<br/> <input type="checkbox"/> AES 192<br/> <input type="checkbox"/> AES 128<br/> <input type="checkbox"/> 3 DES             </td> <td> <input type="checkbox"/> Blowfish 256<br/> <input type="checkbox"/> Blowfish 192<br/> <input type="checkbox"/> Blowfish 128             </td> <td> <input type="checkbox"/> Camellia 256<br/> <input type="checkbox"/> Camellia 192<br/> <input type="checkbox"/> Camellia 128             </td> </tr> <tr> <td style="background-color: #eee;">Integrity</td> <td> <input type="checkbox"/> SHA2 512<br/> <input type="checkbox"/> SHA1 96             </td> <td> <input type="checkbox"/> SHA2 384<br/> <input type="checkbox"/> MD5 96             </td> <td> <input type="checkbox"/> SHA2 256             </td> </tr> </table> | Enable IPsec  | <input type="checkbox"/> Enabled  |  |  | Tunnel configuration | [IPsec tunnel 1]<br><small>Please select IPsec tunnel you would like to configure</small> |  |  | Enable tunnel | <input type="checkbox"/> Enabled |  |  | Local Interface | Interface<br>[GSM] | Default route<br><input type="checkbox"/> |  | Local subnet | Type<br>[Host only] | Network<br><input type="text"/> | Netmask<br><input type="text"/> | Remote host(s) | IP Address<br><input type="text"/> Any host<br><input checked="" type="checkbox"/><br><small>Enter the public IP address of the remote host or check Any host for server role.</small> |  |  | Remote subnet | Type<br>[Host only] | Network<br><input type="text"/> | Netmask<br><input type="text"/> | Connection | [Always on] |  |  | NAT-T | <input type="checkbox"/> <b>Enable NAT Traversal (NAT-T)</b><br><small>Set this option to force use of NAT-T (i.e. the encapsulation of ESP in UDP packets), which can help with clients that are behind restrictive firewalls.</small> |  |  | <b>Phase 1 proposal (Authentication)</b> |  |  |  | Protocol | [IKE v2] |  |  | Change default algorithms proposal | <input type="checkbox"/> Enabled |  |  | Encryption | <input type="checkbox"/> AES 256<br><input type="checkbox"/> AES 192<br><input type="checkbox"/> AES 128<br><input type="checkbox"/> 3 DES | <input type="checkbox"/> Blowfish 256<br><input type="checkbox"/> Blowfish 192<br><input type="checkbox"/> Blowfish 128 | <input type="checkbox"/> Camellia 256<br><input type="checkbox"/> Camellia 192<br><input type="checkbox"/> Camellia 128 | Integrity | <input type="checkbox"/> SHA2 512<br><input type="checkbox"/> SHA1 96 | <input type="checkbox"/> SHA2 384<br><input type="checkbox"/> MD5 96 | <input type="checkbox"/> SHA2 256 |
| Enable IPsec   | <input type="checkbox"/> Enabled   |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Tunnel configuration   | [IPsec tunnel 1]<br><small>Please select IPsec tunnel you would like to configure</small>  |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Enable tunnel  | <input type="checkbox"/> Enabled   |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Local Interface  | Interface<br>[GSM]   | Default route<br><input type="checkbox"/>   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Local subnet   | Type<br>[Host only]  | Network<br><input type="text"/>   | Netmask<br><input type="text"/>   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Remote host(s)   | IP Address<br><input type="text"/> Any host<br><input checked="" type="checkbox"/><br><small>Enter the public IP address of the remote host or check Any host for server role.</small>   |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Remote subnet  | Type<br>[Host only]  | Network<br><input type="text"/>   | Netmask<br><input type="text"/>   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Connection   | [Always on]  |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| NAT-T  | <input type="checkbox"/> <b>Enable NAT Traversal (NAT-T)</b><br><small>Set this option to force use of NAT-T (i.e. the encapsulation of ESP in UDP packets), which can help with clients that are behind restrictive firewalls.</small>  |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| <b>Phase 1 proposal (Authentication)</b>   |  |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Protocol   | [IKE v2]   |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Change default algorithms proposal   | <input type="checkbox"/> Enabled   |   |   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Encryption   | <input type="checkbox"/> AES 256<br><input type="checkbox"/> AES 192<br><input type="checkbox"/> AES 128<br><input type="checkbox"/> 3 DES   | <input type="checkbox"/> Blowfish 256<br><input type="checkbox"/> Blowfish 192<br><input type="checkbox"/> Blowfish 128 | <input type="checkbox"/> Camellia 256<br><input type="checkbox"/> Camellia 192<br><input type="checkbox"/> Camellia 128 |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |
| Integrity  | <input type="checkbox"/> SHA2 512<br><input type="checkbox"/> SHA1 96  | <input type="checkbox"/> SHA2 384<br><input type="checkbox"/> MD5 96  | <input type="checkbox"/> SHA2 256   |  |  |                      |   |  |  |               |                                  |  |  |                 |                    |   |  |              |                     |                                 |                                 |                |  |  |  |               |                     |                                 |                                 |            |             |  |  |       |   |  |  |  |  |  |  |          |          |  |  |                                    |                                  |  |  |            |  |   |   |           |   |  |                                   |

## 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 crt.*

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 AS30GSM420P-IO, należy dezaktywować hasło do klucza prywatnego:

*openssl rsa -in private/device1key.pem -out private/device1key.pem\_nopass*

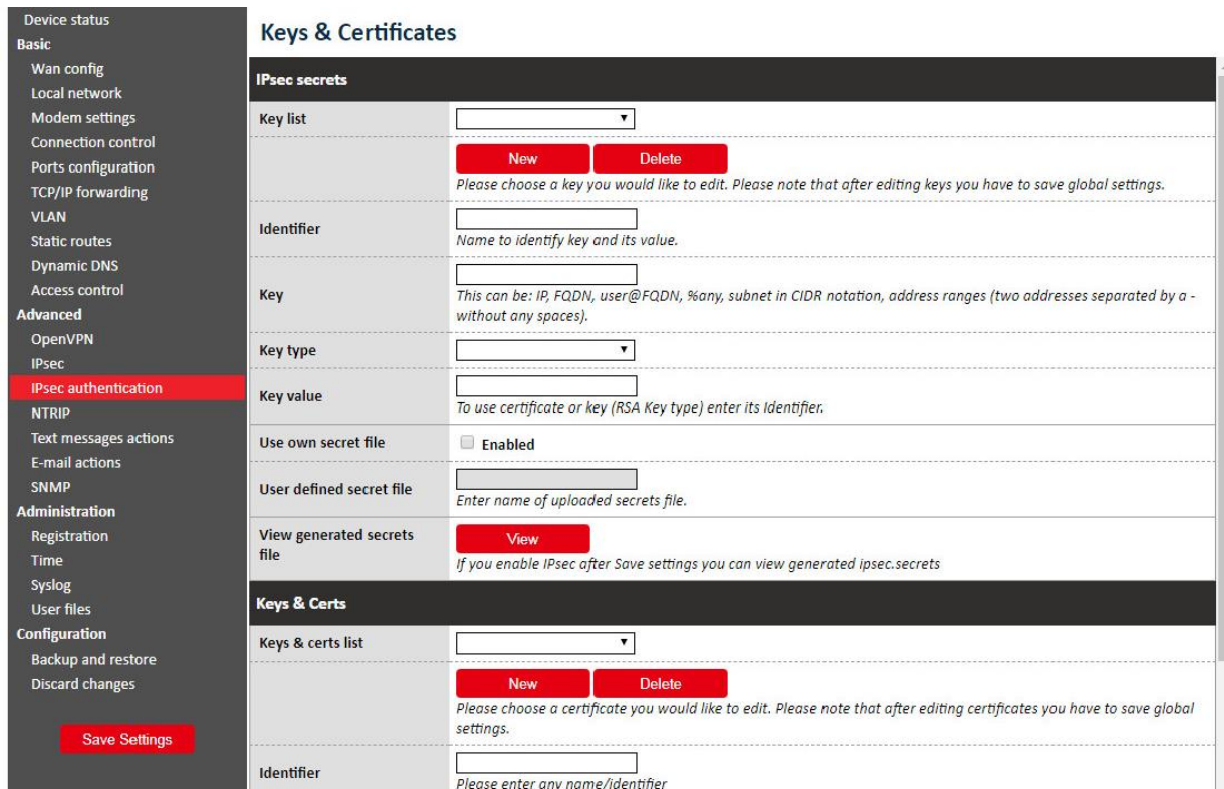
Całą procedurę należy powtórzyć dla każdego urządzenia (należy pamiętać o przedzieleniu różnych nazw wspólnych (Common Name) i nazw plików do poszczególnych urządzeń!).

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 *ca.cert.pem*, w pole "Server/Client cert" – zawartość pliku *device1.cert.pem*, w pole "Server/Client private key" zaś – zawartość pliku *device1.key.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.

|  |   |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
|--|---|--------------|---|-----------------------|----------------------|-------------|----------------------|-----------------|----------------------|-----------------|----------------------|-------------------------|---|-----------------|---|------------------|---|--------------------------|------------------------------------|-------------------|---|
| Device status<br>Basic<br>Wan config<br>Local network<br>Modem settings<br>Connection control<br>Ports configuration<br>TCP/IP forwarding<br>VLAN<br>Static routes<br>Dynamic DNS<br>Access control<br>Advanced<br>OpenVPN<br>IPsec<br>IPsec authentication<br><b style="background-color: red; color: white;">NTRIP</b><br>Text messages actions<br>E-mail actions<br>SNMP<br>Administration<br>Registration<br>Time<br>Syslog<br>User files<br>Configuration<br>Backup and restore<br>Discard changes<br><br><div style="text-align: center; background-color: red; color: white; padding: 2px; width: fit-content; margin: 0 auto;">Save Settings</div> | <h3 style="margin: 0;">NTRIP</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;"><b>NTRIP</b></td> <td><input type="checkbox"/> <b>Enabled</b><br/><small>Set this option to enable NTRIP service</small></td> </tr> <tr> <td><b>Server address</b></td> <td><input type="text"/></td> </tr> <tr> <td><b>Port</b></td> <td><input type="text"/></td> </tr> <tr> <td><b>Username</b></td> <td><input type="text"/></td> </tr> <tr> <td><b>Password</b></td> <td><input type="text"/></td> </tr> <tr> <td><b>Initial position</b></td> <td><input type="checkbox"/> <b>Enabled</b><br/><small>Set this option to enable login to NTRIP server with fixed position.<br/>Use this option when there is no external source of NMEA frames connected via RS232.</small></td> </tr> <tr> <td><b>Latitude</b></td> <td>N <input type="text" value="52"/> ° <input type="text" value="0"/> ' <input type="text" value="0"/></td> </tr> <tr> <td><b>Longitude</b></td> <td>W <input type="text" value="22"/> ° <input type="text" value="0"/> ' <input type="text" value="0"/></td> </tr> <tr> <td><b>Data request mode</b></td> <td>NTRIP Version 2.0 Caster in TCP/IP</td> </tr> <tr> <td><b>Mountpoint</b></td> <td><input type="text"/> <span style="background-color: red; color: white; padding: 2px 5px;">Get List</span></td> </tr> </table> | <b>NTRIP</b> | <input type="checkbox"/> <b>Enabled</b><br><small>Set this option to enable NTRIP service</small> | <b>Server address</b> | <input type="text"/> | <b>Port</b> | <input type="text"/> | <b>Username</b> | <input type="text"/> | <b>Password</b> | <input type="text"/> | <b>Initial position</b> | <input type="checkbox"/> <b>Enabled</b><br><small>Set this option to enable login to NTRIP server with fixed position.<br/>Use this option when there is no external source of NMEA frames connected via RS232.</small> | <b>Latitude</b> | N <input type="text" value="52"/> ° <input type="text" value="0"/> ' <input type="text" value="0"/> | <b>Longitude</b> | W <input type="text" value="22"/> ° <input type="text" value="0"/> ' <input type="text" value="0"/> | <b>Data request mode</b> | NTRIP Version 2.0 Caster in TCP/IP | <b>Mountpoint</b> | <input type="text"/> <span style="background-color: red; color: white; padding: 2px 5px;">Get List</span> |
| <b>NTRIP</b>   | <input type="checkbox"/> <b>Enabled</b><br><small>Set this option to enable NTRIP service</small>   |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
| <b>Server address</b>  | <input type="text"/>  |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
| <b>Port</b>  | <input type="text"/>  |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
| <b>Username</b>  | <input type="text"/>  |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
| <b>Password</b>  | <input type="text"/>  |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
| <b>Initial position</b>  | <input type="checkbox"/> <b>Enabled</b><br><small>Set this option to enable login to NTRIP server with fixed position.<br/>Use this option when there is no external source of NMEA frames connected via RS232.</small>   |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
| <b>Latitude</b>  | N <input type="text" value="52"/> ° <input type="text" value="0"/> ' <input type="text" value="0"/>   |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
| <b>Longitude</b>   | W <input type="text" value="22"/> ° <input type="text" value="0"/> ' <input type="text" value="0"/>   |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
| <b>Data request mode</b>   | NTRIP Version 2.0 Caster in TCP/IP  |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |
| <b>Mountpoint</b>  | <input type="text"/> <span style="background-color: red; color: white; padding: 2px 5px;">Get List</span>   |              |   |                       |                      |             |                      |                 |                      |                 |                      |                         |   |                 |   |                  |   |                          |                                    |                   |   |

## 5.2.17 Ustawienia zaawansowane: Text messages actions

Zakładka "Text Messages Actions" umożliwia użytkownikowi definiowanie skryptów, które będą wykonywane każdorazowo, gdy router odbierze wiadomość 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.

Device status

**Basic**

Wan config

Local network

Modem settings

Connection control

Ports configuration

TCP/IP forwarding

VLAN

Static routes

Dynamic DNS

Access control

**Advanced**

OpenVPN

IPsec

IPsec authentication

NTRIP

Text messages actions

E-mail actions

SNMP

**Administration**

Registration

Time

Syslog

User files

**Configuration**

Backup and restore

Discard changes

Save Settings

## Text messages actions

**Text messages (SMS) server**

|                   |  |
|-------------------|--|
| <b>Management</b> | <a href="#">Incoming text messages (SMS)</a><br><a href="#">Sent text messages (SMS)</a><br><a href="#">Report text messages (SMS)</a><br><a href="#">Help</a> |
|-------------------|--|

**Text messages (SMS) configuration**

|                |                                  |
|----------------|----------------------------------|
| <b>Enabled</b> | <input type="checkbox"/> Enabled |
|----------------|----------------------------------|

**Text messages (SMS) actions**

|   |  |
|---|--|
| <b>Text messages (SMS) actions list</b> | <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">SMSback my IP</div>  |
|   | <div style="display: flex; justify-content: center; gap: 10px;"> <div style="background-color: red; color: white; padding: 5px 10px; border-radius: 3px;">New</div> <div style="background-color: red; color: white; padding: 5px 10px; border-radius: 3px;">Delete</div> </div> <p style="font-size: small; color: #666;">Please choose action you would like to edit. Please note that after editing rules you have to save global settings.</p> |
| <b>Identifier</b>                       | <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">SMSback my IP</div><br><small>Please enter any identifier</small>  |
| <b>Command</b>                          | <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Myip</div><br><small>Please enter command (content of text message)</small>  |
| <b>Script</b>                           | <div style="border: 1px solid #ccc; padding: 5px; font-family: monospace; font-size: small;"> <pre>#!/bin/bash smssend.sh \$SMS_SENDER "GSM IP: \$(myip gsm); LAN IP: \$(myip lan)"</pre> </div> <small>This script will be executed after receiving text message (SMS) command</small>  |

## 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 umożliwi również konfigurację skryptu uruchamianego automatycznie (wiadomości mogą być wysyłane z załącznikami i dostępna jest opcja kompresji pliku przed wysyłką).



Device status

**Basic**

Wan config

Local network

Modem settings

Connection control

Ports configuration

TCP/IP forwarding

VLAN

Static routes

Dynamic DNS

Access control

**Advanced**

OpenVPN

IPsec

IPsec authentication

NTRIP

Text messages actions

E-mail actions

SNMP

**Administration**

Registration

Time

Syslog

User files

**Configuration**

Backup and restore

Discard changes

Save Settings

### E-mail Actions

**E-mail configuration**

|                       |   |
|-----------------------|---|
| <b>E-mail sending</b> | <input type="checkbox"/> <b>Enabled</b><br><i>Set this option if you want to allow router send e-mails.</i>                 |
| <b>Recipient</b>      | <input type="text"/><br><i>All messages will be delivered to this e-mail address</i>  |
| <b>From:</b>          | <input type="text"/><br><i>Enter "From:" field of e-mails here e.g. "me@example.com"</i>                                    |
| <b>Host name</b>      | <input type="text"/><br><i>Enter host name here e.g. "smtp.gmail.com"</i>   |
| <b>Port</b>           | <input type="text"/><br><i>Enter port number here e.g. "587"</i>  |
| <b>Username</b>       | <input type="text"/><br><i>Enter your username of e-mail service</i>  |
| <b>Password</b>       | <input type="password"/><br><input type="password"/> (confirmation)<br><i>Enter password from your e-mail service twice</i> |

**E-mail Actions**

|  |   |
|--|---|
| <b>E-mail actions list</b>                           | <input type="text"/>  |
|  | <input type="button" value="New"/> <input type="button" value="Delete"/>  |
|  | <i>Please choose action you would like to edit. Please note that after editing rules you have to save global settings.</i>  |
| <b>Identifier</b>                                    | <input type="text"/><br><i>Please enter any identifier</i>  |
| <b>Date (Month/Day of month) of script execution</b> | <input type="text"/> <input type="text"/><br><i>Please enter month(s) and day(s) of month(s) when script will be executed. Ranges can be defined with dashes e.g. "1-15", you can also use commas e.g. "1,6,7". Note, that using "*" replaces all months/days, and "1-12/2" means "every 2 months/days from range 1-12 (2,4,6,...)"</i> |

## 5.2.19 Ustawienia zaawansowane: SNMP

Device status

Basic

Wan config

Local network

Modem settings

Connection control

Ports configuration

TCP/IP forwarding

VLAN

Static routes

Dynamic DNS

Access control

Advanced

OpenVPN

IPsec

IPsec authentication

NTRIP

Text messages actions

E-mail actions

SNMP

Administration

Registration

Time

Syslog

User files

Configuration

Backup and restore

Discard changes

Save Settings

### SNMP

|                                   |   |   |
|-----------------------------------|---|---|
| <b>SNMP</b>                       | <input type="checkbox"/> <b>Enabled</b><br><small>Set this option to enable SNMP service.</small>   |   |
| <b>RBMTX MIB file</b>             | <a href="#" style="background-color: red; color: white; padding: 2px 10px;">Download</a>  |   |
| <b>SNMP networking</b>            |   |   |
| <b>Protocol &amp; Port</b>        | Protocol<br><input type="text" value="UDP"/>  | Port<br><input type="text" value="161"/>          |
| <b>Interfaces</b>                 | <input checked="" type="checkbox"/> LAN<br><input type="checkbox"/> WIFI<br><input type="checkbox"/> GSM<br><small>Choose on which interfaces SNMP should be accessible</small>   |   |
| <b>SNMP information</b>           |   |   |
| <b>System location</b>            | <input type="checkbox"/> <input type="text" value="Location info"/><br><small>Set description of system location</small>  |   |
| <b>Administrator contact</b>      | <input type="checkbox"/> <input type="text" value="Contact info"/><br><small>Set contact information to system administrator</small>  |   |
| <b>SNMP users</b>                 |   |   |
| <b>Username</b>                   | <input type="text" value=""/><br><a href="#" style="background-color: red; color: white; padding: 2px 5px;">New</a> <a href="#" style="background-color: red; color: white; padding: 2px 5px;">Delete</a><br><small>Please choose a username you would like to edit. Please note that after editing you have to save global settings.</small> |   |
| <b>Username &amp; access type</b> | Access type<br><input type="text" value=""/>  | Username<br><input type="text" value=""/>         |
| <b>Authentication</b>             | Protocol<br><input type="text" value=""/>   | Password<br><input type="text" value=""/>         |
|                                   |   | Confirm password<br><input type="text" value=""/> |
| <b>Encryption</b>                 | Protocol<br><input type="text" value=""/>   | Password<br><input type="text" value=""/>         |
|                                   |   | Confirm password<br><input type="text" value=""/> |

## 5.2.20 Ustawienia administracyjne: Time

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



Device status

Basic

Wan config

Local network

Modem settings

Connection control

Ports configuration

TCP/IP forwarding

VLAN

Static routes

Dynamic DNS

Access control

Advanced

OpenVPN

IPsec

IPsec authentication

NTRIP

Text messages actions

E-mail actions

SNMP

Administration

Registration

Time

Syslog

User files

Configuration

Backup and restore

Discard changes

Save Settings

### NTP

RTC time (UTC) 2019-01-16 15:01:48

---

**NTP Peer 1 preferred server**  Enabled   Enter NTP Server as domain name  
Enter IP address NTP server

---

**NTP Peer 2 server**  Enabled   Enter NTP Server as domain name  
Enter IP address NTP server

---

**NTP Peer 3 server**  Enabled   Enter NTP Server as domain name  
Enter IP address NTP server

---

Set Date(Y/M/D) and Time(h:m:s)       Set  
Please enter date/time below and press Set button

---

**NTP Status**

| s | remote          | refid         | st | t | when | pool | reach | delay   | offset | jitter |
|---|-----------------|---------------|----|---|------|------|-------|---------|--------|--------|
| * | 212.110.158.28  | 89.109.251.21 | 2  | u | 27   | 1024 | 377   | 100.079 | -0.936 | 1.806  |
| + | tkswf.friesenec | .GPS.         | 1  | u | 36   | 1024 | 377   | 85.498  | -4.783 | 1.421  |

## 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.

Device status

**Basic**

Wan config

Local network

Modem settings

Connection control

Ports configuration

TCP/IP forwarding

VLAN

Static routes

Dynamic DNS

Access control

**Advanced**

OpenVPN

IPsec

IPsec authentication

NTRIP

Text messages actions

E-mail actions

SNMP

**Administration**

Registration

Time

Syslog

User files

**Configuration**

Backup and restore

Discard changes

Save Settings

## SYSLOG

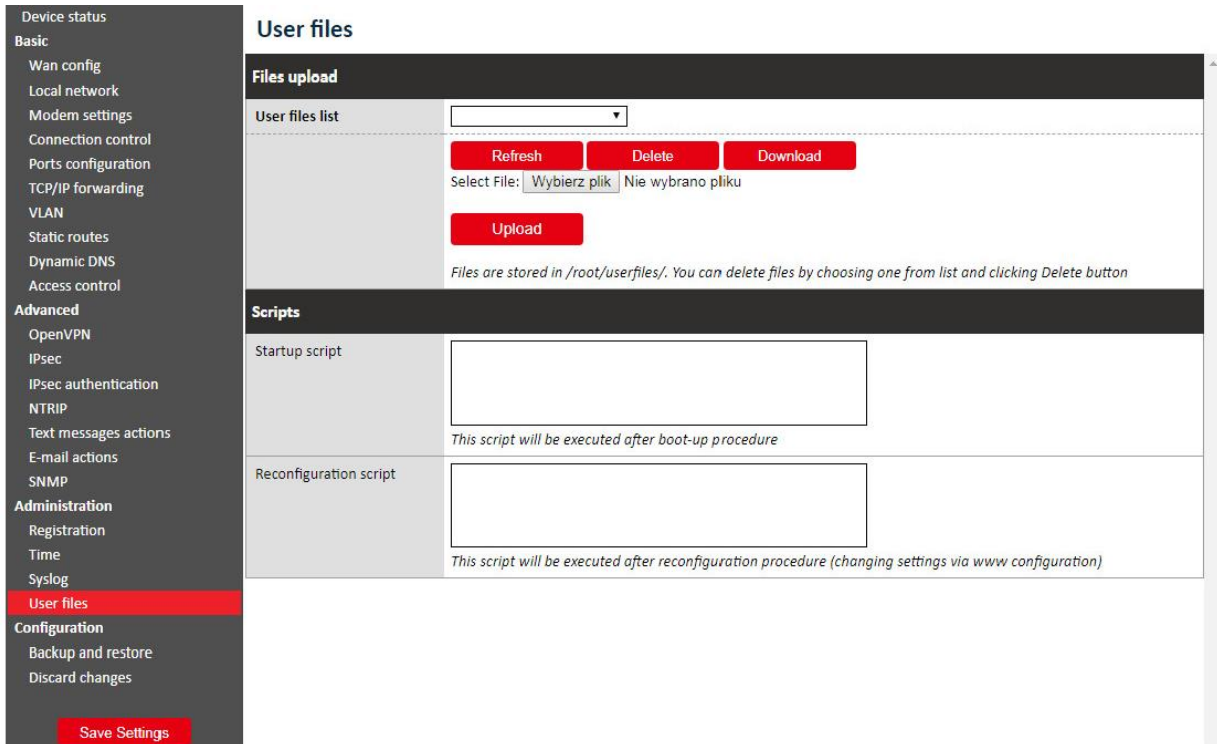
|                                   |  |
|-----------------------------------|--|
| <b>Local service log</b>          | <span style="background-color: red; color: white; padding: 2px 5px;">View</span> <span style="background-color: red; color: white; padding: 2px 5px; margin-left: 10px;">Download</span> |
| <b>Remote service</b>             | <input type="checkbox"/> <b>Enabled</b><br><i>If this option is set, device will store system logs on remote host</i>  |
| <b>SYSLOG host</b>                | <input style="width: 100px;" type="text"/><br><i>Enter SYSLOG host IP address here</i>   |
| <b>SYSLOG host as domain name</b> | <input type="checkbox"/> <b>Enter SYSLOG host as domain name</b>   |
| <b>Heartbeat</b>                  | <span style="background-color: red; color: white; padding: 5px 15px;">Send</span>  |

## 5.2.22 Ustawienia administracyjne: User files

Użytkownik może wgrzywać 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`.

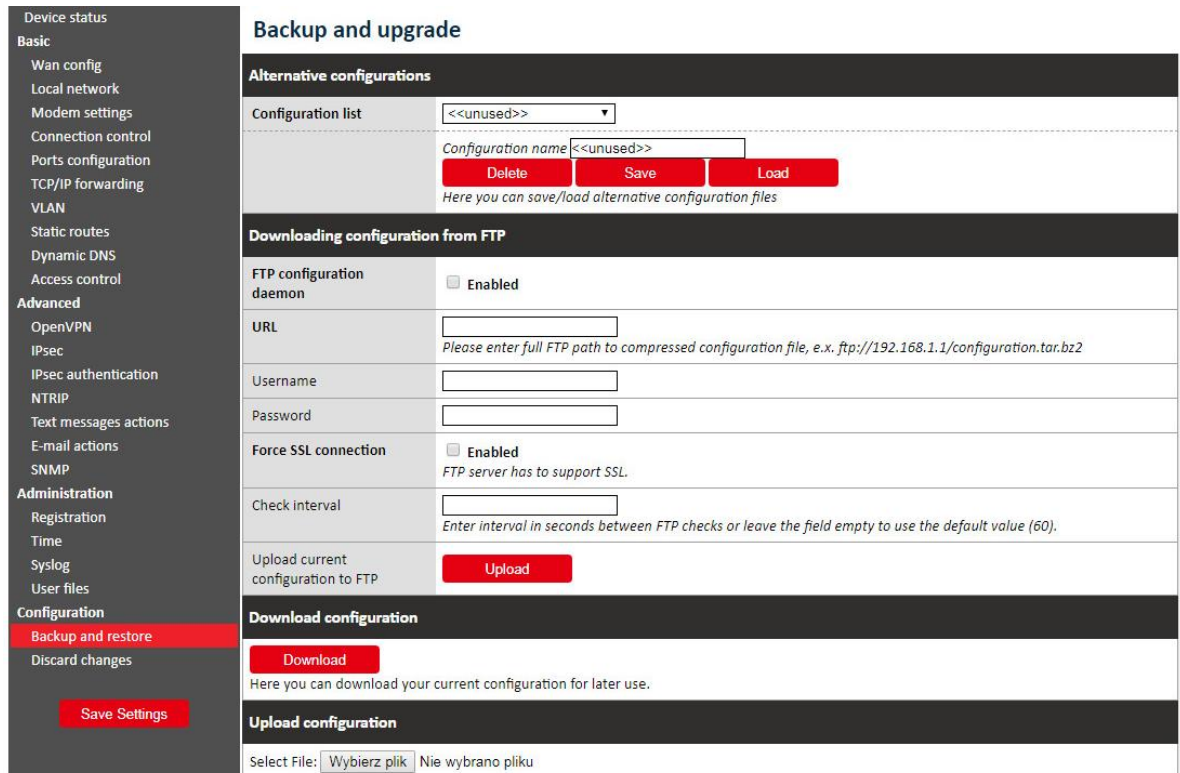
**OSTRZEŻENIE:** Pliki binarne wgrzywane do routera powinny być skompilowane dla procesora użytego w routerze (patrz tabela w pkt 2.3)!



## 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: AS30GSM420P-IO - 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"
  
```

## 5.4 Astraada Device Manager

Astraada Device Manager jest aplikacją umożliwiającą użytkownikowi wyszukiwanie routerów AS30GSM420P-IO 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.

| IP address    | HW Address        | Device type | Firmware version | Uptime   | Reset |
|---------------|-------------------|-------------|------------------|----------|-------|
| 192.168.1.234 | 36:07:26:BE:2A:4C | RBMTX - H24 | 120515           | 00:02:06 |       |

| IP address    | HW Address        | Device type | Firmware version | Uptime   | Reset |
|---------------|-------------------|-------------|------------------|----------|-------|
| 192.168.1.223 | 36:07:26:BE:2A:4C | RBMTX - H24 | 120515           | 00:04:56 |       |



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).

| IP address    | HW Address        | Device type | Firmware version | Uptime   | Reset   |  |
|---------------|-------------------|-------------|------------------|----------|---------|--|
| 192.168.1.223 | 36:07:26:8E:2A:4C | RBMTX - H24 | 120515           | 00:04:56 | IMEI OK | <input type="button" value="Scan"/><br><input type="button" value="Clear list"/><br><input type="button" value="Reset"/> |

| IP address    | HW Address        | Device type | Firmware version | Uptime   | Reset |  |
|---------------|-------------------|-------------|------------------|----------|-------|--|
| 192.168.1.234 | 36:07:26:8E:2A:4C | RBMTX - H24 | 120515           | 00:03:41 | done  | <input type="button" value="Scan"/><br><input type="button" value="Clear list"/><br><input type="button" value="Reset"/> |

## 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.



## 7. Charakterystyka techniczna

### 7.1 Charakterystyka mechaniczna

|                    |   |
|--------------------|---|
| Wymiary maksymalne | 116 x 100 x 23 mm (bez złączy)                    |
| Masa               | ≈ 150 g (dotyczy routera bez złączy zewnętrznych) |
| Objętość           | ≈ 260 cm <sup>3</sup> (bez złączy)                |

### 7.2 Charakterystyka elektryczna

#### 7.2.1 Zasilanie

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

#### 7.2.2 Charakterystyka RF

##### 7.2.2.1 Zakresy częstotliwości – wersja UMTS/HSPA

| Pasma    | 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       |

### 7.3.2.2 Zakresy częstotliwości – wersja LTE

| Pasma        | 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       |

### 7.3.2.3 Charakterystyka Wi-Fi

|                  |  |
|------------------|--|
| Standard:        | 802.11b/g/n  |
| Częstotliwość:   | 2.4 Ghz  |
| Moc wyjściowa:   | 13 dBm@11n<br>17 dBm@11b<br>15 dBm@11g<br>Tolerancja $\pm 2$ 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 $\Omega$   |
| Impedancja DC:                | 0 $\Omega$  |
| 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 wewnętrzną, aby zwiększyć moc odbieranego sygnału.

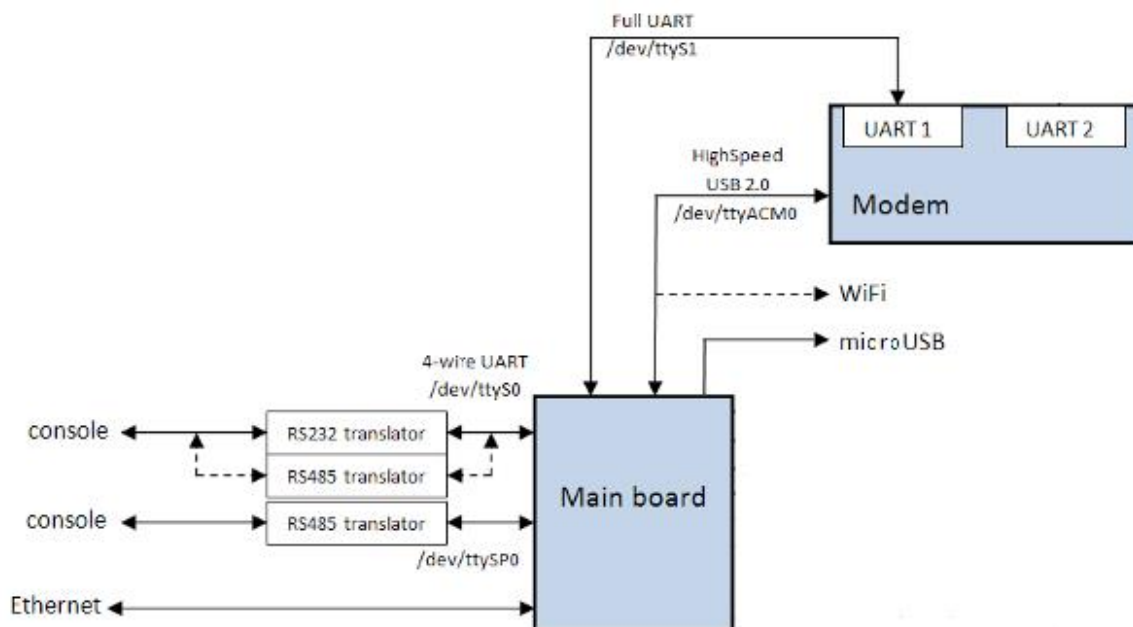
## 7.4 Charakterystyka środowiskowa

**Uwaga!** Przekroczenie poniższych wartości może spowodować trwałe uszkodzenie routera.

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

## 8. Architektura routera

Schemat poniżej przedstawia uproszczoną architekturę routera AS30GSM420P-IO. Funkcje oznaczone liniami kropkowanymi są funkcjami opcjonalnymi.



## 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 **wyłączyć**:

- 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 wzniesienie 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 AS30GSM420P-IO 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 zapyłonych.
- 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 Astraada 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.).

## 10. 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 zasilac z źródła stabilizowanego napięcia, okablowanie zaś musi spełniać wymagania przepisów przeciwpożarowych i bezpieczeństwa.

Z produktem należy obchodzić się z ostrożnością, unikać kontaktu ze stykami, gdyż wyładowania elektrostatyczne mogą uszkodzić produkt. Stosowanie analogicznych środków ostrożności dotyczy również postępowania 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](http://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en).

## 11. Certyfikaty

### 11.1 Zagadnienia dotyczące oceny zgodności

Produkt AS30GSM420P-IO 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.



### 11.2 Deklaracje zgodności

Produkt AS30GSM420P-IO jest zgodny z następującymi normami lub z pozostałymi dokumentami normatywnymi:

### 11.3 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. |
|----------|---|



## 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   | 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                                  |

|      |   |
|------|---|
| 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 Unlocking 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 |

## 13. Wsparcie online

Astraada zapewnia kompleksową obsługę klienta w trybie online, obejmującą:

- najnowszą wersję niniejszego dokumentu,
- najnowsze sterowniki do routera AS30GSM420P-IO,
- wsparcie techniczne.

Stosowne informacje są dostępne na stronie [www.astor.com.pl](http://www.astor.com.pl)