



Router Astraada AS30GSM200P Instrukcja użytkowania

Spis treści

| | |
|---|----|
| Opakowanie i zawartość | 4 |
| Opakowanie | 4 |
| Zawartość opakowania | 4 |
| Wersje modemu..... | 4 |
| Opis ogólny..... | 6 |
| Panel przedni..... | 6 |
| Panel tylni..... | 6 |
| Złącza zewnętrzne..... | 6 |
| Złącze SMA anteny GSM | 6 |
| Port szeregowy modemu (RS232/RS485) | 7 |
| Złącze RJ-45 | 7 |
| Złącze zasilania | 7 |
| Port audio..... | 7 |
| Złącze 20-pinowe (opcja) | 8 |
| Port karty SIM | 8 |
| Etykieta produktu..... | 9 |
| Podstawowe funkcje i usługi..... | 10 |
| Korzystanie z modemu | 11 |
| Rozpoczynanie pracy z modemem | 11 |
| Konfiguracja modemu..... | 11 |
| Ustanowienie połączenia | 11 |
| Status modemu (Device status) | 12 |
| Sieć lokalna LAN (Local network) | 13 |
| Sieć GSM (GSM network) | 14 |
| Ustawienia połączeń (Connection control)..... | 15 |
| Ustawienia portów (Ports configuration) | 16 |
| TCP/IP forwarding | 17 |
| VLAN | 18 |
| Static routes | 19 |
| Dynamic DNS..... | 20 |
| Access control | 21 |
| Open VPN | 23 |
| IPsec static/IPsec mobile..... | 25 |
| Generowanie certyfikatów SSL | 28 |
| N2N | 30 |
| CARP | 31 |
| NTRIP configuration page | 32 |
| SMS Actions..... | 33 |
| GPIO | 34 |

| | |
|--|----|
| CAN..... | 36 |
| Time..... | 37 |
| Syslog..... | 38 |
| Pliki użytkownika..... | 39 |
| Zapisywanie/przywracanie kopii zapasowej konfiguracji modemu | 40 |
| Discard changes | 40 |
| Save settings | 40 |
| Opis logów systemowych..... | 41 |
| Aktualizacja oprogramowania | 42 |
| Rozwiązywanie problemów | 43 |
| Brak połączenia/komunikacji z modemem | 43 |
| Modem połączony, brak połączenia z internetem | 43 |
| Charakterystyka techniczna | 44 |
| Charakterystyka mechaniczna | 44 |
| Obudowa..... | 44 |
| Charakterystyka elektroniczna..... | 45 |
| Zasilanie..... | 45 |
| Charakterystyki RF - Zakres częstotliwości | 45 |
| Charakterystyki RF - Wydajność RF..... | 45 |
| Charakterystyki RF - Zewnętrzna antena | 45 |
| Charakterystyka otoczenia..... | 46 |
| Architektura | 47 |
| Zalecenia dotyczące bezpieczeństwa..... | 48 |
| Ogólne bezpieczeństwo | 48 |
| Eksploatacja i konserwacja | 48 |
| Akcesoria | 49 |
| Akcesoria niezbędne | 49 |
| Akcesoria dodatkowe..... | 49 |
| Anteny kierunkowe | 49 |
| Anteny dookólne..... | 51 |
| Kabel zasilający..... | 51 |
| Kabel I/O..... | 51 |
| Kabel RS232/485 | 52 |
| Mocowanie DIN..... | 52 |
| Mocowanie Bur..... | 52 |
| Znak towarowy..... | 53 |
| Zalecenia dotyczące bezpieczeństwa..... | 54 |
| Lista skrótów | 55 |
| Wsparcie techniczne | 57 |

Opakowanie i zawartość

Opakowanie

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

Zawartość opakowania



W opakowaniu znajdują się:

- Modem Astraada o numerze katalogowym AS200GSM200P
- Antena GSM (złącze SMA)
- Zasilacz

Wersje modemu

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

| Opcja | Typowo | Opcje |
|-----------|----------------------|----------------------|
| Zasilanie | 6...30V | 5V |
| CPU | LPC3130, ARM9 180MHz | LPC3141, ARM9 270MHz |

| | | |
|--------------|---|--|
| Pamięć | 32MB RAM, 256MB MicroSD (część wykorzystana dla systemu Linux, pojemność karty może ulec zmianie) | NAND FLASH lub DATAFLASH |
| RS232 | Konsola systemowa (jeżeli CAN to RTS/CTS niedostępne) | RS485 |
| Złącza we/wy | - | 4 wejścia cyfrowe, 4 wyjścia cyfrowe, wejście AC, 2 wejścia analogowe, I2C, interfejs CAN, wyjście zasilające 3.3V, audio we/wy, miniUSB 2.0 (tylko bez modemu z WiFi) |
| Połączenie | GPRS lub EDGE | UMTS lub CDMA |
| SIM | Zewnętrzna | Wewnętrzna |
| Dual SIM | - | Niedostępny dla CDMA. |
| Audio | - | Mikrofon mono, wejście stereo LINE IN, wyjście stereo LINE OUT, lub wyjście do głośnika SPK OUT |
| LAN | Ethernet 10/100Mbps | Modem WiFi (tylko bez miniUSB) |

Konfiguracja portów zależy od modułu GSM zainstalowanego w urządzeniu. Dostępne moduły z opisami interfejsów są w tabeli poniżej.

| | G24 | H24 | CDMA | HE910 |
|-----------------|--------------------------------------|------------------------------|--------------|-----------------------------|
| USB | /dev/ttyACM0 | /dev/ttyACM0 & /dev/ttyUSB0 | /dev/ttyUSB0 | /dev/ttyACM0 & /dev/ttyACM3 |
| UART /dev/ttyS1 | Informacje o modemie lub Nie dotyczy | Informacje o modemie lub GPS | Nie dotyczy | Nie dotyczy |

Opis ogólny

Panel przedni



Panel tylni



Złącza zewnętrzne

Złącze SMA anteny GSM

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

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

Port szeregowy modemu (RS232/RS485)

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

| Wersja | | Router AS30GSM200P - PC | | | |
|-----------------|--------------|-------------------------|---------------|---|---|
| sygnał RS232 | sygnał RS485 | RB-MTX RJ45 | PC RS232 DB9F | | |
| nc | RT | 1 | nu | 1 | 1 |
| nc | nc | 2 | nu | 2 | 2 |
| (RXD) | RT(-) | 3 | nu | 3 | 3 |
| GND | GND | 4 | 5 | 4 | 4 |
| TXD | RX/TX+ | 5 | 2 | 5 | 5 |
| RXD | RX/TX- | 6 | 3 | 6 | 6 |
| RTS | nc | 7 | 8 | 7 | 7 |
| CTS | nc | 8 | 7 | 8 | 8 |
| RT – terminator | | | | 9 | 9 |

| | RB-MTX RJ45 | PC RS232 DB9F | |
|---|-------------|---------------|---|
| 1 | NC | NC | 1 |
| 2 | NC | | 2 |
| 3 | NC | | 3 |
| 4 | | NC | 4 |
| 5 | | | 5 |
| 6 | | NC | 6 |
| 7 | | | 7 |
| 8 | | | 8 |
| | | NC | 9 |

| | RB-MTX RJ45 | PC RS232 DB9F | |
|---|-------------|---------------|---|
| 1 | NC | NC | 1 |
| 2 | NC | | 2 |
| 3 | NC | +++++ | 3 |
| 4 | +++++ | NC | 4 |
| 5 | | +++++ | 5 |
| 6 | +++++ | NC | 6 |
| 7 | | +++++ | 7 |
| 8 | +++++ | | 8 |
| | | NC | 9 |

**L
U
B**

Rozłączenie komunikacji RS485.

W celu rozłączenia komunikacji RS485 należy zakończyć połączenie po obu stronach. Można zrealizować to przez użycie zewnętrznego rozłączania (terminator) lub z użyciem sygnałów RT (piny 1 oraz 3 złącza RS485). Wbudowany terminator dopasowany jest do impedancji 120Ω.

Złącze RJ-45

Złącze RJ-45 znajduje się na przednim panelu modemu AS30GSM200P i używane jest do komunikacji z komputerem PC w sieci Ethernet. W celu uruchomienia stron konfiguracyjnych modemu podłącz kabel typu UTP pomiędzy złączem RJ-45 komputera, a złączem RJ-45 terminala. Strona konfiguracyjna dostępna jest pod adresem IP określonym w konfiguracji modemu (ustawienie fabryczne to 192.168.1.234).

Złącze zasilania

Modem AS30GSM200P powinien być zasilany napięciem z zakresu 6-30 VDC, aby zapewnić optymalne zasilanie urządzenia, szczególnie w celu uniknięcia stanów nieustalonych pochodzących od zasilaczy indukcyjnych. W innym przypadku modem Astraada może ulec uszkodzeniu.

Port audio

Wejścia i wyjścia audio dostępne są jako opcja. Możliwe jest wyposażenie modemu w następujące wejścia/wyjścia:

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

Złącze 20-pinowe (opcja)

Modem AS30GSM200P dostępny jest w wersji ze złączem 20-pinowym również jako opcja. Szczegółowy opis złącza znajduje się w poniższej tabeli

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

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

NC – nie podłączono.

Port karty SIM



Złącze na kartę SIM znajdują się na przednim panelu AS30GSM200P. Aby umieścić kartę SIM należy:

1. Wyjąć szufladkę (kieszon) na kartę SIM przyciskając żółty przycisk.
2. Umieść kartę SIM w kieszeni.
3. Sprawdź czy karta SIM jest poprawnie umieszczona w szufladzie.
4. Umieść kieszeń w modemie.

Aby możliwe było korzystanie z usług sieci GSM należy umieścić w modemie aktywną kartę SIM.

Etykieta produktu

Na etykiecie produktu znajdują się następujące informacje:

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

Podstawowe funkcje i usługi

Podstawowe funkcje i usługi modemu zawarto w tabeli poniżej.

| Funkcja/usługa | Opis |
|---------------------------------------|--|
| Podstawowe właściwości modemu | Zakres pracy: Quad band 850/900/1800/1900/2100 MHz Zgodny z E-GSM Moc nadawana: 850/900 MHz Class 4 (2W) 1800/1900 MHz Class 1 (1W) UMTS 2100 MHz Class 3 (0.25W) EDGE 850/900 MHz Class E2 (0.5W) EDGE 1800/1900 MHz Class E2 (0.4W) Wymiary: 83 x 60 x 34 mm (ze złączami) Temperatura pracy: Min. 0°C Max. 60°C |
| Transfer danych | HSPA+ (downlink 21 Mbit/s, uplink 5,76 Mbit/s) UMTS (HSDPA 7,2 Mbit/s) EDGE (Multi-slot class 10, max BR downlink 236,8 Kb/s) GPRS (Multi-slot class 10, max BR downlink 85,6 Kb/s) CSD (Max BR 14,4 Kb/s) Wspiera protokoły: TCP/IP, UDP/IP, SSL, HTTP, HTTPS, FTP, SMTP, POP3, IBM MQTT Class B GSM 07.10 protokół multipleksujący |
| Interfejsy (wersja podstawowa modemu) | Złącze anteny GSM: SMA 2x SIM: 3V standard RS232 lub RS485 przez RJ-45 (DB9 do specjalnego użytku*) RJ-45 (x2) Złącze zasilania |
| Opcje* | Dual SIM (nie w CDMA) Interfejsy I/O (CAN, wyjście 3.3V, miniUSB) Audio I/O |

*opcja, w zależności od zamówienia

Korzystanie z modemu

Rozpoczęcie pracy z modemem

1. W celu uruchomienia modemu wykonaj następujące kroki:
2. Wciśnij żółty przycisk na przednim panelu i wyjmij „szufladkę” na kartę SIM
3. Umieść kartę SIM w szufladce (modemy dostępne są z jedną lub z dwoma złączami na kartę SIM)
4. Przykręć antenę GSM lub obie anteny: GSM i GPS/ZigBee (opcje dodatkowe) do złącza SMA
5. Podłącz kabel zasilacza do złącza PWR znajdującego się na tylnym panelu modemu.
6. Podłącz kabel UTP do gniazda RJ-45

Konfiguracja modemu

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

Uwaga: Pamięć cache resetowana jest przy restarcie lub rozłączeniu zasilania

Uwaga: Dostęp do niektórych zakładek uwarunkowany jest wersją modemu

Ustanowienie połączenia

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

Status modemu (Device status)

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

- Nazwa użytkownika: **admin**
- Hasło: **12345**

Jeżeli wszystko skonfigurowane jest poprawnie pojawi się następujące statusu modemu. Zawiera ona status połączenia do sieci oraz parametry PPP połączenia.

ASTRAADA AS30GSM200P GPRS/HSPA Router Configuration Panel
Modem HE910, 1 SIM, RS-232, firmware:140704

Device status


- Basic**
 - Local network
 - GSM network
 - Connection control
 - Ports configuration
 - TCP/IP forwarding
 - VLAN
 - Static routes
 - Dynamic DNS
 - Access control
- Advanced**
 - OpenVPN
 - IPsec static
 - IPsec mobile
 - IPsec authentication
 - N2N
 - CARP
 - NTRIP
 - SMS Actions
 - GPIO
 - CAN
- Administration**
 - Time
 - Syslog
 - User files
- Configuration**
 - Backup and restore
 - Discard changes
 - Save settings

Status

| | | | | | | | | | | | | | | | | | |
|-----------------------------|---|-------------------|--|------|--|-----|--|--------------------|----------------|-----------------------------|--|-----------------------|--|---------------------|--|---------------|--|
| Connection status | CONNECTED <input type="button" value="Disconnect"/> | | | | | | | | | | | | | | | | |
| Modem Information | <table border="1"> <tr><td>Model, firm. ver.</td><td></td></tr> <tr><td>IMEI</td><td></td></tr> <tr><td>PIN</td><td></td></tr> <tr><td>Operator Selection</td><td>Please wait...</td></tr> <tr><td>Network Registration Status</td><td></td></tr> <tr><td>Signal Strength (CSQ)</td><td></td></tr> <tr><td>Packet Data Service</td><td></td></tr> <tr><td>GSM selection</td><td></td></tr> </table> | Model, firm. ver. | | IMEI | | PIN | | Operator Selection | Please wait... | Network Registration Status | | Signal Strength (CSQ) | | Packet Data Service | | GSM selection | |
| Model, firm. ver. | | | | | | | | | | | | | | | | | |
| IMEI | | | | | | | | | | | | | | | | | |
| PIN | | | | | | | | | | | | | | | | | |
| Operator Selection | Please wait... | | | | | | | | | | | | | | | | |
| Network Registration Status | | | | | | | | | | | | | | | | | |
| Signal Strength (CSQ) | | | | | | | | | | | | | | | | | |
| Packet Data Service | | | | | | | | | | | | | | | | | |
| GSM selection | | | | | | | | | | | | | | | | | |
| GSM information | <table border="1"> <tr><td>GSM IP</td><td></td></tr> <tr><td>RX</td><td></td></tr> <tr><td>TX</td><td></td></tr> </table> | GSM IP | | RX | | TX | | | | | | | | | | | |
| GSM IP | | | | | | | | | | | | | | | | | |
| RX | | | | | | | | | | | | | | | | | |
| TX | | | | | | | | | | | | | | | | | |

Sieć lokalna LAN (Local network)

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




AS30GSM200P GPRS/HSPA Router Configuration Panel
Modem HE910, 1 SIM, RS-232, firmware:140704

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|------------------------|--|-------------------|--|-------------|--|------------------------|---|--------------------------|---|--------------|----------------------|--------------|----------------------|--------------------|--|--------------------|--|------------------|--|-------------------|---|-------------------|---|------------|----------------------|-----------|----------------------|
| <div style="background-color: #2c3e50; color: white; padding: 5px;">Device status</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Basic</div> <div style="background-color: #e74c3c; color: white; padding: 5px;">Local network</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">GSM network</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Connection control</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Ports configuration</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">TCP/IP forwarding</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">VLAN</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Static routes</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Dynamic DNS</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Access control</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Advanced</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">OpenVPN</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">IPsec static</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">IPsec mobile</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">IPsec authentication</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">N2N</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">CARP</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">NTRIP</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">SMS Actions</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">GPIO</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">CAN</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Administration</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Time</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Syslog</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">User files</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Configuration</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Backup and restore</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Discard changes</div> <div style="background-color: #2c3e50; color: white; padding: 5px;">Save settings</div> | <h3 style="margin: 0;">Networking</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Get IP via DHCP</td> <td><input checked="" type="checkbox"/> Enabled</td> </tr> <tr> <td>IP Address</td> <td><input type="text" value="192.168.1.239"/> <small>Enter IP address here</small></td> </tr> <tr> <td>Mask</td> <td><input type="text" value="255.255.255.0"/> <small>Enter mask here</small></td> </tr> <tr> <td>Default gateway</td> <td><input type="text" value="Auto via GSM"/> <input type="text" value="192.168.1.1"/> <small>Enter gateway IP here</small></td> </tr> <tr> <td>DNS configuration</td> <td><input type="text" value="Auto via GSM"/></td> </tr> <tr> <td>DNS 1</td> <td><input type="text"/></td> </tr> <tr> <td>DNS 2</td> <td><input type="text"/></td> </tr> </table> <div style="background-color: #2c3e50; color: white; padding: 5px; margin-top: 10px;">DHCP server</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">DHCP Server</td> <td><input checked="" type="checkbox"/> Enabled <small>Set this option to enable DHCP server</small></td> </tr> <tr> <td>Range start</td> <td><input type="text" value="192.168.1.240"/></td> </tr> <tr> <td>Range end</td> <td><input type="text" value="192.168.1.250"/></td> </tr> </table> <div style="background-color: #2c3e50; color: white; padding: 5px; margin-top: 10px;">DHCP server: Bind MAC to IP</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Binds list</td> <td><input type="text"/> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input type="button" value="New"/> <input type="button" value="Delete"/> </div> <small>Please choose DHCP bind you would like to edit. Please note that after editing DHCP binds you have to save global settings.</small></td> </tr> <tr> <td>Identifier</td> <td><input type="text"/> <small>Please enter any name/identifier</small></td> </tr> <tr> <td>MAC</td> <td><input type="text"/></td> </tr> <tr> <td>IP</td> <td><input type="text"/></td> </tr> </table> | Get IP via DHCP | <input checked="" type="checkbox"/> Enabled | IP Address | <input type="text" value="192.168.1.239"/> <small>Enter IP address here</small> | Mask | <input type="text" value="255.255.255.0"/> <small>Enter mask here</small> | Default gateway | <input type="text" value="Auto via GSM"/> <input type="text" value="192.168.1.1"/> <small>Enter gateway IP here</small> | DNS configuration | <input type="text" value="Auto via GSM"/> | DNS 1 | <input type="text"/> | DNS 2 | <input type="text"/> | DHCP Server | <input checked="" type="checkbox"/> Enabled <small>Set this option to enable DHCP server</small> | Range start | <input type="text" value="192.168.1.240"/> | Range end | <input type="text" value="192.168.1.250"/> | Binds list | <input type="text"/> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input type="button" value="New"/> <input type="button" value="Delete"/> </div> <small>Please choose DHCP bind you would like to edit. Please note that after editing DHCP binds you have to save global settings.</small> | Identifier | <input type="text"/> <small>Please enter any name/identifier</small> | MAC | <input type="text"/> | IP | <input type="text"/> |
| Get IP via DHCP | <input checked="" type="checkbox"/> Enabled | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IP Address | <input type="text" value="192.168.1.239"/> <small>Enter IP address here</small> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | <input type="text" value="255.255.255.0"/> <small>Enter mask here</small> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Default gateway | <input type="text" value="Auto via GSM"/> <input type="text" value="192.168.1.1"/> <small>Enter gateway IP here</small> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DNS configuration | <input type="text" value="Auto via GSM"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DNS 1 | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DNS 2 | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DHCP Server | <input checked="" type="checkbox"/> Enabled <small>Set this option to enable DHCP server</small> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Range start | <input type="text" value="192.168.1.240"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Range end | <input type="text" value="192.168.1.250"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Binds list | <input type="text"/> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input type="button" value="New"/> <input type="button" value="Delete"/> </div> <small>Please choose DHCP bind you would like to edit. Please note that after editing DHCP binds you have to save global settings.</small> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Identifier | <input type="text"/> <small>Please enter any name/identifier</small> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| MAC | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IP | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Sieć GSM (GSM network)

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



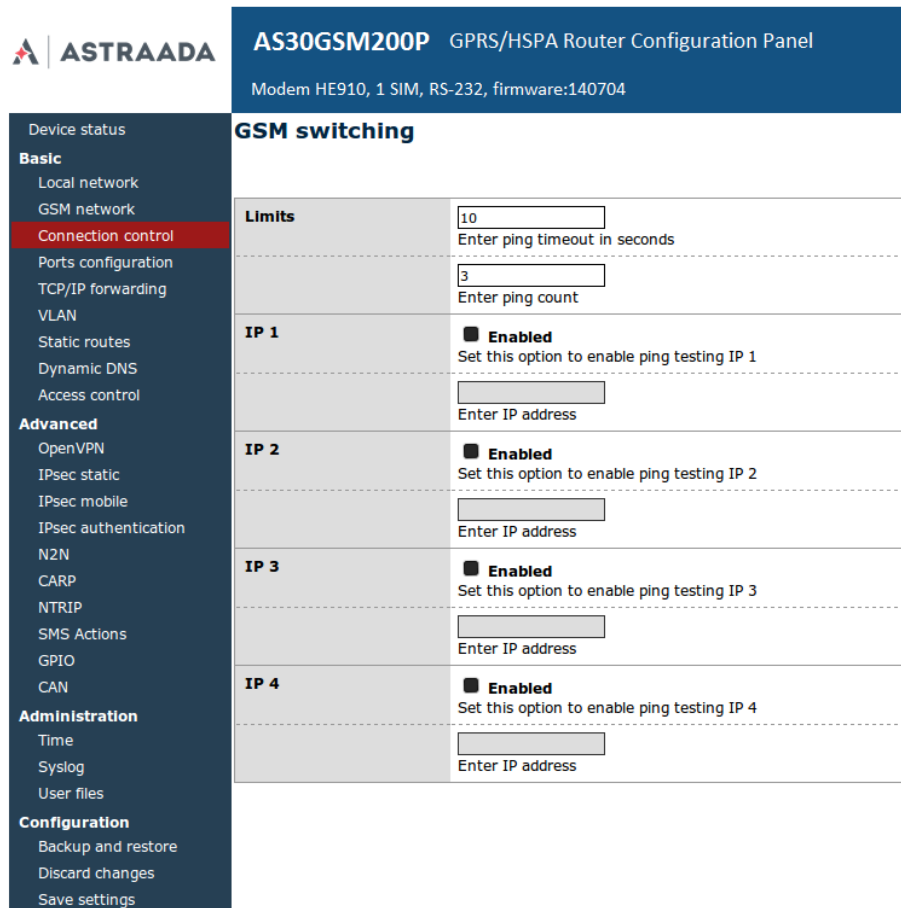
AS30GSM200P GPRS/HSPA Router Configuration Panel
Modem HE910, 1 SIM, RS-232, firmware:140704

| | Master | Slave |
|-------------------|---|---|
| SIM slot | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled |
| PIN | <input type="text"/> <small>Enter PIN here</small> | <input type="text"/> <small>Enter PIN here</small> |
| APN | <input type="text" value="internet"/> <small>Enter APN here</small> | <input type="text" value="monitoringprasy.pl"/> <small>Enter APN here</small> |
| CSD | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled |
| | <input type="text"/> <small>Enter CSD here</small> | <input type="text"/> <small>Enter CSD here</small> |
| Username | <input type="text"/> <small>Enter username here</small> | <input type="text"/> <small>Enter username here</small> |
| Password | <input type="text"/> <small>Enter password here</small> | <input type="text"/> <small>Enter password here</small> |
| ISP IP | <input checked="" type="checkbox"/> Enabled | <input checked="" type="checkbox"/> Enabled |
| | <input type="text"/> <small>Enter ISP IP here</small> | <input type="text"/> <small>Enter ISP IP here</small> |
| Modem band | <input type="text" value="2G and 3G"/> <small>Select modem band</small> | <input type="text" value="2G and 3G"/> <small>Select modem band</small> |
| Connection | <input type="text" value="Always on"/> <small>Modem connect</small> | <input type="text" value="Always on"/> <small>Modem connect</small> |
| | <input type="text" value="120"/> <small>Idle time before suspend (range 0-86400 sec)</small> | <input type="text" value="120"/> <small>Idle time before suspend (range 0-86400 sec)</small> |

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

Ustawienia połączeń (Connection control)

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



The screenshot shows the configuration interface for the AS30GSM200P router. The left sidebar contains a navigation menu with categories: Device status, Basic (Local network, GSM network, Connection control, Ports configuration, TCP/IP forwarding, VLAN, Static routes, Dynamic DNS, Access control), Advanced (OpenVPN, IPsec static, IPsec mobile, IPsec authentication, N2N, CARP, NTRIP, SMS Actions, GPIO, CAN), Administration (Time, Syslog, User files), and Configuration (Backup and restore, Discard changes, Save settings). The 'Connection control' option is selected and highlighted in red.

The main content area is titled 'GSM switching' and contains the following settings:


| AS30GSM200P GPRS/HSPA Router Configuration Panel | |
|--|---|
| Modem HE910, 1 SIM, RS-232, firmware:140704 | |
| Limits | <input type="text" value="10"/> Enter ping timeout in seconds |
| | <input type="text" value="3"/> Enter ping count |
| IP 1 | <input checked="" type="checkbox"/> Enabled Set this option to enable ping testing IP 1 |
| | <input type="text"/> Enter IP address |
| IP 2 | <input checked="" type="checkbox"/> Enabled Set this option to enable ping testing IP 2 |
| | <input type="text"/> Enter IP address |
| IP 3 | <input checked="" type="checkbox"/> Enabled Set this option to enable ping testing IP 3 |
| | <input type="text"/> Enter IP address |
| IP 4 | <input checked="" type="checkbox"/> Enabled Set this option to enable ping testing IP 4 |
| | <input type="text"/> Enter IP address |

Ustawienia portów (Ports configuration)

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

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

Każdy port może być przekierowany (forwarding) na port TCP/UDP (jakoś serwer lub klient). Ponadto port **/dev/ttyS0** można przekierować na sterowanie modemem lub transfer danych – w tym przypadku żaden inny tryb nie może zostać uruchomiony na tym porcie. Uruchomienie niektórych trybów dla **dev/ttyS0** i **/dev/ttyS1** umożliwia ustawienie parametrów takich jak: liczba bitów na sekundę (baud rate), bity danych, parzystość (parity), bity stopu i protokół. W przypadku gdy jakiś parametr jest niedostępny użytkownik nie ma możliwości jego zmiany.



ASTRAADA

AS30GSM200P GPRS/HSPA Router Configuration Panel
Modem HE910, 1 SIM, RS-232, firmware:140704

Ports

| Port settings | | | |
|---------------|---|---|--|
| Port type | Serial RS-232 External /dev/ttyS0 | Modem control Internal /dev/ttyS1 | Modem data Internal /dev/ttyACM0 |
| Mode | Terminal | SMS | Data |
| Baud rate | 115 200 | 115 200 | |
| Data bits | 8 | 8 | |
| Parity | None | None | |
| Stop bits | 1 | 1 | |
| Flow control | None | | |

| Forwarding configuration | | | |
|--------------------------|--------|--------|--------|
| To | | | |
| Mode | Client | Client | Client |
| Interface | LAN | LAN | LAN |
| Protocol | TCP | TCP | TCP |
| Server IP | | | |
| Port | | | |

Device status

Basic

- Local network
- GSM network
- Connection control
- Ports configuration
- TCP/IP forwarding
- VLAN
- Static routes
- Dynamic DNS
- Access control

Advanced

- OpenVPN
- IPsec static
- IPsec mobile
- IPsec authentication
- N2N
- CARP
- NTRIP
- SMS Actions
- GPIO
- CAN

Administration

- Time
- Syslog
- User files

Configuration

- Backup and restore
- Discard changes
- Save settings

Device status

Basic

- Local network
- GSM network
- Connection control
- Ports configuration
- TCP/IP forwarding
- VLAN
- Static routes
- Dynamic DNS
- Access control

Advanced

- OpenVPN
- IPsec static
- IPsec mobile
- IPsec authentication
- N2N
- CARP
- NTRIP
- SMS Actions
- GPIO
- CAN

Administration


- Time
- Syslog
- User files

Configuration

- Backup and restore
- Discard changes
- Save settings

TCP/IP forwarding

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


ASTRAADA

AS30GSM200P GPRS/HSPA Router Configuration Panel
Modem HE910, 1 SIM, RS-232, firmware:140704

- Device status
- Basic**
- Local network
- GSM network
- Connection control
- Ports configuration
- TCP/IP forwarding
- VLAN
- Static routes
- Dynamic DNS
- Access control
- Advanced**
- OpenVPN
- IPsec static
- IPsec mobile
- IPsec authentication
- N2N
- CARP
- NTRIP
- SMS Actions
- GPIO
- CAN
- Administration**
- Time
- Syslog
- User files
- Configuration**
- Backup and restore
- Discard changes
- Save settings

TCP/IP forwarding

Single port rules


| | |
|----------------------|--|
| Rules list | <input style="width: 100%;" type="text"/> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> New Delete </div> <p style="font-size: 0.8em; margin: 0;">Please choose a rule you would like to edit. Please note that after editing rules you have to save global settings.</p> |
| Identifier | <input style="width: 100%;" type="text"/> <p style="font-size: 0.8em; margin: 0;">Please enter any name/identifier</p> |
| Enable rule | <input checked="" type="checkbox"/> Enabled Set this option to enable this rule |
| External port | <input style="width: 100%;" type="text"/> |
| Internal port | <input style="width: 100%;" type="text"/> |
| Protocol | <input style="width: 100%;" type="text" value="TCP"/> |
| IP address | <input style="width: 100%;" type="text"/> |

Port range rules

| | |
|--------------------|--|
| Rules list | <input style="width: 100%;" type="text"/> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> New Delete </div> <p style="font-size: 0.8em; margin: 0;">Please choose a rule you would like to edit. Please note that after editing rules you have to save global settings.</p> |
| Identifier | <input style="width: 100%;" type="text"/> <p style="font-size: 0.8em; margin: 0;">Please enter any name/identifier</p> |
| Enable rule | <input checked="" type="checkbox"/> Enabled Set this option to enable this rule |
| First port | <input style="width: 100%;" type="text"/> |
| Last port | <input style="width: 100%;" type="text"/> |
| Protocol | <input style="width: 100%;" type="text" value="TCP"/> |

VLAN

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



AS30GSM200P GPRS/HSPA Router Configuration Panel
Modem HE910, 1 SIM, RS-232, firmware:140704

Device status

Basic

Local network

GSM network

Connection control

Ports configuration

TCP/IP forwarding

VLAN

Static routes

Dynamic DNS

Access control

Advanced

OpenVPN

IPsec static

IPsec mobile

IPsec authentication

N2N

CARP

NTRIP

SMS Actions

GPIO

CAN

Administration

Time

Syslog

User files

Configuration

Backup and restore

Discard changes

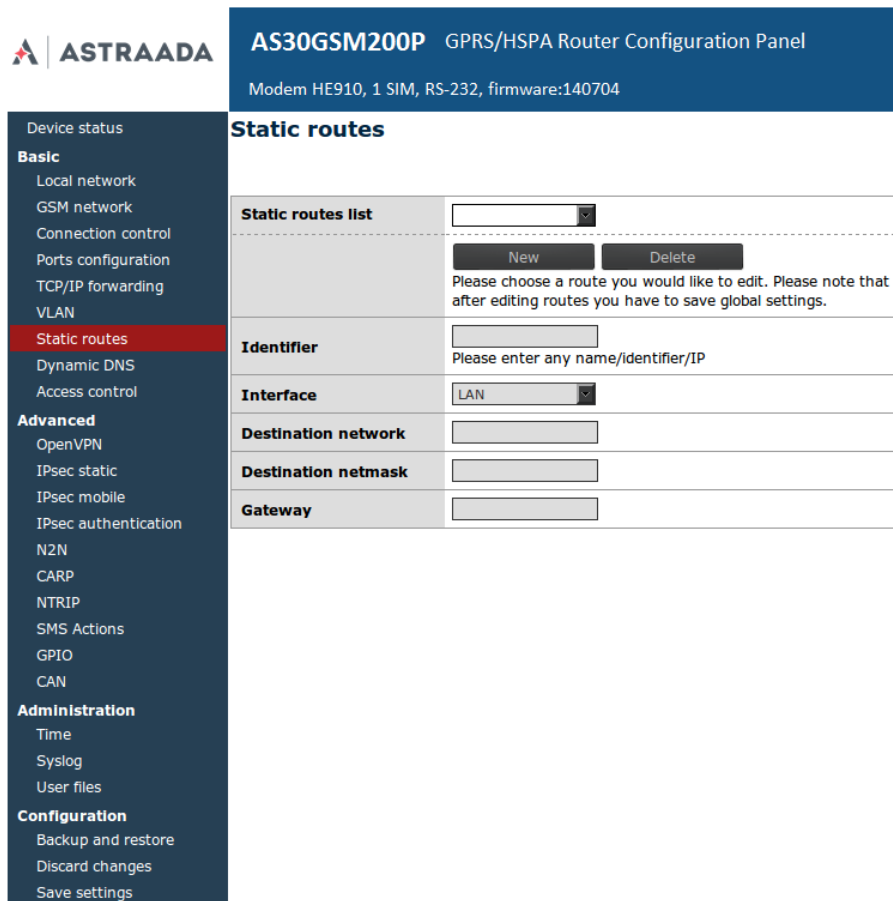
Save settings

VLAN/Virtual IP configuration

| | |
|-----------------------------|--|
| VLAN Virtual IP list | <input style="width: 80%;" type="text"/> |
| | <input type="button" value="New"/> <input type="button" value="Delete"/> |
| | Please choose VLAN you would like to edit. Please note that after editing those things you have to save global settings. |
| Enable VLAN | <input checked="" type="checkbox"/> Enabled Set this option to enable this VLAN |
| Description | <input style="width: 80%;" type="text"/> Please enter VLAN description. |
| IEEE 802.1Q tagging | <input checked="" type="checkbox"/> Enabled Set this option to enable IEEE 802.1Q tagging |
| Identifier | <input style="width: 80%;" type="text"/> Please enter number from range 0-4095. |
| IP | <input style="width: 80%;" type="text"/> |
| Netmask | <input style="width: 80%;" type="text"/> |

Static routes

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



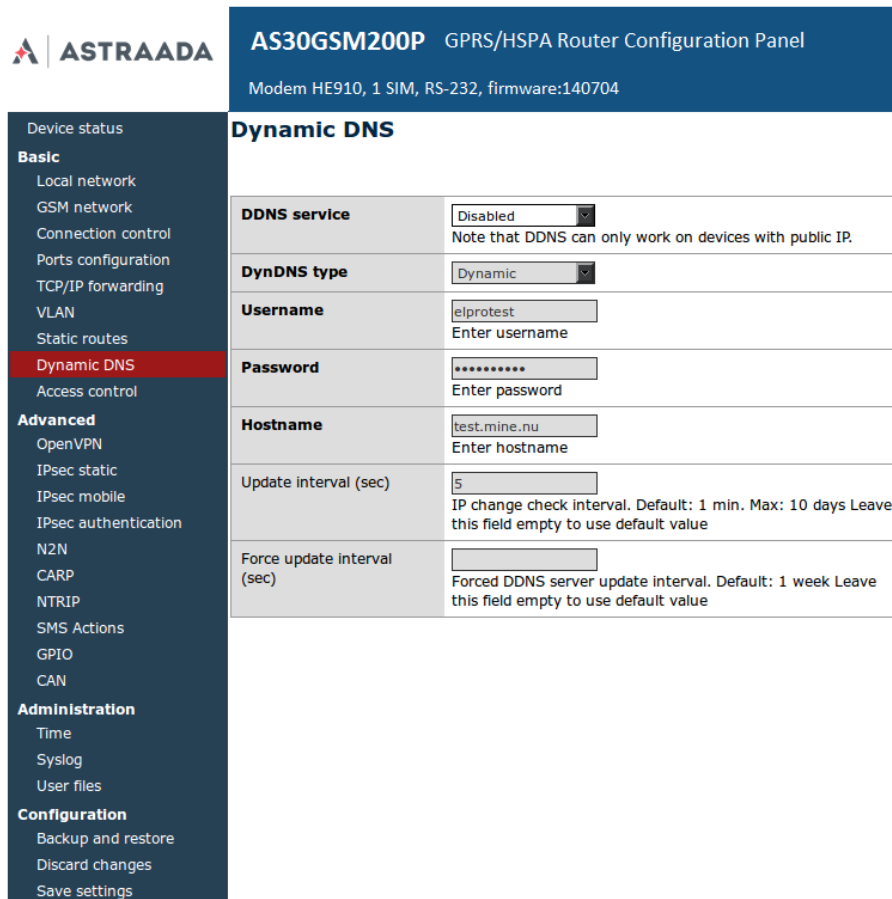
The screenshot shows the configuration interface for the AS30GSM200P router. The top header includes the Astraada logo and the title 'AS30GSM200P GPRS/HSPA Router Configuration Panel'. Below the title, it specifies 'Modem HE910, 1 SIM, RS-232, firmware:140704'. A left-hand navigation menu lists various settings categories: Device status, Basic (Local network, GSM network, Connection control, Ports configuration, TCP/IP forwarding, VLAN, Static routes, Dynamic DNS, Access control), Advanced (OpenVPN, IPsec static, IPsec mobile, IPsec authentication, N2N, CARP, NTRIP, SMS Actions, GPIO, CAN), Administration (Time, Syslog, User files), and Configuration (Backup and restore, Discard changes, Save settings). The 'Static routes' menu item is highlighted in red.

The main content area is titled 'Static routes' and features a 'Static routes list' section with a dropdown menu. Below this are 'New' and 'Delete' buttons. A note states: 'Please choose a route you would like to edit. Please note that after editing routes you have to save global settings.' The configuration form includes the following fields:

| | |
|----------------------------|---|
| Identifier | <input type="text"/> Please enter any name/identifier/IP |
| Interface | <input type="text" value="LAN"/> |
| Destination network | <input type="text"/> |
| Destination netmask | <input type="text"/> |
| Gateway | <input type="text"/> |

Dynamic DNS

Dynamic DNS to usługa, która pozwala na udostępnienie urządzenia pod określonym adresem internetowym niezależnie od zmian jego adresu IP. Aby było to możliwe potrzebne jest utworzenie konta na jednym z serwisów internetowych obsługujących tę usługę. Aktualnie obsługiwane serwisy przez modem AS30GSM200P to **DynDNS.org** oraz **No-IP.com**. Po założeniu konta w jednym z serwisów ustawiamy w zakładce *Dynamic DNS* usługodawcę, dla dyndns.org dodatkowo rodzaj usługi, nazwę użytkownika, hasło, nazwę hosta oraz dwa parametry: *update interval* i *force update interval*. Pierwszy z nich określa jak często następuje sprawdzenie, czy adres IP uległ zmianie i ewentualne powiadomienie o tym fakcie usługodawcy, drugi określa czas pomiędzy wymuszonymi aktualizacjami, tzn. takimi, które występują nawet gdy adres IP się nie zmienił. W razie wątpliwości można pozostawić te pola puste-zostaną wtedy użyte domyślne wartości.



ASTRAADA AS30GSM200P GPRS/HSPA Router Configuration Panel
 Modem HE910, 1 SIM, RS-232, firmware:140704

Dynamic DNS

| | |
|------------------------------------|--|
| DDNS service | <input type="text" value="Disabled"/> Note that DDNS can only work on devices with public IP. |
| DynDNS type | <input type="text" value="Dynamic"/> |
| Username | <input type="text" value="elprotest"/> Enter username |
| Password | <input type="password" value="*****"/> Enter password |
| Hostname | <input type="text" value="test.mine.nu"/> Enter hostname |
| Update interval (sec) | <input type="text" value="5"/> IP change check interval. Default: 1 min. Max: 10 days Leave this field empty to use default value |
| Force update interval (sec) | <input type="text"/> Forced DDNS server update interval. Default: 1 week Leave this field empty to use default value |

Navigation Menu:

- Device status
- Basic**
 - Local network
 - GSM network
 - Connection control
 - Ports configuration
 - TCP/IP forwarding
 - VLAN
 - Static routes
 - Dynamic DNS**
 - Access control
- Advanced**
 - OpenVPN
 - IPsec static
 - IPsec mobile
 - IPsec authentication
 - N2N
 - CARP
 - NTRIP
 - SMS Actions
 - GPIO
 - CAN
- Administration**
 - Time
 - Syslog
 - User files
- Configuration**
 - Backup and restore
 - Discard changes
 - Save settings

Access control

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

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

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

The screenshot shows the configuration interface for the AS30GSM200P router. The left sidebar contains a navigation menu with categories: Device status, Basic (Local network, GSM network, Connection control, Ports configuration, TCP/IP forwarding, VLAN, Static routes, Dynamic DNS), Access control (highlighted), Advanced (OpenVPN, IPsec static, IPsec mobile, IPsec authentication, N2N, CARP, NTRIP, SMS Actions, GPIO, CAN), Administration (Time, Syslog, User files), and Configuration (Backup and restore, Discard changes, Save settings). The main content area is titled 'Access control' and contains the 'SSH configuration' section. This section includes: 'SSH enabled' (checked 'Enabled'), 'Interfaces' (checked 'LAN', unselected 'GSM', 'OpenVPN', 'IPsec'), 'OpenVPN tunnels' (selected '1', '2', '3', '4'), 'IPsec tunnels' (selected '1', '2', '3', '4'), 'Port' (65535), 'SSH login as root' (checked 'Enabled'), 'SSH root password' (masked), 'SSH service password' (masked), 'SSH root key' (with a text area containing a public key and buttons for 'Generate', 'Get private key', 'Get public key'), and 'SSH service key' (with a text area containing a public key and buttons for 'Generate', 'Get private key', 'Get public key').

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

Open VPN

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

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

Po wprowadzeniu wszystkich niezbędnych informacji użytkownik powinien wypełnić cztery pola certyfikatów, które generowane są na dowolnym komputerze (sprawdź VPN online help w celu uzyskania dodatkowych informacji). Zawartość plików powinna zostać wklejona w odpowiednie pola w karcie konfiguracji VPN. Istnieje możliwość dodatkowego zabezpieczenia połączenia VPN poprzez ustalenie wspólnego **klucza TLS** i wpisania go w pole *TLS key* dla wszystkich urządzeń w sieci VPN. Ostatnia opcja to przełączanie kompresji **LZO** (zalecane włączenie w celu poprawy komunikacji sieciowej) oraz dodatkowy parametr w polu *Additional configuration*.

- Device status
- Basic**
 - Local network
 - GSM network
 - Connection control
 - Ports configuration
 - TCP/IP forwarding
 - VLAN
 - Static routes
 - Dynamic DNS
 - Access control
- Advanced**
 - OpenVPN**
 - IPsec static
 - IPsec mobile
 - IPsec authentication
 - N2N
 - CARP
 - NTRIP
 - SMS Actions
 - GPIO
 - CAN
- Administration**
 - Time
 - Syslog
 - User files
- Configuration**
 - Backup and restore
 - Discard changes
 - Save settings

OpenVPN tunnels

| | |
|----------------------------------|--|
| Tunnel configuration | <input type="text" value="openVPN tunnel 2"/> Please select VPN tunnel you would like to configure |
| OpenVPN mode | <input type="text" value="Disabled"/> |
| Connection mode | <input type="text" value="Router (TUN) sing"/> |
| Remote Server IP | <input type="text"/> |
| VPN device | <input type="text" value="LAN"/> |
| NAT-T | <input checked="" type="checkbox"/> Enable NAT Traversal (NAT-T) Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls. |
| Port | <input type="text"/> |
| Protocol | <input type="text" value="TCP"/> |
| Network | <input type="text"/> |
| Netmask | <input type="text"/> |
| Server IP | <input type="text"/> |
| Client IP | <input type="text"/> |
| CA cert | <input type="text"/> |
| Server/client cert | <input type="text"/> |
| Server/client private key | <input type="text"/> |

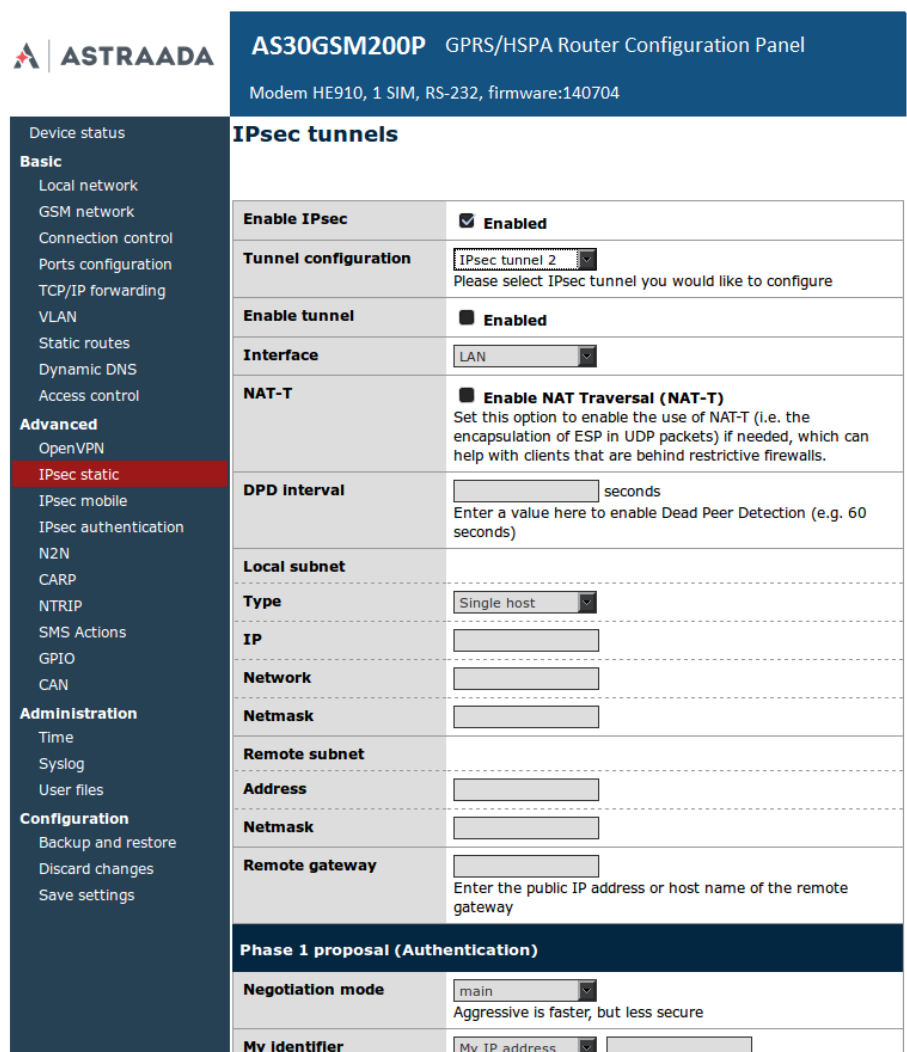
IPsec static/IPsec mobile

IPsec to zbiór protokołów internetowych pozwalający na stworzenie bezpiecznego połączenia pomiędzy urządzeniami. Do konfiguracji takiego połączenia na modemie AS30GSM200P służą trzy zakładki konfiguracji: *Tunnels*, *Mobile Clients*, *Keys and Certificates*. Aby włączyć program obsługujący protokół należy przede wszystkim w zakładce *Tunnels* zaznaczyć opcję *Enable Ipsec*. Pod tą opcją mamy pole wyboru pozwalające nam na przełączanie pomiędzy konfiguracjami czterech tuneli. Aby włączyć dany tunel wybieramy go z listy, a następnie zaznaczamy pole *Enable tunnel*. Następnie należy wybrać interfejs sieciowy, przez który zostanie przeprowadzone połączenie. Nie sposób omówić wszystkich możliwości nawiązywania połączenia za pomocą protokołu *IPsec*, dlatego poniżej zostanie opisana przykładowa konfiguracja.

Przykładowa konfiguracja

Załóżmy, że chcemy połączyć ze sobą dwa modemy AS30GSM200P o adresach 123.45.67.1 oraz 123.45.67.2. Pole *DPD interval* określa czas, po którym połączenie zostanie zamknięte jeżeli drugie urządzenie nie odpowie. Dla ustalenia uwagi wpisujemy 3600 sekund. Kolejnym ustawieniem jest określenie lokalnej podsieci, z której pakiety będą przekazywane poprzez bezpieczne połączenie. Możemy tu wybrać *Single host* (tylko nasz AS30GSM200P), *Network* (sieć kilku urządzeń) lub *LAN subnet* (podsieć lokalnej sieci). Ponieważ nie wiemy, czy nie będziemy chcieli dodać więcej urządzeń w przyszłości wybierzemy opcję *Network*, w pole IP wpisując 192.168.36.1, w pole Network 192.168.36.0, a w pole Netmask 255.255.255.0. Oczywiście powinno być, że wybrany adres IP powinien być zgodny z wybraną siecią i jej maską. W pola Address i Netmask w sekcji *remote subnet* musimy wpisać podsieć lokalną, którą określimy na drugim urządzeniu. Na drugim urządzeniu wpisujemy w sekcji *Local subnet* IP=192.168.35.1, Network=192.168.35.0 i Netmask=255.255.255.0, dlatego też w pola Address i Netmask tej sekcji musimy wpisać Address=192.168.35.0 i Netmask=255.255.255.0 (czyli po prostu przepisujemy pola Network i Netmask z sekcji Local subnet na drugim urządzeniu). Oczywiście w sekcji *remote subnet* na drugim urządzeniu należy przepisać odpowiednie pola z pierwszego urządzenia. Kolejnym polem jest *Remote gateway*, gdzie wpisujemy adres IP drugiego urządzenia, tzn. wpisujemy na krzyż: w pierwszym urządzeniu 123.45.67.2, a w drugim 123.45.67.1. Następnym krokiem jest zdefiniowanie dwóch faz negocjacji połączenia. Musimy określić jakim identyfikatorem będzie się przedstawiać nasze urządzenie. Najczęstszym wyborem jest *My IP Address* (mój adres IP) lub *RSA Cert Subject* (ale tylko wtedy, gdy używamy do autoryzacji certyfikatów, o czym za chwilę). Algorytm szyfrowania (*Encryption algorithm*) i algorytm funkcji skrótu (*Hash algorithm*) określamy wedle własnego uznania, należy jednak pamiętać, żeby na wszystkich urządzeniach ustawić te same ustawienia. Najszybszym algorytmem szyfrowania jest z reguły *Blowfish*, a najwolniejszym (ale i najbezpieczniejszym)-*AES*. Następnym ustawieniem jest *DH key group*, czyli długość kodu *Diffiego-Hellmana*. Tu również ustawienia po obu stronach połączenia powinny być zgodne. W polu *Lifetime* należy określić maksymalny czas negocjacji w fazie pierwszej, przykładowo 180 sekund, czyli 3 minuty. Jeżeli nie jesteśmy pewni co wpisać możemy pozostawić to pole puste. Najważniejszym ustawieniem fazy pierwszej jest *Authentication method*, czyli metoda uwierzytelnienia. Najprostszą metodą jest *Pre-shared key* (PSK), czyli mówiąc prościej hasło, które jest zgodne dla obu stron. Jeżeli zależy nam na lepszym bezpieczeństwie możemy wybrać *RSA signature*. Ta metoda jest jednak bardziej kłopotliwa, gdyż wymaga wygenerowania certyfikatów i kluczy. Jeżeli zdecydujemy się na tę metodę mamy dwie możliwości: podać własny klucz, własny certyfikat oraz certyfikat drugiego urządzenia (*peer certificate*) lub

własny klucz, certyfikat i certyfikat CA (sposób dodawania certyfikatów CA został opisany w dalszej części rozdziału).




The screenshot shows the configuration panel for the AS30GSM200P router. The left sidebar contains a navigation menu with categories: Device status, Basic, Advanced, Administration, and Configuration. The 'IPsec static' option is selected. The main content area is titled 'IPsec tunnels' and contains the following configuration fields:

| | |
|--|--|
| Enable IPsec | <input checked="" type="checkbox"/> Enabled |
| Tunnel configuration | IPsec tunnel 2 Please select IPsec tunnel you would like to configure |
| Enable tunnel | <input type="checkbox"/> Enabled |
| Interface | LAN |
| NAT-T | <input checked="" type="checkbox"/> Enable NAT Traversal (NAT-T) Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls. |
| DPD interval | <input type="text"/> seconds Enter a value here to enable Dead Peer Detection (e.g. 60 seconds) |
| Local subnet | |
| Type | Single host |
| IP | <input type="text"/> |
| Network | <input type="text"/> |
| Netmask | <input type="text"/> |
| Remote subnet | |
| Address | <input type="text"/> |
| Netmask | <input type="text"/> |
| Remote gateway | <input type="text"/> Enter the public IP address or host name of the remote gateway |
| Phase 1 proposal (Authentication) | |
| Negotiation mode | main Aggressive is faster, but less secure |
| My identifier | My IP address <input type="text"/> |

W drugiej fazie negocjacji należy ustalić protokół: *AH* (tylko uwierzytelnienie) lub *ESP* (uwierzytelnienie z szyfrowaniem), algorytmy szyfrowania i funkcji skrótu (można zaznaczyć kilka, ważne, aby przynajmniej jeden pokrywał się po obu stronach), długość klucza *PFS* (*Perfect Forward Secrecy*) oraz czas trwania drugiej fazy negocjacji (to pole można zostawić puste aby użyć wartości domyślnej). Po zapisaniu ustawień powinniśmy mieć gotowe bezpieczne połączenie *IPsec*. Jeżeli wybraliśmy metodę autoryzacji poprzez certyfikaty *RSA* nie określając certyfikatu partnera (*peer certificate*), musimy dodać certyfikat *CA*. W tym celu wybieramy zakładkę *Keys and Certificates*. Mamy tu możliwość zapisywania dodatkowych kluczy prywatnych (*Pre-Shared keys*) oraz certyfikatów *CA*. Metoda zapisu jest taka sama dla obu typów zabezpieczeń i zostanie opisana na przykładzie certyfikatów *CA*. Jeżeli nie określiliśmy wcześniej żadnego certyfikatu *CA* najprawdopodobniej lista certyfikatów jest pusta. Aby dodać pierwszy certyfikat musimy najpierw kliknąć przycisk *Add new*. W ten sposób odblokowane zostaną pola, w których należy wpisać kolejno: identyfikator (może być dowolny, jest widoczny jedynie w konfiguracji *www* i ma pomóc użytkownikowi rozróżnić certyfikaty), certyfikat oraz listę wykluczeń certyfikatu (*CRL*). Ostatnie pole jest opcjonalne, służy do ewentualnego zablokowania dostępu części użytkowników.

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



AS30GSM200P GPRS/HSPA Router Configuration Panel
Modem HE910, 1 SIM, RS-232, firmware:140704

Device status

Basic

- Local network
- GSM network
- Connection control
- Ports configuration
- TCP/IP forwarding
- VLAN
- Static routes
- Dynamic DNS
- Access control

Advanced

- OpenVPN
- IPsec static
- IPsec mobile
- IPsec authentication
- N2N
- CARP
- NTRIP
- SMS Actions
- GPIO
- CAN

Administration

- Time
- Syslog
- User files

Configuration

- Backup and restore
- Discard changes
- Save settings

IPsec mobile clients

| | |
|--|---|
| Allow mobile clients | <input checked="" type="checkbox"/> Enabled |
| NAT-T | <input type="checkbox"/> Enable NAT Traversal (NAT-T) Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls. |
| DPD interval | <input type="text"/> seconds Enter a value here to enable Dead Peer Detection (e.g. 60 seconds) |
| Phase 1 proposal (Authentication) | |
| Negotiation mode | <input type="text" value="main"/> Aggressive is faster, but less secure |
| My identifier | <input type="text" value="My IP address"/> <input type="text" value="domena.com"/> |
| Encryption algorithm | <input type="text" value="3DES"/> Must match the setting chosen on the remote side |
| Hash algorithm | <input type="text" value="SHA1"/> Must match the setting chosen on the remote side |
| DH key group | <input type="text" value="1"/> 1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit Must match the setting chosen on the remote side. |
| Lifetime | <input type="text"/> seconds This field is optional |
| Authentication method | <input type="text" value="Pre-shared key"/> Must match the setting chosen on the remote side |
| Certificate | <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> Paste a certificate in X.509 PEM format here. |
| Key | <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> |

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

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

Generowanie certyfikatów SSL

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

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

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

Oraz podkatalogi, w których będą trzymane klucze i certyfikaty:

```
mkdir private certs newcerts crl
```

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

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

Uwaga: należy dokładnie zapamiętać hasło do klucza prywatnego!

Należy wygenerować certyfikat CA:

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

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

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

Należy wygenerować wniosek o wystawienie certyfikatu:

```
openssl req -new -key private/urzedzeniekey.pem -out urzedzenie1req.pem
```

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

```
openssl ca -notext -in urzedzenie1req.pem -out urzedzenie1cert.pem
```

Aby móc wykorzystać certyfikat w modemie AS30GSM200P należy zdjąć hasło z klucza prywatnego:

```
openssl rsa -in private/urządzenie1key.pem -out
private/urządzenie1key.pem_bezhasla
```

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

W konfiguracji www w zakładce *IPsec/Tunnels* (jeżeli ten protokół będzie wykorzystywany) w pole *Certificate* wklejamy zawartość pliku `urządzenie1cert.pem`, w pole *Key* `urządzenie1key.pem_bezhasla`. W pole *peer certificate* powinno się wkleić certyfikat drugiego urządzenia lub pozostawić je puste i wtedy w zakładce *Keys and Certificates* dodać nowy certyfikat CA i wkleić zawartość pliku `cacert.pem`.

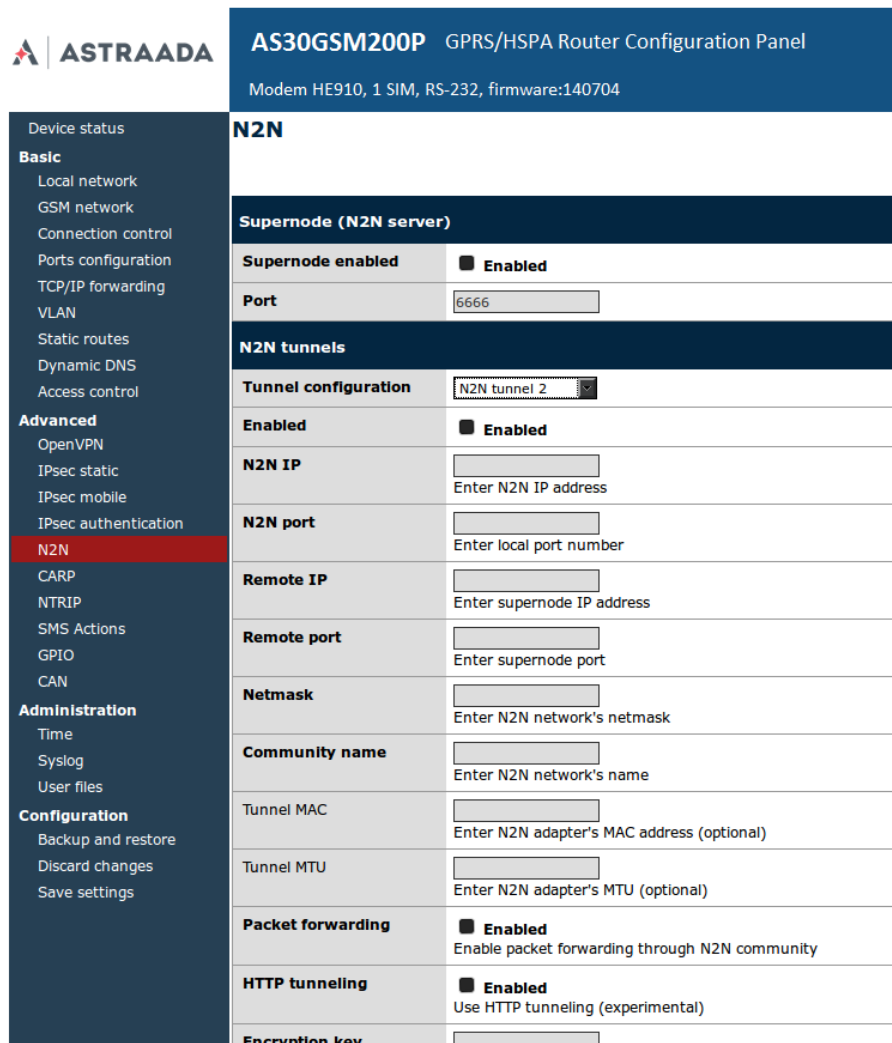
Jeżeli potrzebne będzie korzystanie z protokołu OpenVPN, to konfiguracji www w zakładce OpenVPN w pole *CA cert* należy wkleić zawartość pliku `cacert.pem`, w pole *Server/Client cert* zawartość pliku `urządzenie1cert.pem`, a w pole *Server/Client private key* zawartość pliku `urządzenie1key.pem_bezhasla`. Dodatkowo dla *OpenVPN* powinno się wygenerować plik parametrami Diffiego-Hellmana:

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

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

N2N

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




The screenshot shows the configuration interface for the AS30GSM200P router. The left sidebar contains a navigation menu with categories: Device status, Basic, Advanced, Administration, and Configuration. The 'N2N' option is highlighted in red. The main content area is titled 'N2N' and contains the following configuration sections:

- Supernode (N2N server)**
 - Supernode enabled: Enabled
 - Port:
- N2N tunnels**
 - Tunnel configuration:
 - Enabled: Enabled
 - N2N IP: Enter N2N IP address
 - N2N port: Enter local port number
 - Remote IP: Enter supernode IP address
 - Remote port: Enter supernode port
 - Netmask: Enter N2N network's netmask
 - Community name: Enter N2N network's name
 - Tunnel MAC: Enter N2N adapter's MAC address (optional)
 - Tunnel MTU: Enter N2N adapter's MTU (optional)
 - Packet forwarding: Enabled
Enable packet forwarding through N2N community
 - HTTP tunneling: Enabled
Use HTTP tunneling (experimental)
 - Encryption key:

CARP

CARP jest protokołem sieciowym umożliwiającym połączenie pomiędzy wieloma urządzeniami (*redundancy group*), które będą dostępne jako jedno urządzenie pod wskazanym adresem sieciowym. Przykładowo możesz wybrać urządzenia, które mają adresy IP 192.168.1.2 i 192.168.1.3 aby były dostępne pod adresem 192.168.1.115. Jeżeli jedno przestanie pracować, drugie z nich nie przestanie obsługiwać użytkowników. Urządzenie które jest aktualnie aktywne pod dzielnym adresem nazywane jest typu master, podczas gdy pozostałe nazywamy backup. Jeżeli chcesz skonfigurować *CARP*, wybierz interfejs sieciowy pod którym będzie dostępny klient *CARP* oraz wybierz identyfikator grupowy odpowiadający pozostałym urządzeniom z tej grupy – musi być to numer pomiędzy 1 a 255. Wprowadź wirtualny dzielnony adres IP. Opcje *Advertisement frequency* oraz *Advertisement skew* regulują jak często urządzenia będą komunikować się między sobą. Pamiętaj aby zdefiniować skrypty up oraz down, które ustawią/skasują routing gdy urządzenia przechodzą w stany master/backup.



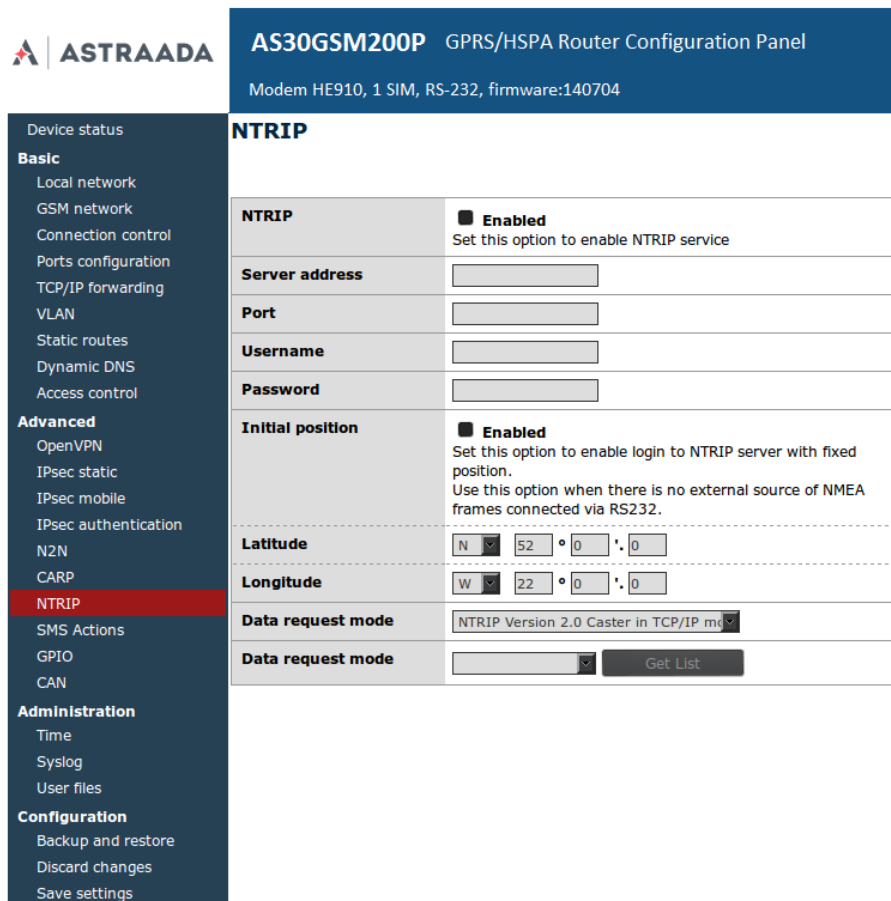
AS30GSM200P GPRS/HSPA Router Configuration Panel
Modem HE910, 1 SIM, RS-232, firmware:140704

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|-------------------------|--|-------------------|--|------------------|----------------------------------|------------------------------|---|-----------------|----------------------|--------------------------------|--|---------------------|---|----------------------------------|----------------------|--------------------------------|--|---------------------------|--|-----------|--|-------------|----------------------|
| Device status Basic Local network GSM network Connection control Ports configuration TCP/IP forwarding VLAN Static routes Dynamic DNS Access control Advanced OpenVPN IPsec static IPsec mobile IPsec authentication N2N CARP NTRIP SMS Actions GPIO CAN Administration Time Syslog User files Configuration Backup and restore Discard changes Save settings | <h3>CARP</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">CARP groups list</td> <td style="padding: 5px;"> <input type="text"/> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> New Delete </div> <small>Please choose group you would like to edit. Please note that after editing rules you have to save global settings.</small> </td> </tr> <tr> <td style="padding: 5px;">Identifier</td> <td style="padding: 5px;"> <input type="text"/> <small>Please enter any name/identifier/IP</small> </td> </tr> <tr> <td style="padding: 5px;">Interface</td> <td style="padding: 5px;"> <input type="text" value="LAN"/> </td> </tr> <tr> <td style="padding: 5px;">Virtual IP Identifier</td> <td style="padding: 5px;"> <input type="text"/> <small>Please enter value between 1 and 255. Value must be same on all devices in group. All groups in network must have unique values.</small> </td> </tr> <tr> <td style="padding: 5px;">Password</td> <td style="padding: 5px;"><input type="text"/></td> </tr> <tr> <td style="padding: 5px;">Become preferred master</td> <td style="padding: 5px;"> <input checked="" type="checkbox"/> Enabled <small>This option will set the device to become master as soon as possible.</small> </td> </tr> <tr> <td style="padding: 5px;">Neutral mode</td> <td style="padding: 5px;"> <input checked="" type="checkbox"/> Enabled <small>Don't run downscript at start if backup.</small> </td> </tr> <tr> <td style="padding: 5px;">Virtual shared IP address</td> <td style="padding: 5px;"><input type="text"/></td> </tr> <tr> <td style="padding: 5px;">Advertisement frequency</td> <td style="padding: 5px;"> <input type="text"/> <small>Interval in seconds that advertisements will occur. Please enter value between 0 and 255.</small> </td> </tr> <tr> <td style="padding: 5px;">Advertisement skew</td> <td style="padding: 5px;"> <input type="text"/> <small>Please enter value between 0 and 255.</small> </td> </tr> <tr> <td style="padding: 5px;">Up script</td> <td style="padding: 5px;"> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>This script will be executed when becoming master. To view hint, please enter valid virtual shared IP address.</small> </td> </tr> <tr> <td style="padding: 5px;">Down script</td> <td style="padding: 5px;"><input type="text"/></td> </tr> </table> | CARP groups list | <input type="text"/> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> New Delete </div> <small>Please choose group you would like to edit. Please note that after editing rules you have to save global settings.</small> | Identifier | <input type="text"/> <small>Please enter any name/identifier/IP</small> | Interface | <input type="text" value="LAN"/> | Virtual IP Identifier | <input type="text"/> <small>Please enter value between 1 and 255. Value must be same on all devices in group. All groups in network must have unique values.</small> | Password | <input type="text"/> | Become preferred master | <input checked="" type="checkbox"/> Enabled <small>This option will set the device to become master as soon as possible.</small> | Neutral mode | <input checked="" type="checkbox"/> Enabled <small>Don't run downscript at start if backup.</small> | Virtual shared IP address | <input type="text"/> | Advertisement frequency | <input type="text"/> <small>Interval in seconds that advertisements will occur. Please enter value between 0 and 255.</small> | Advertisement skew | <input type="text"/> <small>Please enter value between 0 and 255.</small> | Up script | <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>This script will be executed when becoming master. To view hint, please enter valid virtual shared IP address.</small> | Down script | <input type="text"/> |
| CARP groups list | <input type="text"/> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> New Delete </div> <small>Please choose group you would like to edit. Please note that after editing rules you have to save global settings.</small> | | | | | | | | | | | | | | | | | | | | | | | | |
| Identifier | <input type="text"/> <small>Please enter any name/identifier/IP</small> | | | | | | | | | | | | | | | | | | | | | | | | |
| Interface | <input type="text" value="LAN"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| Virtual IP Identifier | <input type="text"/> <small>Please enter value between 1 and 255. Value must be same on all devices in group. All groups in network must have unique values.</small> | | | | | | | | | | | | | | | | | | | | | | | | |
| Password | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| Become preferred master | <input checked="" type="checkbox"/> Enabled <small>This option will set the device to become master as soon as possible.</small> | | | | | | | | | | | | | | | | | | | | | | | | |
| Neutral mode | <input checked="" type="checkbox"/> Enabled <small>Don't run downscript at start if backup.</small> | | | | | | | | | | | | | | | | | | | | | | | | |
| Virtual shared IP address | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | |
| Advertisement frequency | <input type="text"/> <small>Interval in seconds that advertisements will occur. Please enter value between 0 and 255.</small> | | | | | | | | | | | | | | | | | | | | | | | | |
| Advertisement skew | <input type="text"/> <small>Please enter value between 0 and 255.</small> | | | | | | | | | | | | | | | | | | | | | | | | |
| Up script | <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>This script will be executed when becoming master. To view hint, please enter valid virtual shared IP address.</small> | | | | | | | | | | | | | | | | | | | | | | | | |
| Down script | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | |

NTRIP configuration page

Jeden z trybów pracy portu **/dev/ttyS0** jest komunikacja z urządzeniem zewnętrznym z użyciem protokołu NTRIP. Jeżeli zdecydujesz się użyć tego trybu, niezbędne będzie ustawienie tego trybu w zakładce **RS232 Port**. Następnie wejdź w zakładkę **NTRIP**. Pola adresu serwera, portu i pozycji początkowej są wymagane. Nazwa użytkownika i hasło są opcjonalne. Możliwe jest także uruchomienie trybu *Data Request*. Po wprowadzeniu wymaganych danych w pola, kliknij przycisk *Get List* aby pobrać listę źródeł z serwera – może to zająć chwilę. Po zakończeniu pobierania wybierz jedno ze źródeł.

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

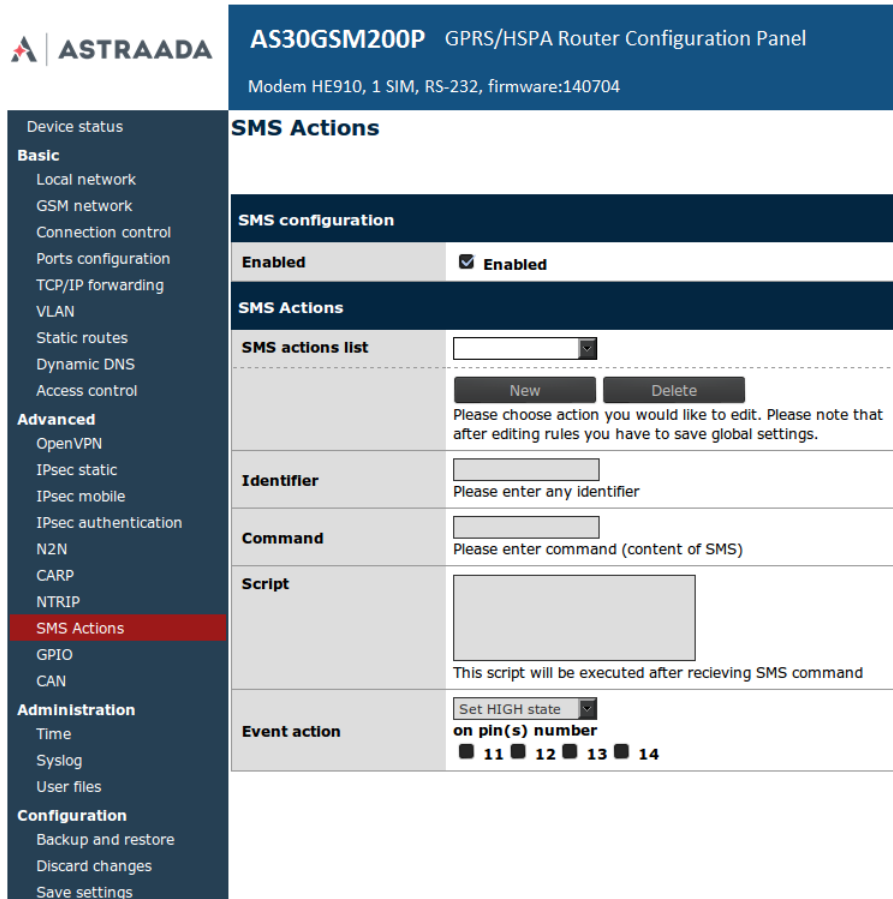


The screenshot shows the configuration interface for the AS30GSM200P router. The left sidebar contains a menu with categories: Device status, Basic (Local network, GSM network, Connection control, Ports configuration, TCP/IP forwarding, VLAN, Static routes, Dynamic DNS, Access control), Advanced (OpenVPN, IPsec static, IPsec mobile, IPsec authentication, N2N, CARP), NTRIP (highlighted), SMS Actions, GPIO, CAN, Administration (Time, Syslog, User files), and Configuration (Backup and restore, Discard changes, Save settings). The main content area is titled 'NTRIP' and contains the following configuration fields:

| | |
|--------------------------|--|
| NTRIP | <input checked="" type="checkbox"/> Enabled Set this option to enable NTRIP service |
| Server address | <input type="text"/> |
| Port | <input type="text"/> |
| Username | <input type="text"/> |
| Password | <input type="text"/> |
| Initial position | <input checked="" type="checkbox"/> Enabled Set this option to enable login to NTRIP server with fixed position. Use this option when there is no external source of NMEA frames connected via RS232. |
| Latitude | N <input type="text" value="52"/> ° <input type="text" value="0"/> ' <input type="text" value="0"/> " |
| Longitude | W <input type="text" value="22"/> ° <input type="text" value="0"/> ' <input type="text" value="0"/> " |
| Data request mode | <input type="text" value="NTRIP Version 2.0 Caster in TCP/IP mode"/> |
| Data request mode | <input type="text"/> <input type="button" value="Get List"/> |

SMS Actions

Zakładka *SMS Actions* umożliwia użytkownikowi zdefiniowanie skryptów które zostaną uruchomione gdy modem odbierze SMS z określoną zawartością. Aby włączyć tę opcję należy upewnić się że globalne pole *SMS Actions* jest zaznaczone oraz że jeden z portów jest ustawiony w tryb *SMS receiving* w zakładce *Ports configuration*. Następnie należy kliknąć w przycisk *New*, wprowadzić jakikolwiek identyfikator oraz komendę SMS która wywoływać będzie akcję. Możliwe jest zainicjowanie dowolnego skryptu (typu shell) i/oraz ustawienie akcji na GPIO.



The screenshot shows the configuration interface for the AS30GSM200P router. The left sidebar contains a navigation menu with categories: Device status, Basic, Advanced, Administration, and Configuration. The 'SMS Actions' option is highlighted in red. The main content area is titled 'SMS Actions' and includes a status toggle set to 'Enabled'. Below this is a table for 'SMS actions list' with 'New' and 'Delete' buttons. The table has columns for 'Identifier', 'Command', 'Script', and 'Event action'. The 'Event action' is currently set to 'Set HIGH state on pin(s) number' with radio buttons for pins 11, 12, 13, and 14.

| SMS configuration | |
|-------------------|--|
| Enabled | <input checked="" type="checkbox"/> Enabled |
| SMS Actions | |
| SMS actions list | <input type="text"/> <div style="display: flex; justify-content: space-around;"> New Delete </div> <p>Please choose action you would like to edit. Please note that after editing rules you have to save global settings.</p> |
| Identifier | <input type="text"/> Please enter any identifier |
| Command | <input type="text"/> Please enter command (content of SMS) |
| Script | <div style="border: 1px solid gray; height: 40px;"></div> This script will be executed after receiving SMS command |
| Event action | <input type="text" value="Set HIGH state"/> on pin(s) number <div style="display: flex; gap: 10px;"> <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 </div> |

GPIO

Dzięki ustawieniom w zakładce GPIO konfiguracji www możliwa jest obsługa zewnętrznych portów wejściowych i wyjściowych GPIO. W momencie przełączenia zakładki na GPIO automatycznie wczytuje się aktualny stan portów GPIO reprezentowany przez osiem pól w górnej części strony. W całej konfiguracji przyjęto konwencję zaznaczone pole-stan wysoki, odznaczone pole-stan niski. Poprawne wczytanie stanu sygnalizuje napis „OK”, w razie błędu wyświetlany jest napis „ERROR!”. Jeżeli użytkownik chce odświeżyć stan portów, należy kliknąć przycisk *Refresh*. Pola 11,12,13,14 w sekcji *Initial States* pozwalają na ustalenie początkowego stanu wyjść. Stan początkowy jest ustalany w momencie włączania modemu oraz w przypadku zmiany i zapisania nowej konfiguracji GPIO.

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

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

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

ASTRAADA
AS30GSM200P GPRS/HSPA Router Configuration Panel

Modem HE910, 1 SIM, RS-232, firmware:140704

Device status

Basic

Local network

GSM network

Connection control

Ports configuration

TCP/IP forwarding

VLAN

Static routes

Dynamic DNS

Access control

Advanced

OpenVPN

IPsec static

IPsec mobile

IPsec authentication

N2N

CARP

NTRIP

SMS Actions

GPIO

CAN

Administration

Time

Syslog

User files

Configuration

Backup and restore

Discard changes

Save settings

GPIO

| | |
|---------------------------------|---|
| Read current GPIO states | <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input type="button" value="OK"/> <input type="button" value="Refresh"/> |
| Initial states | <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 These are initial states of GPIO pins that are set after the modem is powered on. Checked checkbox means HIGH state, unchecked means LOW state. |

GPIO events

| | |
|-------------------------|---|
| GPIO events list | <input style="width: 100%;" type="text"/> <input type="button" value="New"/> <input type="button" value="Delete"/> Please choose event you would like to edit. Please note that after editing rules you have to save global settings. |
| Identifier | <input style="width: 100%;" type="text"/> Please enter any identifier |
| Event type | <input style="width: 100%;" type="text"/> One time |
| Repeat every: | |
| Days:H:M:S | <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> |
| Execute once | Please enter UTC date/time |
| Y/M/D | <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> |
| H:M:S | <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> |
| Event action | on pin(s) number <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input style="width: 100%;" type="text"/> High state <input type="button" value="Test"/> |

Przykłady:

192.168.1.234/gpio.php?cmd=readall -Wyświetla stan wszystkich portów

192.168.1.234/gpio.php?cmd=read&pins=14 -Wyświetla stan wyjścia numer 14 (fizycznie)

192.168.1.234/gpio.php?cmd=write&pins=11,12&state=L -Ustawia stan niski na wyjściach numer 11 i 12 (fizycznie). Po poprawnym wykonaniu skryptu nic nie jest wyświetlane.

CAN

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

ASTRAADA

AS30GSM200P GPRS/HSPA Router Configuration Panel

Modem HE910, 1 SIM, RS-232, firmware:140704

CAN

| | |
|-----------------------------------|---|
| CAN bitrate | <input type="text" value="10kbit"/> |
| User bitrate | <input type="text"/> |
| Forwarding with slcanpty | |
| Service enabled | <input checked="" type="checkbox"/> Enabled |
| Interface | <input type="text" value="LAN"/> |
| Connection mode | <input type="text" value="Client"/> |
| IP address | <input type="text"/> Please enter destination IP address |
| Port | <input type="text"/> Please enter port number |
| Forwarding with socketcand | |
| Service enabled | <input checked="" type="checkbox"/> Enabled |
| Interface | <input type="text" value="LAN"/> |
| Port | <input type="text" value="1234"/> Please enter port number |

Device status

Basic

- Local network
- GSM network
- Connection control
- Ports configuration
- TCP/IP forwarding
- VLAN
- Static routes
- Dynamic DNS
- Access control

Advanced

- OpenVPN
- IPsec static
- IPsec mobile
- IPsec authentication
- N2N
- CARP
- NTRIP
- SMS Actions
- GPIO
- CAN**

Administration


- Time
- Syslog
- User files

Configuration

- Backup and restore
- Discard changes
- Save settings

Time

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

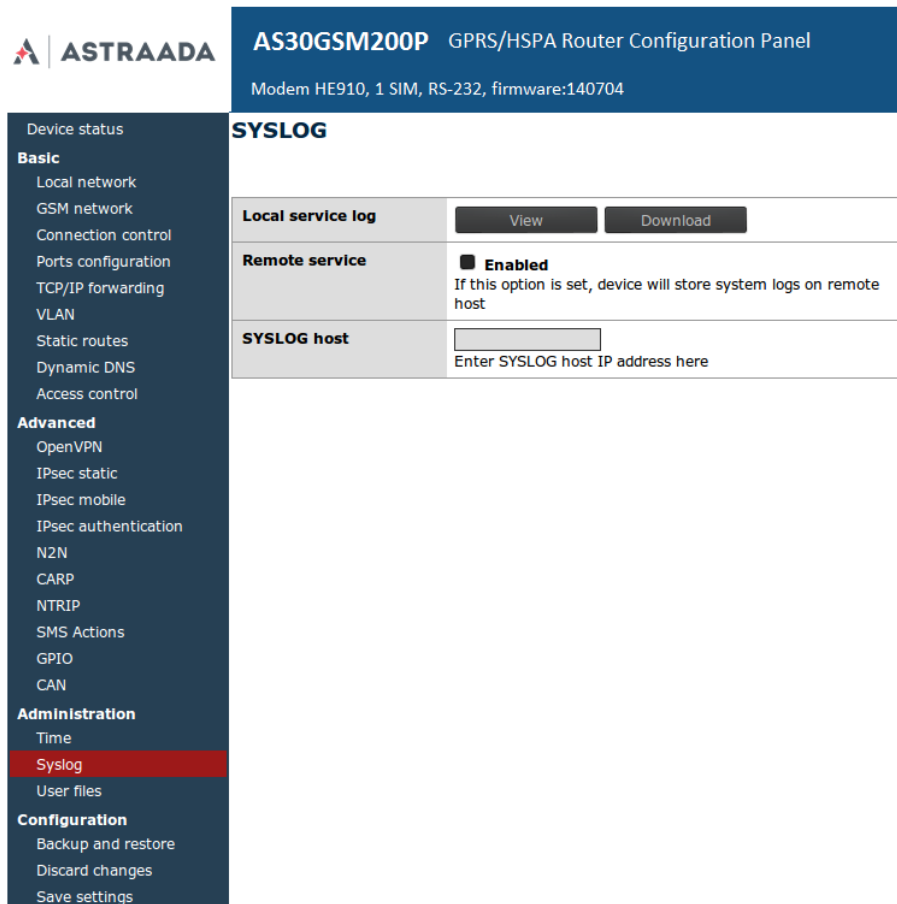


AS30GSM200P GPRS/HSPA Router Configuration Panel
Modem HE910, 1 SIM, RS-232, firmware:140704

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|-----------------------|----------------------------|------------------------------------|--|--|---|--------------------------|---|--|---|--------------------------|---|--|---|---------------------|--|---------------------|---|----------------------|---|
| Device status Basic Local network GSM network Connection control Ports configuration TCP/IP forwarding VLAN Static routes Dynamic DNS Access control Advanced OpenVPN IPsec static IPsec mobile IPsec authentication N2N CARP NTRIP SMS Actions GPIO CAN Administration Time Syslog User files Configuration Backup and restore Discard changes Save settings | <h3>NTP</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #f2f2f2;">RTC time (UTC)</td> <td>2013-09-02 08:51:02</td> </tr> <tr> <td style="background-color: #e0ffe0;">NTP Peer 1 preferred server</td> <td> <input checked="" type="checkbox"/> Enabled Set this option to enable peer 1 server querying </td> </tr> <tr> <td></td> <td> <input style="width: 100px;" type="text" value="192.168.1.2"/> Enter IP address NTP server </td> </tr> <tr> <td style="background-color: #f2f2f2;">NTP Peer 2 server</td> <td> <input type="checkbox"/> Enabled Set this option to enable peer 2 server querying </td> </tr> <tr> <td></td> <td> <input style="width: 100px;" type="text"/> Enter IP address NTP server </td> </tr> <tr> <td style="background-color: #f2f2f2;">NTP Peer 3 server</td> <td> <input type="checkbox"/> Enabled Set this option to enable peer 3 server querying </td> </tr> <tr> <td></td> <td> <input style="width: 100px;" type="text"/> Enter IP address NTP server </td> </tr> <tr> <td style="background-color: #f2f2f2;">Date (Y/M/D)</td> <td> <input style="width: 40px;" type="text" value="2013"/> <input style="width: 40px;" type="text" value="9"/> <input style="width: 40px;" type="text" value="2"/> </td> </tr> <tr> <td style="background-color: #f2f2f2;">Time (h:m:s)</td> <td> <input style="width: 40px;" type="text" value="8"/> <input style="width: 40px;" type="text" value="50"/> <input style="width: 40px;" type="text" value="48"/> </td> </tr> <tr> <td style="background-color: #f2f2f2;">Set date/time</td> <td> <input type="button" value="Set"/> Please enter date/time below and press Set button </td> </tr> </table> | RTC time (UTC) | 2013-09-02 08:51:02 | NTP Peer 1 preferred server | <input checked="" type="checkbox"/> Enabled Set this option to enable peer 1 server querying | | <input style="width: 100px;" type="text" value="192.168.1.2"/> Enter IP address NTP server | NTP Peer 2 server | <input type="checkbox"/> Enabled Set this option to enable peer 2 server querying | | <input style="width: 100px;" type="text"/> Enter IP address NTP server | NTP Peer 3 server | <input type="checkbox"/> Enabled Set this option to enable peer 3 server querying | | <input style="width: 100px;" type="text"/> Enter IP address NTP server | Date (Y/M/D) | <input style="width: 40px;" type="text" value="2013"/> <input style="width: 40px;" type="text" value="9"/> <input style="width: 40px;" type="text" value="2"/> | Time (h:m:s) | <input style="width: 40px;" type="text" value="8"/> <input style="width: 40px;" type="text" value="50"/> <input style="width: 40px;" type="text" value="48"/> | Set date/time | <input type="button" value="Set"/> Please enter date/time below and press Set button |
| RTC time (UTC) | 2013-09-02 08:51:02 | | | | | | | | | | | | | | | | | | | | |
| NTP Peer 1 preferred server | <input checked="" type="checkbox"/> Enabled Set this option to enable peer 1 server querying | | | | | | | | | | | | | | | | | | | | |
| | <input style="width: 100px;" type="text" value="192.168.1.2"/> Enter IP address NTP server | | | | | | | | | | | | | | | | | | | | |
| NTP Peer 2 server | <input type="checkbox"/> Enabled Set this option to enable peer 2 server querying | | | | | | | | | | | | | | | | | | | | |
| | <input style="width: 100px;" type="text"/> Enter IP address NTP server | | | | | | | | | | | | | | | | | | | | |
| NTP Peer 3 server | <input type="checkbox"/> Enabled Set this option to enable peer 3 server querying | | | | | | | | | | | | | | | | | | | | |
| | <input style="width: 100px;" type="text"/> Enter IP address NTP server | | | | | | | | | | | | | | | | | | | | |
| Date (Y/M/D) | <input style="width: 40px;" type="text" value="2013"/> <input style="width: 40px;" type="text" value="9"/> <input style="width: 40px;" type="text" value="2"/> | | | | | | | | | | | | | | | | | | | | |
| Time (h:m:s) | <input style="width: 40px;" type="text" value="8"/> <input style="width: 40px;" type="text" value="50"/> <input style="width: 40px;" type="text" value="48"/> | | | | | | | | | | | | | | | | | | | | |
| Set date/time | <input type="button" value="Set"/> Please enter date/time below and press Set button | | | | | | | | | | | | | | | | | | | | |

Syslog

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

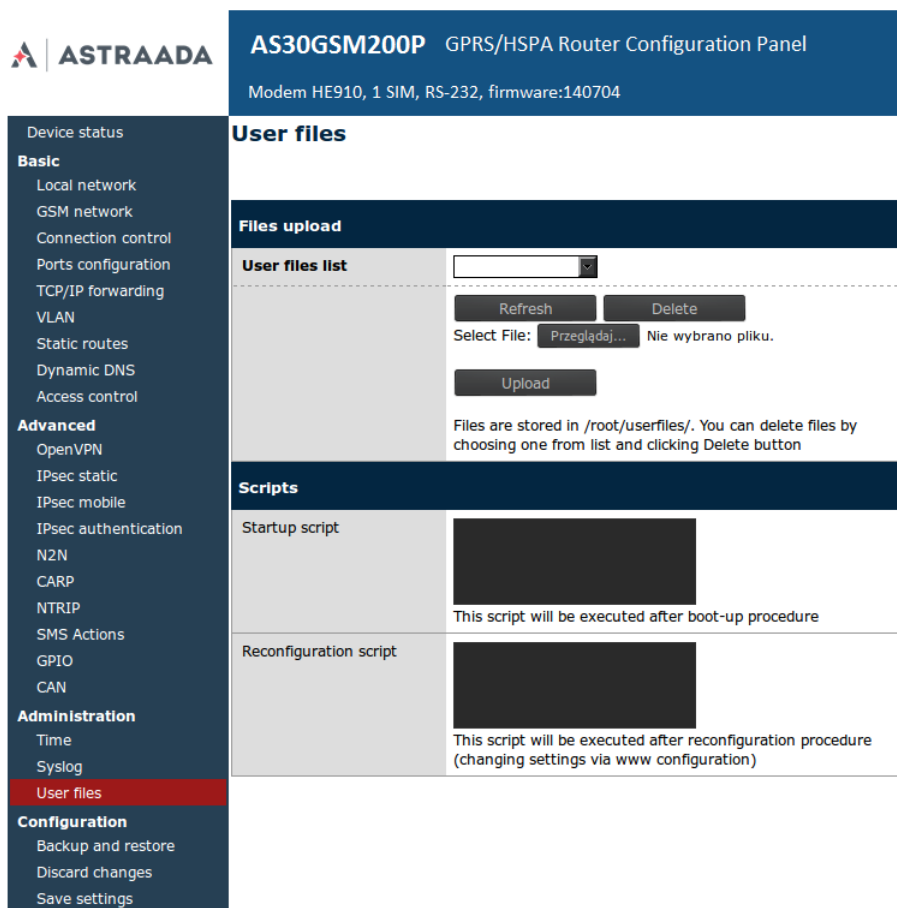


The screenshot shows the configuration panel for the AS30GSM200P router. The left sidebar contains a menu with categories: Device status, Basic, Advanced, Administration, and Configuration. The 'Syslog' option under 'Administration' is highlighted. The main content area is titled 'SYSLOG' and contains a table with three rows: 'Local service log', 'Remote service', and 'SYSLOG host'. The 'Remote service' row has a checkbox labeled 'Enabled' which is checked, and a descriptive text below it. The 'SYSLOG host' row has an input field and a label 'Enter SYSLOG host IP address here'.

| AS30GSM200P GPRS/HSPA Router Configuration Panel | |
|--|---|
| Modem HE910, 1 SIM, RS-232, firmware:140704 | |
| SYSLOG | |
| Local service log | <input type="button" value="View"/> <input type="button" value="Download"/> |
| Remote service | <input checked="" type="checkbox"/> Enabled If this option is set, device will store system logs on remote host |
| SYSLOG host | <input type="text"/> Enter SYSLOG host IP address here |

Pliki użytkownika

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



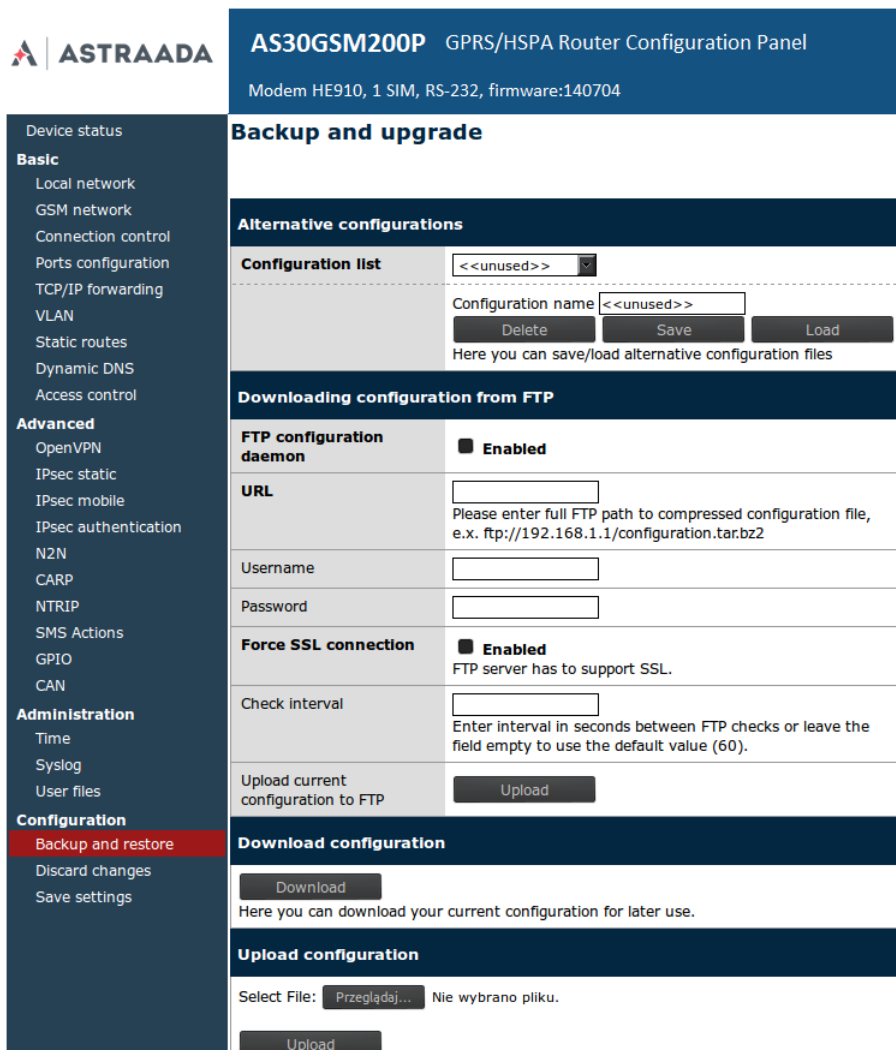
The screenshot shows the configuration panel for the AS30GSM200P router. The left sidebar contains a navigation menu with categories: Basic, Advanced, Administration, and Configuration. The 'User files' option is highlighted in red. The main content area is titled 'User files' and includes a 'Files upload' section with a 'User files list' table, a 'Refresh' button, a 'Delete' button, and an 'Upload' button. Below this is a 'Scripts' section with two rows: 'Startup script' and 'Reconfiguration script', each with a text area and a description of when the script is executed.

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

Zapisywanie/przywracanie kopii zapasowej konfiguracji modemu

Zakładka *Backup and restore* umożliwia następujące operacje:

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



The screenshot shows the configuration interface for the AS30GSM200P router. The left sidebar contains a navigation menu with categories: Device status, Basic, Advanced, Administration, and Configuration. The 'Configuration' category is expanded, and 'Backup and restore' is selected. The main content area is titled 'Backup and upgrade' and includes the following sections:

- Alternative configurations:** A 'Configuration list' dropdown menu currently shows '<<unused>>'. Below it is a 'Configuration name' input field, also showing '<<unused>>', with 'Delete', 'Save', and 'Load' buttons. A note states: 'Here you can save/load alternative configuration files'.
- Downloading configuration from FTP:**
 - FTP configuration daemon:** Enabled
 - URL:** An empty input field. A note says: 'Please enter full FTP path to compressed configuration file, e.x. ftp://192.168.1.1/configuration.tar.bz2'.
 - Username:** An empty input field.
 - Password:** An empty input field.
 - Force SSL connection:** Enabled. A note says: 'FTP server has to support SSL.'
 - Check interval:** An empty input field. A note says: 'Enter interval in seconds between FTP checks or leave the field empty to use the default value (60).'
 - Upload current configuration to FTP:** An 'Upload' button.
- Download configuration:** A 'Download' button. A note says: 'Here you can download your current configuration for later use.'
- Upload configuration:** A 'Select File:' label, a 'Przeglądaj...' button, and the text 'Nie wybrano pliku.'. Below this is an 'Upload' button.

Discard changes

Porzucenie zmian możliwe jest po wciśnięciu przycisku Discard changes.

Save settings

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

Opis logów systemowych

Poniżej znajdują się przykładowy log wraz z opisem podstawowych czynności:

```

01/01/0000:00:30 rbmtx syslogd 1.4.1: restart.
01/01/0000:00:31 rbmtx Start: RBMTX - G24 FIRM:120312 - info o modemie i firmware
01/01/0000:00:35 rbmtx supervisor[560]: SIM Holder open/closed - Kieszeń SIM zamknięta/otwara przez oprogramowanie.
01/01/0000:00:36 rbmtx supervisor[560]: Modem init 1 - pierwsza próba inicjalizacji
01/01/0000:01:09 rbmtx supervisor[560]: Init /dev/ttyS1 - inicjalizacja portu
01/01/0000:01:10 rbmtx supervisor[560]: Init /dev/ttyACM0
01/01/0000:01:13 rbmtx supervisor[560]: Modem is not registered on the GSM network - modem nie może zalogować się do sieci
01/01/0000:01:13 rbmtx supervisor[560]: Entering Modem is ready
01/01/0000:01:13 rbmtx supervisor[560]: Entering PIN OK - modem gotowy do połączenia
01/01/0000:01:13 rbmtx supervisor[560]: Entering PIN error code: - zły kod PIN
01/01/0000:01:14 rbmtx login[811]: unable to change tty `/dev/ttyS0' for user `root'
01/01/0000:01:14 rbmtx login[811]: ROOT LOGIN on `ttyS0'
01/01/0000:01:20 rbmtx pppd[901]: pppd 2.4.5 started by root, uid 0 - połączenie
01/01/0000:01:21 rbmtx chat[903]: timeout set to 2 seconds
01/01/0000:01:21 rbmtx chat[903]: send (AT)
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: AT
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (ATZ0)
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: ATZ0
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (AT)
01/01/0000:01:21 rbmtx chat[903]: abort on (NO DIALTONE)
01/01/0000:01:21 rbmtx chat[903]: abort on (ERROR)
01/01/0000:01:21 rbmtx chat[903]: abort on (NO ANSWER)
01/01/0000:01:21 rbmtx chat[903]: abort on (BUSY)
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: AT
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (ATZ0)
01/01/0000:01:21 rbmtx chat[903]: abort on (NO CARRIER)
01/01/0000:01:21 rbmtx chat[903]: timeout set to 30 seconds
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: ATZ0
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (AT)
01/01/0000:01:21 rbmtx chat[903]: expect (OK)
01/01/0000:01:21 rbmtx chat[903]: AT
01/01/0000:01:21 rbmtx chat[903]: OK
01/01/0000:01:21 rbmtx chat[903]: send (AT+CGDCONT=1,"ip","example.apn")
01/01/0000:01:22 rbmtx chat[903]: clear abort on (ERROR)
01/01/0000:01:22 rbmtx chat[903]: send (dddATD*99#)
01/01/0000:01:23 rbmtx supervisor[560]: pppd check loop:1
01/01/0000:01:25 rbmtx chat[903]: expect (CONNECT)
01/01/0000:01:25 rbmtx chat[903]: AT+CGDCONT=1,"ip","example.apn"
    
```

Aktualizacja oprogramowania

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

Do aktualizacji potrzebne są następujące pliki:

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

W celu zaktualizowania oprogramowania należy poczynić następujące kroki:

Uruchom plik upload_img.bat z parametrami: plik i adres IP

upload_img.bat upgrade_20101001.bin 192.168.1.234

- W systemie Windows (pamiętaj o znaku ":" na końcu wiersza):

```
pscp -scp -i servicekey.ppk -P 65535 service@192.168.1.234:
```

W systemie Linux:

```
scp -i service.key -P 65535 upgrade.bin service@IP:
```
- Uruchom plik

```
upgrade.bat 192.168.1.234
```

Windows OS:

```
plink -ssh -i servicekey.ppk -P 65535 service@192.168.1.234 upgrade
```

Linux OS:

```
ssh -i service.key -p 65535 service@192.168.1.234 upgrade
```
- Możesz użyć także komend reboot, delusblog, help, np. by zresetować:

```
plink -ssh -i servicekey.ppk -P 65535 service@192.168.1.234 reboot
```

Rozwiązywanie problemów

Brak połączenia/komunikacji z modemem

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

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

Modem połączony, brak połączenia z internetem

W przypadku gdy nie ma połączenia z Internetem zrób następujące:

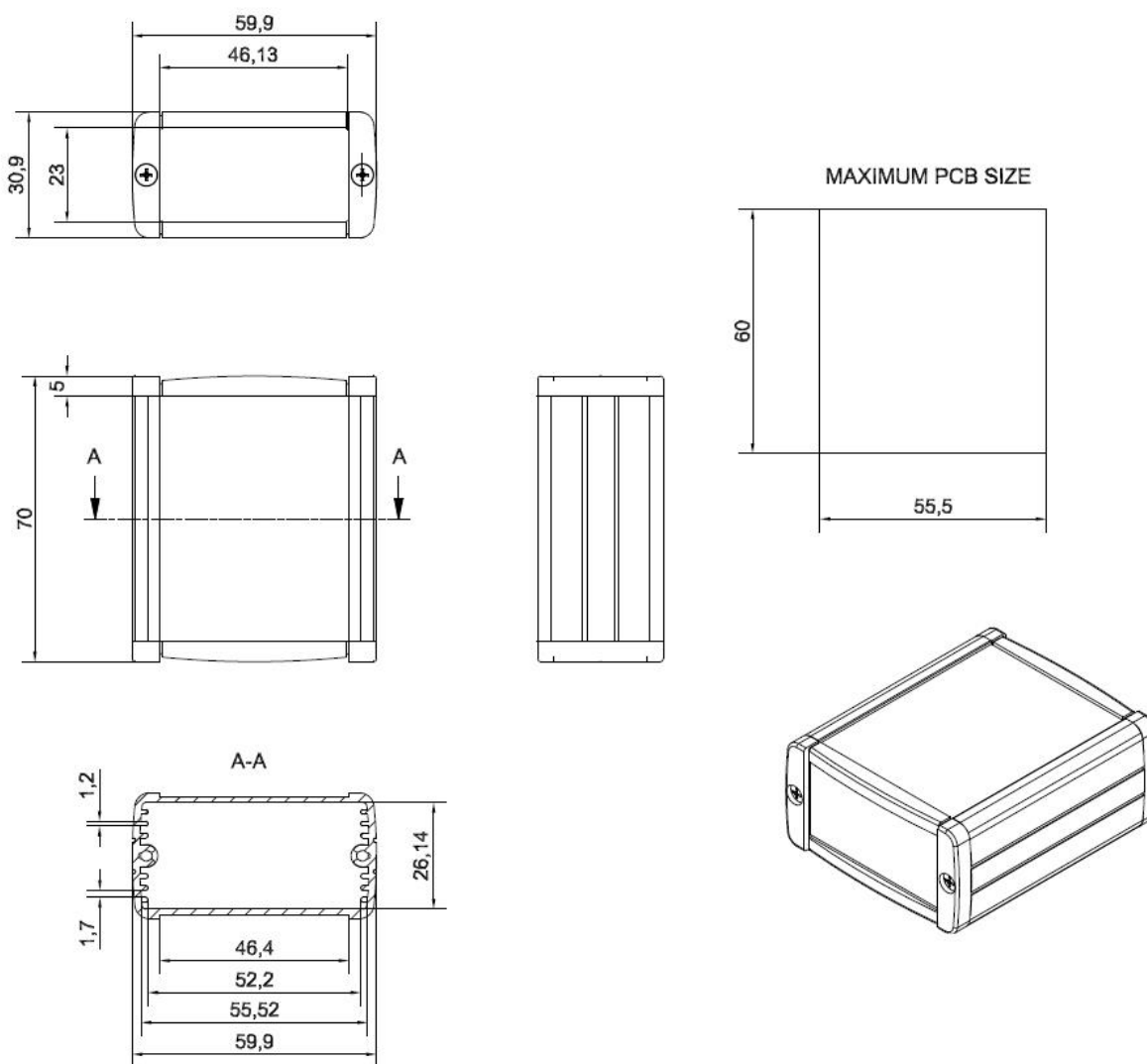
- Sprawdź podłączenie anteny
- Sprawdź zasięg sieci GPRS/EDGE/HSPA w miejscu użytkowania (np. na stronie operatora GSM)
- Sprawdź czy modem skonfigurowany jest poprawnie (parametry punktów dostępowych APN)
- W celu korzystania z internetu mobilnego należy mieć uruchomioną usługę internetu, jeżeli Twoja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

Charakterystyka techniczna

Charakterystyka mechaniczna

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

Obudowa



Charakterystyka elektroniczna

Zasilanie

- Nominalny zakres zasilania: 6-30 VDC
- Maksymalna (średnia) wartość prądu ciągłego: +800 mA max
- Pik (chwilowy), prąd: 2 A

Charakterystyki RF - Zakres częstotliwości

Zakres zależy od zamontowanego modułu głównego i wybranej sieci.

| Parametr | Przypadek | Specyfikacja |
|----------|-----------|-----------------|
| GSM 850 | TX | 824 – 849 MHz |
| | RX | 869 – 894 MHz |
| GSM 900 | TX | 880 – 915 MHz |
| | RX | 925 – 960 MHz |
| DCS 1800 | TX | 1710 – 1785 MHz |
| | RX | 1805 – 1880 MHz |
| PCS 1900 | TX | 1850 – 1910 MHz |
| | RX | 1930 – 1990 MHz |
| IMT 2100 | TX | 1920–1980 MHz |
| | RX | 2110–2170 MHz |

Charakterystyki RF - Wydajność RF

Minimalna wydajność RF przedstawiona jest w tabeli poniżej:

| Zakres | | 850/900 | 1800/1900 |
|----------|-----------|---------|-----------|
| GSM/GPRS | TRP [dBm] | 22 | 24,5 |
| | TIS [dBm] | -99 | -101,5 |
| EGPRS | TRP [dBm] | 20,5 | 19,5 |
| | TIS [dBm] | -92,5 | -93,5 |

Charakterystyki RF - Zewnętrzna antena

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

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

Antena wybrana do pracy z modemem powinna być jak najlepiej dopasowana do warunków otoczenia w którym pracuje modem. Jeżeli modem umieszczony jest w pomieszczeniu, w którym zasięg sygnału jest zbyt niski, powinna być zastosowana zewnętrzna (na zewnątrz budynku) albo

specyficzna wewnętrzna (wewnątrz pomieszczenia) antena aby zwiększyć moc odbieranego sygnału.

Charakterystyka otoczenia

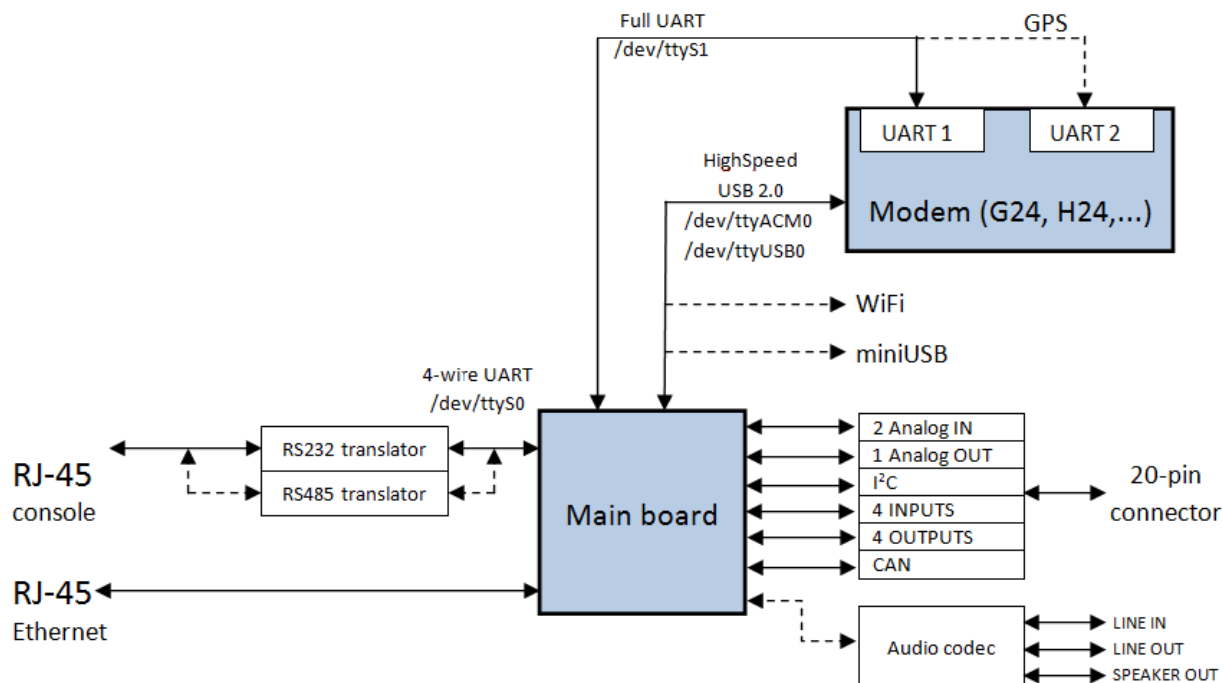
Poniższa tabela przedstawia warunki w jakich może pracować moduł

Uwaga! Przekroczenie poniższych wartości może spowodować uszkodzenie modułu.

| Parametr | Warunek | Min | Max | Unit |
|---|------------------|-----|------|------|
| Temperatura otoczenia w czasie pracy urządzenia | | -20 | 60 | °C |
| Temperatura przechowywania | | -40 | 85 | °C |
| ESD | Na złączu anteny | | | KV |
| | Połączone | | ± 6 | |
| | W powietrzu | | ± 15 | |
| | Na złączu | | ± 1 | |

Architektura

Poniższy diagram przedstawia uproszczony schemat architektury modemu AS30GSM200P. Dodatkowe funkcjonalności, dostępne jako opcja zaznaczono liniami przerywanymi.



Zalecenia dotyczące bezpieczeństwa

Ogólne bezpieczeństwo

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

Wyłącz modem GSM w następujących okolicznościach:

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

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

Eksploatacja i konserwacja

Modem AS30GSM200P jest urządzeniem elektronicznym które powinno być używane z ostrożnością. Proszę zastosować się do sugestii podanych poniżej aby Twój modem mógł działać przez wiele lat:

- Nie wystawiaj modemu na ekstremalne warunki jak wysoka temperatura lub wysoka wilgotność,
- Nie trzymaj modemu w brudnych i zakurzonych miejscach,
- Nie demontuj modemu AS30GSM200P,
- Nie wystawiaj modemu na działanie wody, deszczu czy pary,
- Nie narażaj modemu na duże wstrząsy i wibracje
- Nie umieszczaj modemu blisko urządzeń magnetycznych np. kart magnetycznych,

Akcesoria

Tabele poniżej przedstawiają akcesoria polecane do użycia z modemem Astraada AS30GSM200P.

Akcesoria niezbędne

Tabela poniżej przedstawia akcesoria krytyczne dla użytkowania modemu, bez nich praca z modemem nie jest możliwa.

| Akcesoria | Opis | Numer |
|-----------|------------|--------------|
| Zasilacz | 6V ... 30V | PS6V1500MA |
| Antena | - | ANTDBSMRMSMA |

Akcesoria dodatkowe

Tabela poniżej przedstawia akcesoria, które nie są wymagane do pracy modemu, ale mogą być bardzo użyteczne lub potrzebne.

| Akcesoria | Opis | Numer |
|-----------------------|---------------------------|------------------|
| Antena kierunkowa (1) | Antena kierunkowa GSM900 | AK 5GSM/X |
| Antena kierunkowa (2) | Antena kierunkowa GSM1900 | AK 7/DCS-UMTS/10 |
| Antena dookólna (1) | Antena dookólna | AK PN |
| Antena dookólna (2) | Antena dookólna | AK C1 |
| Kabel zasilania | - | ? |
| Kabel IO | - | ? |
| Kabel RS232/485 | - | ? |
| Mocowanie DIN | - | ? |
| Mocowanie Bur | - | ? |

Anteny kierunkowe

Używaj anten kierunkowych (wewnątrz lub na zewnątrz budynku) jeżeli sygnał odbierany przez zwykłą antenę jest zbyt niski lub bardzo niski. Antena kierunkowa może zwiększyć moc sygnału. Korzystanie z takiej anteny nie może zagwarantować wystarczającego sygnału – jest to zależne od pokrycia GSM w miejscu używania modemu. Lepiej używać anteny która pracuje w wyższej częstotliwości (GSM1900), ale zależy czy sygnał GSM1900 jest transmitowany w miejscu używania modemu/anteny – jeżeli nie użyj anteny dla niższej częstotliwości (GSM900). Jeżeli nie ma sygnału GSM żadna antena nie pomoże.

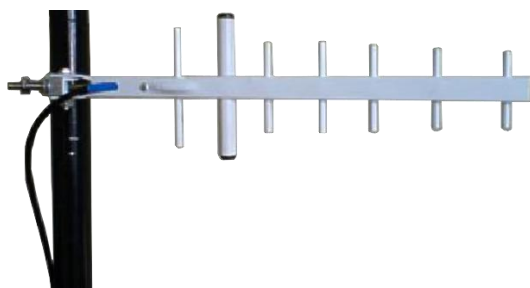


Antena kierunkowa AK 5GSM/X



Antena kierunkowa AK 7/DCS-UMTS/10

Możliwe jest że nie ma sygnału wewnątrz budynku – w tym przypadku można zamontować antenę na dachu budynku lub w pomieszczeniu gdzie sygnał jest wystarczający do poprawnego działania modemu. Antena może być zamontowana na zewnętrznym maszcie antenowym (jak pokazane na rysunku poniżej) lub w jakiś inny stabilny sposób. Wszelkie instrukcje na temat poprawnego zamontowania anteny powinny być podane przez producent danej anteny.



Jeżeli antena podłączana jest przez złącze FME (pokazane na rysunku poniżej) można zastosować konwerter FMA – SMA:



Anteny dookólne

W przypadku gdy poziom mocy odbieranego sygnału jest słaby możesz zastosować także antenę dookólną. Sygnał odbierany przez taką antenę jest słabszy niż ten odbierany przez antenę kierunkową, jednak w dużej części przypadków wystarcza on do prawidłowego odbioru. Możliwe jest zastosowanie anteny o podstawie magnetycznej lub mocowanej np. na ścianie



AK PN antena z podstawką magnetyczną



AK C1 antena mocowana na ścianie

Kabel zasilający



Kabel I/O



Kabel RS232/485



Mocowanie DIN



Mocowanie Bur



Znak towarowy

Modem AS30GSM200P spełnia wymagania zasadnicze dla urządzeń telekomunikacyjnych końcowych i radiowych nadawczych zawarte w postanowieniach Dyrektyw Rady R&TTE 1999/05/EC.



Zalecenia dotyczące bezpieczeństwa

PRZECZYTAJ UWAŻNIE

Upewnij się, że korzystanie z produktu w Twoim kraju oraz środowisku docelowym jest dozwolone. Obowiązkiem użytkownika jest zapoznanie się z przepisami kraju w którym modem będzie użytkowany oraz z przepisami regulującymi sposób jego wykorzystania. Zastosowanie tego produktu może być niebezpieczne i powinno się go unikać w następujących sytuacjach:

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

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

Zalecamy stosowanie się do instrukcji dotyczących odpowiedniego podłączenia przewodów. Produkt należy zasilć stabilizowanym napięciem oraz zadbać, aby okablowanie było dostosowane do przepisów przeciwpożarowych i bezpieczeństwa. Z produktem należy obchodzić się z rozwagą, unikać kontaktu z złączami, ponieważ elektrostatyczne wyładowania mogą uszkodzić produkt. Te same środki ostrożności należy przedsięwziąć z kartą SIM – sprawdź dokładnie instrukcje jej użytkowania. Nie wkładaj lub usuwaj karty SIM, gdy produkt jest w trybie oszczędzania energii. Integrator systemu odpowiedzialny jest za funkcjonowanie produktu końcowego; w związku z tym należy zwrócić uwagę na zewnętrzne komponenty dołączane do modułu, jak również zastosowanie w projektach lub instalacjach, ponieważ istnieje ryzyko zaburzenia pracy sieci GSM lub zewnętrznych urządzeń, lub negatywny wpływ na zabezpieczenia. W przypadku wątpliwości odnieś się do dokumentacji technicznej i obowiązujących przepisów.

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

Lista skrótów

| | |
|-------|--|
| ACM | Accumulated Call Meter |
| ASCII | American Standard Code for Information Interchange |
| AT | Attention commands |
| CB | Cell Broadcast |
| CBS | Cell Broadcasting Service |
| CCM | Call Control Meter |
| CLIP | Calling Line Identification Presentation |
| CLIR | Calling Line Identification Restriction |
| CMOS | Complementary Metal-Oxide Semiconductor |
| CR | Carriage Return |
| CSD | Circuit Switched Data |
| CTS | Clear To Send |
| DAI | Digital Audio Interface |
| DCD | Data Carrier Detected |
| DCE | Data Communications Equipment |
| DRX | Data Receive |
| DSR | Data Set Ready |
| DTA | Data Terminal Adaptor |
| DTE | Data Terminal Equipment |
| DTMF | Dual Tone Multi Frequency |
| DTR | Data Terminal Ready |
| EMC | Electromagnetic Compatibility |
| ETSI | European Telecommunications Equipment Institute |
| FTA | Full Type Approval (ETSI) |
| GPRS | General Radio Packet Service |
| GSM | Global System for Mobile communication |
| HF | Hands Free |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| IRA | Internationale Reference Alphabet |
| ITU | International Telecommunications Union |
| IWF | Inter-Working Function |
| LCD | Liquid Crystal Display |
| LED | Light Emitting Diode |
| LF | Linefeed |
| ME | Mobile Equipment |
| MMI | Man Machine Interface |
| MO | Mobile Originated |
| MS | Mobile Station |
| MT | Mobile Terminated |
| OEM | Other Equipment Manufacturer |
| PB | Phone Book |
| PDU | Protocol Data Unit |
| PH | Packet Handler |
| PIN | Personal Identity Number |
| PLMN | Public Land Mobile Network |
| PUCT | Price per Unit Currency Table |
| PUK | PIN Unblocking Code |
| RACH | Random Access Channel |
| RLP | Radio Link Protocol |

| | |
|------|---|
| RMS | Root Mean Square |
| RTS | Ready To Send |
| RI | Ring Indicator |
| SAR | Specific Absorption Rate (e.g. of the body of a person in an electromagnetic field) |
| SCA | Service Center Address |
| SIM | Subscriber Identity Module |
| SMD | Surface Mounted Device |
| SMS | Short Message Service |
| SMSC | Short Message Service Center |
| SPI | Serial Protocol Interface |
| SS | Supplementary Service |
| TIA | Telecommunications Industry Association |
| UDUB | User Determined User Busy |
| USSD | Unstructured Supplementary Service Data |

Wsparcie techniczne

Firma ASTOR zapewnia wsparcie online, które zawiera:

- Najnowszą wersję tego dokumentu
- Najnowsze sterowniki AS30GSM100P
- Wsparcie techniczne

Te i inne informacje mogą państwo znaleźć na stronie www.astor.com.pl/gsm

Aby uzyskać więcej informacji skontaktuj się z nami:

ASTOR Centrala
ul. Smoleńsk 29
31-112 Kraków

tel. 12 428 63 00

fax 12 428 63 09

e-mail: info@astor.com.pl