BIBLIOTEKA
POLSKIEGO KRÓTKOFALOWCA

27

Krzysztof Dąbrowski
OE1KDA

Poradnik Hamnetu

wydanie 2

Wiedeń 2021

Poradnik Hamnetu

Krzysztof Dąbrowski OE1KDA

Wydanie 2

Wiedeń, październik 2021

Spis treści

Sommaire
Ouvrage pratique de Hamnet

Wstęp do wydania 1

Sieć „Hamnetu" jest radiową siecią amatorską opartą na technologii internetowej – zestawie protokółów TCP/IP. Pracuje ona jednak w pełni niezależnie od ogólnie dostępnego Internetu i nie zapewnia dostępu do niego i nie ma go również zastępować. Jest więc ona zasadniczo krótkofalarskim Intranetem. Nie korzysta ona także pomocniczo z łączy internetowych a pracuje niezależnie korzystając jedynie z łączy radiowych działających w pasmach amatorskich: obecnie są to pasma 13 i 6 cm. W wyjątkowych przypadkach możliwa jest jednostronna i ściśle ograniczona transmisja danych np. przekazywanie odebranych komunikatów APRS do znanych powszechnie serwerów internetowych (APRS-IS).
Możliwości sieci i zasady jej pracy są szczegółowo opisane w pierwszej części tomu 22, dlatego też pomijamy te tematy w tomie obecnym. Jest on poświęcony w przeważającej części stronie praktycznej: niezbędnemu wyposażeniu stacji, połączeniom poszczególnych składowych w funkcjonującą całość, niezbędnemu oprogramowaniu i oczywiście ich konfiguracji. Dzięki temu, że publicznie dostępne pasma radiowe wykorzystywane w bezprzewodowych sieciach komputerowych WLAN pokrywają się częściowo z pasmami amatorskimi 2,4, 3,4 i 5,6 GHz krótkofalowcy mogą wykorzystywać powszechnie dostępne wyposażenie dla tych sieci, nie będąc jednocześnie skrępowanymi przepisami ograniczającymi np. moc wyjściową jak to ma miejsce w sieciach powszechnego użytku (pod warunkiem, że częstotliwości pracy znajdują się w granicach pasm amatorskich). Obecnie w większości krajów wykorzystywane są pasma 2,4 (standardy 802.11b/g/n) i 5,6 GHz (standardy 802.11a/n) ale tam gdzie dostępne jest pasmo 3,4 GHz mogłoby być również używane. Dodatkowo dzięki masowej produkcji sprzęt ten jest dostępny po stosunkowo korzystnych cenach.
Krótkofalowcy w wielu krajach, w tym również i w Polsce eksperymentują z wykorzystaniem kolejnych modeli sprzętu, dostosowują jego oprogramowanie do potrzeb amatorskich, instalują kolejne przemienniki (lub inaczej mówiąc punkty albo węzły dostępowe). Należy więc w najbliższym czasie spodziewać się dynamicznego rozwoju „Hamnetu" w całej Europie. Dzięki niezależności od sieci publicznych i autonomicznemu zasilaniu wielu stacji przemiennikowych nasza sieć może być wykorzystywana nie tylko w zwykłych łącznościach krótkofalarskich ale także w łącznościach ratunkowych i w przypadku katastrof żywiołowych, których oby było jak najmniej.
Przed podjęciem decyzji o zakupie wyposażenia dobrze jest zorientować się w stopniu rozbudowy sieci w najbliższej okolicy, w planach na przyszłość i upewnić się, że trasy połączenia z najbliższymi przemiennikam „Hamnetu" nie są zasłonięte przez przeszkody w rodzaju wysokich budynków, wysokich drzew, wzgórz itp. Mikrofale jak wiadomo rozchodzą się po liniach prostych dlatego też wymienione lub podobne przeszkody mogą uniemożliwić połączenie z przemiennikiem „Hamnetu". W niektórych przypadkach możliwe są także łączności za pośrednictwem odbić, ale sprawa ta wymaga w każdej sytuacji dokładniejszego zbadania. W odróżnieniu od krótkich łączności np. w zawodach, kiedy chodzi jedynie o wymianę prostych raportów (i które w obecności szumów lub innych utrudnień można powtarzać wielokrotnie) skuteczna transmisja danych wymaga zapewnienia dostatecznej siły sygnału i dostatecznego odstępu od poziomu szumów przez cały czas.
Sieć „Hamnetu" pozwala oprócz łączności głosowych i pisemnych także na rozpowszechnianie zdjęć i obrazów telewizyjnych, komunikatów APRS itd. – dodatkowo do takiej oczywistej funkcji jak dostęp do witryn WWW. W kolejnych rozdzialach skryptu przedstawiono przykłady dostępu do różnorakich usług Hamnetowych. Nie oznacza to jednak, że są one wszędzie dostępne w pełnym zestawie. Przed zainstalowaniem odpowiednich programów i skonfigurowaniem i rozpoczęciem prób dostępu należy poinformować się, które z nich są aktualnie dostępne, a jak wygladają plany rozbudowy w najbliższej przyszłości.
Ze względu na to, że krajowa sieć „Hamnetu" znajduje się dopiero w początkowym stadium rozbudowy w skrypcie przytoczono szereg przykładów ze sceny austriackiej. Mogą one w przyszłości ułatwić konfigurację programów u użytkowników indywidualnych dzięki wyjaśnieniu znaczenia najważniejszych parametrów, a także stanowić inspirację w dalszej rozbudowie sieci i dostępnych usług hamnetowych w kraju.
Adresy IP (w Polsce seria 44.165.x.x) używane w sieci są administrowane przez krótkofalowców, nie ma też również żadnych blokad kanałów logicznych (ang. *port*), zapór przeciwwłamaniowych (ang. *firewall*) ani innych przeszkód technicznych. W sieci dopuszczalne są jedynie treści dozwolone w łącznościach amatorskich, bez reklam i treści komercyjnych.

Podobnie jak wiele poprzednich skryptów z tej serii również i obecny jest przeznaczony w pierwszym rzędzie dla szerokiego grona użytkowników i potencjalnych użytkowników systemu.
Koledzy zajmujący się uruchamianiem sieci i jej rozwojem mają z pewnością wystarczająco dużą wiedzę w tej dziedzinie i pewnie zawartość skryptu mniej im się przyda.
Korzystając z dobrodziejstw „Hamnetu" pamiętajmy jednak, że jest to sieć budowana i utrzymywana przez krótkofalowców i niemal w całości z ich prywatnych środków i nie oczekujmy prawie 100 % dyspozycyjności jak w przypadku Internetu publicznego. Porównując środki stojące do dyspozycji na budowę i utrzymanie sieci publicznych ze środkami, którymi dysponują krótkofalowcy można naszym sieciom D-Starowym, DMR, Echolinku, Hamnetu itd. wystawić ocenę bardzo dobrą z plusem.

Krzysztof Dąbrowski OE1KDA
Wiedeń
lipiec 2015

Wstęp do wydania 2

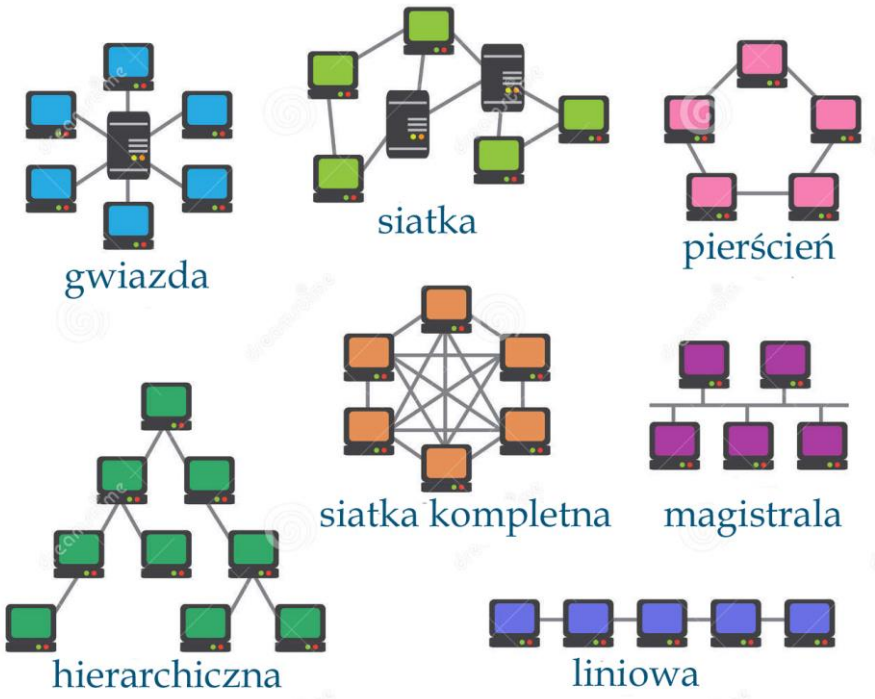
Drugie wydanie skryptu poświęconego krótkofalarskiej sieci *Hamnetu* zostało uzupełnione o tematy nie poruszone w pierwszym, takie jak telefonia hamnetowa SIP i wykorzystanie sieci w łącznościach kryzysowych. Jednocześnie uwzględniono zmiany wynikłe z postępu technicznego, zmieniającej się oferty sprzętu i oprogramowania oraz nowe (w stosunku do poprzedniego) koncepty krótkofalarskie jak modemy dostępowe dla niższych pasm albo połączenia telefoniczne SIP z siecią DMR.
Dostęp do Hamnetu w pasmach mikrofalowych nie jest niestety możliwy w wielu miejscach, dlatego też od kilku lat prowadzone są prace na wejściami w pasmach 70 cm do 6 m. Szybkości transmisji są oczywiście niższe aniżeli na mikrofalach i wystarczają jedynie do korzystania z części usług, ale za to rokują korzyści wynikające ze zwiększonego zwiększonego zasięgu. W użyciu znajdzie się m.in. standard IEEE 802.22 (WRAN). Oprócz niego do użytku wchodą nowe rozwiązania jak norma IEEE 802.11af.
Hamnet pozostaje w dalszym ciągu siecią amatorską, nie mającą zastępować Internetu i nie oferować dostępu do niego, a zwłaszcza do treści normalnych w Internecie, ale nie dopuszczalnych w krótkofalarstwie, jak wszystkie informacje komercyjne, reklamy, sklepy internetowe itp. nawet gdyby ich oferta była skierowana do krótkofalowców.

Krzysztof Dąbrowski OE1KDA
Wiedeń
19 października 2021

1. Wyposażenie stacji

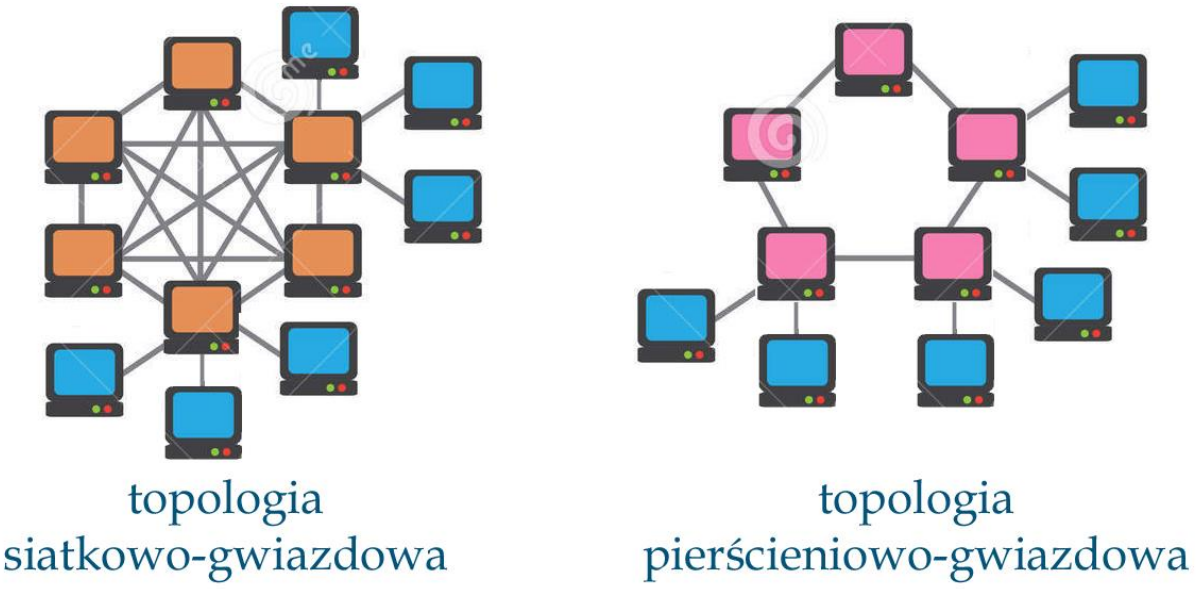
1.1. Sieci

Sieć komputerowa jest systemem wzajemnie powiązanych stacji roboczych, urządzeń peryferyjnych i innych urządzeń albo też mówiąc inaczej zbiorem komputerów połączonych siecią komunikacyjną. Jej celem jest zapewnienie bezpiecznej efektywnej i swobodnej komunikacji. W miarę rozwoju sieci komputerowych konieczne było opracowanie standardów zapewniających kompatybilność sprzętową i programową. Rozróżniane są następujące najważniejsze typy sieci: sieci obszerne WAN (ang. *Wide Area Network*) łączące ośrodki na dużych odległościach, sieci obejmujące duże ośrodki miejskie MAN (ang. *Metropolitan Area Network*), WRAN (ang. *Wide Range Area Network*), lokalne sieci w ramach dużych ośrodków o urządzeniach zlokalizowanych w odleglościach do kilkuset metrów LAN (ang. *Local Area Network*) oraz sieci urządzeń znajdujących sie w nieznacznych odległościach (do kilkunastu lub kilkudziesięciu metrów) PAN (ang. *Private Area Network*). Popularnie na określenie tych ostatnich jest używana również nazwa LAN.
Ze względu na typ transmisji sieci można podzielić na następujące rodzaje:
– sieć kolizyjna, w której poszczególne węzły przed rozpoczęciem nadawania sprawadzają czy kanał (linia) jest wolny i rozpoczynają nadawanie. Możliwe jest jednak wystąpienie kolizji pakietów. Przykładami mogą być Ethernet (802.3), AX.25 lub WiFi (802.11).
– sieć typu krążącego żetonu – buławy – (ang. *Token Ring*), w której węzły otrzymują zezwolenie na nadwanie po odebraniu żetonu (buławy) od czynnego poprzednio. Po zakończeniu transmisji żeton jest przekazywany dalej.
– sieć z wykorzystaniem szczelin czasowych (ang. *slot*), w której każde urządzenie ma przydzielony czas nadawania. Przykładami mogą być sieci GSM, WiMAX (802.16).
Topologia sieci oznacza jej fizyczną konstrukcję i sposób połączenia poszczególnych urządzeń.



Rys. 1.1.1. Podstawowe topologie sieci komputerowych. W topologii gwiazdy rozgałęzionej węzły końcowe gwiazdy zwykłej są środkami gwiazd podporządkowanych lub węzłem początkowym sieci hierarchicznej, węzły w topologii siatki lub pierścienia mogą być również środkami podporządkowanych gwiazd lub sieci hierarchicznych. Można więc łatwo wyobrazić sobie szereg topologii kombinowanych (źródło: *fr.dreanstime.com*)

Rozróżniane są następujące topologie:
– magistrala (ang. *bus*), w której wszystkie urządzenia są podłączone do jednego wspólnego kanału fizycznego, zwykle kabla;
– pierścień (ang. *loop*), w którym wszystkie urządzenia są połączone z dwoma sąsiadami i całość tworzy zamknięty krąg; w transmisji węzły przekazują sobie kolejno żeton (buławę) i każdy z nich pełni też funkcję regeneratora sygnału;
– podwójny pierścień, różni się od rozwiązania poprzedniego jedynie tym, że urządzenia są połączone podwójnymi łączami; awaria jednego urządzenia nie przerywa działania sieci; topologia jest stosowana m.in. w budowie sieci szkieletowych i miejskich;
– gwiazda (ang. *star*), jest topologia podstawową w sieciach komputerowych i polega na tym, że wszystkie urządzenia są połączone ze sobą w jednym wspólnym punkcie, którym może być serwer nadrzędny; jest ona spotykana m.in. w krajowych sieciach DMR gdzie stacje przemiennikowe lub użytkowniką są podłączone do krajowego serwera (ang. *master*) BM albo IPSC2, dla prywatnych mikroprzemienników (ang. *hotspot*) zainstalowane są oddzielne serwery; topologia gwiazdowa jest stosowana rownież w sieci Hamnetu dla stacji skupionych wokół lokalnego węzła (przemiennika; ang. *node*); awaria punktu centralnego (koncentratora) może sparaliżować całą sieć; awaria każdego z pozostałych węzłów nie wpływa na resztę sieci;
– rozszerzona gwiazda, rozgałęziona gwiazda, topologia rozszerzonej gwiazdy polega na połączeniu poszczególnych sieci gwiaździstych ze wspólnym ponktem centralnym w gwiazdę nadrzędną.
– hierarchiczna, topologia podobna do rozszerzonej gwiazdy, ewentualnie z większą liczbą stopni hierarchii; każdy z punktów centralnych steruje dostępem do sieci dla urządzeń podległych;
– siatka (ang. *mesh*), w typowej dla sieci miejskich lub rozległych topologii siatki każde z urządzeń jest połączone z więcej niż jednym urządzeniem, w przypadkach szczególnych nawet ze wszystkimi pozostałymi, zapewnia to redundantność połączeń i wysoką odporność na awarie łączy i urządzeń; topologia spotykana m.in. w połączeniach między serwerami sieci DMR albo w Hamnecie na obszarach pozostających poza zasięgiem stacji węzłowych.



Rys. 1.1.2. Przykłady topologii kombinowanych

Wymianę danych w sieciach regulują protokóły transmisji. Są to zbiory reguł definiujących procesy komunikacji urządzeń zarówno pomiędzy warstwami równoległymi w modelu komunikacji jak i pomiędzy warstwami sąsiadującymi. Są to więc swego rodzaju kodeksy drogowe dla danych. Określają one budowę sieci fizycznej, sposoby łączenia komputerów z siecią, sposoby formatowania danych do transmisji, sposoby ich wysyłania i sposoby reakcji na błędy i przekłamania. W związku z rozpowszechnieniem Internetu do najczęściej stosowanych należy grupa (rodzina) protokółów TCP/IP (ang. *TCP/IP Stack*).

1.1.1 Protokóły TCP/IP

Grupa protokołów TCP/IP jest podzielona na warstwy podobnie jak w przypadku modelu komunikacyjnego OSI (ISO). Mimo opracowania jej niezależnie od wspomnianego modelu możliwe jest łatwe przyporządkowanie poszczególnych protokółów odpowiednim warstwom OSI (ISO) lub ich grupom (tabela 1.1.1.1) Organizacja warstwowa oznacza, że poszczególne warstwy (usługi, moduły programów) wyższe komunikują się z warstwami podległymi przekazując rozkazy i odbierając dane, a każda z nich jest odpowiedzialna za pewien zespół zadań, jak przekodowywanie i grupowanie danych, wybór trasy połączenia (trasowanie), transmisja danych na łączu fizycznym lub sprawdzanie jej poprawności. Każda z warstw, to jest każdy z protokółów otrzymuje od warstwy niższej informacje we właściwym dla niej formacie i porządku, a wszelkie akcje podejmowane przez warstwy niższe są dla niej niewidoczne (ukryte). Umożliwia to wymienność protokółów w ramach systemu i udoskonalanie ich działania.
Warstwowy model rodziny protokółów TCP/IP ogranicza się do (wyróżnionych w tabeli kolorami) warstw: zastosowań (aplikacji) – odpowiadającej warstwom 5 –7, warstwy transportowej odpowiadającej warstwie 4, warstwy internetowej odpowiadającej warstwie 3 i warstwy dostępu do sieci równoważnej warstwom 1 – 2 ISO. Model ten jest obecnie podstawowym modelem komunikacji w sieciach lokalnych i w Internecie.
W sieciach TCP/IP dane są transmitowane w postaci datagramów, czyli bloków zawierających oprócz informacji użytecznej także wiadomości służbowe pozwalające na prawidłową transmisję bloku przez sieć do adresata i ponowne złożenie ich w całość W zależności od sposobów transmisji datagramy mogą być dzielone na mniejsze jednostki – pakiety AX.25 lub ethernetowe – i uzupełniane o dodatkowe informaje niezbędne dla ich prawidłowego przekazania. Informacje te, zawarte w nagłówkach pakietów są następnie usuwane po stronie odbiorczej, a pakiety są składane w datagramy. Informacje użytkowe i administracyjne przekazane przez warstwy wyższe nie ulegają zmianom i są dostępne dla odpowiednich warstw po stronie przeciwnej.

Tabela 1.1.1.1
Układ warstw TCP/IP na tle modelu ISO (OSI)

<table>
<tr><th>Model OSI (ISO)</th><th colspan="4">Protokóły TCP/IP</th></tr>
<tr><td rowspan="3">7. Warstwa zastosowań</td><td colspan="4">Warstwa zastosowań</td></tr>
<tr><td rowspan="3">Telnet, RLOGIN, RSH, REXEC</td><td rowspan="3">DNS (ang. Dynamic Name System), DHCP (ang. Dynamic Host Configuration Protocol)</td><td rowspan="3">HTTP, HTTPS</td><td rowspan="3">FTP (ang. File Transfer Protocol), SMTP (ang. Simple Mail Transfer Protocol), POP3 (ang. Post Office Protocol)</td></tr>
<tr><td>6. Warstwa prezentacji</td></tr>
<tr><td>5. Warstwa posiedzenia (sesji)</td></tr>
<tr><td rowspan="2">4. Warstwa transportu</td><td colspan="4">Warstwa transportu</td></tr>
<tr><td>TCP</td><td>SCTP</td><td>UDP</td><td>UDP-Lite</td></tr>
<tr><td rowspan="2">3. Warstwa sieciowa3</td><td colspan="4">Wartswwa internetu</td></tr>
<tr><td>IP, IPsec</td><td>ARP</td><td>ICMP</td><td></td></tr>
<tr><td rowspan="2">2. Warstwa przęsła (łącza danych)</td><td colspan="4">Warstwa dostępu do sieci</td></tr>
<tr><td rowspan="2">AX.25</td><td rowspan="2">X.25, Ethernet (IEEE 802.3), IEEE802.11 (WLAN)</td><td rowspan="2">PPP, MAC (ang. Media Access Protocol)</td><td rowspan="2">SLIP, CSLIP</td></tr>
<tr><td>1. Warstwa fizyczna</td></tr>
</table>

Uwagi:
– Siedmiowarstwowy model OSI (ISO/IEC7498-1:1994) można uzupełnić o warstwę ósmą do której zalicza się użytkowników i urządzenia wykorzystywane bezpośrednio przez nich, lub też w innym ujęciu o warstwę finansową, a do warstwy 9 (politycznej) zalicza się m.in. ogólną sytuację polityczną,
– Warstwa zastosowań jest także nazywana warstwą aplikacji,
– W tabeli podano tylko niektóre najważniejsze protokóły TCP/IP.

Transmitowany strumień danych – stanowiący zawartość wybranego pliku lub dokumentu i przekazany przez protokóły wyższych warstw – jest dzielony przez protokół TCP (ang. *Transmission Control Protocol*) na segmenty (datagramy) o określonej długości (np. 500 oktetów; często stosowane są długości 1500, 1000 lub 576 oktetów, długość ta może być również negocjowana w momencie nawiązania połączenia, przy czym każdy z datagramów jest uzupełniany o nagłówek zawierający numer kanału logicznego (ang. *port*) nadawcy i adresata, numer potwierdzenia i sumę kontrolną. Długość nagłówka wynosi dwadzieścia oktetów. Jednostką tutaj używaną jest oktet mający długość ośmiu bitów podobnie jak bajt, jednak dla uniknięcia nieporozumień we współpracy komputerów o różnej szerokości słowa i dla podkreślenia uniwersalności systemu nie stosuje się terminu bajt. Datagramy odebrane prawidłowo są kwitowane przez odbiorcę (a raczej przez protokół TCP po jego stronie), odebrane błędnie lub nieodebrane (niepokwitowane) są powtarzane po pewnym czasie. Dla przyspieszenia transmisji dopuszczalne jest nadawanie dalszych datagramów jeszcze przed otrzymaniem pokwitowania, pod warunkiem nieprzekroczenia dopuszczalnej liczby nie pokwitowanych datagramów. Liczba ta nie jest stała, lecz zależna od pojemności i zapełnienia buforów po stronie odbiorczej i jest każdorazowo sygnalizowana nadawcy. Wybór długości datagramu wpływa na efektywną szybkość transmisji, ponieważ krótsze datagramy zawierają procentowo więcej danych administracyjnych i wymagają częstszych pokwitowań, jednocześnie dłuższe datagramy są bardziej narażone na przekłamania w wyniku zakłóceń.
Tak utworzone datagramy protokół TCP przekazuje warstwie trzeciej – protokółowi IP (ang. *Internet Protocol*) z podaniem adresu numerycznego stacji docelowej. Zadaniem protokółu IP jest wybór odpowiedniej trasy transmisji i nie musi on analizować treści otrzymanego datagramu. Protokół IP umieszcza na początku każdego datagramu swój własny nagłówek zawierający adresy internetowe nadawcy i adresata, informację o protokóle warstwy wyższej (nie musi być to jedynie protokół TCP) oraz własną sumę kontrolną dla sprawdzania poprawności odbieranego nagłówka. Nagłówek IP zawiera między innymi pole określające maksymalną liczbę retransmisji datagramu w sieci i zmniejszaną o jeden po każej retransmisji. Zapobiega to nieograniczonemu krążeniu datagramu w przypadku zapętlenia się tras łączności, czego w bardziej rozbudowanych sieciach nie sposób uniknąć. Pole to nazwane jest TTL (ang. *Time To Live*). Datagramy o zerowym stanie licznika TTL są usuwane z sieci – tzn. nie są dalej retransmitowane. Rozróżniane są trasy statyczne wprowadzone przez operatora i dynamiczne wprowadzane przez system w oparciu o obserwacje sieci i jakości połączeń.
Wybór tras retransmisji jest dokonywany na bieżąco, tzn. każda ze stacji węzłowych na trasie rozstrzyga po otrzymaniu datagramu i po przeanalizowaniu adresu docelowego o tym, do której stacji sąsiadujących (logicznie) należy go skierować. Decyzja jest podejmowana częściowo w oparciu o wymieniane automatycznie informacje o jakości i obciążeniu łączy. Oznacza to, że trasa połączenia może ulegać wielokrotnym i niezauważalnym przez użytkownika zmianom w trakcie trwania sesji łączności. Jedną z konsekwencji tego faktu jest przemieszanie kolejności datagramów u odbiorcy (przykładowo datagramy nadane później docierają korzystniejszą trasą przed niektórymi nadanymi wcześniej). Uporządkowanie kolejności datagramów należy do zadań protokółu TCP.
Warstwa IP przekazuje datagramy uzupełnione o swoje nagłówki warstwie drugiej. W zależności od stosowanego w sieci sposobu transmisji danych warstwa druga może odpowiadać protokółowi ethernetowemu (X.25), AX.25 lub innym. Warstwa ta stosuje własny system adresów różny od adresów internetowych. W przypadku Ethernetu są to 48-bitowe adresy MAC znormalizowane w skali światowej, a w przypadku protokółu AX.25 są to również jednoznaczne znaki wywoławcze stacji. Protokół warstwy drugiej uzupełnia nadawane datagramy o swój własny nagłówek zawierający specyficzne adresy sprzętowe (np. znaki wywoławcze stacji albo adresy MAC) i kod warstwy wyższej oznaczający używany przez nią protokół oraz ewentualnie typ pakietu. Na końcu pakietu dołączana jest suma kontrolna. W zależności od wybranych parametrów datagramy są dzielone po stronie nadawczej na pakiety o mniejszej długości i składane z tych pakietów u adresata.
Po stronie adresata pakiety, a następnie złożone z ich zawartości datagramy są przekazywane kolejnym warstwom wyższym, przy czym każda z warstw analizuje swój nagłówek w celu wykrycia ewentualnych przekłamań, a następnie usuwa go. Każda z warstw otrzymuje więc datagram w postaci identycznej z nadaną przez odpowiednią warstwę nadawczą.
Podsumowując przebieg komunikacji: protokóły warstwy 5 – 7 przekazują w dół hierarchii dane, z których na poziomie warstwy 4 tworzone są segmenty lub datagramy, na poziomie warstwy 3 pakiety,

na poziomie drugiej – ramki, transmisja w warstwie fizycznej odbywa się bitowo, a po stronie odbiorczej cały proces przebiega odwrotnie.
Warstwa druga przekazuje pakiety do transmisji przez łącze radiowe lub kablowe korzystając przykładowo z protokółu SLIP (ang. *Serial Line Interface Protocol*), PPP (ang. *Point to Point Protocol*) lub innych. W komunikacji z modemami TNC w połączeniach AX.25 może być to przykładowo protokół KISS (ang. *Keep It Simply Stupid*)[1].
Grupa protokółów TCP/IP pozwala na jednoczesne nawiązanie kontaktu w większej liczbie kanałów logicznych (np. jednoczesną transmisję plików przy użyciu protokółu FTP i wymianę poczty elektronicznej). Każdy z tych protokółów jest nadrzędny w stosunku do TCP, odpowiada więc grupie warstw 5 – 7 modelu ISO-OSI. Jednoznaczne przyporządkowanie datagramów do poszczególnych zadań (usług) wymaga zaopatrzenia ich w numer wykorzytywanego kanału logicznego TCP. Jest to swego rodzaju adres usługi na fizycznym sewerze, który może równolegle oferować więcej z nich (można by wyobrazić sobie tą sytuację przez analogię do urzędu, w którym w zależności od rodzaju sprawy petent musi się udać do właściwego okienka lub pokoju, ale w tym samym gmachu). Datagramy zawierają wprawdzie numery kanałów nadawcy i adresata, dla stacji docelowej znaczenie ma jedynie numer kanału u adresata. Numery kanałów logicznych leżą w zakresie 0 – 65535, z tym, że znacznie pierwszych 1023 zostało standardowo określone, a z pozostałych można korzystać dowolnie w miarę potrzeb, chociaż niektóre stały się już praktycznie standardem j.np. kanał 8080.

Tabela 1.1.1.2
Funkcje najważniejszych protokółów z rodziny TCP/IP

Protokół	Znaczenie
HTTP (ang. *Hypertext Transfer Protocol*)	Udostępnianie stron www
HTTPS	Zabezpieczony dostęp do stron www
TELNET (RLOGIN)	Zdalny dostęp do systemów w sieci
RSH	Zdalne wywoływanie programów na komputerach w sieci
REXEC	
SSH (ang. *Secure Shell*)	Zabezpieczony zdalny dostęp do systemów
SMTP (ang. *Simple Mail Transfer Protocol*)	Transmisja poczty elektronicznej, SMTP w kierunku serwera, POP3 – odbieranie z serwera
POP3 (ang. *Post Office Protocol*)	
FTP (ang. *File Transfer Protocol*)	Transmisja plików, uwzględnia prawa dostępu
TFTP (ang. *Trivial File Transfer Protocol*)	Transmisja plików, nie wyposażony w mechanizmy kontroli dostępu
TCP (ang. *Transmission Control Protocol*)	Podział na datagramy i ich transmisja zabezpieczona przed przekłamaniami w ramach połączenie między korespondentami
UDP (ang. *Used Datagram Protocol*)	Niezabezpieczona (bezpołączeniowa) transmisja datagramów, rozgłaszanie, transmisja strumieni danych fonicznych, wizyjnych itp.
UDP-Lite	
NTP (ang. *Network Time Protocol*)	Protokół synchronizacji czasu
SCTP (ang. *Strean Control Transmission Protocol*)	Protokół stosowany w transmisji strumieni danych
IP (ang. *Internet Protocol*)	Wybór tras transmisji w sieci (trasowanie)
IPsec	Protkół IP z zabezpieczeniami
RIP (ang. *Routing Information Protocol*)	Protokół automatycznego wyboru tras transmisji w sieci
OSPF (ang. *Open Shortest Path First*)	Korzystanie priorytetowo z najkrótszej trasy

[1] Być może jakaś odmiana takiego protokółu znalazłaby zastosowanie w rozmowach z różnymi politykami

ICMP (ang. *Internet Control Message Protocol*)	Sprawdzenie „drożności” połączenia z dowolnym uczestnikiem w sieci, polecenie *ping*
DHCP (ang. *Dynamic Host Configuration Protocol*)	Protokół służący do przyznawania adresów IP w sieci, adresy przyznawane automatycznie są adresami dynamicznymi. Operator może jednak wprowadzić adresy statyczne – stałe i niezależne od dynamicznych
DNS (ang. *Domain Name Service*)	Protokół poszukiwania powiązań nazw komputerów (węzłów) w sieci z adresami IP
ARP (ang. *Address Resolution Protocol*)	Protokół poszukiwania powiązań adresów IP z fizycznymi adresami sprzętu, np. 48-bitowymi jednoznacznymi w skali światowej adresami sprzętowymi MAC (ang. *Media Access Control*) albo znakami wywoławczymi stacji amatorskich AX.25
SNMP (ang. *Simple Network Management Protocol*)	Protokół ułatwiający wymianę informacji służbowych związanych z zarządzaniem siecią. Jest często używany do zbierania informacji statystycznych z punktów dostępowych, komutatorów, bramek i innych skladników sieci
SLIP (ang. *Serial Line Internet Protocol*)	Protokóły warstwy 2 ISO (OSI); warstwy dostępu do sieci w modelu TCP/IP. PPP – protokół używany w łączach szeregowych zapewniający powiązanie z siecią IP
CSLIP (ang. *Compressed Serial Line Internet Protocol*)	
PPP (ang. *Point to Point Protocol*)	
X.25	
AX.25	

Tabela 1.1.1.3
Najważniejsze standardowe kanały logiczne TCP (ang. *well known ports*)

Numer kanału	Znaczenie
20	Kanał danych FTP
21	Kanał sterowania FTP
22	Kanał protokółu SSH
23	Kanał Telnetu
25	Protokół pocztowy SMTP
53	Serwer DNS
67	Serwer DHCP
68	Klient DHCP
80	HTTP
110	Protokół pocztowy POP3
123	Protokół synchronizacji czasu NTP
143	Protokół wymiany informacji IMAP
179	Protokół trasowania BGP
194	IRC (ang. *Internet Relay Chat*)
443	HTTPS
520	Protokół RIP
8080	Alternatywny kanał HTTP

Transmisja danych dźwiękowych lub wizyjnych, zwłaszcza do wielu użytkowników naraz nie może odbywać się przy użyciu protokółu TCP ponieważ powstające w wyniku oczekiwania na pokwitowanie lub w wyniku powtórzeń pakietów opóźnienia byłyby nie do przyjęcia dla widzów lub słuchaczy i oznaczały większe niedogodności dla nich aniżeli brak pojedyńczych datagramów. Nie mówiąc już o transmisji do wielu adresatów naraz. Powódź napływających od nich pokwitowań i żądań powtórzenia uniemożliwiłaby jakąkolwiek transmisję. W tych przypadkach stosowana jest nie zabezpieczona przed przekłamaniami transmisja w protokóle UDP (ang. *User Datagram Protocol*). W ten sposób

transmitowane są m.in. pakiety głosowe pochodzące z sieci Echolinku, D-Starowej, DMR-owej, C4FM itd. Protokół UDP używany jest także przy zapytaniach kierowanych do serwerów DNS czy DHCP albo w połączeniach przez tunel VPN (ang. *Virtual Private Network*). Ponieważ protokół UDP nie posiada żadnych zabezpieczeń ewentualne wykrywanie i korektę przekłamań pozostawiono korzystającym z niego zastosowaniom. Może być to przykładowo korekcja wyprzedzająca FEC. Dane FEC stanowią część danych użytkowych i nie zajmują oddzielnego pola w pakiecie UDP (nie są one widzialne dla protokółu UDP). Jest ona powszechnie stosowana w transmisji strumieni danych wizyjnych i fonicznych. Wersją uproszczoną, zapewniającą zmniejszenie opóźnień w transmisji jest protokół UDP-Lite. W transmisji strumieni danych stosowany jest także protokół SCTP (ang. *Stream Control Transmission Protocol*).
W diagnozie stanu połączeń stosowany jest protokół ICMP (ang. *Internet Control Message Protocol*). Od jego kontrolą nadawane jest żądanie odpowiedzi (echa) pod wybrany adres IP – *ping*. Zapytany adresat powinien w normanej sytuacji udzielić odpowiedzi. Wysłanie zapytania *ping* pod adres pętli wewnętrznej 127.0.0.1 pozwala na stwierdzenie czy lokalna obsługa rodziny protokółów TCP/IP funkcjonuje prawidłowo. W odpowiedzi na zapytanie wyświetlane jest zestawienie informujące o czasie nadejścia odpowiedzi, liczbie pakietów nadanych, odebranych i straconych oraz o procentowej stopie strat. Odpowiedzi „request timed out" i „destination unreachble" oznaczają odpowiednio, przekroczenie czasu oczekiwania na odpowiedź i niedostępność adresata zapytania. Mogą one być spowodowane także przez niewłaściwy wybór trasy domyślnej albo domyślnej bramki internetowej.
Dokładniejsze informacje o przebiegu trasy połączenia i jej jakości otrzymuje się w odpowiedzi na polecenie *tracert* (z ang. *trace route*) – „prześledź trasę". Ułatwia to także wykrycie ewentualnych pętli na trasach.
Polecenie *nslookup* z podaniem dowolnego adresu symbolicznego np. *www.pzk.org.pl* pozwala na sprawdzenie dostępu do serwera DNS i otrzymywanych odpowiedzi. W diagnozie stanu sieci i ruchu w niej pomocne mogą być też programy narzędziowe dostępne w Internecie.

1.1.2. Adresy internetowe

Do jednoznacznej identyfikacji systemów komputerowych w sieciach TCP/IP służy specjalny adres numeryczny tzw. adres internetowy. W standardzie IPv4 ma on długość 4 bajtów czyli 32 bitów i jest zapisywany w postaci czterech liczb dziesiętnych oddzielonych kropkami co daje prawie 4,3 mld adresów.
Obszar adresowy IP został podzielony na pięć klas o różnym zasięgu. Pierwszą grupę stanowią adresy klasy A. Ich pierwszy bajt adresu IP leży w zakresie 1 – 126, co oznacza liczbę 126 sieci i maksymalną możliwą liczbę podłączonych komputerów 16777214. Jest wśród nich krótkofalarska sieć 44. Adresy sieci klasy A można zapisywać jako 44.0.0.0/8, co oznacza, że do ich odróżnienia potrzebne jest pierwszych osiem bitów. Pozostałe 3 bajty czyli 24 bity służą do odróżniania poszczególnych uczestników (są indywidualną częścią adresu). Zależność tą można zapisać także przy użyciu maski sieci 255.0.0.0. Logiczna operacja I (AND) między maską i adresem daje w wyniku adres sieci. Zakres wartości pierwszego bajtu 128 – 191 jest przeznaczony dla sieci klasy B. Adres sieci stanowi pierwszych 14 bitów, jako standardową maskę przyjmuje się 255.255.0.0, co jest równoważnie z zapisem /16. Indywidualna część adresu ma długość 16 bitów. Liczba sieci wynosi 16384 i do każdej z nich może być podłączonych 65534 uczestników. Kolejną klasą jest klasa C. Zakres wartości jej pierwszego bajtu adresowego wynosi 192 – 223. Jej standardową maską jest 255.255.255.0, co odpowiada zapisowi /24. Indywidualna część adresu składa się z 8 bitów. Liczba sieci wynosi 2097150, a z każdą z nich może być połączonych 254 uzytkowników. Do celów specjalnych i zastosowań przyszłościowych zdefiniowano także klasy D i E. Liczba komputerów mogących pracować w danej sieci jest mniejsza od liczby dwójkowej o danej liczbie bitów ponieważ adresy zakończone na 0 są adresami sieci, a zakończone na 255 adresują wszystkie komputery w sieci – są więc adresami rozgłoszeniowymi (ang. *broadcast*).
Klasa A o adresie 127 jest przeznaczona do łączności wewnętrznych (pętli wewnętrznych) i do celów diagnostycznych. Najczęściej spotykanym adresem w pętli wewnętrznej jest 127.0.01.
Zbiór adresów IPv4 jest już praktycznie wyczerpany i utrzymywany przy życiu dzięki podziałom na podsieci i innym „sztuczkom" jak maski o płynnie zmienianej długości. Stopniowo jest on zastępowany przez system IPv6. Adres IPv6 składa się z 8 rozdzielonych dwukropkami grup po 16 bitów (czyli 128 bitów). Są one przedstawione w zapisie szesnastkowym (ang. *hexadecimal*), przykładowo

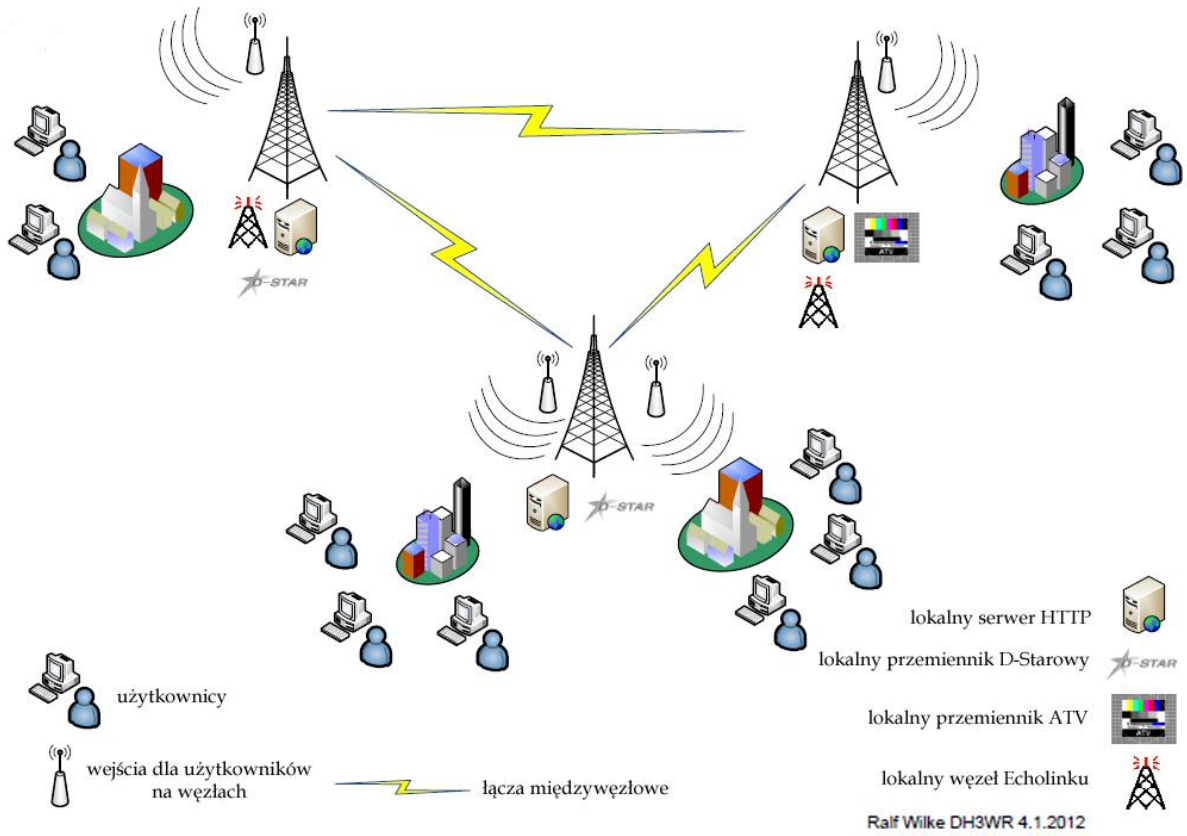
2001:0db8:85a3:08d3:0000:0000:0000:0001, dopuszczalny jest też zapis skrócony, w którym grupy o wartości 0 są zastąpione przez podwójny dwukropek. Ich liczba wynika z uzupełnienia adresu do pełnej długości i nie jest podana w zapisie: 2001:0db8:85a3:08d3::0001. Liczba adresów IPv6 jest na tyle duża, że powinna wystarczyć na dłuższy czas nawet przy uwzględnieniu potrzeb Internetu przedmiotów (IoT).
Adresy numeryczne są niezbyt praktyczne do zapamiętania dlatego też w sieciach TCP/IP stosowane są adresy symboliczne – nazwy mówiące więcej użytkownikom. Powiązanie adresów symbolicznych z numerycznymi jest zadaniem serwerów DNS (ang. *Domain Name Server*). Serwer korzysta z internetowej książki adresowej i odpowiada na zapytania w rodzaju „Jaki adres IP ma serwer XXXX?".
Adresy IPv4 wyczerpałyby się już dawno gdyby w sieciach lokalnych nie stosowano adresów należących do grup nie koordynowanych światowo. Adresy należące do tych grup mogą powtarzać się dowolnie w sieciach lokalnych pod warunkiem, że nie są widoczne na zewnątrz – są to adresy prywatne. Należą do nich serie 10.x.x.x (należąca do klasy A; 10.0.0.0/8), 172.16.x.x – 173.31.255.255 (klasa B; 172.16.0.0./12) i 192.168.x.x (klasa C; 192.168.0.0/16). Sieci lokalne widoczne są na zewnątrz pod wspólnym adresem. Dla sieci domowych wystarczy pojedyńczy adres. Zadaniem modemu internetowego (trasownika, ang. *router*) jest odpowiednie kierowanie komunikatów i poleceń do Internetu od każdego z wchodzących w skład sieci lokalnej komputerów lub innych urządzeń i kierowanie nadchodzących z zewnątrz odpowiedzi do właściwego urządzenia (przekierowywanie adresów), przy użyciu protokółu NAT (ang. *Network Address Translation*). Może on jednak być źródłem problemów w transmisji głosu przez sieć (VoIP).
Sieci lokalne występują na zewnątrz pod wspólnym adresem przyznanym przez operatora internetowego z jego puli adresów. Mogą być to adresy koordynowane globalnie albo też analogicznie do sieci lokalnych adresy z grupy niekoordynowanej i wówczas operator internetowy jest dopiero widoczny w sieci światowej przez grupę adresów globalnie koordynowanych (globalnych).
W regularnych odstępach czasu (przykładowo raz na dobę) operator przerywa połączenie z klientami i jeżeli ponowne jego nawiązanie jest możliwe (modem u klienta jest włączony i funkcjonuje) klienci otrzymują od nowa adresy IP i są one z reguły różne od poprzednich (są to więc adresy dynamiczne). Pozwala to operatorom na efektywniejsze zarządzanie pulą adresów IP i nie blokowanie niepotrzebnie nieużywanych w danym momencie. Oznacza to jednak, że użytkownicy nie mogą być dostępni pod stałym adresem (statycznym) od strony Internetu, i że prywatne serwery albo urządzenia do zdalnego sterowania radiostacjami nie mogłyby wypełniać swoich zadań. Lekarstwem na tą sytuację są usługi w rodzaju *dyndns*, *noip* i podobnych. Część z nich jest bezpłatna, przynajmniej w ograniczonym, ale wystarczającym dla zastosowań prywatnych, zakresie. Usługi te oferują klientom stały adres symboliczny (lub kilka) i regularnie odpytują adresy IP modemów u klientów, tak że w krótkim czasie po zmianie adresu IP znane jest już powiązanie aktualnego adresu dynamicznego IP klienta z jego stałym stałym adresem symbolicznym zarejestrowanym u usługodawcy. Oznacza to, że adresy takie jak *telemetria.oe1kda.ddns.net* albo *ic705.oe1kda.ddns.net* są zawsze osiągalne z zewnątrz i pozwalają w tym przykładzie na odczytyt danych pomiarowych czy meteorologicznych z własnego serwera http albo na zdalne sterowanie radiostacją. Modemy internetowe mają w swoich konfiguracjach przeważnie możliwość włączenia jednej z takich usług. Dla przedsiębiorstw usługi takie o szerszym zakresie możliwości są dostępne odpłatnie.
Jeżeli na komputerze użytkownika uruchomionych jest więcej serwerów równolegle i występują one dzięki temu od jednym wspólnym adresem IP wewnątrz sieci lokalnej do ich rozróżnienia stosuje się kanały logiczne. Przykładowo więc adres *oe1kda.ddns.net:8080* oznaczałby skorzystanie z serwera HTTP u OE1KDA, a adres *oe1kda.ddns.net:1234* z serwera zdalnego sterowania radiostacją.
Adresy globalne przeważnie nie są potrzebne użytkownikom prywatnym, ale w szczególnych sytuacjach konieczne jest skontaktowanie się z operatorem. Jednym z takich szczególnych przypadków jest, sądząc z opisu w instrukcjach Icoma, korzystanie z funkcji punktu dostępowego („Access Point") albo terminnalowej („Terminal") nowszych modeli radiostacji D-Starowych.

1.1.3 Protokół AX.25

W protokóle AX.25 (ang. *packet-radio*) pochodzącym od profesjonalnego protokółu X.25 występują również dwa rodzaje transmisji danych. W połączeniach między dwoma korespondentami nadawane są pakiety numerowane typu I. Zawierają one sumę kontrolną CRC i są po odebraniu kwitowane pozytyw-

nie w przypadku nie wystąpienia przekłamań na trasie lub negatywnie, przez zażądanie powtórzenia w przypadku stwierdzenia przekłamań. W przypadku nie otrzymania powtórzenia w zadanym czasie nadawca automatycznie powtarza pakiet. Mechanizm zabezpieczeń tego typu nosi oznaczenie ARQ (ang. *Automatic Repeat Request*). Dla zwiększenia przepustowości łącza możliwe jest nadawanie kilku pakietów przed otrzymaniem pokwitowania. Ich maksymalna liczba wynosi 7 i jest ustalana za pomocą parametru MAXFRAME w konfiguracji TNC. Połączenia tego typu występują w komunikacji dwóch stacji przez sieć *packet-radio*, co w tej chwili należy do rzadkości.
W drugim przypadku, gdy dane są transmitowane do wielu odbiorców nadawane są nienumerowane, bezpołączeniowe pakiety typu UI. Nie są one ani kwitowane, ani wyposażone w inne mechanizmy kontroli przekłamań albo ich korekty. W razie potrzeby dane użytkowe muszą być uzupełnione o dane korekcyjne (FEC). Transmisja przy użyciu pakietów nienumerowanych występuje m.in. w systemie APRS.
W protokóle AX.25 jako adresy służą znaki wywoławcze stacji z ewentualnym dodatkiem rozszerzenia, np. OE1KDA-11. W systemie APRS rozszerzeniom znaku są przypisane konkretne znaczenia informujące odbiorców o rodzaju stacji: domowa, samochodowa, piesza, meteorologiczna itd. W komunikatach APRS znajdują się jednak odniesienia do tabel informujących o tym dokładniej. Szczegółowe omówienie formatów komunikatów APRS zawiera tom 8 „Biblioteki polskiego krótkofalowca”.

1.2. Hamnet



Rys. 1.2.1. Struktura sieci

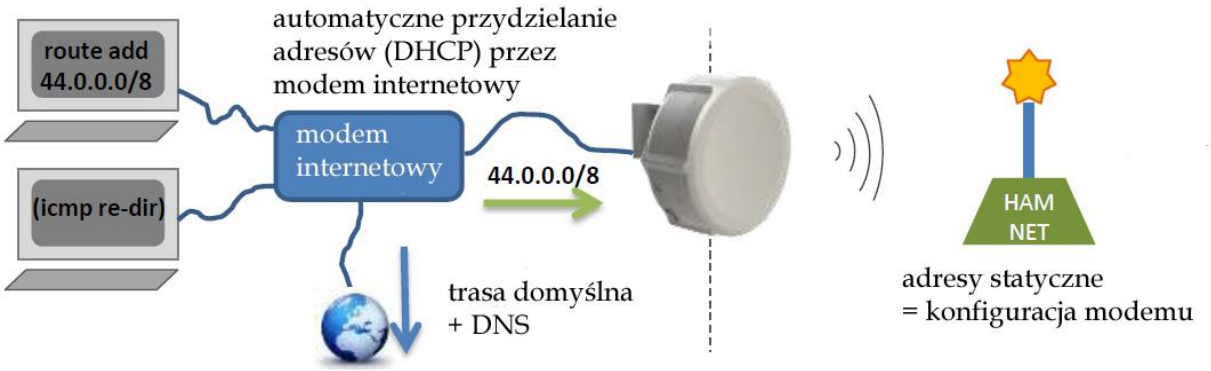
Sieć Hamnetu (***H**ighspeed **A**mateurradio **M**ultimedia **Net**work*) stanowi amatorską sieć radiową opartą na technice stosowanej w Internecie opartej o protokół IP i na szybkich łączach mikrofalowych. Nie jest ona jednak amatorskim wejściem do Internetu i nie ma go zastępować, jest natomiast zamkniętą siecią krótkofalarską dostępną dla wszystkich licencjonowanych nadawców. Wykorzystywane są w niej: zestaw protokółów TCP/IP, oprogramowanie serwerów świadczących typowe usługi internetowe jak dostęp do stron www (HTTP), wymiana poczty elektronicznej, transmisja plików (FTP), wymiana meldunków tekstowych i głosowych, łączności głosowe VoIP (głos przez IP), telefonia SIP itd. oraz

wyposażenie stosowane w dostępie do Internetu takie jak modemy i punkty dostępowe albo trasowniki (ang. *router*) – w tym zwłaszcza wyposażenie radiowe WLAN (*Wireless Locak Area Network*) i wchodzące stopniowo do użytku wyposażenie WRAN IEEE 802.22 (*Wireless Regional Area Network*). Oprócz usług znanych z Internetu w Hamnecie występują usługi typowo krótkofalarskie jak połączenia między przemiennikami fonicznymi (zwłaszcza systemów cyfrowych D-STAR, DMR itd.), dostęp do telewizji amatorskiej (ATV i D-ATV), dostęp do Echolinku, połączenia z siecią APRS i packet-radio, zastępowanie dotychczasowych łączy packet-radio, dostęp do sieci Winlinku, do odbiorników programowalnych (SDR), zdalna obsługa radiostacji i innych urządzeń krótkofalarskich itp. Zasadniczo w sieci Hamnetu można uruchamiać dowolne usługi i systemy oparte o transmisję IP, oczywiście w zakresie związanym z krótkofalarstwem.
Sieć zapewnia większą przepustowość i niezawodność aniżeli dawniejsza sieć packet-radio (AX.25), pracuje niezależnie od profesjonalnego Internetu (i przynajmniej częściowo korzysta z niezależnego zasilania awaryjnego) i może przyczynić się do zwiększenia atrakcyjności krótkofalarstwa w ogólności, a zwłaszcza w oczach młodzieży. Dalszą korzyścią jest możliwość rozszerzania wiedzy technicznej przez krótkofalowców, zwłaszcza wiedzy dotyczącej sieci komputerowych, jej elementów i działania.
Przepustowości na łączach Hamnetu leżą w granicach od 10 Mb/s do kilkuset Mb na sekundę co umożliwia szybką wymianę dużych ilości danych. Wybór tras (trasowanie) jest dokonywany dynamicznie jak w sieci Internetu.
Sieć Hamnetu można podzielić na trzy warstwy: warstwę sieci szkieletowej – łączy między węzłami, warstwę usług – świadczonych przez węzły, np. serwer HTTP, węzeł Echolinku – i wejścia dla użytkowników (rys.1.2.1) – warstwę użytkownika. W wyborze tras stosowany jest protokół BGP.
Pod względem funkcjonalnym zastosowania Hamnetu można podzielić na dwie grupy:
1. Wykorzystanie jako infrastruktury dla stacji automatycznych:
   - Połączenia oparte o protokół IP,
   - Podstawa nowoczesnej radiowej sieci transmisji danych,
   - APRS, Echolink, D-STAR, DMR, sieć przywoławcza (np. DAPNET), serwery HTTP, serwery transmisji danych (FTP), serwery NTP, bazy danych map, wyszukiwarki itp.
2. Wykorzystanie jako platformy do łączności osobistych:
   - Transmisja głosu (VoIP): np. Skype, telefonia SIP, Mumble, kółeczka konferencyjne
   - Transmisja obrazu: telewizja amatorska analogowa (ATV) i cyfrowa (D-ATV), wejścia i wyjścia, konferencje wizyjne,
   - Witryny HTTP: prezentacje projektów, prezentacje autorów, konstruktorów itp.,
   - Rozprowadzanie biuletynów (komunikatów) krótkofalarskich,
   - Prywatne witryny, ułatwienia w prezentacji informacji dzięki dostępowi przez przeglądarkę internetową,
   - Prezentacje własnych konstrukcji, systemów łączności opartych na protokóle IP itd.,
   - Udostępnianie odbiorników z cyfrową obróbką sygnałów (SDR), skrzynek *DX-Cluster* itp.

Dużą pomocą w uruchamianiu węzłów indywidualnych jest zestaw programów *HamserverPi* dostępny w postaci odwzorowania pamięci dla *Maliny*. Zawiera on także system operacyjny i dodatkowe pliki (skrypty) sterujące ułatwiające korzystanie ze wszystkich funkcji.
Do wyboru tras w Hamnecie używany jest protokół BGP (ang. *Border Gateway Protocol*). Odpowiada on trzeciej warstwie modelu OSI (ISO) i opiera się na protokole IP. Na jego potrzeby sieć jest podzielona na logicznie niezależne segmenty zwane systemami autonomicznymi (AS). Każdy z tych autonomicznych systemów otrzymuje 16-bitowy numer (prywatny adres; ASN) z obejmującego 1023 elementy zakresu 64512 – 65534, przy czym poszczególnym krajom przypisane są węższe podzakresy (dla Polski – 64800 – 64839). Stopniowo do użytku wchodzą numery (adresy) 32-bitowe (10-pozycyjne) z obejmującego 94967295 elementów zakresu 4200000000 – 4294967294, dla Polski jest to podzakres 4226000000 – 4226199999 – patrz *RFC6996*. Pierwsze dwie cyfry (42) oznaczają zakres przeznaczony do użytku prywatnego, następne trzy oznaczają kod kraju zgodnie z normą przyjętą w sieciach telefonii komórkowej, DMR itd. (MCC wg. E.212, patrz dokument X.121 ITU), a pozostałe cyfry mogą być dowolnie zagospodarowane w każdym kraju. Kodem MCC dla Polski jest 260, dla Austrii 232, a dla Niemiec 262 i 263.

Wewnątrz regionów stosowany jest wariant iBGP, a pomiędzy regionami – eBGP. Adresy te są potrzebne w łączach międzywęzłowych i muszą być podane w konfiguracji węzłów. Protokółowi BGP jest poświęcony tom 22 „Biblioteki polskiego krótkofalowca".
W węzłach Hamnetowych mających połączenie z internetem możliwe jest udostępnienie wejść przez tunel VPN po uruchomieniu na nich serwera VPN (protokół PPTP). Pozwala to na korzystanie z nich przez użytkowników nie mogących korzystać z drogi radiowej. Łącze internetowe musi zapewniać wystarczającą przepustowość.

Rys. 1.2.2. Najprostsza konfiguracja wyposażenia dla stacji indywidualnej (źródło: *http://routerboard.com*)



Rys. 1.2.3. Zasada konfiguracji sieci domowej dla integracji Hamnetu z Internetem (źródło: *http://routerboard.com*)

Na rys. 1.2.2. serwer DHCP punktu dostępowego Hamnetu przydziela adres IP komputerowi w sieci LAN użytkownika (np. z serii 192.168.x.x), a od strony Hamnetu otrzymuje adres z sieci 44.x.x.x.
Na rys. 1.2.3 polecenie *route add 44.0.0.0/8* definiuje trasę połączenia z Hamnetem, pozostałe trasy prowadzą domyślnie do Internetu. Komputery sieci domowej użytkownika mogą być połączone radiowo przez WiFi lub kablowo z modemem internetowym (punktem dostępowym). Do niego podłączony jest punkt dostępowy do Hamnetu i wyjście internetowe, a także w miarę potrzeby lokalny serwer na „Malinie" (*HamServer*, serwer SIP, serwer RMS Winlinku itp.).

1.3. Sieci WiFi

Sieci bezprzewodowe WLAN (ang. *Wireless Local Area Network*; *Wireless LAN*, W-LAN, WLAN) są sieciami radiowymi opartymi na normach z rodziny IEEE 802.11. Odpowiadają one warstwom 1 i 2 modelu ISO. Występują w nich rozmaite rodzaje modulacji.
Infrastruktura sieci jest zbliżona do infrastruktury sieci telefonii komórkowej i zawiera stacje bazowe (punkty dostępowe; ang. *Access Point*) koordynujące pracę pozostałych uczestników korzystających z tej samej częstotliwości (klientów).
Stacja bazowa nadaje w ustalonych odstępach (przeważnie 10 razy na sekundę) czasu krótkie pakiety – pakiety radiolatarni (ang. *beacons*) odbierane przez wszystkie znajdujące się w jej zasięgu stacje. Pakiety te zawierają nazwę sieci („*Service Set Identifier*", SSID) oraz informują o stosowanych normach transmisji i zabezpieczeniach dostępu.
W Hamnecie i w jego sieci szkieletowej jako nazwy (SSID) stosowane są znaki wywoławcze w z góry ustalonym formacie.

Łącza sieci szkieletowej Hamnetu pracują obecnie najczęściej w paśmie 6 cm lub w wyższych. Stosowane są szerokości kanałów 5, 10 lub 20 MHz, a przepustowości brutto (szybkości transmisji) dochodzą do 54 Mbit/s. Przepustowości netto zależą od chwilowych rzeczywistych potrzeb i używanych protokółów. Różnice między przepustowością brutto i netto zależą od ilości danych stosowanych służbowo przez protokół.
Obecnie w Europie w zakresie WiFi 2,4 GHz używanych jest 13 kanałów o szerokościach 20 MHz i częstotliwościach środkowych rozmieszczonych co 5 MHz pomiędzy 2412 i 2472 MHz. Jak z tego wynika większość z nich zachodzi na siebie, a jedynymi rozdzielnymi kanałami o szerokościach 20/22 MHz są kanały 1 (2399,5 – 2424,5 MHz, środek 2412 MHz), kanał 6 (2424,5 – 2449,5 MHz, środek 2437 MHz) i 11 (2449,5 – 2474,5 MHz, środek 2462 MHz) lub przy większych odstępach między nimi nr 1, 7 i 13. Przy szerokości kanału 40 MHz rozdzielne pozostawały by jedynie kanały 3 i 11. Wybór kanałów rozłącznych przy szerokościach 5 MHz stosowanych w Hamnecie jest większy. Krótkofalowcy mają do dyspozycji w niektórych krajach dodatkowe kanały oznaczane jako 0 (środek 2407 MHz), -1 (2402 MHz) i -2 (2397 MHz). W paśmie 5 GHz kanały WLAN 36 – 64 leżą w zakresie 5,15 – 5,35 GHz, a więc poza pasmem amatorskim. Z kanałów 100 – 140 znajdujących się pomiędzy 5,5 – 5,7 GHz część pokrywa się z amatorskim pasmem 6 cm. Dodatkowo do dyspozycji krótkofalowców są kanały w paśmie 9 cm. Zmniejszenie szerokości kanałów w stosunku do zastosowań powszechnie używanych uniemożliwia albo przynajmniej bardzo znacznie utrudnia dostęp do Hamnetu niekrótkofalowcom.
Stosowany w nowszych modelach punktów dostępowych technika MIMO (ang. *Multiple Input Multiple Output*) pozwala dzięki zastosowaniu kilku anten nadawczych i odbiorczych w tym samym kanale na zwiększenie przepustowości i zmniejszenie wpływu odbić fali (pod warunkiem dostatecznego odsprzężenia anten).

Tabela 1.3.1
Najczęściej stosowane kanały Hamnetu w Europie i ich szerokości

Częstotliwość środkowa [MHz]	Szerokość kanału [MHz]
2362	5
2395	5
2397	5/10
2404	5
2407	5
2412	5
2417	5
2422	5/10
2427	5
2432	5
2437	5
2442	5
2447	5
2472	5
3415	10
3425	10
3435	10
3445	10
3455	10
5675	10
5680	5
5685	10
5690	10
5695	10
5700	10
5705	10
5715	10

7525	5
5730	10
5735	20
5745	5/10/20
5750	10
5770	5
5775	5/10
5785	5/10/20
5795	10
5805	10
5815	10
5820	5
5825	5/10
5830	5

Uwagi:
1) oprócz kanałów leżących w pasmach krótkofalarskich możliwa jest również praca w pozostałych zakresach WiFi, ale pod warunkiem przestrzegania ostrzejszych ograniczeń mocy. Nie używane są wówczas znaki wywoławcze i dozwolone jest szyfrowanie transmisji, ale jest to rozwiązanie leżące na pograniczu krótktofalarstwa.

1.3.1. Normy IEEE 802.11

Transmisje krótkofalarskie w pasmach WiFi muszą być ogólnie dostępne i nie szyfrowane. W przypadku stosowania kluczy WEP/WPA muszą one być publicznie znane. Zasadniczo nie są więc one zabezpieczone przed piratami komputerowymi w takim stopniu jak łączności w prywatnych i profesjonalnych sieciach komputerowych. W łącznościach hamnetowych stosowany jest przeważnie standard IEEE 802.11n, a w sieci AREDN (BBHN – ang. *Broadband Hamnet*) – IEEE 802.11g. W dostępie na niższych pasmach do użytku wchodzi IEEE 802.22.

1.3.1.1. Norma IEEE 802.11b

Jest historycznie pierwszą normą opracowaną dla potrzeb sieci użytkowników indywidualnych. Przewidziane w niej są szybkości transmisji do 11 Mbit/s, w tym jako typowe występują 5,5 Mbit/s, 2 Mbit/s i 1 Mbit/s. Do dyspozycji przewidziano 8 zachodzących na siebie kanałów w paśmie 2,4 GHz. Do rozpraszania widma stosowana jest metoda bezpośredniego szybkiego kluczowania fazy sygnału w.cz. (ang. *DSSS*).

1.3.1.2. Norma IEEE 802.11g

W paśmie 2,4 GHz używanych jest 8 szybkości transmisji: 6, 9, 12, 18, 24, 36, 48 i 54 Mbit/s. Modele niektorych producentów oferują także szybkość 108 Mbit/s ale tylko między sobą. W zależności od jakości połączenia (stopy błędów) wybierana jest automatycznie mniejsza lub większa szybkość transmisji. Standardowo stosowana modulacja jest OFDM zamiast kluczowania fazy jak w normie 802.11b. Norma stosowana jest w pasmach 2,4 i 5 GHz.
W trybie kompatybilności z normą IEEE 802.11b dostępne są 4 szybkości transmisji: 11; 5,5; 2 i 1 Mbit/s, z tym że niektórzy producenci umożliwiają też korzystanie z szybkości 22 i 44 MBit/s. W tym trybie stosowane jest rozpraszanie widma z kluczowaniem fazy (DSSS).

1.3.1.3. Norma IEEE 802.11a

Standardowo stosowane są – dobierane automatycznie – szybkości transmisji 6, 9, 12, 18, 24, 36, 48 i 54 Mbit/s, a praca odbywa się w paśmie 6 cm (w 12 nie zachodzących na siebie kanałach). Niektórzy producenci oferują także szybkość 108 Mbit/s.

W zależności od jakości połączenia (stopy błędów) wybierana jest automatycznie mniejsza lub większa szybkość transmisji.
Dla szybkości 6 i 9 Mbit/s stosowana jest modulacja BPSK, dla 12 i 18 Mbit/s – QPSK, dla 24 i 36 Mbit/s – 16-QAM i dla 48 i 54 Mbit/s – 64-QAM.

1.3.1.4. Norma IEEE 802.11ac

Norma stosowana jest w paśmie 5 GHz. Korzysta ona z tych samych rozwiązań antenowych MIMO co w normie 802.11n, ale stosowane są szersze kanały. Przepustowość dochodzi do 1 Gbit/s. Stosowana jest modulacja OFDM.

1.3.1.5. Norma IEEE 802.11n

Sieci pracują w pasmach 2,4 i 5 GHz, teoretyczne szybkości transmisji netto dochodzą do 240 Mbit/s, a brutto – do 600 Mbit/s przy szerokościach kanałów 20 lub 40 MHz. Stosowane są złożone systemy kluczowania: OFDM jako modulacja podstawowa, a każda z podnośnych jest dodatkowo zależnie od warunków transmisji kluczowana fazowo 2-PSK albo 4-PSK lub amplitudowo-fazowo 16-QAM albo 64-QAM. Stosowana jest technika antenowa wielokrotnych wejść i wyjść (MIMO – ang. *multiple input multiple output*). W paśmie 2,4 GHz używane są te same zachodzące na siebie kanały co i w normach poprzednich.

1.3.1.6. Norma IEEE 802.22

Jest ona przeznaczona dla sieci regionalnych WRAN (ang. *Wireless Regional Area Network*). W zastosowaniach profesjonalnych pozwala m.in. na wykorzystanie luk w pasmach telewizyjnych pomiędzy 54 a 862 MHz. Jedną z istotnych właściwości jest możliwość dynamicznego zarządzania zasobami częstotliwości (ang. *cognitive radio*). Sieć pracuje w topologii gwiaździstej i jest złożona z centralnej stacji bazowej i indywidualnych stacji użytkowników. Stosowana jest modulacja OFDMA z przepustowością dochodzącą do 19 Mbit/s dla kanałów o szerokości 7 – 8 MHz.
Dodatkowo do normy IEEE 802.22 została opracowana norma IEEE 802.11af z dynamicznym zarządzaniem zasobami częstotliwości. W odróżnieniu po poprzedniej jest ona przewidziana do pracy na odległościach 1 zamiast 100 km.

1.4. Wyposażenie sprzętowe

W zależności od pokrycia zasięgiem i natężenia pola najbliższych przemienników hamnetowych możemy wyróżnić dwie zasadnicze sytuacje. W sytuacji pierwszej, czyli stacji znajdujących się w zasięgu czynnych stale stacji przemiennikowych użytkownicy łączą się bezpośrednio ze stacjami przemiennikowymi korzystając ze stosunkowo prostego wyposażenia punktów dostępowych. Przykładami takiego szeroko używanego wyposażenia są omówione dalej modele „Nanostation" i „Bullet", a także „Nanostation Loco", „Nanobeam", „Powerbeam", „NanoBridge", „AirGrid" itd. firmy Ubiquiti – odpowiednio M2 lub M5 w zależności od zakresu pracy, 2,4 GHz lub 5 GHz, albo ich nowsze wersje. W przeważającej części są one zintegrowane w anteną i zasilane kablem ethernetowym przez gniazdo PoE (ang. *Power on Ethernet*). Ważne jest aby dysponowały one możliwością ograniczenia szerokości pasma transmisji. W zależności od zakresu stosowane są szerokości pasma 5 lub 10 MHz, ale w zakresie 6 cm także 20 MHz. Urządzenia firmy Ubiquiti są tańsze od przedstawionych w następnym akapicie produktów firmy „Mikrotik", ale nie pozwalają na korzystanie z protokółu wyboru tras (trasowania) BGP, można je więc stosować tylko w stacjach indywidualnych, a nie na łączach między węzłami. Ich konfiguracji dokonuje się w internetowej powierzchni obsługi. W grę wchodzi także sprzęt *TP-Linku*, j.np. WR740, WR841 i inne. Te ostatnie pozwalają na wgranie oprogramowania OpenWRT i dzięki temu na pracę w sieci o topologii siatki (ang. *mesh*).

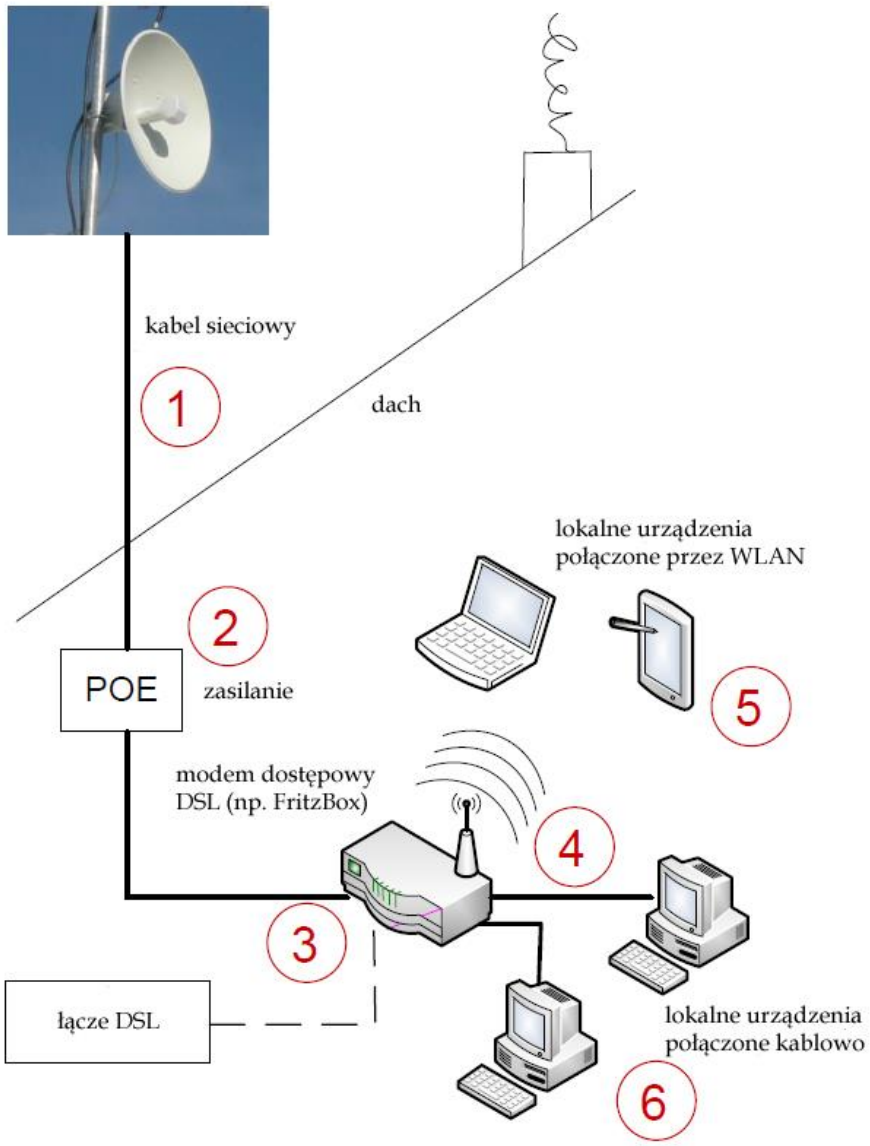
Nieco bardziej rozbudowane i o nieznacznie bardziej skomplikowanej konfiguracji modele RB411(AH) lub RB433(AH) firmy „MikroTik" są wprawdzie przeważnie stosowane w sieci szkieletowej „Hamnetu", ale nic nie stoi na przeszkodzie, aby korzystali z nich także użytkownicy indywidualni. Pozwalają one na korzystanie z protolółu wyboru tras BGP. Z biegiem czasu do użytku krótkofalarskiego wejdą także i inne modele punktów dostępowych – po ewentualnym opracowaniu dla nich pasującego oprogramowania. Podane w następnych rozdziałach przykładowe konfiguracje sprzętu i oprogramowania mogą się wprawdzie różnić od niezbędnych dla innych modeli wyposażenia i dla trochę inaczej skonfigurowanego dostępu do różnych usług, ale bez trudu można będzie i tak zidentyfikować najważniejsze parametry i opierając się na poniższych opisach i objaśnieniach prawidłowo skonfigurować wyposażenie. Urządzenia muszą być skonfigurowane jako trasowniki (ang. *router*), a lokalna trasa jako 44.0.0.0/8 (*route add -p 44.0.0.0 mask 255.0.0.0 gw 192.168.1.100*, gdzie 192.168.1.100 jest przykładowym lokalnym adresem IP urządzenia od strony sieci kablowej).

Użytkowników należących do tej grupy można nazwać użytkownikami bezpośrednimi (ang. *power user*). Adresy IP są przeważnie przydzielane dynamicznie i automatycznie chociaż osoby potrzebujące adresów statycznych do różnych zastosowań i eksperymentów nie powinny mieć z tym żadnych kłopotów, w przeciwieństwie do Internetu publicznego.

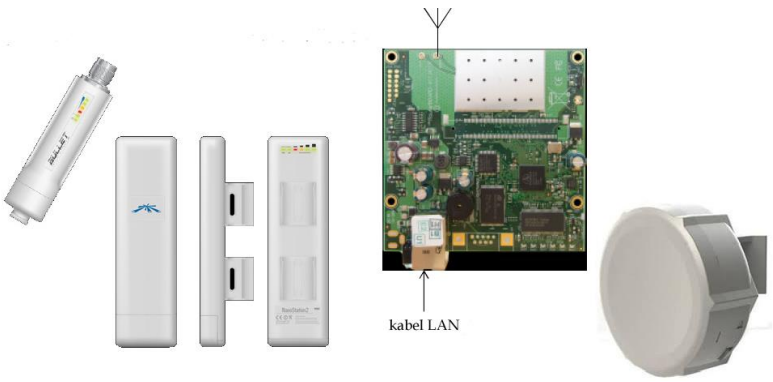
W sytuacji drugiej użytkownicy znajdują się poza zasięgiem przemienników sieci „Hamnetu" i muszą pomagać sobie tworząc lokalne sieci radiowe. Wyposażenie każdej ze stacji użytkowników stanowi jednocześnie pomocniczą stację przemiennikową pośredniczącą w przekazywaniu danych od użytkownika do sieci „Hamnetu" i odwrotnie (sieć ma topologię siatki – ang. *mesh* – pełnej lub nie). Jest to w dużym przybliżeniu sytuacja zbliżona do występującej w szczenięcych latach packet-radio kiedy to stacje indywidualne były wykorzystywane jako przemienniki cyfrowe poszerzające w znacznym stopniu zasięgi. Wybór tras czyli dynamiczne łączenie się stacji w sieć następuje automatycznie. We wspomnianych już ówczesnych sieciach packet radio trasy były podawane ręcznie, o ile stacje sąsiednich korespondentów nie były wyposażone w oprogramowanie sieciowe „Netrom", „Flexnet", X1J lub odpowiedniki. Ale to są jedynie uwagi na marginesie. Do pracy w lokalnych sieciach radiowych konieczne jest otrzymanie stałego (statycznego) adresu IP. Sytuacja druga występuje obecnie znacznie rzadziej niż pierwsza.

W stacjach użytkowników tworzących lokalne sieci wykorzystuje się bardziej rozbudowane i lekko zmodyfikowane internetowe punkty dostępowe. Powinny być one wyposażone w procesor *Broadcom BCM2050* lub jego nowocześniejszy odpowiednik. Do wypróbowanych modeli należą „Linksys WRT54GL", „Linksys WRT54GS (V1.1)" i „ASUS WL500gp (V 1.2)". Spis wchodzących w grę modeli, na których można zainstalować system OpenWRT można znaleźć w Internecie pod adresem *http://openwrt.org/supported_devices*.

Wyposażenie stacji użytkowników różni się w obu przypadkach na tyle, że nie może być zastosowane w drugiej z sytuacji.

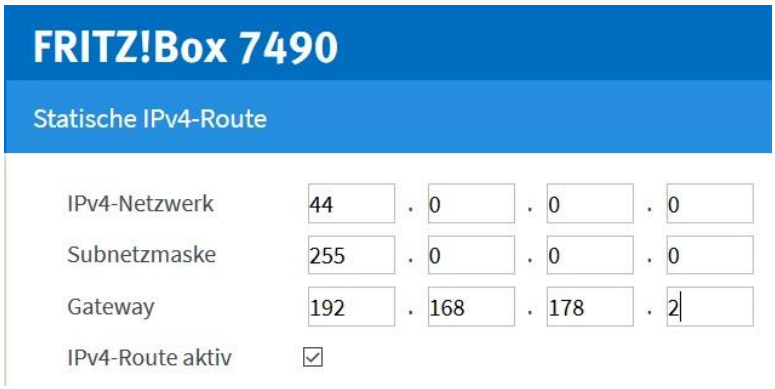


Rys. 1.4.1. Hamnet w domowej sieci: 1. Kabel sieciowy między „Nanobridge M5" i modemem; 2. Zasilanie przez gniazdo POE; 3. Podłączenie kabla do modemu (trasa tylko dla adresów 44.0.0.0/8); 4. Hamnet dostępny na wszytkich komputerach w domowej sieci; 5. zarówno bezprzewodowo; 6. jak i kablowo; modem DSL oddziela Hamnet od Internetu – trasa domyślna do łącza DSL



Rys. 1.4.2. Ubiquiti Bullet2, Nano2 (2,4, GHz) względnie Bullet5, Nano5 (5 GHz), Mikrotik 411R, Mikrotik SXT

Na rysunku 1.4.1 przedstawiony jest przykład integracji dostępu do Hamnetu w sieci domowej. Jako modem internetowy może służyć „FritzBox" albo inny model. Sieć korzysta ze wspólnej podsieci adresowej np. 192.168.172.x. Adresy w niej mogą być przydzielane dynamicznie przez DHCP, ale w uzasadnionych przypadkach operator może przyznawać adresy stałe – statyczne. Maską sieci lokalnej jest 255.255.255.0. Wszystkie zapytania o adresy IP Hamnetu (*ampr*) 44.0.0.0/8 są kierowane do hamnetowego punktu dostępowego. Punkt dostępowy (trasownik, ang. *router*) zintegrowany z anteną jest zainstalowany na maszcie, aby zapewnić dobrą widoczność anteny węzła sieci. Jest on zasilany z „dołu" przez rozgałęźnik i gniazdo PoE (ang. *Power on Ethernet*). Należy zastosować kabel ethernetowy dobrej jakości i o dobrym ekranowaniu. Zainstalowane na urządzeniach *Ubiquiti* oprogramowanie *AirOS* wymaga skonfigurowania przez internetową powierzchnię obsługi (patrz rozdz. 3 i 4).



Rys. 1.4.3. Kierowanie łączności hamnetowej przez antenowy punkt dostępowy („Gateway"). W tym przykładzie założono, że jego adres IP w domowej sieci wynosi 192.168.178.2

W związku ze sprzedażą przez krótkofalowców amerykańskich, do których należą adresy sieci 44, części z nich firmie Amazon i przeprowadzeniu koniecznej zmiany adresów w sieciach amatorskich sieć 44.0.0.0 będzie reprezentowana przez dwa zakresy adresów: 44.0.0.0/9 i 44.128.0.0/10.
Przed podjęciem decyzji o zakupie wyposażenia i uruchomieniu własnej indywidualnej stacji Hamnetowej warto dokładnie poinformować się o stanie sieci w najbliższej okolicy, zasięgu przemienników dostępowych do niej, paśmie w którym pracują, dostępnych już usługach i planach rozbudowy zarówno infrastruktury jak i dostępnych usług. Do najważniejszych spraw należy także upewnienie się, że na trasie połączenia z przemiennikiem dostępowym do Hamnetu nie znajdują się żadne przeszkody w rodzaju wysokich budynków lub innych konstrukcji, wzgórz, wysokich drzew itp. zasłaniających widok i uniemożliwiających przez to łączność mikrofalową. Zaniedbania na tych polach mogą spowodować, że cała inwestycja okaże się chybiona – przynajmniej do czasu dalszej rozbudowy infrastruktury sieci, albo też nie da spodziewanej satysfakcji jeżeli dostępne na razie usługi nie będą spełniały oczekiwań użytkownika. Oczywiście w sieci amatorskiej dużą rolę odgrywa możliwość eksperymentowania z nowymi rozwiązaniami i technologiami i należy wziąć pod uwagę i ten aspekt, mogący zrównoważyć w jakimś tam stopniu słabsze strony na pozostałych polach.

1.5. Programy

W sieci Hamnetu dostępnych jest obecnie wiele usług różnego rodzaju j.np.:

- Wymiana bieżących komunikatów i prowadzenie dialogów („Instant Messaging") – np. przy użyciu serwerów „Jabber" lub XMPP; jako klient może służyć przedstawiony dalej „Pidgin",
- Połączenia głosowe („VOIP") – przez „Skype" lub „Mumble",
- Połączenia cyfrowej ATV (H264) i archiwum wizyjne,
- Echolink (przez serwer „Proxy") – „Svxlink", patrz też: tom 19 „Biblioteki polskiego krótkofalowca",
- Połączenia Packet-Radio, APRS – patrz też: tom 7 „Biblioteki polskiego krótkofalowca"),
- Intranet amatorski, czyli dostęp do stron *www* o tematyce krótkofalarskiej w protokóle HTTP, dostęp do kamer internetowych i innych urządzeń, serwery plików,
- Dostęp do skrzynek elektronicznych „DX Cluster",

- Udostępnienie cyfrowych łączy do połączenia przemienników analogowych, D-Starowych, DMR itp.,
- Dostęp do sieci Winlinku – patrz też: tomy 9 i 10 „Biblioteki polskiego krótkofalowca”,
- Korzystanie z „Ratflektorów” do wymiany danych w standardzie D-STAR przy użyciu programu D-RATS i ich instalacja – patrz też: tom 15 „Biblioteki polskiego krótkofalowca”,
- Dostęp do szerokopasmowych odbiorników z cyfrową obróbką sygnałów (ang. *SDR*) – patrz też tomy 36 i 40 serii;
- Zdalna obsługa radiostacji – prywatnych lub publicznych – przez sieć; rozwiązania techniczne są zasadniczo identyczne jak dla stacji dostępnych przez Internet (bez konieczności korzystania z usług *dyndns* itp.), patrz też tomy 58 i 59 serii;
- Zdalne sterowanie różnymi urządzeniami, w tym przemiennikami amatorskimi albo odczyt danych telemetrycznych np. przy użyciu „Maliny” czy innych mikrokomputerów (patrz też tomy 24, 33, 58 i 59 „Biblioteki”),
- Transmisja danych telemetrycznych,
- I wiele innych.

Spis powyższy nie oznacza, że wszytkie z nich są dostępne wszędzie i w tym samym zakresie. Z biegiem czasu i w miarę rozbudowy sieci pojawią się z pewnością nowe funkcjonalności dotąd nie występujące jeszcze w „Hamnecie”. Oczywiście udostępniane treści i informacje są związane z krótkofalarstwem, nie zawierają reklamy i treści niedopuszczalnych w łącznościach krótkofalarskich.
Korzystanie z niektórych z nich wymaga zainstalowania i uruchomienia dodatkowych programów takich jak „Echolink”, „Paxon” i „Flexnet”, klient „Skypa” lub „Mumble”, „Pidgin”, SDR#, D-RATS, „RMS Express”, *Asterisk* itp. Sprawom tym poświęconych jest kilka dalszych rozdziałów niniejszego skryptu. Instalacja i uruchomienie niektórych z nich jest dokładniej omówione w podanej powyżej literaturze.
Praktycznym rozwiązaniem jest, istniejąca również w wersji bezpłatnej, dystrybucja Linuksa *ClearOS* (obecnie w wersji 7). Jest ona łatwa w instalacji, konfiguracji i w zarządzaniu przy użyciu graficznej powierzchni obsługi. Zawiera ona szeroki wybór programów i usług przydatnych w Hamnecie: serwer HTTP/HTTPS, FTP (jako klienta FTP można użyć *FileZilli*), pocztowy SMTP i POP3 z programem antywirusowym, serwery DHCP, DNS, VPN, NTP, LDAP, serwer bazy danych i inne. Protokół LDAP (ang. *Lightweight Directory Access Protocol*) służy do dostępu i zarządzania katalogami (folderami) rozproszonymi w sieci. Możliwa jest też synchronizacja własnych zbiorów danych z Dropboxem. Więcej szczegółów na jego temat można znaleźć w Internecie w witrynie ClearOS *www.clearos.com*.

Użytkownicy pragnący uruchomić własne serwery świadczące dowolne usługi w sieci „Hamnetu” są w znacznie korzystniejszej sytuacji aniżeli w przypadku publicznego Internetu. Uzyskanie stałego adresu IP niezbędnego dla powszechnej dostępności serwera wymaga jedynie skontaktowania się z (lokalnymi) administratorami sieci. Niepotrzebne jest korzystanie z usług przeadresowujących w rodzaju *dyndns*, *no-ip* itp., niezbędnych w tej samej sytuacji w Internecie. Adresy w sieci „Hamnetu” (adresy z serii 44) przydzielają, oczywiście bezpłatnie, w ramach serii przyznanych poszczególnym krajom, krajowi lub okręgowi koordynatorzy adresów. Dostęp do „Hamnetu” jako sieci krótkofalarskiej jest oczywiście również bezpłatny. Większość stosowanego przez krótkofalowców oprogramowania jest także dostępna bezpłatnie.
Przykład rozwiązania serwera z odbiornikiem DVB-T wyposażonym w procesor RTL2832 na „Malinie” przedstawiono w tomie 24. Odbiornik DVB-T jest podłączony do złącza USB „Maliny”. Klienci pragnący skorzystać z odbiornika powinni w programie SDR# jako typ odbiornika wybrać z rozwijanej listy „RTL-SDR / TCP” i podać adres serwera.
Sieć Hamnetu może być też wykorzystywana w łącznościach kryzysowych. Dzięki niezależności od Internetu i zasilaniu awaryjnemu przynajmniej części węzłów może ona stanowić dobre uzupełnienie możliwości krótkofalarstwa na tym polu. Jedną z takich możliwości jest połączenie z siecią Winlinku.

2. Instalacja i konfiguracja Ubiquiti Bullet M2 – M5

2.1. Informacje ogólne

Punkt dostępowy – węzeł – Ubiquiti Bullet M2/M5 nie zawiera własnej anteny, a jedynie gniazdo typu N do jej podłączenia. Ułatwia to korzystanie z dowolnych anten fabrycznych lub własnej konstrukcji i dostosowanie całkowitej konstrukcji do warunków panujących w danej okolicy. Najkorzystniej jest aby antena była wyposażona we wtyk typu N ale można też zastosować odpowiednie przejściówki. Przy tak wysokich częstotliwościach należy jednak w miarę możliwości unikać ich stosowania, ponieważ są one źródłem zauważalnych strat sygnału. Jeżeli ze względów mechanicznych konieczne jest podłączenie „Bulleta" do anteny za pomocą kabla powinien on być jak najkrótszy.

Szczególnie praktyczne w zastosowaniach krótkofalarskich są anteny planarne, sektorowe lub paraboliczne o konstrukcji siatkowej.

Polaryzację fali dobiera się przez odpowiednie zamontowanie anteny.

Nadawanie bez podłączenia anteny lub sztucznego obciążenia może spowodować uszkodzenie nadajnika „Bulletu".

Rys. 2.1.1. Bullet M2 i M5

Tabela 2.1.1.
Przegląd modeli

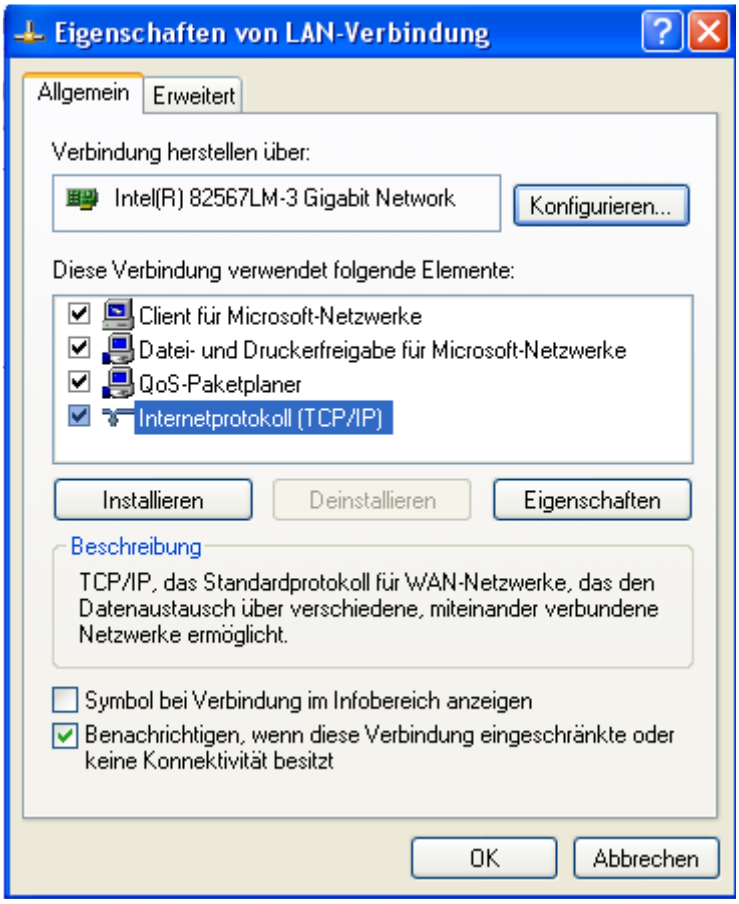
Parametr	Bullet M2	Bullet M5
Procesor	Atheros MIPS 24KC, 400 MHz	
Pamięć	32 MB pamięci roboczej SDRAM, 8 MB pamięci programu	
Złącze sieciowe	1 x Ethernet 10/100 BASE-TX, RJ-45	
Gniazdo w.cz. antenowe	Typu N	
Wymiary	15,2 x 3,7 x 3,1 cm	
Waga	0,18 kg	
Napięcie zasilania	≤ 24 V	
Pobór mocy	7 W	6 W
Zakres częstotliwości	2412–2462 MHz	5170–5825 MHz
Moc wyjściowa	28 dBm (Bullet 2HP – 29 dBm)	25 dBm

Sposób połączenia *Ubiquiti M2/M5* z zasilaczem i komputerem jest podobny do pokazanego na rys. 3.1.3. Kabel sieciowy pomiędzy „Bulletem" a zasilaczem może mieć dowolną nawet znaczną długość (do 30 i więcej metrów) i powinien być podłączony do gniazda zasilacza (lub sumatora napięcia zasilania z sygnałem Ethernetu) podpisanego *POE*. Powinien być to kabel 8-żyłowy ekranowany. Ze względu

na konieczność przeprowadzenia kabla przez uszczelkę wtyk RJ-45 z tej strony kabla nie powinien mieć obudowy. Drugi kabel ethernetowy prowadzi z gniazda *LAN* zasilacza (lub sumatora) do komputera.

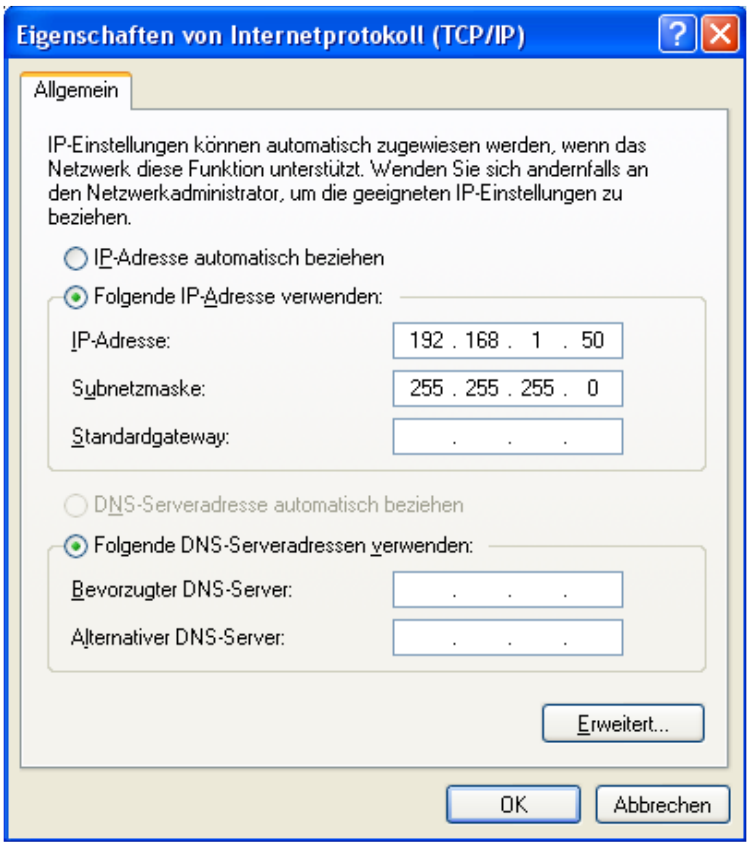
2.2. Konfiguracja do celów „Hamnetu”

Przed rozpoczęciem konfiguracji i uruchamiania stacji należy poinformować się o częstotliwości pracy przemiennika dostępowego do ‘Hamnetu”, stosowanej przezeń szerokości sygnału, polaryzacji fali i w miarę możliwości ustawić w przybliżeniu antenę w jego kierunku. W dokładnym ukierunkowaniu anteny pomocny będzie wskaźnik siły sygnału.
W celu skonfigurowania punktu dostępowego należy wywołać przeglądarkę internetową i w jej polu adresowym podać adres **https://192.168.1.20**. Po nawiązaniu przez komputer połączenia na jego ekranie pojawia się okno meldunkowe, w kórym należy podać **ubnt** jako nazwę użytkownika i jako hasło dostępu.
Po zameldowaniu się na ekranie wyświetlane jest okno konfiguracyjne zawierające 7 zakładek. System operacyjny „Bulleta” *airOS* pozwala na obszerną, intuicyjną konfigurację, a co najważniejsze z krótkofalarskiego punktu widzenia także na ograniczenie szerokości pasma sygnału do wartości ustalonych w przepisach o służbie amatorskiej względnie wybranych dla zwiększenia zasięgu. Konfiguracja dla sieci WLAN powszechnego użytku omówiona jest szczegółowo w dokumentacji sprzętu, dlatego też w niniejszym opracowaniu ograniczymy się jedynie do konfiguracji dla pracy w amatorskiej sieci Hamnetu.
W zależności od dotychczasowych ustawień dostępu do sieci WLAN w komputerze przed połączeniem się przez przeglądarkę internetową może być konieczne ustawienie adresu z podsieci 192.168.1.x tak aby możliwe było połączenie się z podanym powyżej adresem 192.168.1.20.
Należy dokonać tego w ustawieniach połączenia LAN w części dotyczącej sieci w „Panelu sterowania”.



Rys. 2.2.1. Właściwości połączenia LAN

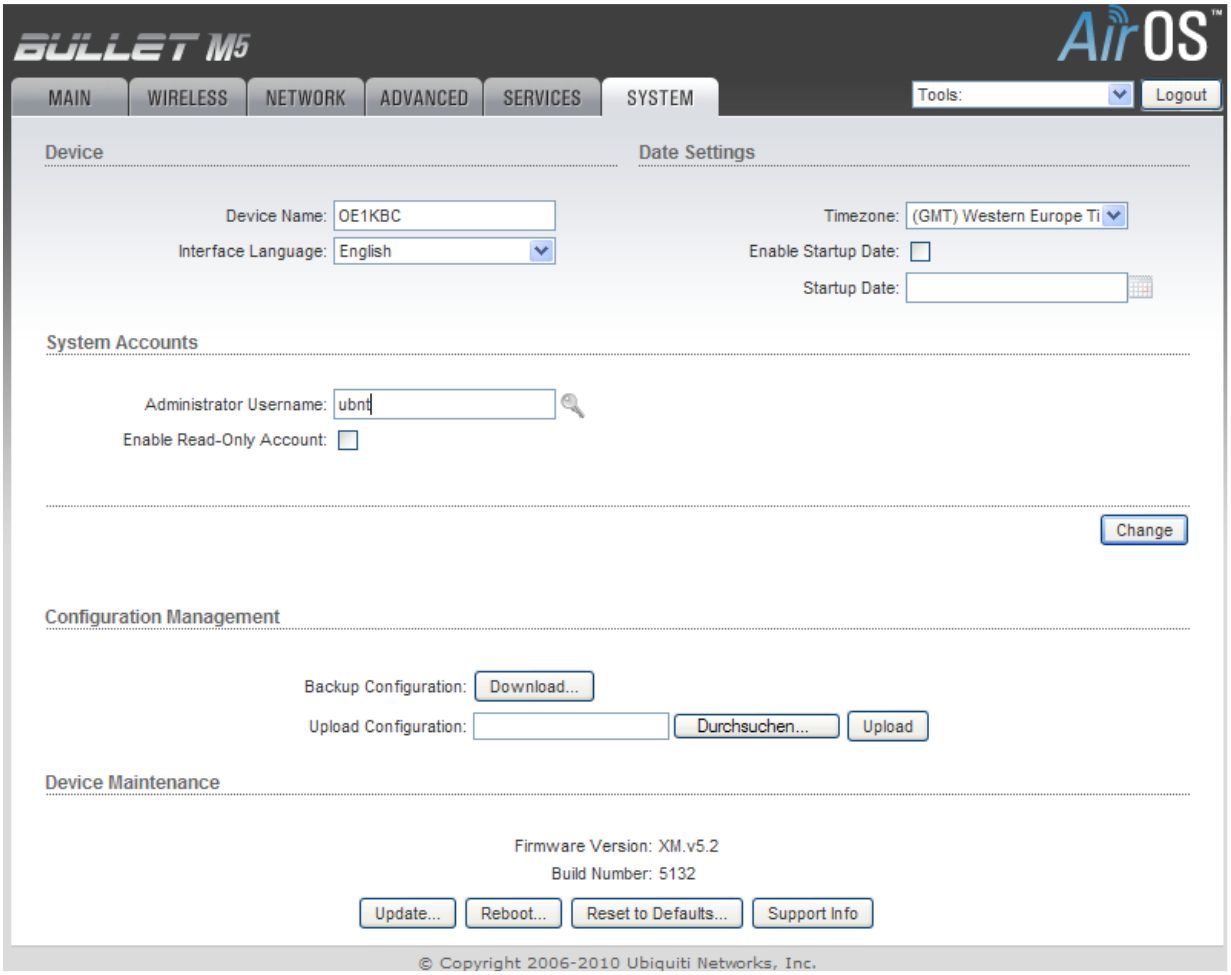
Po podwójnym naciśnięciu w spisie punktu „Protokół internetowy (TCP/IP)” lub naciśnięciu przycisku właściwości po prawej stronie poniżej otwierane jest okno przedstawione na rys. 2.2.2.



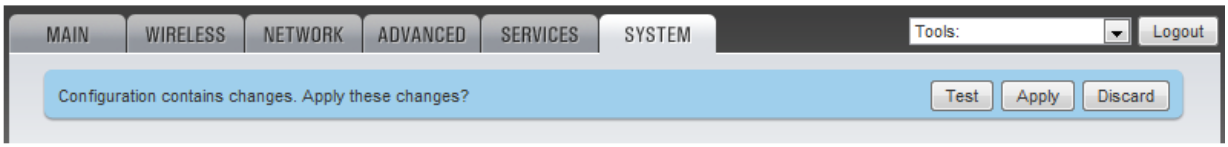
Rys. 2.2.2. Adres w sieci i jej maska

W oknie tym należy wprowadzić adres IP używany przez komputer i maskę podsieci – jest to dowolny adres w podsieci 192.168.1.x, różny oczywiście od używanego przez „Bulleta”.

Po uzyskaniu połączenia na ekranie komputera widoczne jest okno konfiguracyjne sprzętu (rys. 2.2.3) zawierające 7 zakładek. Rozpoczynamy od zakładki „System”. W zakładce tej należy wprowadzić przede wszystkim własny znak wywoławczy w polu „Device name” („Nazwa urządzenia”). Po jego wpisaniu należy zmianę potwierdzić za pomocą przycisku „Change” („Zmień”). Po jego naciśnięciu u góry okna wyświetlana jest niebieska linia (rys. 2.2.4) z przyciskami „Test” („Sprawdź”), „Apply” („Zastosuj”) i „Discard” („Zrezygnuj”). Wszystkie pożądane zmiany należy potwierdzić za pomocą przycisku „Apply” („Zastosuj’) po czym można przejść do następnych. Po naciśnięciu przycisku „Zastosuj” należy odczekać 5-8 sekund na zapisanie danych. Na ekranie nie jest w tym czasie niestety wyświetlany pasek informujący o przebiegu akcji.
Ilustracje w poniższym przykładzie pochodzą z opr. [1] (patrz spis literatury) dotyczącego konfiguracji modelu M5. Konfiguracja M2 przebiega zasadniczo w ten sam sposób.
Należy pamiętać aby po wprowadzeniu danych na każdej z zakładek (lub w ich sekcjach) potwierdzić zmiany za pomocą znajdującego się na danej zakładce gdyż w przeciwnym przypadku po przejściu na następną zmiany zostaną stracone. Wszystkie dane, w tym hasło dostępu dla administratora można zmienić później w dowolnym momencie. Dlatego też zarówno tutaj jak i przy omawianiu następnych zakładek opisywane są zmiany jedynie niezbędnych parametrów.

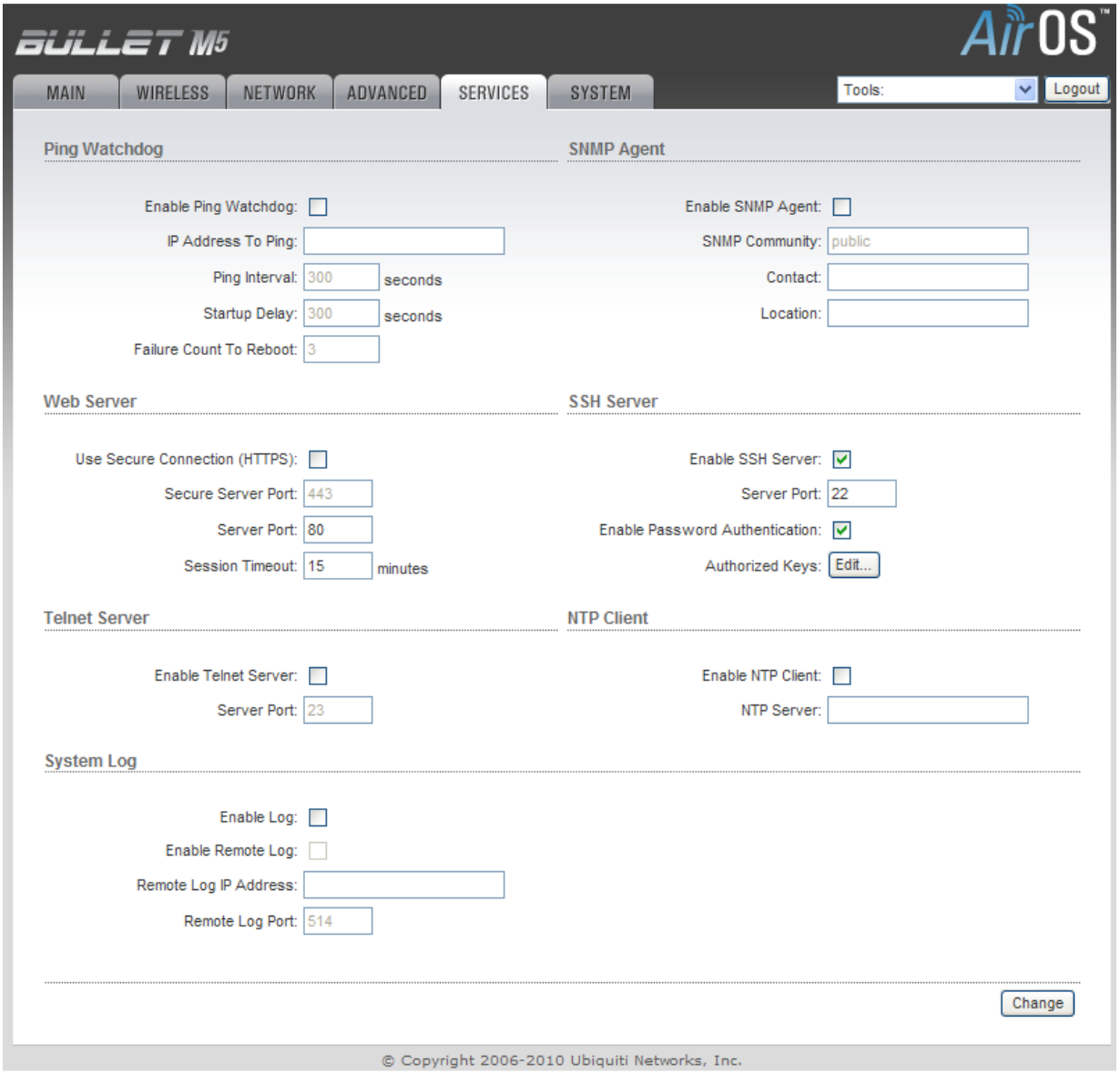


Rys. 2.2.3. Okno konfiguracyjne, zakładka „System”

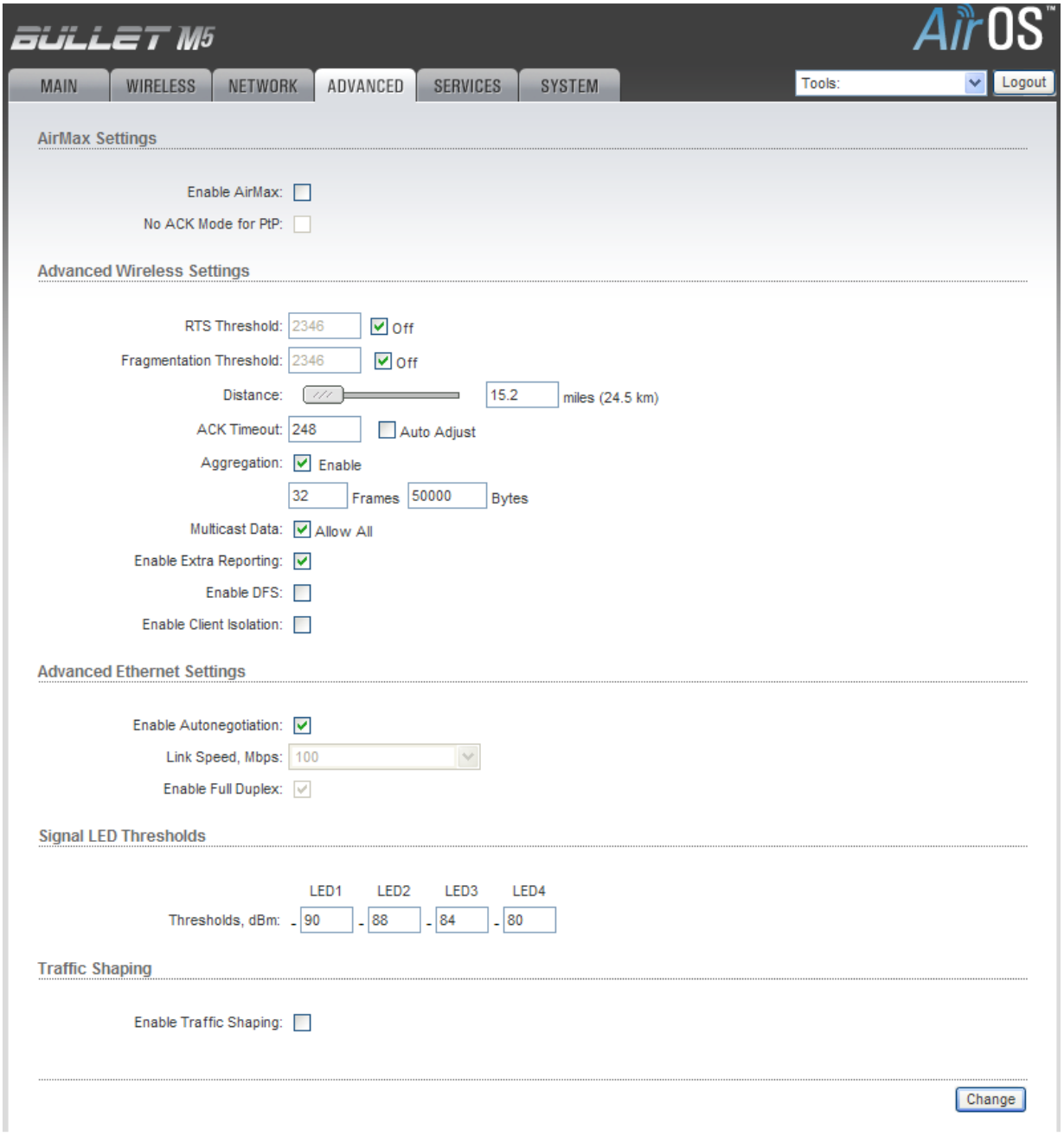


Rys. 2.2.4. Pasek wyboru zastosowania zmian lub rezygnacji z nich

Na następnej zakładce „Services” („Usługi”) – rys. 2.2.5 – wszystko pozostaje w stanie domyślnym.



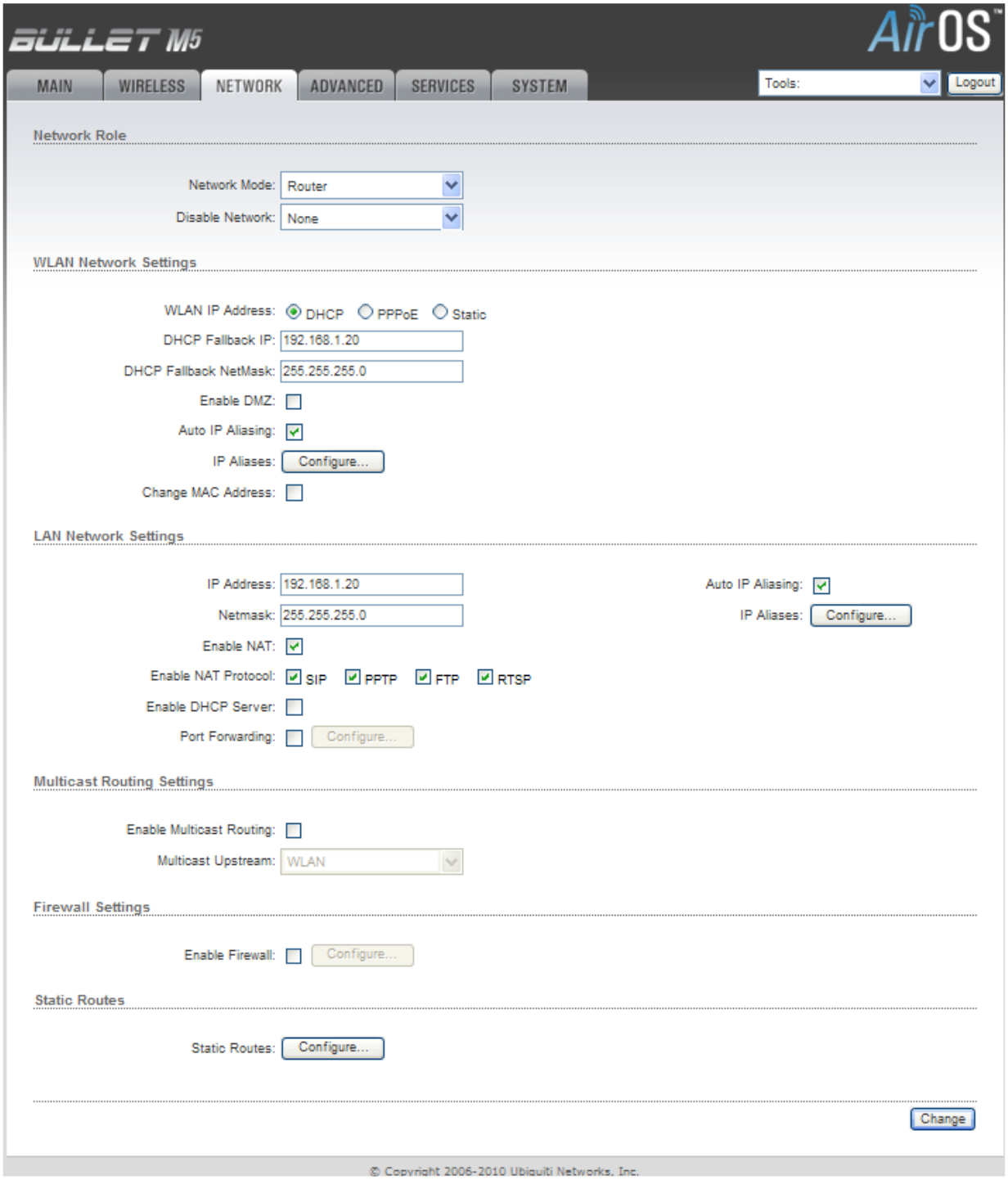
Rys. 2.2.5. Zakładka „Services” („Usługi”)



Rys. 2.2.6. Zakładka „Advanced” („Zaawansowane”)

W zakładce tej należy za pomocą suwaka nastawić orientacyjną odległość do przemiennika wejściowego do sieci (w polu „Distance”).
Wartości progów świecenia dla diod LED1-LED4 widocznego na obudowie wskaźnika siły sygnału można pozostawić bez zmian lub też dostosować je do rzeczywistej sytuacji – siły sygnału przemiennika dostępowego.
Dla słabszych sygnałów mogą to być progi 90, 88, 84 i 80 dBm. Przy należytym doborze progów wskaźnik siły sygnału może być istotną pomocą przy ustawianiu anteny.
W zakładce „Network” („Sieć”) podawany jest adres IP urządzenia w sieci lokalnej. Adres IP w sieci WLAN czyli „Hamnetu” pobierany jest automatycznie z serwera DHCP. W uzasadnionych przypadkach możliwe jest także korzystanie ze stałego (statycznego) adresu IP. W obu przypadkach są to adresy z krótkofalarskiej serii 44.x.x.x.
W przykładzie z rys. 2.8 pozostawiono domyślny adres 192.168.1.20 (należący do zakresu adresów 192.168.0.254 – 192.168.255.0 przeznaczonych dla sieci prywatnych, Intranetów itp.) ale w wielu przypadkach wygodniejsze może być podanie tutaj innego adresu, np. w przypadku gdy punkt (węzeł)

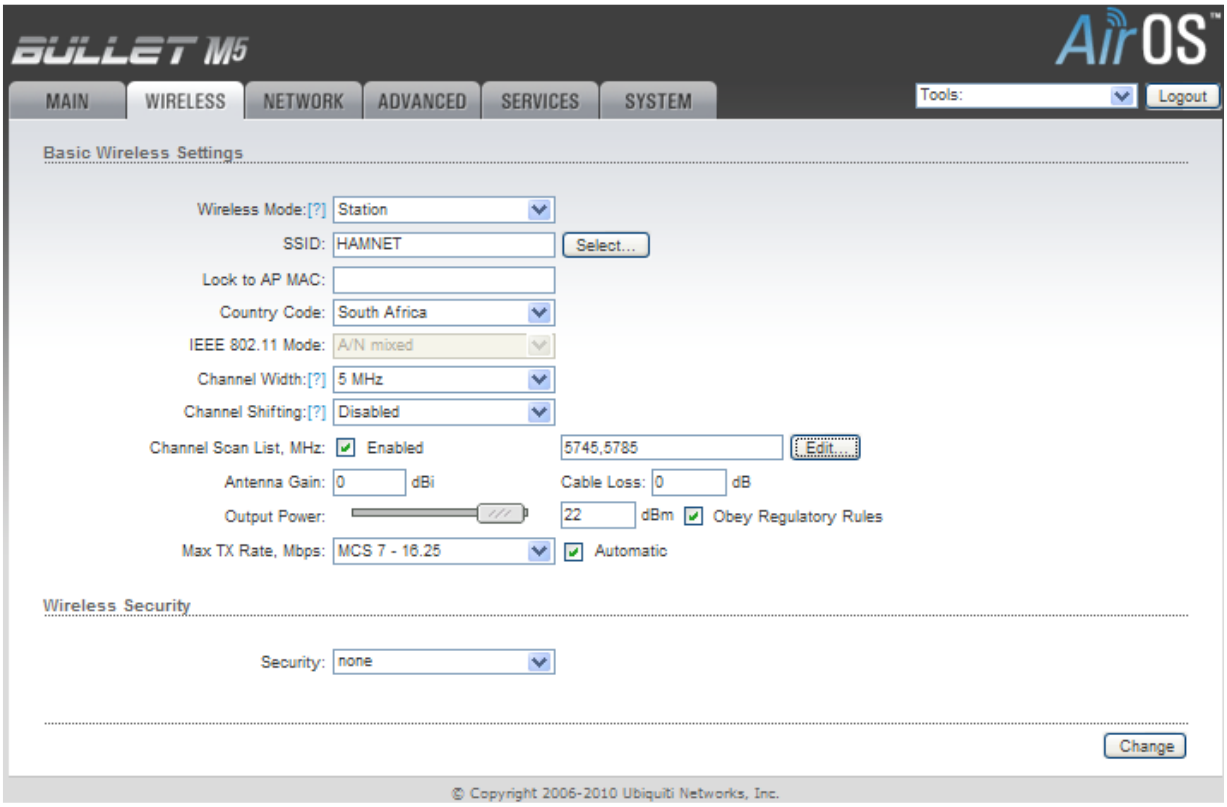
dostępowy (ang. *router*) korzysta z adresu w podsieci 10.x.x..x lub innej, a użytkownik chce bez większych komplikacji korzystać na tym komputerze z dostępów do Internetu i „Hamnetu”.



Rys. 2.2.7. Zakładka sieci

Ostatnim krokiem jest konfiguracja łącza radiowego w zakładce „Wireless” („Łącze radiowe”) – rys. 2.2.8. Podawane w niej są częstotliwość pracy, szerokość pasma sygnału i szybkość transmisji. Ważne jest aby w polu nazwy sieci („SSID”) podać nawę „HAMNET” pisaną dużymi literami. Nieprawidłowo podana nazwa nie tylko uniemożliwia nawiązanie połączenia, ale także i wyświetlanie siły sygnału (ułatwiające nakierowanie anteny). Standardowo używana jest wprawdzie nazwa „HAMNET” ale zdarzają się też lokalnie trochę różne warianty nazwy.

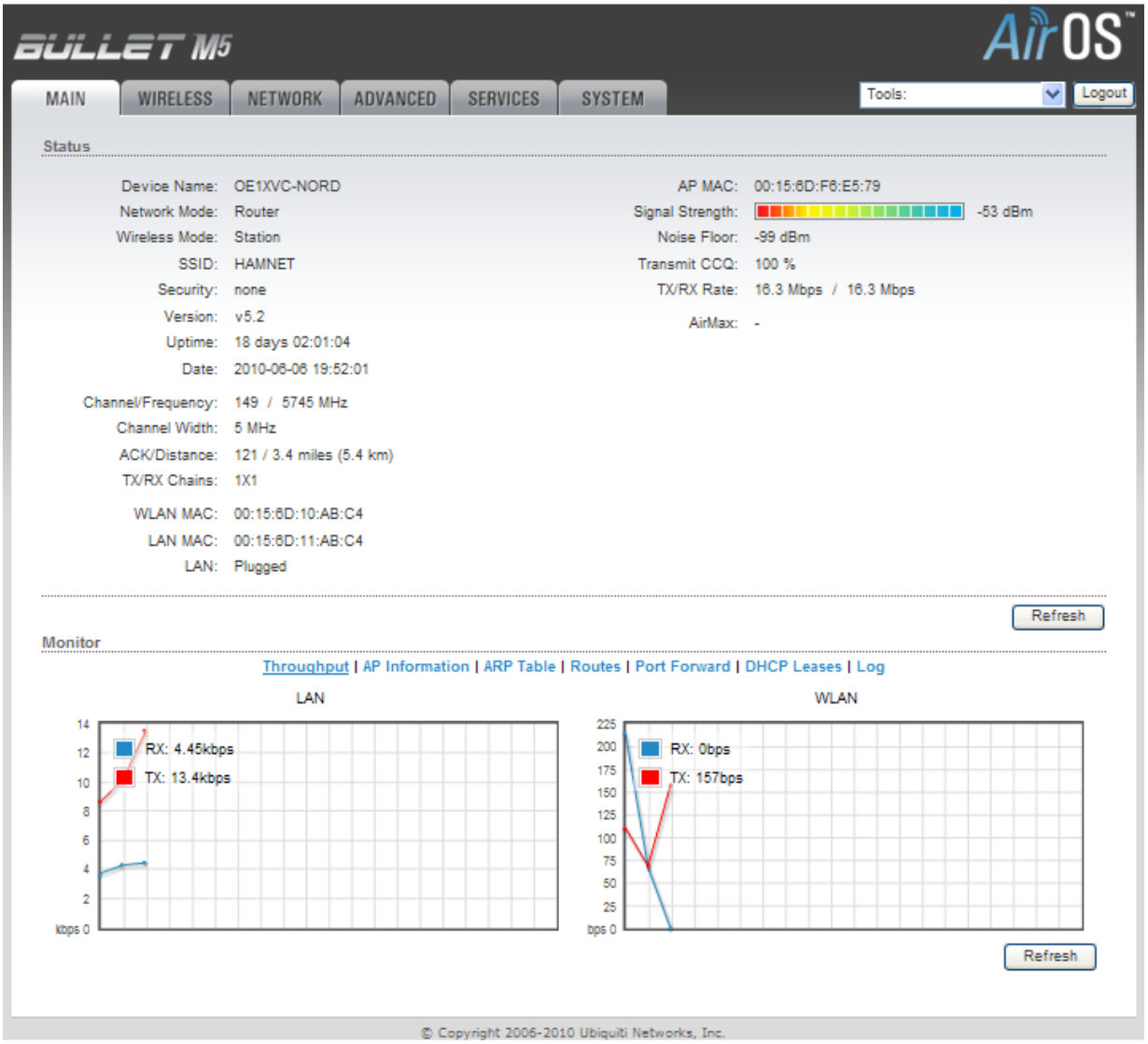
Znajdujący się obok po prawej stronie przycisk „Select” pozwala na przeszukanie pasma i następnie wybranie nazwy ze spisu odbieranych sieci.
W polach kodu kraju („Country code”) i szerokość pasma („Channel width”) można ustawić jako wybór test zgodności (punkt „Compliance test”) i przyjąć ustawienie dokonane przez program.
W przykładzie poniższym ustawiona została szerokość pasma 5 MHz i Pd. Afryka. Najczęściej stosowaną szerokością pasma jest 5 MHz, częściowo 10 MHz, a w paśmie 6 cm także 20 MHz. Szerokość pasma musi być zgodna ze stosowaną przez przemiennnik dostępowy „Hamnetu”.
W polu kanału należy ustawić częstotliwość przemiennika dostępowego. Po zaznaczeniu pola „Enabled” możliwe jest wybranie i zaznaczenie w spisie więcej niż jednej częstotliwości (jeśli stacja znajduje się w zasięgu więcej niż jednego przemiennika dostępowego), a właściwa częstotliwość (najkorzystniejsza) zostanie wybrana automatycznie. W poniższym przykładzie są to dwie częstotliwości wiedeńskie. W przypadku słabego odbioru najlepiej samemu wybrać najkorzystniejszą.



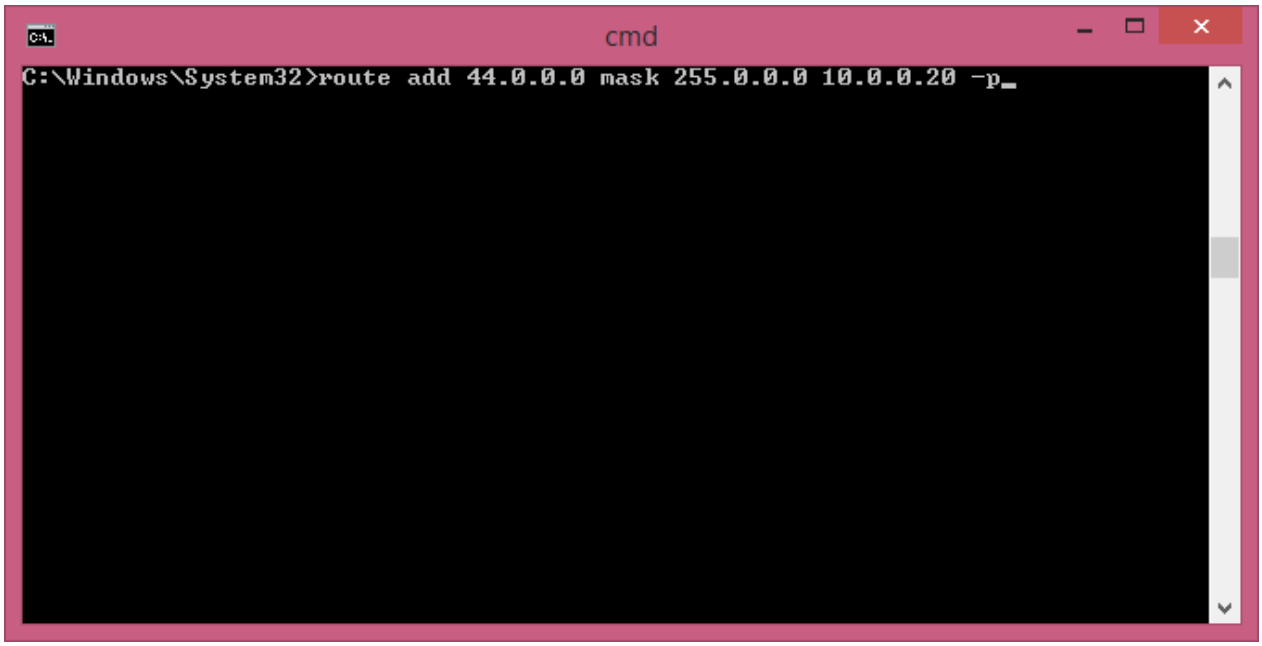
Rys. 2.2.8. Zakładka łącza radiowego

Po potwierdzeniu zmian za pomocą przycisków „Change” („Zmień”) i „Apply” („Zastosuj”) zakładka główna („Main”) może wyglądać podobnie do pokazanej na rys. 2.2.9.
Korygując ustawienie anteny można ewentualnie uzyskać poprawę siły sygnału – wyświetlanej w tej właśnie zakładce.
Dla sprawdzenia jakości połączenia można otworzyć wywołać przeglądarkę internetową i wywołać którąś ze stron internetowych dostępnych w „Hamnecie”. Przed rozpoczęciem prób połączeń warto upewnić się jakie usługi dostępne są w sieci „Hamnetu” i wykorzystać do prób serwer http jeśli jest on dostępny albo jakiś inny. Serwery http występują stosunkowo często w sieciach „Hamnetu” a więc z dużym prawdopodobieństwem właśnie w ten sposób najłatwiej będzie można sprawdzić jakość połączenia. Założeniem twórców sieci jest pokrycie jej zasięgiem możliwie jak największej części terytorium kraju ale w pierwszych fazach budowy i rozbudowy mogą to być niewielkie wysepki różniące się wyposażeniem i dostępnymi usługami – przynajmniej do czasu rozbudowy szkieletowej sieci szybkich łączy. Jak wiadomo nie od razu Kraków zbudowano...
Adresy dostępnych serwerów należą do domeny *ampr.org* (w Austrii przykładowo *ampr.at*), a w formie liczbowej do przyznanej krótkofalowcom serii 44.x.x.x, w której druga grupa oznacza przeważnie kraj.

W przypadku korzystania na tym samym komputerze z dostępu do zarówno do Internetu jak i do „Hamnetu” należy na komputerze wpisać stałą trasę dla adresów serii 44 – czyli 44.0.0.0/8 z podaniem maski sieciowej 255.0.0.0 – prowadzącą przez bramkę o adresie 192.168.1.20 (lub innym podanym w powyższej konfiguracji). Niewpisanie podanej trasy spowoduje, że adresów z serii 44 komputer będzie poszukiwał w Internecie, gdzie ich oczywiście nie znajdzie.
Do wpisania trasy na komputerze należy otworzyć okno wiersza poleceń (rys. 2.11) i wpisać do niego polecenie
route add 44.0.0.0 mask 255.0.0.0 192.168.1.20 –p
gdzie zamiast 192.168.1.20 należy użyć adresu podanego w konfiguracji „Bulleta”. Argument –p oznacza trasę stałą używaną także po następnych uruchomieniach komputera.
W przypadku istniejącej już sieci domowej złożonej z wielu innych urządzeń może okazać się konieczne podanie innego adresu w konfiguracji „Bulleta”. Dla sieci domowych o adresach z serii 10.0.0.0/24 (10.0.0.0 – 10.255.255.255) wygodnie będzie nadać „Bulletowi” adres z tej serii np. 10.0.0.20 (należy go oczywiście użyć w poleceniu *route add* zamiast podanego tam przykładowego). Trzecim zakresem adresów przeznaczonym dla prywatnych sieci domowych, Intranetu itd. jest seria 172.16.x.x (172.16.0.0 – 172.31.0.0). Wrowadzoną w ten sposób trasę można usunąć za pomocą polecenia *route delete* lub skorygować w miarę potrzeby za pomocą polecenia *route change*.
Po zmianie adresu „Bulleta” w konfiguracji i potwierdzeniu za pomocą przycisków „Change” („Zmień”) i „Apply” („Zastosuj”) należy również na komputerze powrócić do adresu z tej serii przed kontynuowaniem dalszej konfiguracji.



Rys. 2.2.9. Zakładka główna



Rys. 2.2.10. Dodanie w komputerze stałej trasy prowadzącej do sieci 44.x.x.x

Rys. 2.2.11. Przykład konstrukcji anteny planarnej PA-5000-23 o zysku 23 dBi na pasmo 5,1 – 5,825 GHz (dla standardów 802.11a/n). Antena ma polaryzację liniową, szerokość wiązki w obu płaszczyznach 16°, wymiary 322 x 322 x 12 mm i waży ok. 1360 g. Dopuszczalna moc doprowadzona do jej zacisków (gniazda N) wynosi 10 W. Zysk przystępnych anten planarnych na pasmo 2,4 GHz jest przeważnie trochę niższy i wynosi ok. 20 dBi. Anteny planarne stanowią praktyczną alternatywę dla rozpowszechnionych anten parabolicznych

3. Instalacja i konfiguracja Ubiquiti Nanostation

3.1. Informacje ogólne

Punkt dostępowy „Nanostation" firmy Ubiquiti zawiera wbudowaną antenę dzięki czemu stanowi zwartą całość dającą się wygodnie umieścić na maszcie antenowym. W komplecie z „Nanostation" sprzedawany jest przeważnie także zasilacz 24 V do zasilania przez kabel ethernetowy (PoE), kabel sieciowy, wiązadła montażowe i krótka instrukcja.
Producent wymaga aby do połączenia z komputerem używać 8-żyłowego ekranowanego kabla ethernetowego i zapewnić należyte uziemienie. Długość kabla pomiędzy „Nanostation", a zasilaczem może dochodzić nawet do 30 i więcej m.
„Nanostation" ma wymiary 294 x 30 x 80 mm i wagę 0,4 (M2/M5) lub 0,5 kg (M3). Maksymalny pobór mocy wynosi 8 W (zasilacz 0,5 A – M2/5, 1 A – M3/365).
„Nanostation Loco" ma natomiast wymiary 163 x 31 x 80 mm (M2/M5) i wagę 0,18 kg. Maksymalny pobór mocy dla modeli M2 i M5 wynosi 5,5 W (zasilacz 0,5 A).
Wszystkie modele „Nanostation" oraz „Nanostation Loco" M2/M5 (w dalszym ciągu określane skrótowo jako „Nanostation") są wyposażone w procesor Atheros MIPS 24KC, 32 MB dynamicznej pamięci RAM i 8 MB pamięci programu programowalnej i kasowanej elektrycznie.

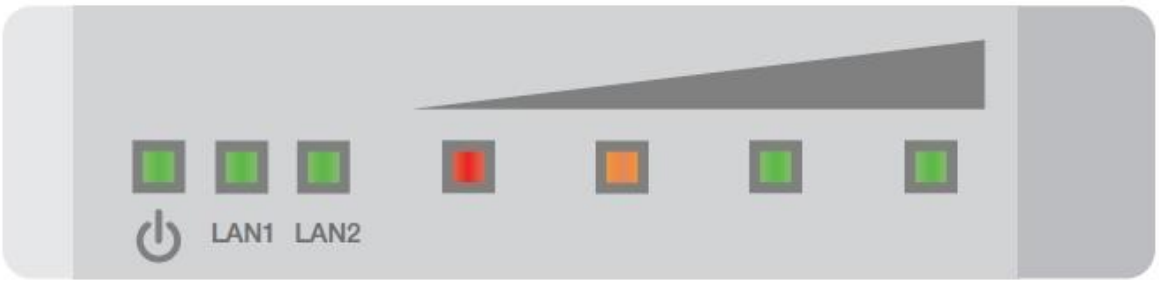
Rys. 3.1.1. Widok „Nanostation". W drugie gniazdo Ethernetu są wyposażone jedynie modele M2/M3/M5. Do zasilania przez kabel ethernetowy należy użyć zasilacza 24 V. „Nanostation Loco" posiada tylko jedno gniazdo

Tabela 3.1.1
Przegląd modeli serii „Nanostation”

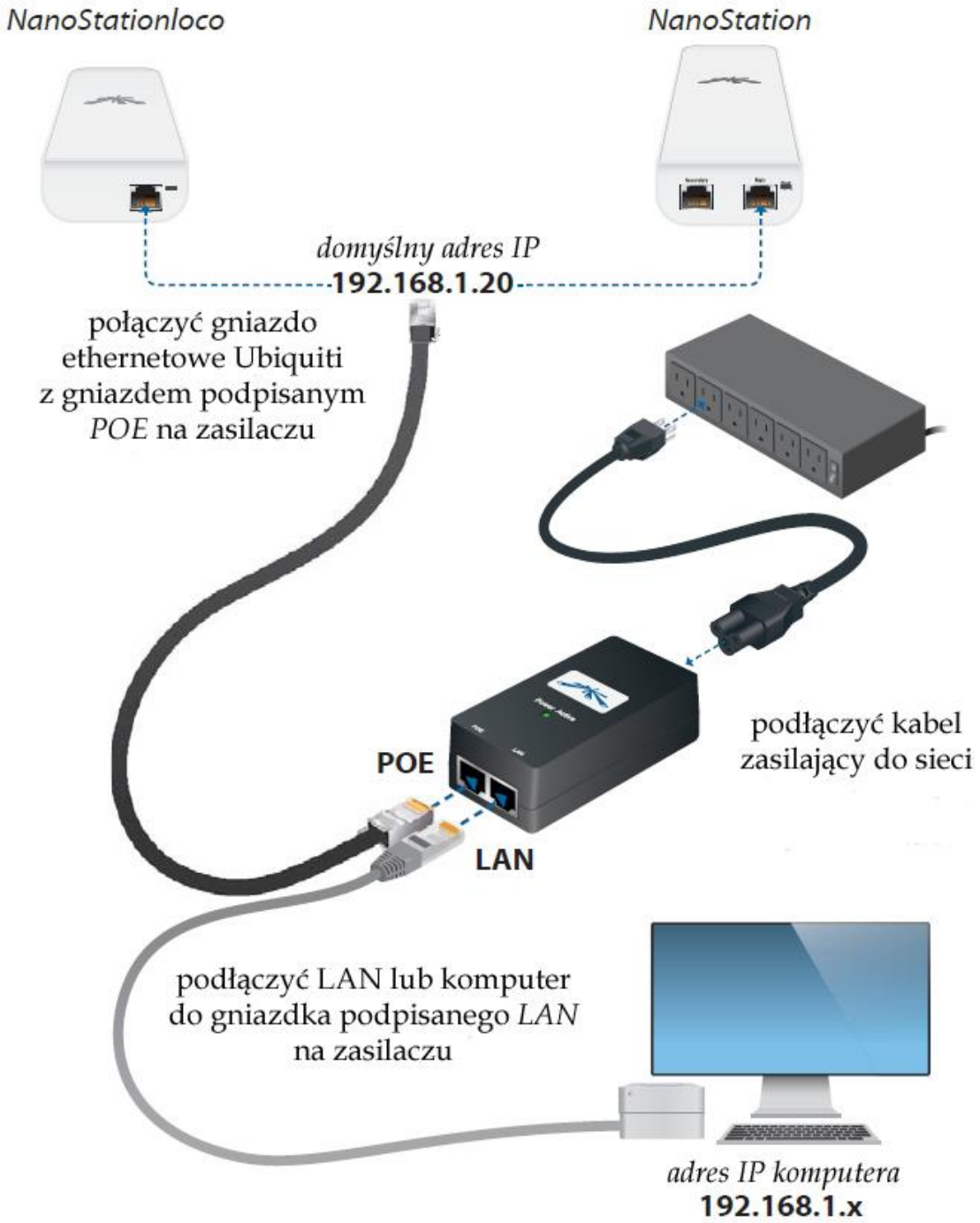
Model	Zakres częstotliwości	Liczba gniazd Ethernetu	Moc wyjściowa	Zysk antenowy
Nanostation M2	2412 – 2462 MHz	2	28 dBm	11 dBi
Nanostation M3	3400 – 3700 MHz	2	25 dBm	13,7 dBi
Nanostation M365	3650 – 3675 MHz	2	25 dBm	13,7 dBi
Nanostation M5	5170 – 5875 MHz	2	27 dBm	16 dBi
Nanostation Loco M9	902 – 928 MHz	1	28 dBm	8 dBi
Nanostation Loco M2	2412 – 2462 MHz	1	23 dBm	8 dBi
Nanostation Loco M5	5170 – 5875 MHz	1	23 dBm	13 dBi

Tabela 3.1.2
Sygnalizacja za pomocą diod świecących

	Zielona dioda sygnalizujaca włączenie zasilania
LAN1	Dioda świeci stale na zielono po podłączeniu gniazda głównego do sieci lokalnej, miga w trakcie wymiany danych
LAN2	Dioda świeci stale na zielono po podłączeniu gniazda pomocniczego do sieci lokalnej, miga w trakcie wymiany danych
	Wskaźnik siły odbieranego sygnału. Progi dla znajdujących się poniżej diod można zmieniać w konfiguracji. Poniżej podane są wartości domyślne.
	Czerwona dioda świeci się gdy siła sygnału przekracza poziom -94 dBm (lub inny ustawiony w konfiguracji)
	Pomarańczowa dioda świeci się gdy siła sygnału przekracza poziom -80 dBm (lub inny ustawiony w konfiguracji)
	Pierwsza zielona dioda świeci się gdy siła sygnału przekracza poziom -73 dBm (lub inny ustawiony w konfiguracji)
	Druga zielona dioda świeci się gdy siła odbieranego sygnału przekracza -65 dBm (lub inny ustawiony w konfiguracji)



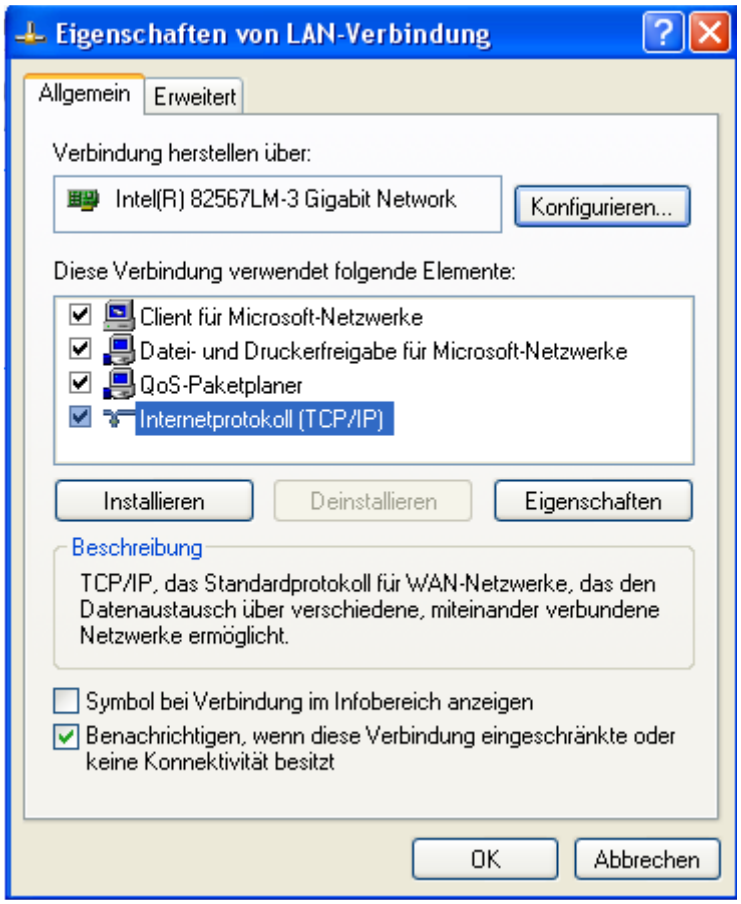
Rys. 3.1.2. Diody sygnalizacyjne na tylnej ściance „Nanostation”



Rys. 3.1.3. Połączenie „Nanostation” lub „Nanostation Loco” z zasilaczem i z komputerem

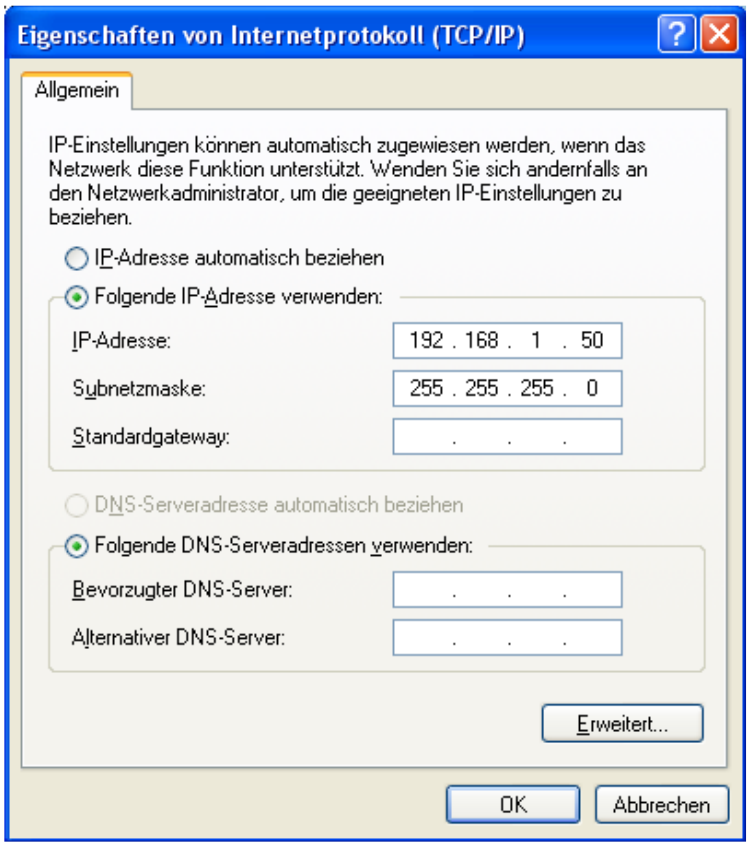
3.2. Konfiguracja do celów „Hamnetu”

W celu skonfigurowania „Nanostation” należy wywołać przeglądarkę internetową i w jej polu adresowym podać adres **https://192.168.1.20**. Po nawiązaniu przez komputer połączenia na jego ekranie pojawia się okno meldunkowe, w kórym należy podać **ubnt** jako nazwę użytkownika i jako hasło dostępu.
Po zameldowaniu się na ekranie wyświetlane jest okno konfiguracyjne zawierające 7 zakładek. System operacyjny „Nanostation” airOS pozwala na obszerną, intuicyjną konfigurację, a co najważniejsze z krótkofalarskiego punktu widzenia także na ograniczenie szerokości pasma sygnału do wartości ustalonych w przepisach o służbie amatorskiej. Konfiguracja dla sieci WLAN powszechnego użytku omówiona jest szczegółowo w dokumentacji sprzętu, dlatego też w niniejszym opracowaniu ograniczymy się jedynie do konfiguracji dla pracy w amatorskiej sieci Hamnetu.
W zależności od dotychczasowych ustawień dostępu do sieci WLAN w komputerze przed połączeniem się przez przeglądarkę internetową może być konieczne ustawienie adresu z podsieci 192.168.1.x tak aby możliwe było połączenie się z podanym powyżej adresem 192.168.1.20.
Należy dokonać tego w ustawieniach połączenia LAN w części dotyczącej sieci w „Panelu sterowania” Windows.



Rys. 3.2.1. Właściwości połączenia LAN

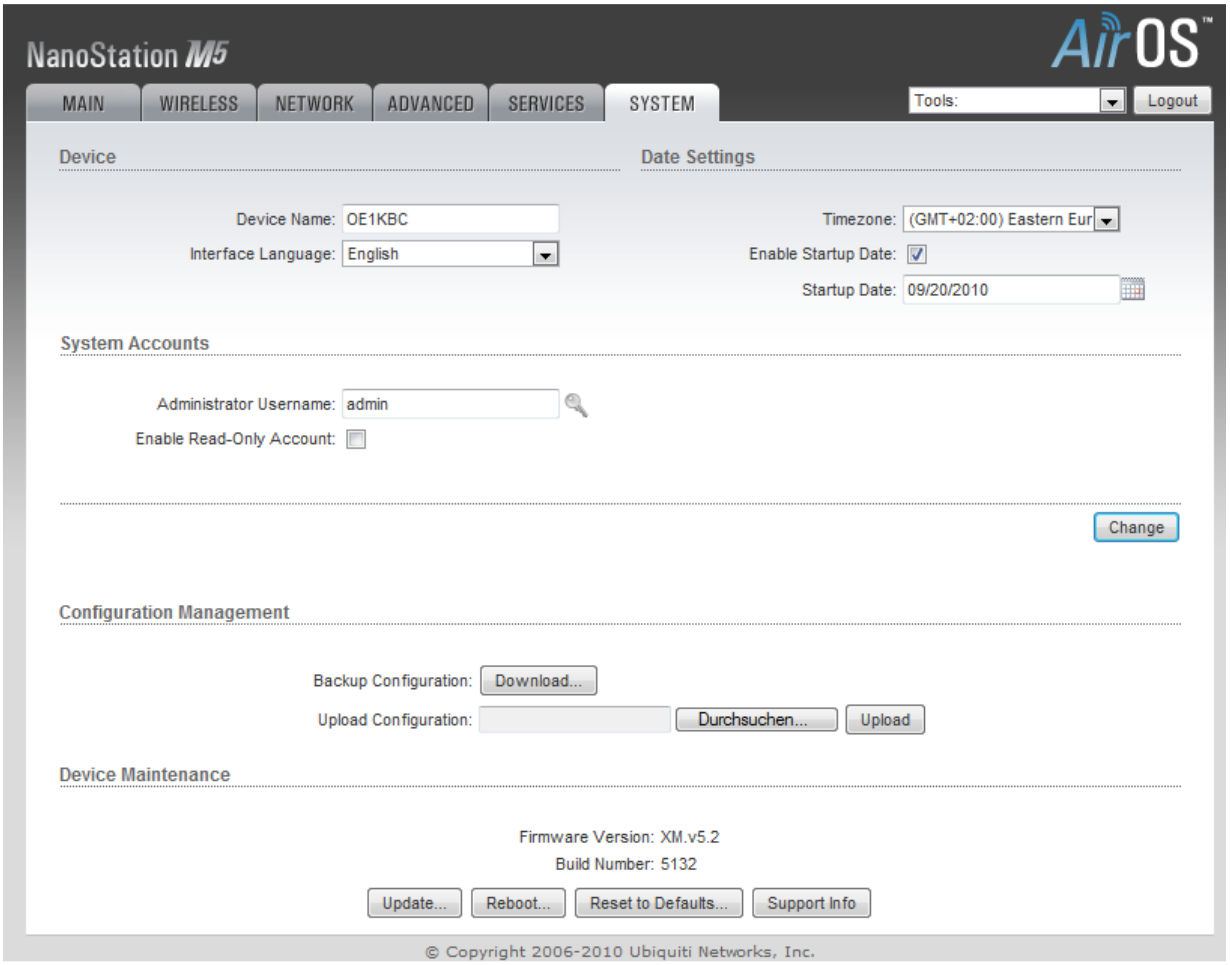
Po podwójnym naciśnięciu punktu „Protokół internetowy (TCP/IP)” lub naciśnięciu przycisku właściwości po prawej stronie poniżej otwierane jest okno przedstawione na rys. 3.2.2.



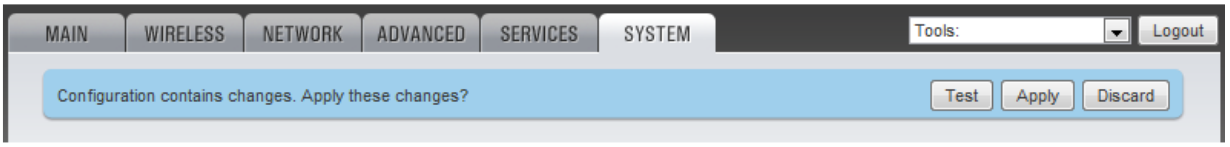
Rys. 3.2.2. Adres w sieci i jej maska

W oknie tym należy wprowadzić adres IP używany przez komputer i maskę podsieci – jest to dowolny adres w podsieci 192.168.1.x, różny oczywiście od używanego przez „Nanostation".

Po uzyskaniu połączenia na ekranie komputera widoczne jest okno konfiguracyjne sprzętu (rys. 3.2.3) zawierające 7 zakładek. Rozpoczynamy od zakładki „System". W zakładce tej należy wprowadzić przede wszystkim własny znak wywoławczy w polu „Device name" („Nazwa urządzenia"). Po jego wpisaniu należy zmianę potwierdzić za pomocą przycisku „Change" („Zmień"). Po jego naciśnięciu u góry okna wyświetlana jest niebieska linia (rys. 2.2.4) z przyciskami „Test" („Sprawdź"), „Apply" („Zastosuj") i „Discard" („Zrezygnuj"). Wszystkie pożądane zmiany należy potwierdzić za pomocą przycisku „Apply" („Zastosuj') po czym można przejść do następnych. Po naciśnięciu przycisku „Zastosuj" należy odczekać 5-8 sekund na zapisanie danych. Na ekranie nie jest w tym czasie niestety wyświetlany pasek informujący o przebiegu akcji.
Ilustracje w poniższym przykładzie pochodzą z opr. [2] (patrz spis literatury) dotyczącego konfiguracji modelu M5. Konfiguracja M2 przebiega zasadniczo w ten sam sposób.
Należy pamiętać aby po wprowadzeniu danych na każdej z zakładek (lub w ich sekcjach) potwierdzić zmiany za pomocą znajdującego się na danej zakładce gdyż w przeciwnym przypadku po przejściu na następną zmiany zostaną stracone. Wszystkie dane, w tym hasło dostępu dla administratora można zmienić później w dowolnym momencie. Dlatego też zarówno tutaj, jak i przy omawianiu następnych zakładek opisywane są zmiany jedynie niezbędnych parametrów.

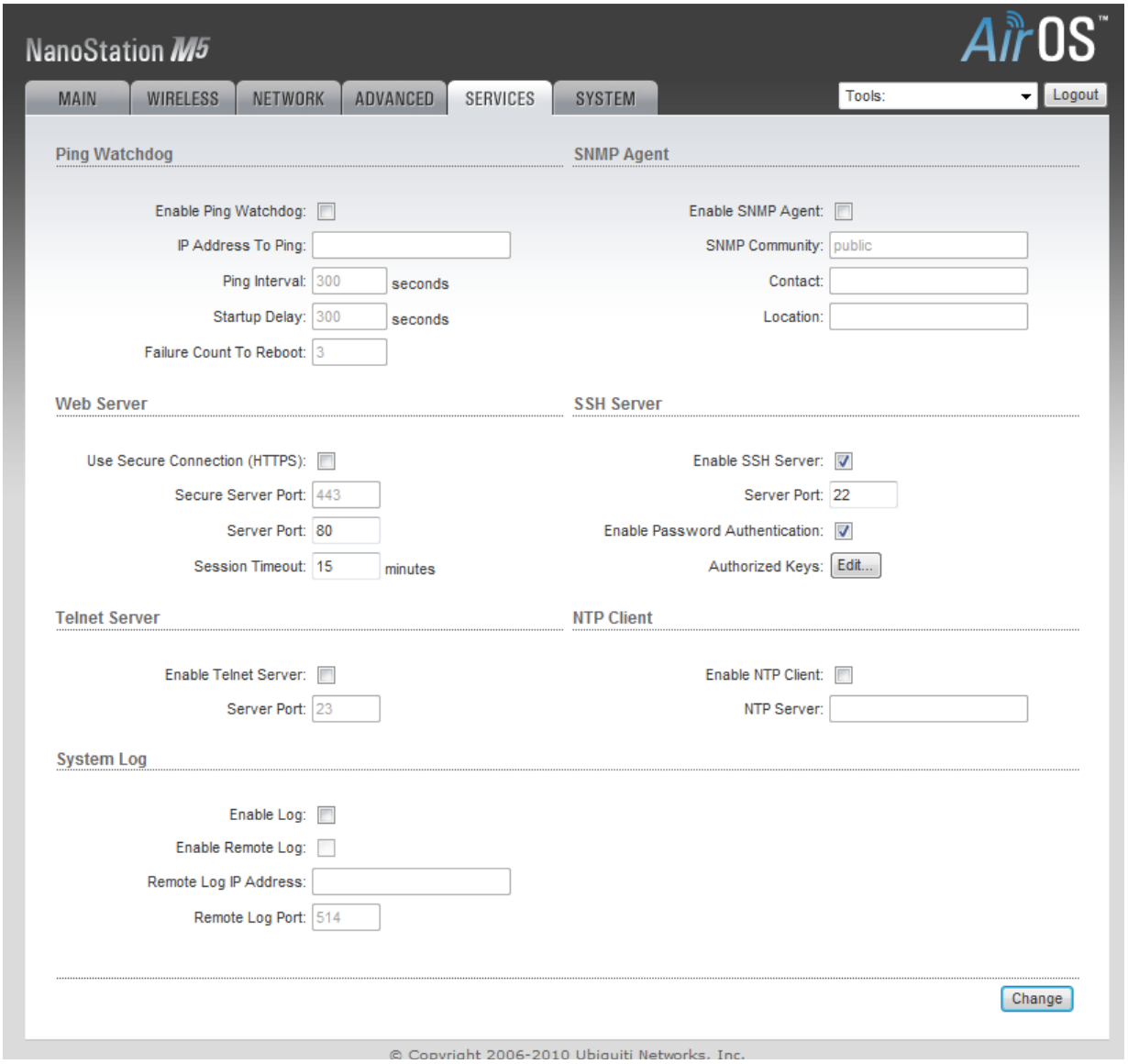


Rys. 3.2.3. Okno konfiguracyjne. Zakładka „System”

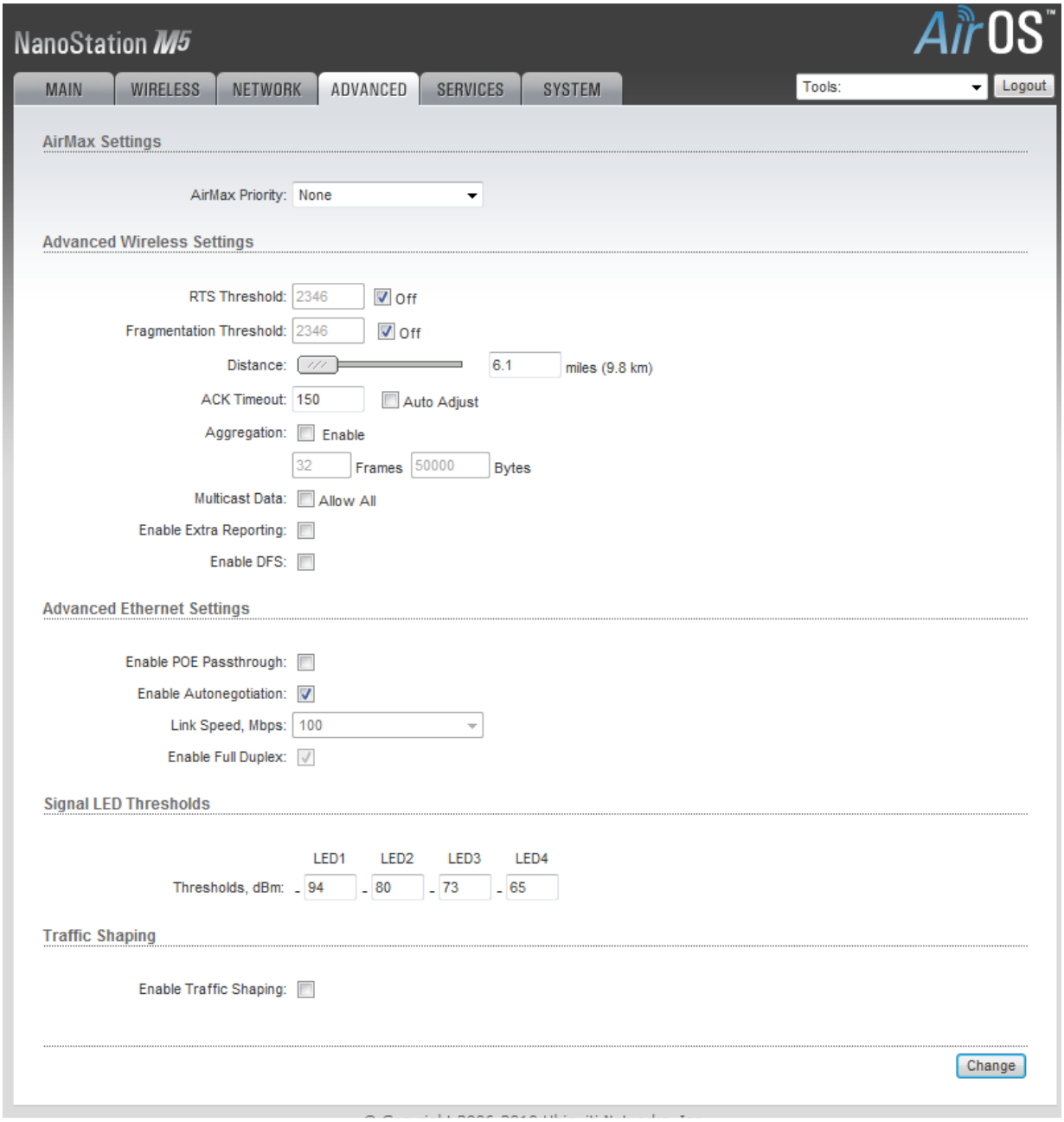


Rys. 3.2.4. Pasek wyboru zastosowania zmian lub rezygnacji z nich

Na następnej zakładce „Services” („Usługi”) – rys. 3.2.5 – wszystko pozostaje w stanie domyślnym.



Rys. 3.2.5. Zakładka „Services” („Usługi”)

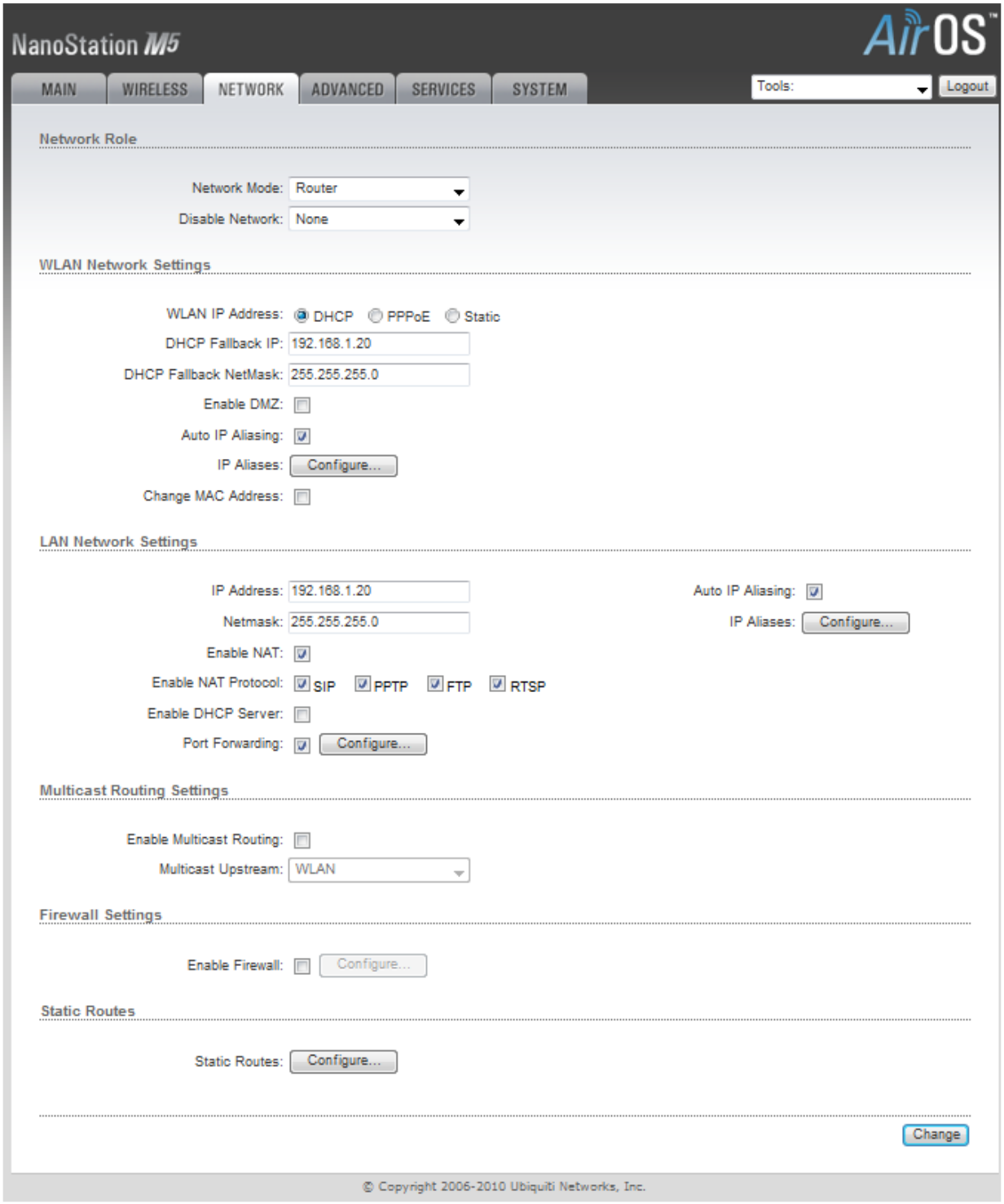


Rys. 3.2.6. Zakładka „Advanced” („Zaawansowane”)

W zakładce tej należy za pomocą suwaka nastawić orientacyjną odległość do przemiennika wejściowego do sieci (w polu „Distance”).
Wartości progów świecenia dla diod LED1–LED4 widocznego na obudowie wskaźnika siły sygnału można pozostawić bez zmian lub też dostosować je do rzeczywistej sytuacji – siły sygnału przemiennika dostępowego.
Dla słabszych sygnałów mogą to być progi 90, 88, 84 i 80 dBm. Przy należytym doborze progów wskaźnik siły sygnału może być istotną pomocą przy ustawianiu anteny.

W zakładce „Network” („Sieć”) podawany jest adres IP urządzenia w sieci lokalnej. Adres IP w sieci WLAN czyli „Hamnetu” pobierany jest automatycznie z serwera DHCP. W uzasadnionych przypadkach możliwe jest także korzystanie ze stałego adresu IP. W obu przypadkach są to adresy z krótkofalarskiej serii 44.x.x.x.
W przykładzie z rys. 3.2.7 pozostawiono domyślny adres 192.168.1.20, ale w wielu przypadkach wygodniejsze może być podanie tutaj innego adresu, np. w przypadku gdy punkt (węzeł) dostępowy (ang.

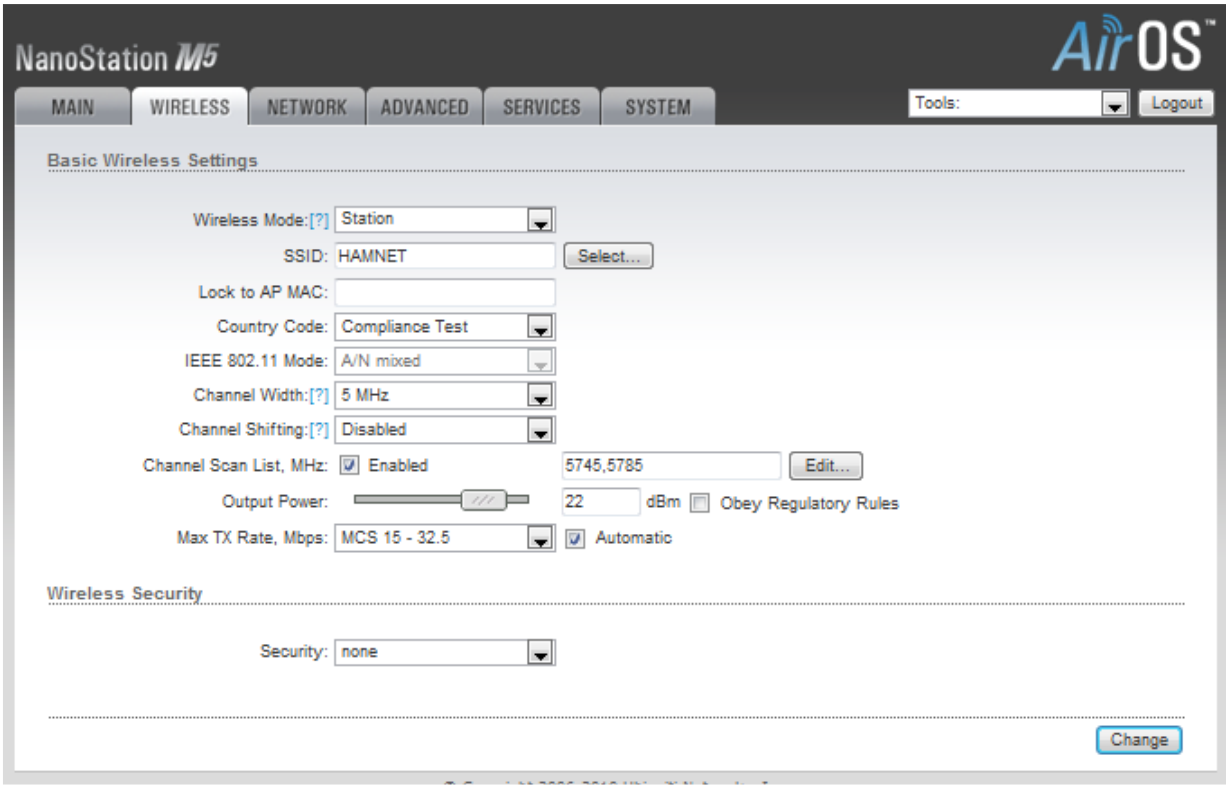
router) korzysta z adresu w podsieci 10.x.x..x lub innej, a użytkownik chce bez większych komplikacji korzystać na tym komputerze z dostępów do Internetu i „Hamnetu”.



Rys. 3.2.7. Zakładka sieci

Ostatnim krokiem jest konfiguracja łącza radiowego w zakładce „Wireless” („Łącze radiowe”) – rys. 3.2.8. Podawane w niej są częstotliwość pracy, szerokość pasma sygnału i szybkość transmisji. Ważne jest aby w polu nazwy sieci („SSID”) podać nawę „HAMNET” pisaną dużymi literami lub jej odmianę używaną w danym rejonie. Nieprawidłowo podana nazwa nie tylko uniemożliwia nawiązanie połączenia, ale także i wyświetlanie siły sygnału.

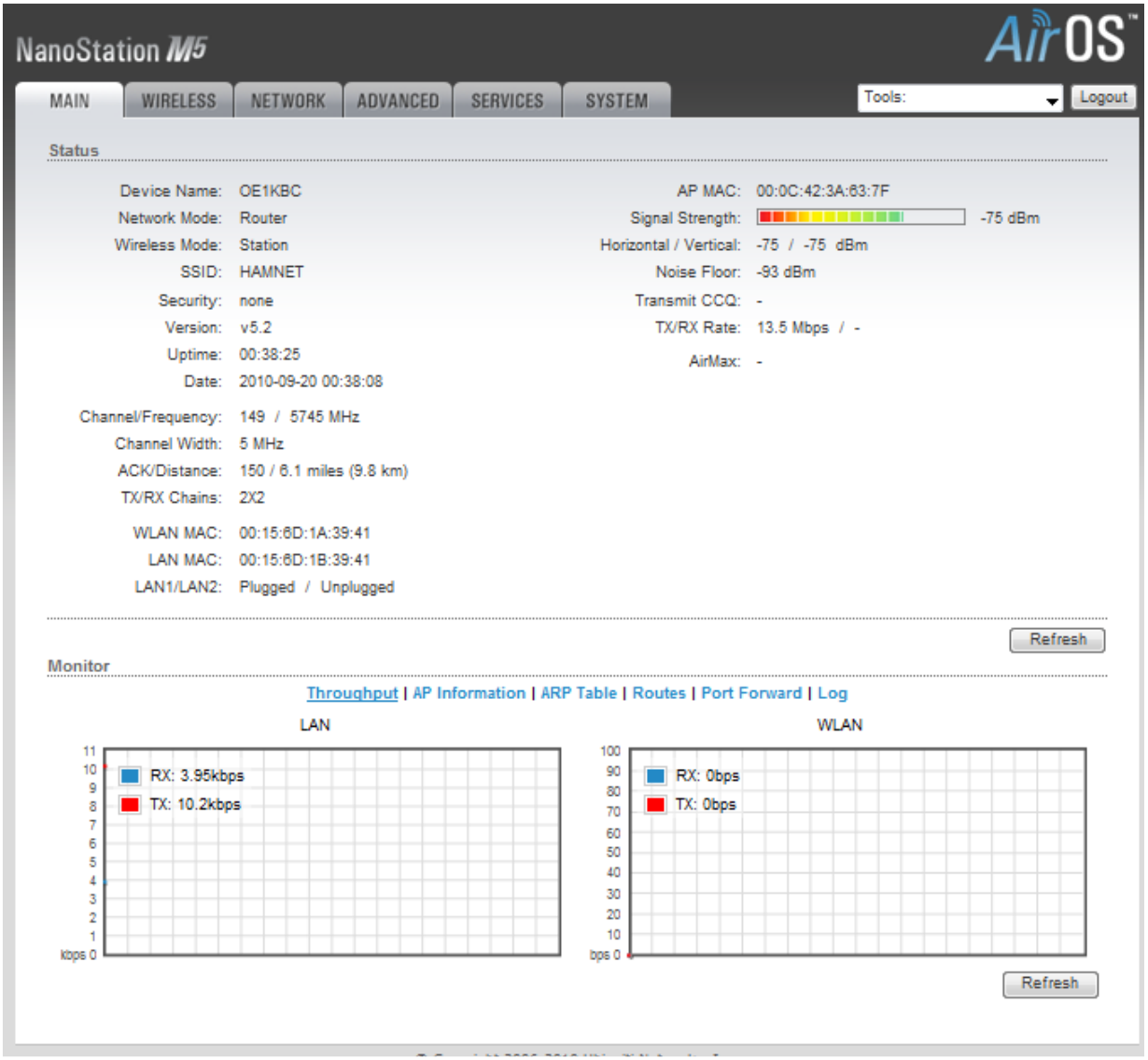
Znajdujący się obok po prawej stronie przycisk „Select” pozwala na przeszukanie pasma i następnie wybranie nazwy ze spisu odbieranych sieci.
W polach kodu kraju („Country code”) i szerokość pasma („Channel width”) można ustawić jako wybór test zgodności (punkt „Compliance test”) i przyjąć ustawienie dokonane przez program. W przykładzie poniższym ustawiona została szerokość pasma 5 MHz i „Compliance test”. Najczęściej stosowana jest szerokość pasma 5 MHz, czasami 10 MHz, a w paśmie 6 cm także 20 MHz.
W polu kanału należy ustawić częstotliwość przemiennika dostępowego. Po zaznaczeniu pola „Enabled” możliwe jest wybranie i zaznaczenie w spisie więcej niż jednej częstotliwości (jeśli stacja znajduje się w zasięgu więcej niż jednego przemiennika dostępowego), a właściwa częstotliwość (najkorzystniejsza) zostanie wybrana automatycznie. W poniższym przykładzie są to dwie częstotliwości wiedeńskie. W przypadku słabego odbioru najlepiej samemu wybrać najkorzystniejszą.



Rys. 3.2.8. Zakładka łącza radiowego

Po potwierdzeniu zmian za pomocą przycisków „Change” („Zmień”) i „Apply” („Zastosuj”) zakładka główna („Main”) może wyglądać podobnie do pokazanej na rys. 2.2.9.
Korygując ustawienie anteny można ewentualnie uzyskać poprawę siły sygnału – wyświetlanej w tej właśnie zakładce.
Dla sprawdzenia jakości połączenia można otworzyć wywołać przeglądarkę internetową i wywołać którąś ze stron internetowych dostępnych w „Hamnecie”. Przed rozpoczęciem prób połączeń warto upewnić się jakie usługi dostępne są w sieci „Hamnetu” i wykorzystać do prób serwer http jeśli jest on dostępny albo jakiś inny. Serwery http występują stosunkowo często w sieciach „Hamnetu” a więc z dużym prawdopodobieństwem właśnie w ten sposób najłatwiej będzie można sprawdzić jakość połączenia. Założeniem twórców sieci jest pokrycie jej zasięgiem możliwie jak największej części terytorium kraju ale w pierwszych fazach budowy i rozbudowy mogą to być niewielkie wysepki różniące się wyposażeniem i dostępnymi usługami – przynajmniej do czasu rozbudowy szkieletowej sieci szybkich łączy. Jak wiadomo nie od razu Kraków zbudowano...
Adresy dostępnych serwerów należą do domeny *ampr.org* (w Austrii przykładowo *ampr.at*), a w formie liczbowej do przyznanej krótkofalowcom serii 44.x.x.x, w ktorej druga grupa oznacza przeważnie kraj.
W przypadku korzystania na tym samym komputerze z dostępu do zarówno do Internetu jak i do „Hamnetu” należy na komputerze wpisać stałą trasę dla adresów serii 44 – czyli 44.0.0.0/8 z podaniem

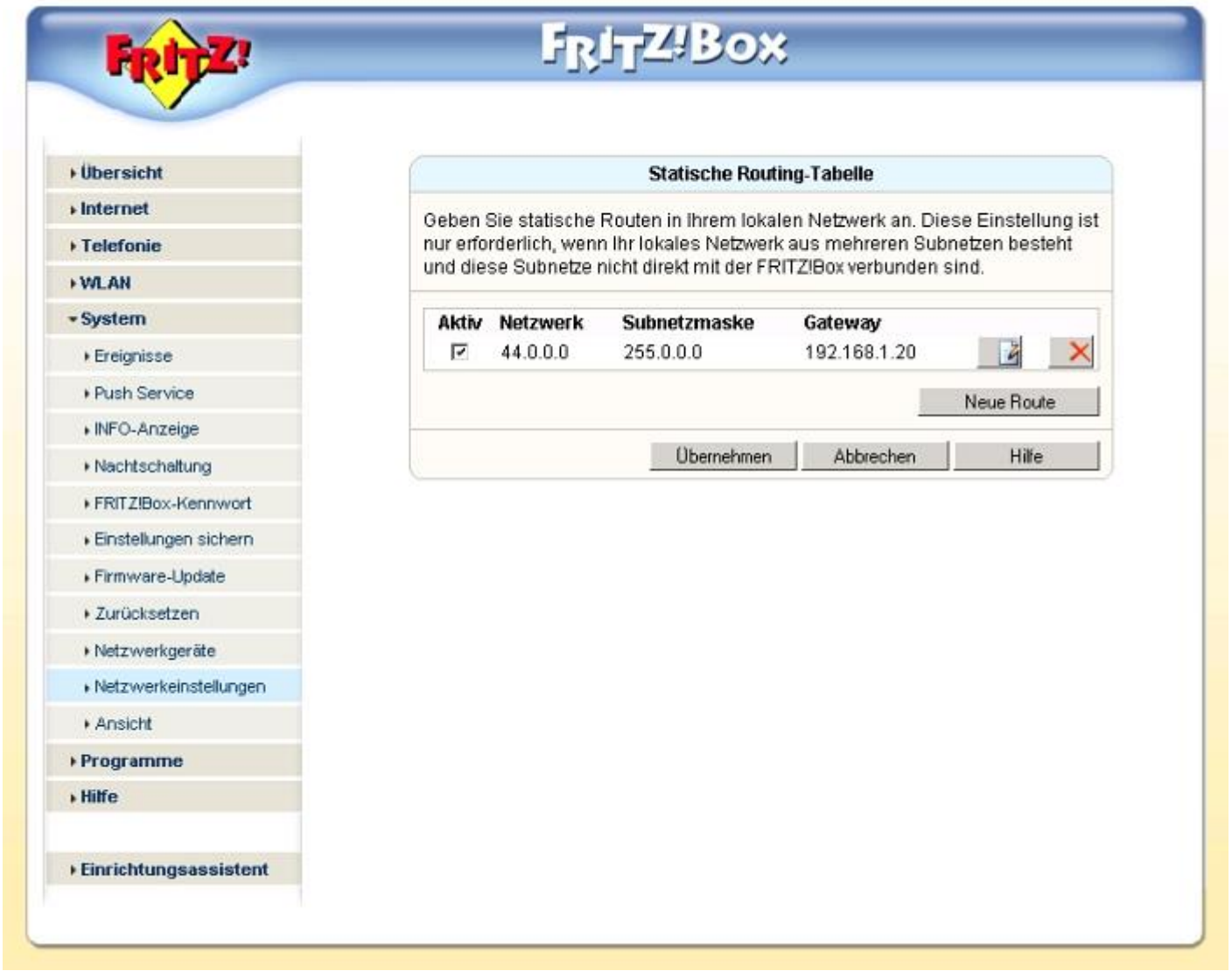
maski sieciowej 255.0.0.0 – prowadzącą przez bramkę o adresie 192.168.1.20 (lub innym podanym w powyższej konfiguracji). Niewpisanie podanej trasy spowoduje, że adresów z serii 44 komputer będzie poszukiwał w Internecie, gdzie ich oczywiście nie znajdzie.



Rys. 3.2.9. Zakładka główna

Do wpisania trasy na komputerze należy otworzyć okno wiersza poleceń i wpisać do niego polecenie
route add 44.0.0.0 mask 255.0.0.0 192.168.1.20 –p
gdzie zamiast 192.168.1.20 należy użyć adresu podanego w konfiguracji „Nanostation". Argument *–p* oznacza trasę stałą używaną także po następnych uruchomieniach komputera.
W przypadku istniejacej już sieci domowej złożonej z wielu innych urządzeń może okazać się konieczne podanie innego adresu w konfiguracji „Nanostation". Dla sieci domowych o adresach z serii 10.0.0.0/24 wygodnie będzie nadać „Nanostation" adres z tej serii np. 10.0.0.20 (należy go oczywiście użyć w poleceniu *route add* zamiast podanego tam przykładowego). Po zmiannie adresu „Nanostation" w konfiguracji i potwierdzeniu za pomocą przycisków „Change" („Zmień") i „Apply" („Zastosuj") należy również na komputerze powrócić do adresu z tej serii przed kontynuowaniem dalszej konfiguracji.
Trasę prowadzącą do „Hamnetu" można wpisać do tabeli w domowym punkcie (węźle) dostępowym do Internetu zamiast wpisywania jej do komputera lub komputerów wchodzących w skład sieci domowej.
Otwierane jest okno „System"| „Ustawienia sieci" (rys. 3.2.10) – lub ich odpowiedniki w innych modelach sprzętu, w którym są wpisywane statyczne trasy połączeń dla dostępnych podsieci, o ile nie są one połączone bezpośrednio z urządzeniem. W kolumnie bramki („Gateway") podawany jest adres

„Nanostation” lub „Bulleta” ustalony w ich konfiguracji ponieważ to właśnie przez nie ma prowadzić trasa połączenia z siecią amatorską.



Rys. 3.2.10. Wpisanie trasy do domowego punktu dostępowego gdy sieć domowa zawiera podsieci nie połączone bezpośrednio z punktem dostępowym do Internetu

4. Instalacja i konfiguracja węzła dla lokalnych sieci radiowych

Konfiguracja ta jest przeznaczona dla użytkowników usytuowanych w takiej odległości od najbliższego przemiennika sieci, że bezpośrednia łączność z nim nie jest możliwa. Użytkownicy tworzą lokalną sieć radiową o strukturze siatki (ang. *mesh*), w której każda ze stacji stanowi jednocześnie przekaźnik dla innych. Zaletą tej topologii jest możliwość automatycznej rekonfiguracji sieci i wyboru najkorzystniejszych tras połączeń w przypadku zmiany stanu sieci (włączenia nowej stacji lub wyłączenia jednej z pracujących dotychczas). Wyłączenie lub awaria jednego ze składników sieci wpływa w małym stopniu na jej funkcjonalność. Połączenia z sąsiednimi stacjami wymagają naogół mniejszej mocy nadawania. Wadą tej topologii jest natomiast konieczność stałej i częstej wymiany informacji o stanie sieci i połączeń między stacjami. Zajmuje to część przepustowości sieci.
Można tu wprawdzie zaobserwować odległą analogię do sieci packet-radio w ich pionierskiej fazie, kiedy każda z czynnych stacji stanowiła stację przekaźnikową dla innych, ale w sieci „Hamnetu" trasy połączeń są wybierane automatycznie, a nie ręcznie jak wówczas w sieci packet-radio. Sieć tworzy się i konfiguruje dynamicznie w zależności od bieżącej sytuacji – liczby i rozmieszczenia czynnych w danej chwili stacji.
Wyposażenie stacji w tym przypadku różni się zdecydowanie od omówionego poprzednio i nie jest z nim kompatybilne.
Przed zakupem wyposażenia warto dokładnie zapoznać się z sytuacją panującą w najbliższej okolicy i skonsultować się z kolegami już aktywnymi w „Hamnecie", aby nie podjąć błędnej decyzji. Topologia siatki jest stosowana m.in. w sieci kryzysowej AREDN.

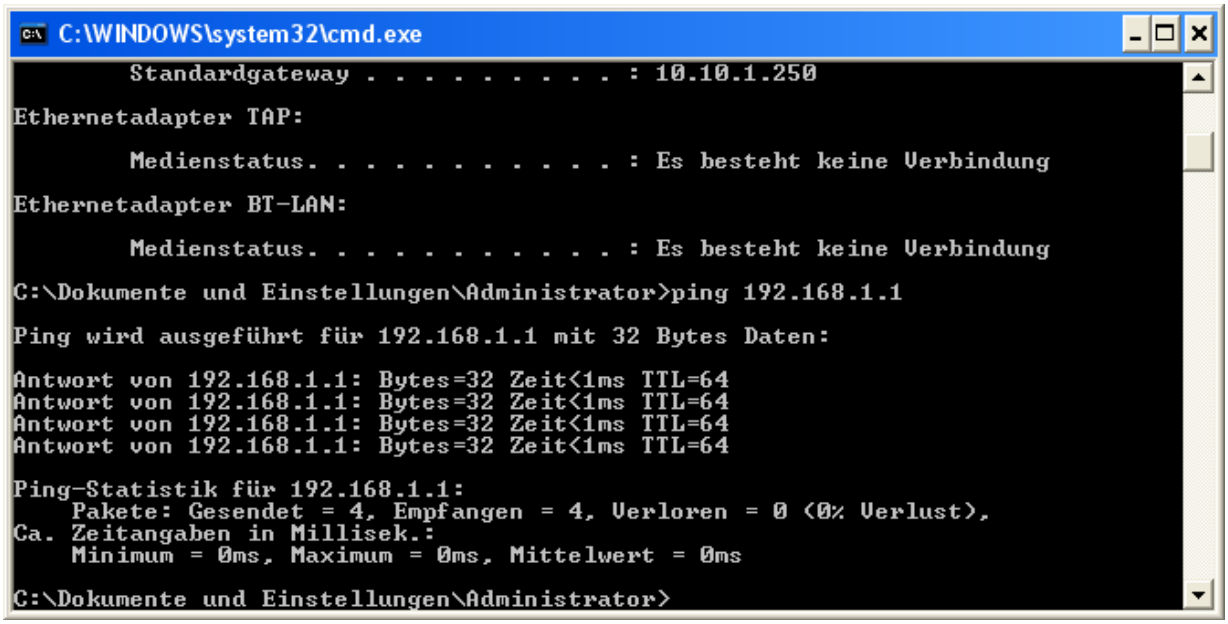
4.1. Sprzęt

Wyposażenie stacji nie jest ograniczone do żadnego konkretnego typu urządzenia, ale musi ono być wyposażone w procesor „Broadcom BCM2050" i pozwalać na zainstalowanie oprogramowania *openwrt* (*http://openwrt.org*). Jest to konieczne ponieważ zastosowanie krótkofalarskie wymaga niewielkiej zmiany częstotliwości zegarowej. Kwarc o częstotliwości 20 MHz sterujący wewnętrzny generator BCM20250 należy zastąpić przez kwarc 19,6608 MHz.
Zmiana częstotliwości zegarowej powoduje zmianę odstępu kanałów w.cz. co uniemożliwia kontakt radiowy pomiędzy urządzeniami nie zmodyfikowanymi i urządzeniami przystosowanymi do potrzeb krótkofalarskich. Zabezpiecza to sieć „Hamnetu" przed dostępem ze strony osób niepożądanych. Szerokość pasma sygnału w.cz. w standardzie 802.11g ulega zmianie z 18 na 17,695 MHz, a odstępy podnośnych w kanale z 200 na 196 kHz. Wartości te odpowiadają przyjętemu standardowi „HAMNETmesh". Przeciętnie doświadczonemu majsterkowiczowi wymiana kwarcu, łącznie z otwarciem urządzenia i zdjęciem blachy ekranującej z procesora, zajmuje nie więcej niż kilka minut.
Do stosowanych modeli należą przykładowo „Linksys WRT54GL (-GS, -G)" i podobne. Spisy aktualnie dostępnych i spełniających podane wymogi modeli można znaleźć w Internecie. Oczywiście konieczna jest także antena zewnętrzna.

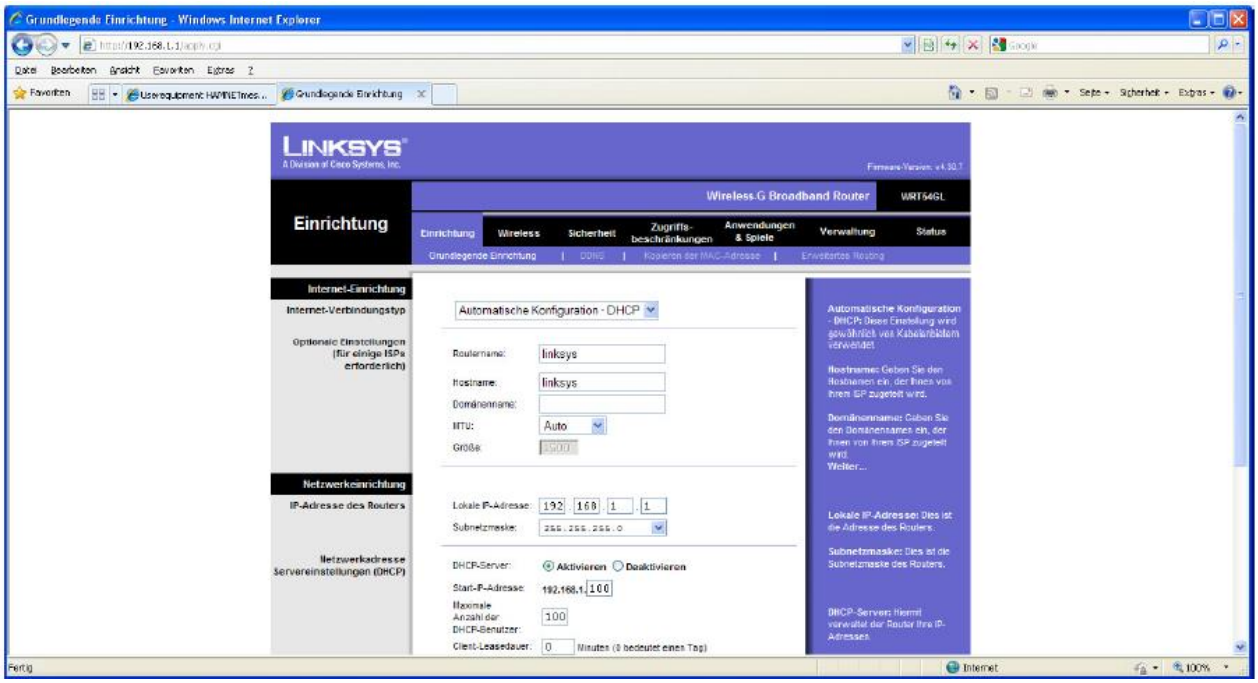
4.2. Oprogramowanie

Oprogramowanie dla punktu dostępowego (węzła) WRT54 i dla dużej liczby innych modeli jest dostępne m.in. w witrynie *https://openwrt.org*. Dla „Maliny" są to wygodne w instalacji obrazy (odwzorowania) pamięci. Obrazy pamięci są do dyspozycji także i dla innych modeli. Oprogramowanie to zapewnia łączność odkrytym tekstem zgodnie z przepisami o łącznościach amatorskich.

Instalacja oprogramowania na WRT54 odbywa się przez lokalną sieć LAN. Należy upewnić się, że adres używany przez urządzenie, a mianowicie 192.168.1.1 jest wolny. Komputer powinien oczywiście korzystać z innego dowolnego adresu, przykładowo 192.168.1.10 i zostać połączony kablowo z punktem dostępowym. W celu sprawdzenia czy połączenie funkcjonuje prawidłowo można je sprawdzić za pomocą pakietu "ping". Sposób ten może się przydać i w wielu innych sytuacjach.
Sposób instalacji oprogramowania dla różnych modeli podano w instrukcjach użycia.



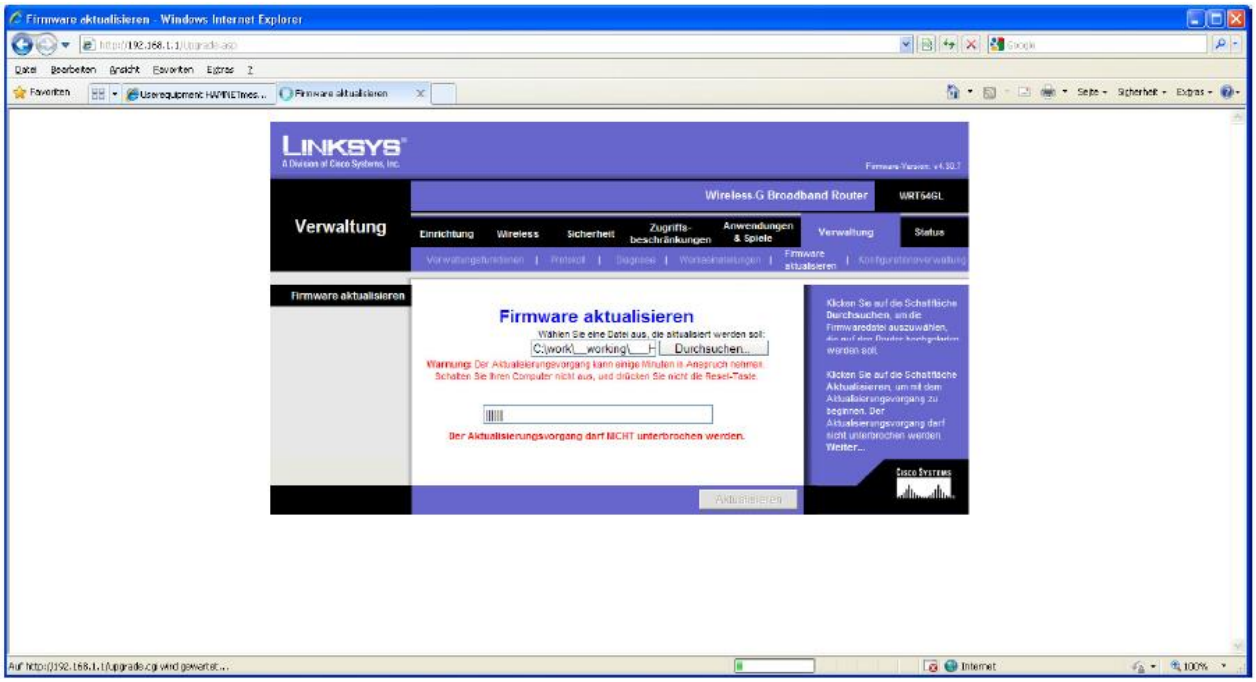
Rys. 4.2.1. Sprawdzanie połączenia za pomocą pakietu próbnego „ping”



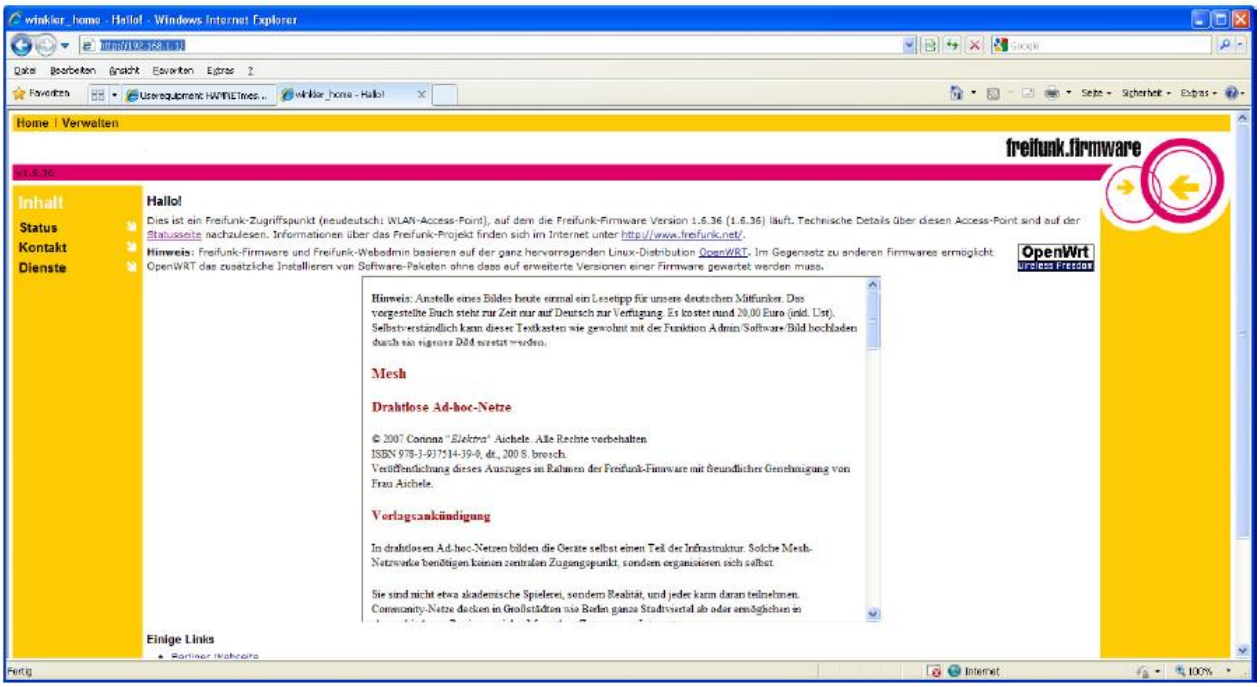
Rys. 4.2.2. Okno zameldowania użytkownika. Nazwa użytkownika i hasło dostępu brzmią „linksys”, w innych modelach mogą się oczywiście różnić

System operacyjny zawarty standardowo w węźle czyli nowym punkcie dostępowym (ang. *router*) musi zostać zastąpiony przez oprogramowanie „HAMNETmesh”. W celu wymiany oprogramowania należy wywołać przegladarkę internetową i w jej polu adresowym wpisać adres urządzenia **http://192.168.1.1**. W odpowiedzi w przeglądarce wyświetlane jest okno zameldowania się użytkownika (podobne do pokazanego na rys. 4.2.2). Hasło dostępu i nazwa użytkownika brzmią „**linksys**”, ale w innych modelach mogą się różnić od tego. Należy je sprawdzić w dokumentacji urządzenia. Wszytkie pokazane na dalszych ilustracjach okna należy potraktować jako przykładowe ponieważ mogą się one różnić w zależności od modelu i wersji jego oprogramowania a także od wersji zainstalowanego na nowo systemu operacyjnego „OpenWRT”. Widoczne na ilustracjach przykłady pochodzą z poz. [4].

Po zameldowaniu się należy znaleźć zakładkę administracji i na niej punkt aktualizacji oprogramowania. Po wywołaniu funkcji aktualizacji należy jako pierwszy wybrać (za pomocą klawisza przeszukiwania) plik *openwrt-g-freifunk-1.6.36-de.bin* ze skomprymowanego archiwum i zaktualizować naciskając przycisk aktualizacji. Proces aktualizacji może trwać do kilku minut. W tym czasie może migać jedna z diod sygnalizacyjnych np. dioda sygnalizująca włączenie (zależnie od modelu urządzenia).
Po zakończeniu aktualizacji należy w następnym oknie nacisnąć przycisk „Dalej”.

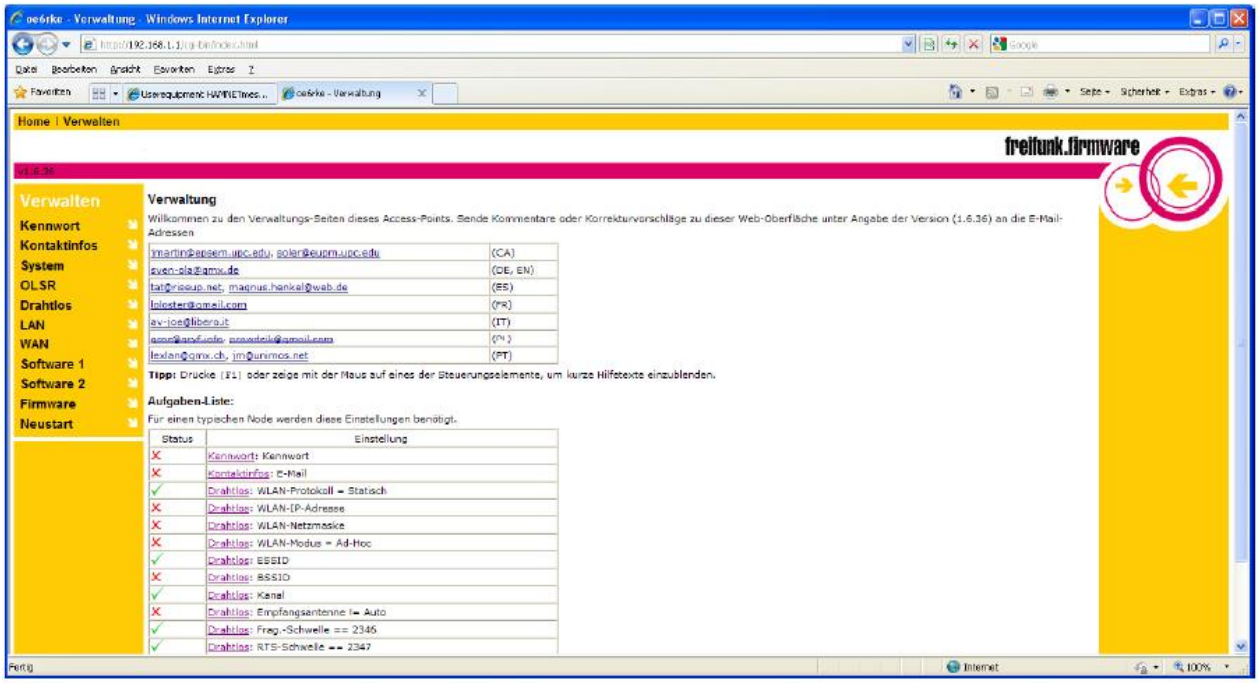


Rys. 4.2.3 Okno aktualizacji oprogramowania



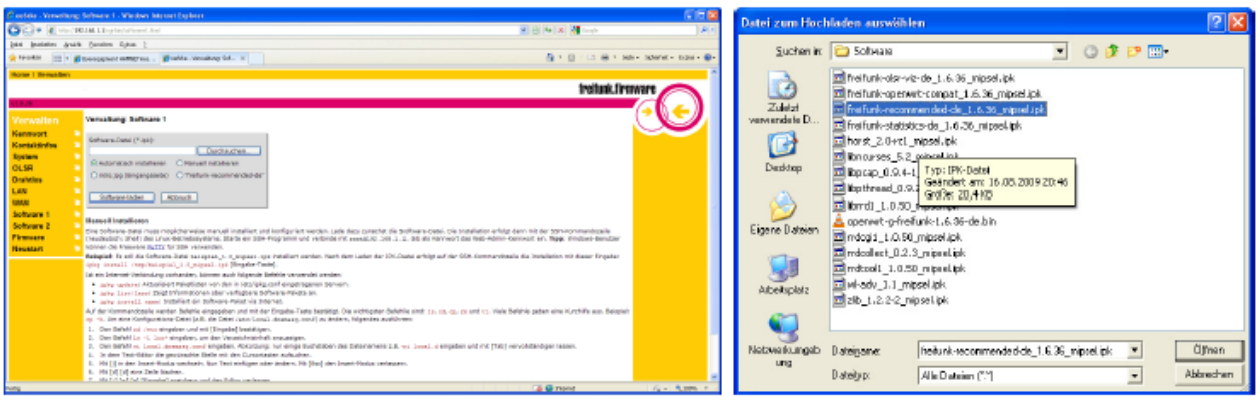
Rys. 4.2.4. Okno główne po wymianie systemu operacyjnego na „OpenWRT”

Po wymianie w opisany sposób systemu operacyjnego na „OpenWRT” należy zameldować się w nowym z nazwą użytkownika „**root**” i hasłem dostępu „**admin**”. Pozwala to na zainstalowanie reszty oprogramowania.
Poprzez odnośnik „Verwalten” („Administracja”) należy przejść do okna administracyjnego pokazanego na ilustracji 4.2.5. W celu zainstalowania i skonfigurowania reszty oprogramowania należy przejść przez widoczne z lewej strony z boku punkty: „Kennwort” („Hasło dostępu”), „Kontaktinfos” („Informacje o użytkowniku/operatorze”), „System”, „Drahtlos” („Łącze radiowe”), i „Softwareinstallation” („Instalacja oprogramowania”).



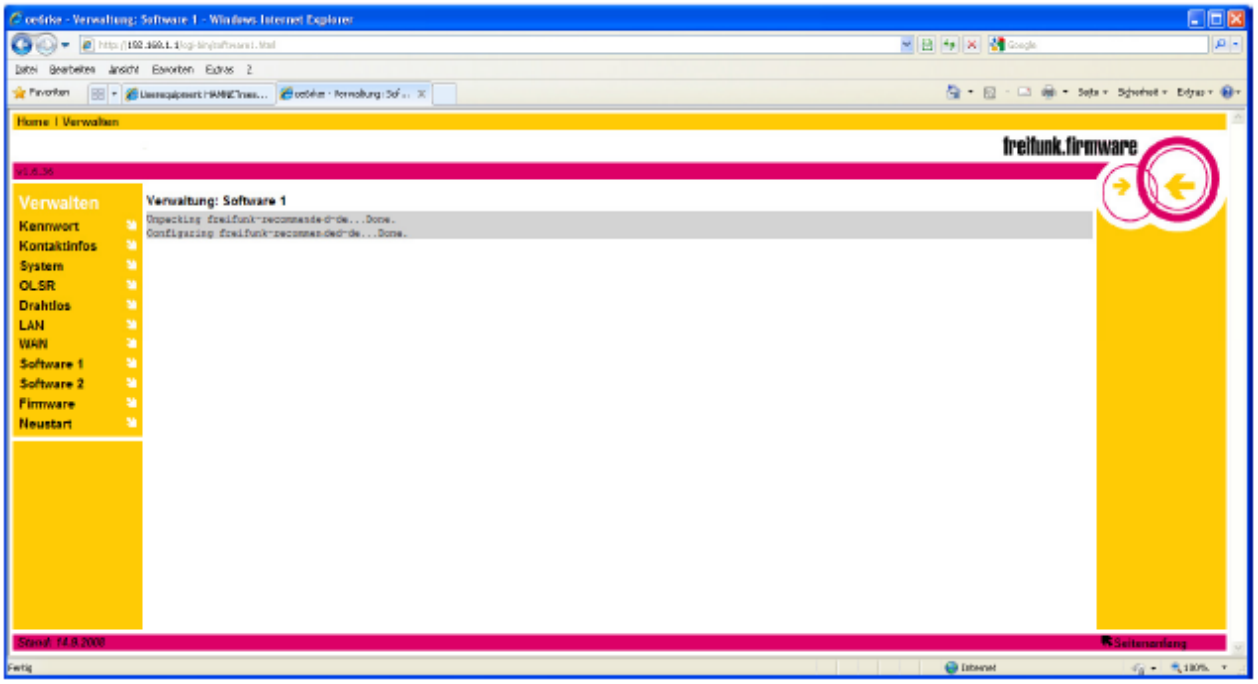
Rys. 4.2.5. Okno administracji „OpenWRT”

Instalację oprogramowania rozpoczynamy od punktu „Software 1” („Oprogramowanie 1”) z menu po lewej stronie. Instalacja dalszych niezbędnych lub i dodatkowych (wymienionych powyżej) plików polega na naciskaniu przycisku przeszukiwania („Durchsuchen”) w szarym okienku widocznym po lewej stronie rys. 4.2.6, wyborze kolejnego pliku w oknie widocznym po prawej stronie, naciśnięciu w szarym okienku przycisku „Ładuj” („Software laden”) i tak dalej. Zaleca się zainstalowanie najpierw plików niezbędnych – aby nie stracić orientacji – a dopiero potem wybranych dodatkowych.

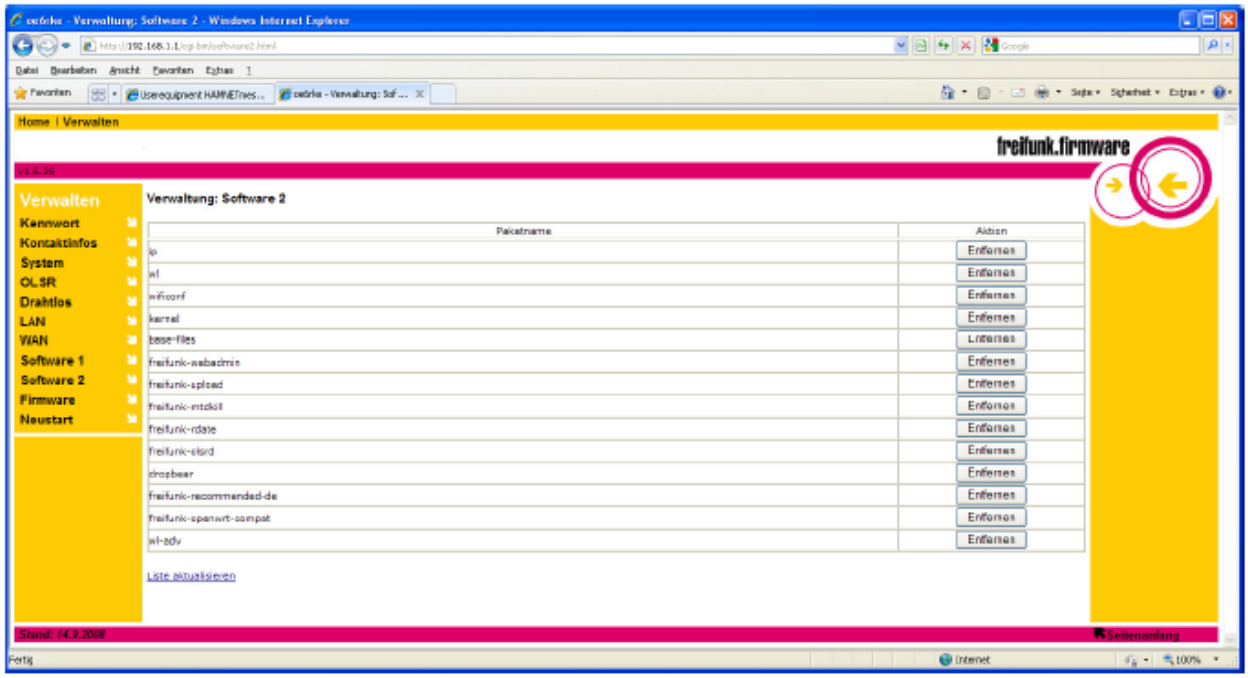


Rys. 4.2.6. Instalowanie dalszych elementów składowych.

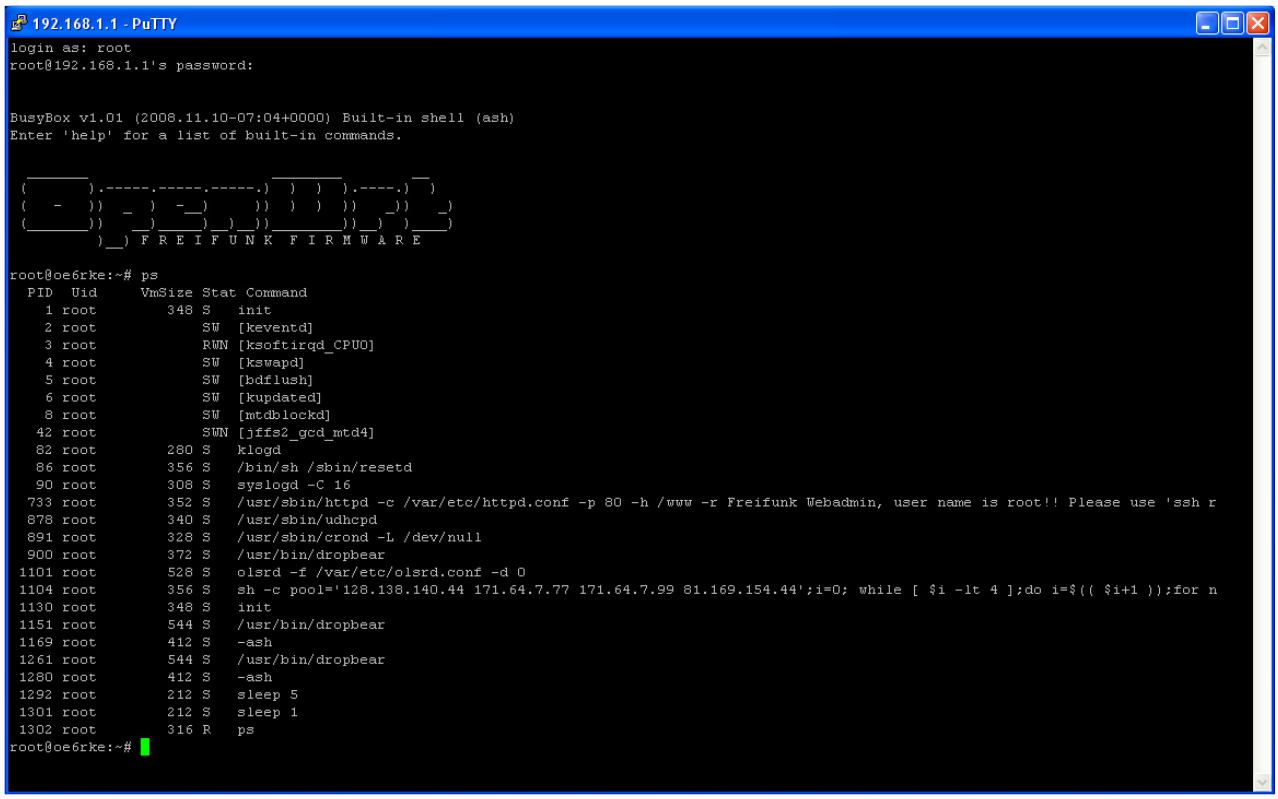
Na zakończenie instalacji wyświetlane jest okno widoczne na rys. 4.2.7. W wywoływanym za pomocą punktu „Software 2” („Oprogramowanie 2”) oknie pokazanym na ilustracji 4.2.8 wyświetlany jest spis zainstalowanych modułów. Pozwala on także na usunięcie modułów uznanych za zbędne lub niepotrzebnie zainstalowane. Służą do tego widoczne w kolumnie po prawej stronie przyciski „Entfernen” („Usuń”).
Po zakończeniu i sprawdzeniu prawidłowości instalacji można przystąpić do konfiguracji, ale przed jej rozpoczęciem korzystne jest dokonanie zmiany hasła dostępu (rys.4.2.10). W celu zapisania hasła i ewentualnych innych wprowadzonych danych należy ponownie wystartować system.



Rys. 4.2.7. Zakończenie instalacji

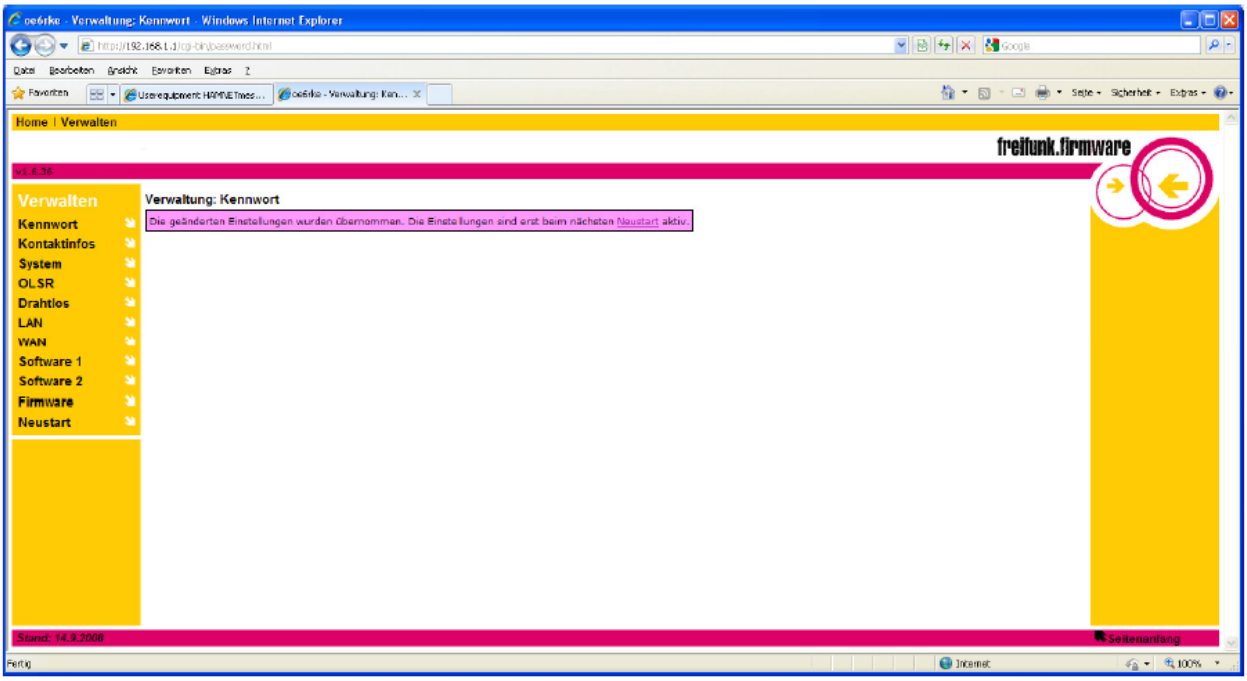


Rys. 4.2.8. Spis zainstalowanych modułów z możliwością ich usuwania



Rys. 4.2.9. Próbny dostęp do systemu „OpenWRT” za pomocą SSH

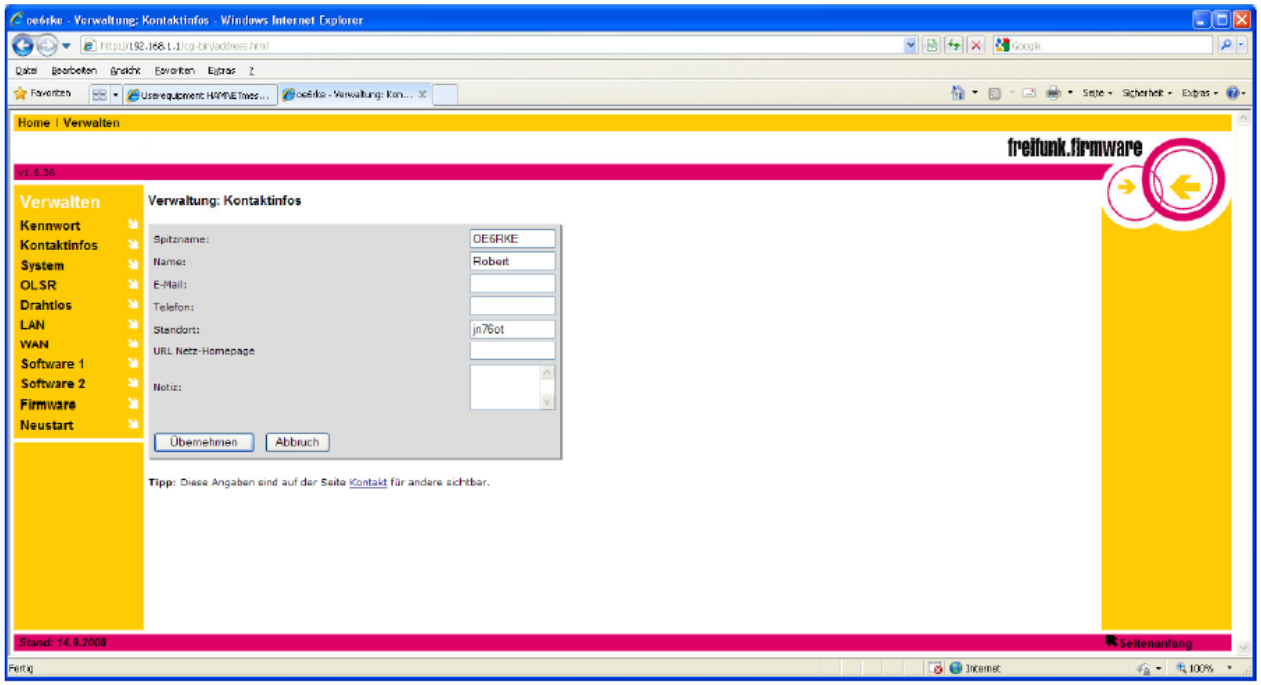
Zainstalowany system, jako linuksowy, jest dostępny z komputera za pomocą SSH np. przy użyciu popularnego programu terminalowego „Putty” lub innego równoważnego. Pozwala to na próbę prawidłowości pracy lub ułatwia diagnozę ewentualnych problemów.



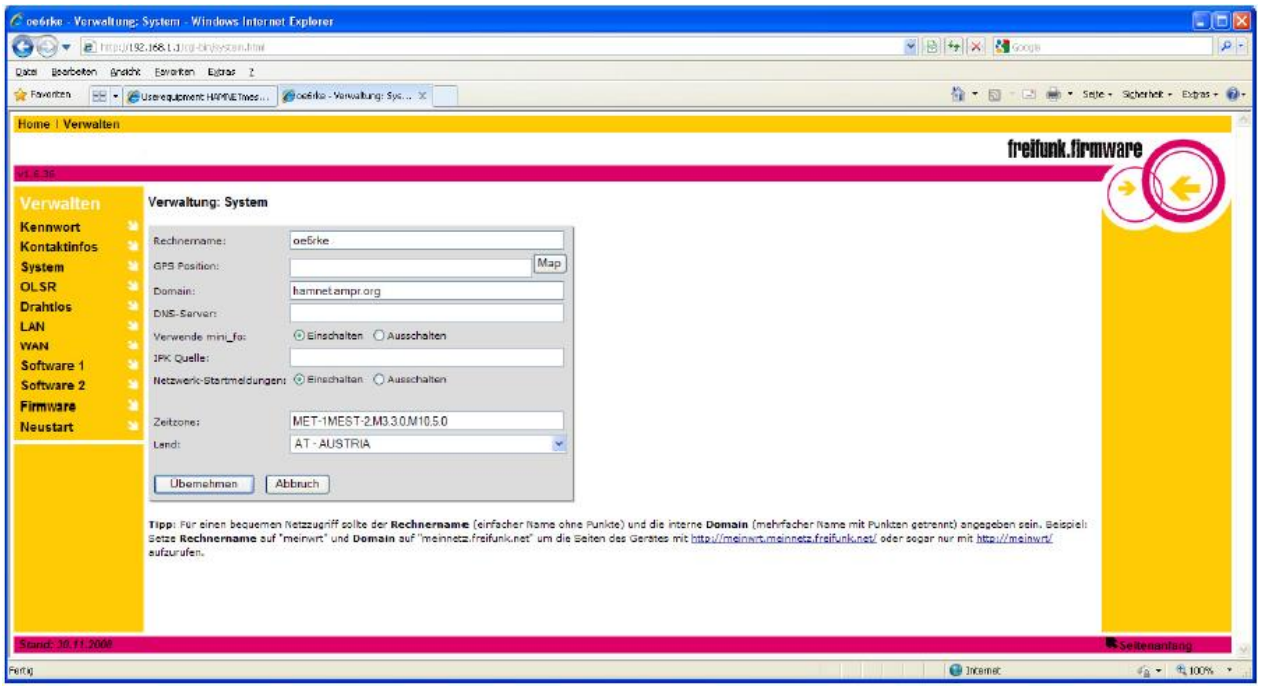
Rys. 4.2.10. Zmiana hasła dostępu

4.3. Konfiguracja węzła

Do najważniejszych parametrów należą adres IP i nazwa serwera DNS. Dane te, a zwłaszcza adres IP należy otrzymać od lokalnego administratora sieci.
W oknie „Kontaktinfos” („Informacje o użytkowniku”) wprowadzany jest znak wywoławczy i imię operatora oraz lokator stacji. Pozostałe dane nie są konieczne, ale zależy to od uznania operatora.

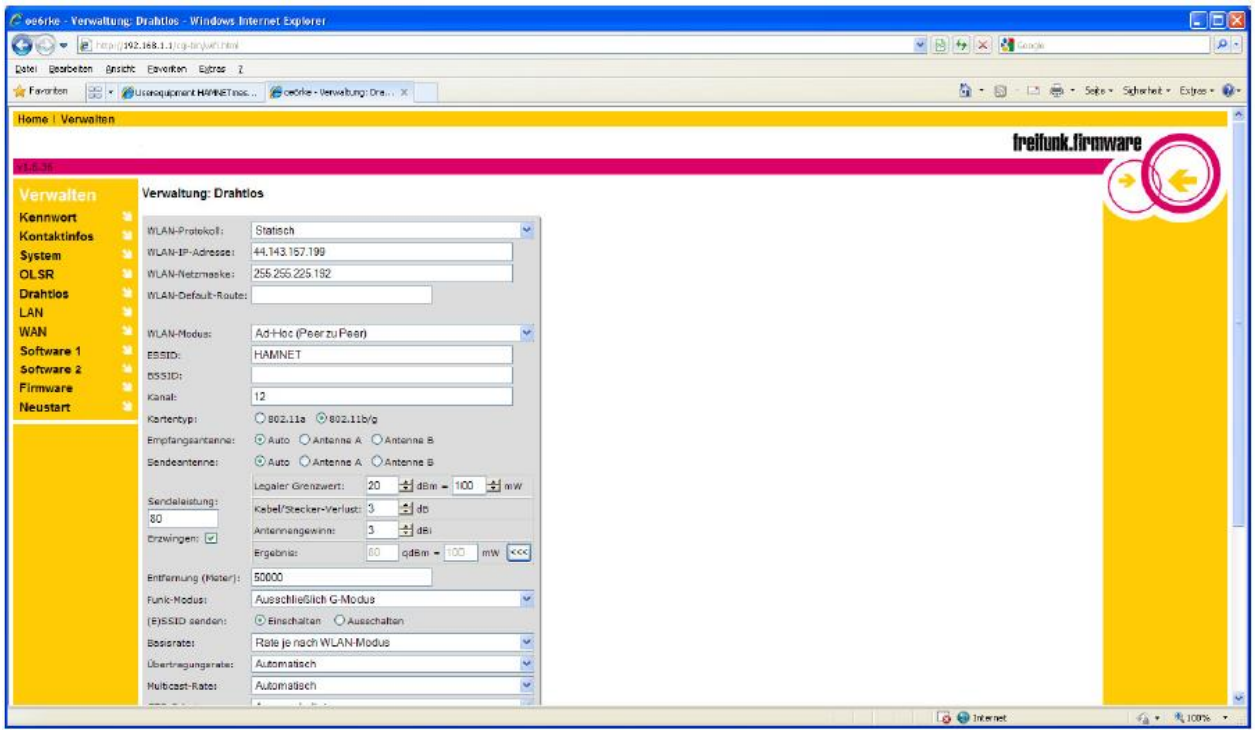


Rys. 4.3.1. Informacje o operatorze



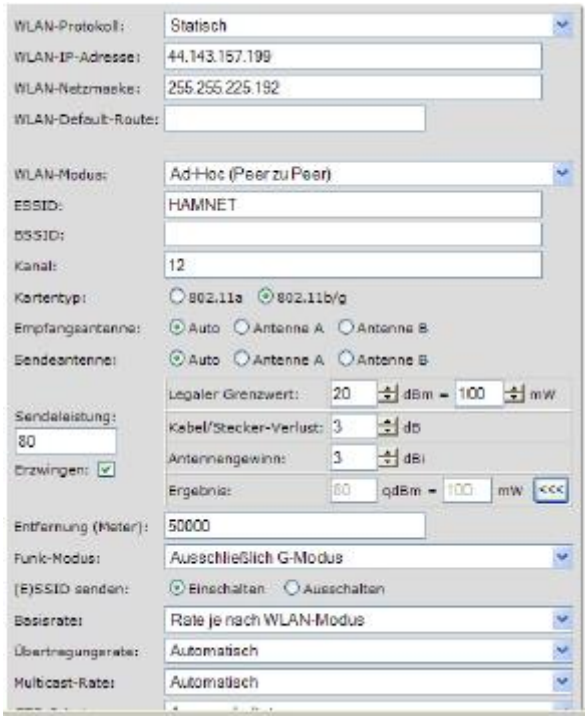
Rys. 4.3.2. Okno „System”

W oknie „System” wprowadzana jest nazwa systemu (należy podać jako nazwę własny znak wywoławczy), jako domenę podaje się *hamnet.ampr.org* i na zakończenie należy wybrać kraj ze spisu.

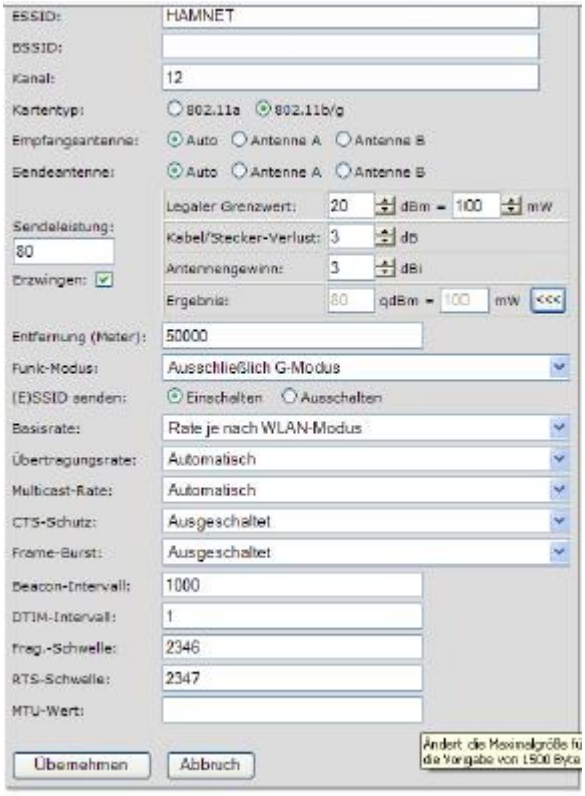


Rys. 4.3.3. Okno łącza radiowego

W oknie tym wybierany jest statyczny protokół WLAN („statisch”) wraz z podaniem adresu IP i maski podsieci.
W sieci WLAN (pole „WLAN modus”) wybierany jest tryb pracy „Ad-Hoc”, nazwa sieci „HAMNET” jest pisana duzymi literami, jako protokół ethernetowy wyłącznie G („Ausschliesslich G-Modus” w polu „Funk-Modus” i zaznaczenie „802.11b/g” w polu „Kartentyp”), i obowiązkowo kanał 12 (2425,125 MHz).
Przy dobrej antenie można podać jako szacunkowy zasięg do 50000 m czyli do 50 km.



Rys. 4.3.4. Szczegóły konfiguracyjne łącza radiowego



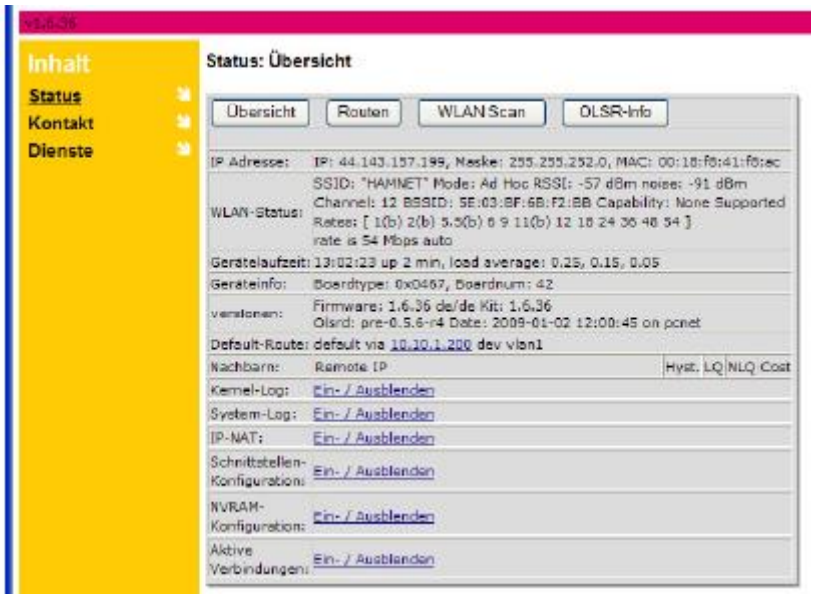
Rys. 4.3.5. Dalsze szczegóły konfiguracyjne łącza radiowego. Większość parametrów nie ulega zmianie. Odstęp czasów transmisji radiolotarni należy zmienić jak podano na 1000 ms czyli 1 sekundę

W oknie WAN podawane są dane dotyczące lokalnej sieci komputerowej: własny adres węzła, maska sieci, domyślna trasa, dopuszczenie protokółów SSH, HTTP, HTTPS, zapytań *ping* itd. (rys. 4.3.6). We własnej sieci możliwe jest używania prywatnych statycznych adresów IP, co ułatwia konfigurację sieci zawierającej dwa lub więcej takich węzłów.

Rys. 4.3.6. Okno „WAN”

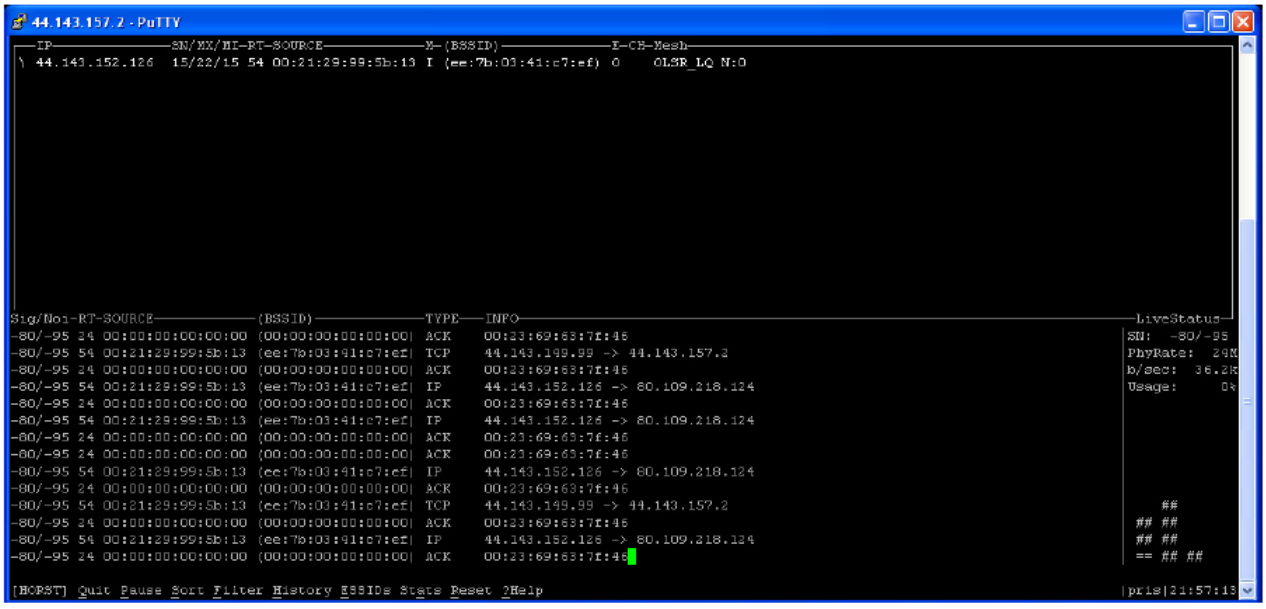
4.4. Praca w eterze

Po uruchomieniu można zacząć poszukiwać w eterze stacji sąsiadujących. Odebranie sygnału powoduje miganie diody sygnalizacyjnej „WLAN”.
Na stronie informacji o odebranych stacjach wyświetlane są bardziej szczegółowe dane o odbieranej stacji.



Rys. 4.4.1. Okno informacji o odebranych stacjach

Komunikaty odbieranych stacji można odczytać dokładniej w oknie programu terminalowego „Putty” (rys.4.4.2).



Rys. 4.4.2. Komunikaty odbieranych stacji w oknie terminalowym PuTTY

Po zainstalowaniu wymienionych powyżej programów statystycznych możliwe jest wywołanie danych stytstycznych. Aby dane te były bardziej wiarygodne dobrze jest odczekać co najmniej pół godziny od rozpoczęcia pracy w eterze.

5. Dostęp do stron WWW

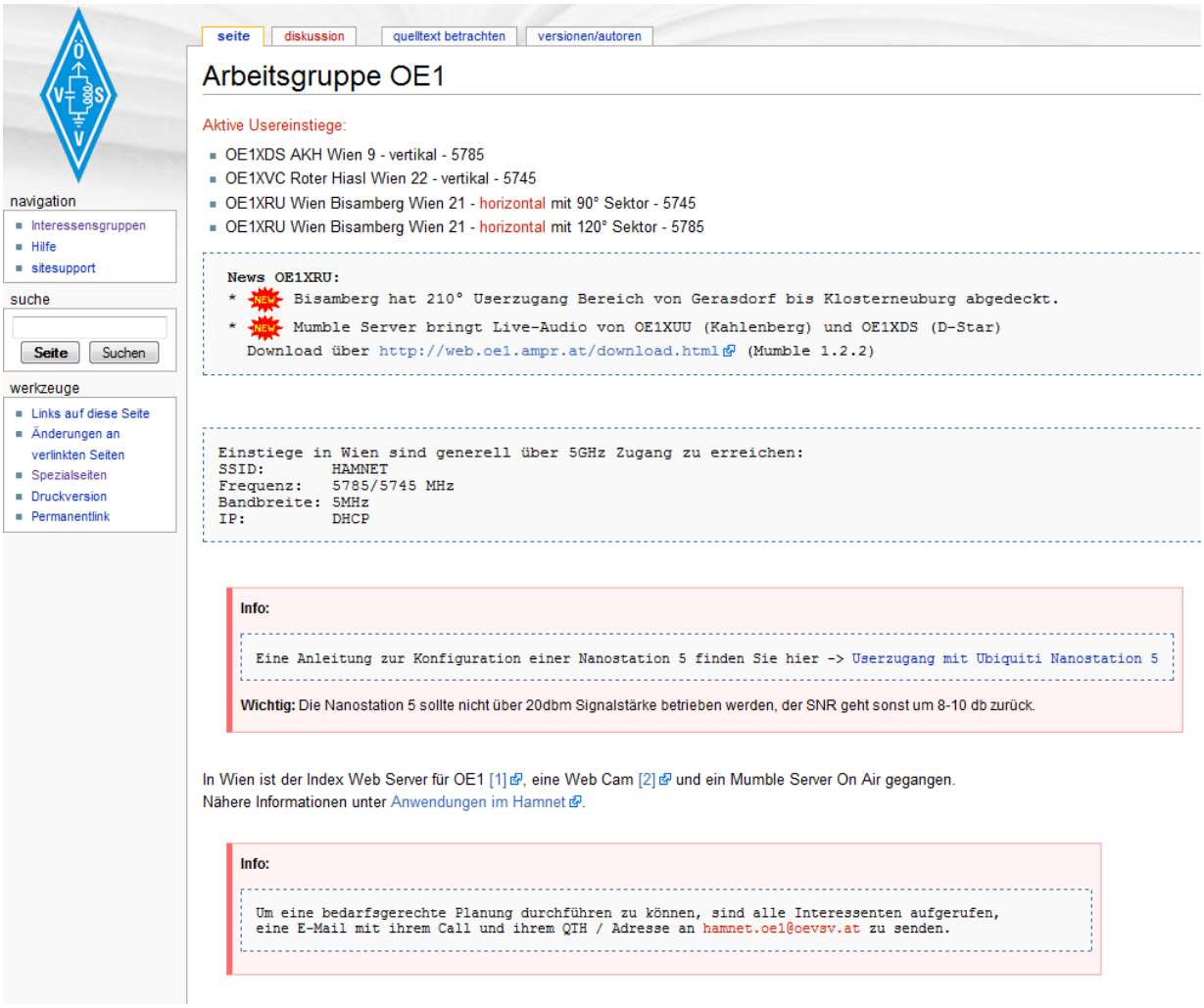
Do przeglądania hamnetowych stron www wystarczy dowolna standardowa przeglądarka internetowa:

- Internet Explorer,
- Chrome,
- Firefox,
- Opera

itd.

Witryny hamnetowe mogą zawierać dowolne treści statyczne lub dynamiczne np. dostęp do kamer standardu internetowego, podgląd obrazów ATV, dane telemetryczne lub meteorologiczne, wyszukiwarki dostępne tylko w „Hamnecie" itp.

Strony o bardziej rozbudowanej funkcjonalności mogą wymagać zainstalowanej Javy, odtwarzacza „Macromedia Flash Player" lub innych rozszerzeń. Użytkownicy korzystający intensywnie z Internetu mają z pewnością zainstalowane nie tylko te, ale również i niektóre dodatki do przeglądarek i nie będą mieli kłopotów z tymi wymaganiami.



Rys. 5.1. Przykład witryny dostępnej przez Hamnet pod adresem *web.oe1.ampr.at*

Proste serwery HTTP, FTP itp. przeznaczone dla mniej licznego grona użytkowników (przykładowo udostępniające treści o specjalnym znaczeniu, wyniki pomiarów, eksperymentów, obserwacje jakichś zjawisk kamerami internetowymi lub serwery potrzebne tylko w określonych okolicznościach, z okazji imprez krótkofalarskich, lotów balonów itp.) mogą wykorzystywać mikrokomputer „Raspberry Pi" i dostępne dla niego bezpłatne oprogramowanie.

Na zakończenie rozdziału przedstawiamy niektóre dalsze pomysły usług hamnetowych wzorowanych na internetowych.

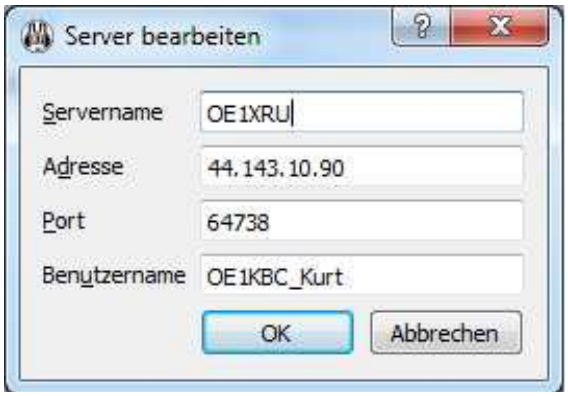
Podobnie jak w internecie również w Hamnecie sieci społecznościowe cieszą się rosnącym zainteresowaniem. Jako klient sieci służy „Hambook". W odróżnieniu jednak od Internetu sieci te nie gromadzą żadnych danych osobistych dla prowadzenia działalności reklamowej czy komercyjnej.
Użytkownicy komputerów pracujących w środowisku Linuksa albo operatorzy linuksowych serwerów w Hamnecie mogą bez korzystania z Internetu pobrać bieżące aktualizacje i wersje systemu ze specjalnych serwerów aktualizacyjnych dla Linuksa..
Podobnie jak dawniej w sieci Packet-Radio (a obecnie w „chmurze" internetowej) również w Hamnecie możliwe jest składowanie plików na specjalnych serwerach pamięciowych – „Cloud server" – zainstalowanych w wielu węzłach sieci i pozwalających na prywatną lub publiczną wymianę plików danych, zasadniczo oczywiście o tematyce krótkofalarskiej. Dostęp do nich możliwy jest albo za pomocą przeglądarki internetowej albo specjalnych programów synchronizujących zbiory danych. Zaleca się pobieranie obszerniejszych plików godzinach nocnych albo innych porach mniejszego ruchu, aby nie przeciążać łączy i nie hamować usług pracujących w czasie rzeczywistym j.np. transmisji głosu.
Przepustowości sieci hamnetowej pozwalają na wywoływanie i oglądanie nagrań wizyjnych o wystarczająco dobrej jakości. Ich treścią mogą być telewizyjne komunikaty krótkofalarskie, prezentacje projektów o tematyce krótkofalarskiej albo mogą to być bieżące obrazy z kamer zainstalowanych w wielu lokalizacjach przemienników. Niektóre z amatorskich przemienników telewizyjnych umożliwiają też nadawanie w eter strumieni wizyjnych otrzymywanych przez Hamnet. Rozpoczęcie pracy ATV wymaga więc (przynajmniej na początek) jedynie komputera, kamery internetowej i dostępu do Hamnetu zamiast drogiego i skomplikowanego wyposażenia.
Analogicznie jak w Internecie, również i w Hamnecie wyszukiwarka może usprawnić korzystanie z sieci. Jeden z rozwojowych projektów w tej dziedzinie opiera się na bezpłatnym oprogramowaniu YaCy. Jest to rozproszony system wyszukiwania przeszukujący najbliższe zasoby wokół każdej z jej lokalizacji. Wyniki przeszukiwań są rozpowszechniane w całej sieci, dzięki czemu wszędzie możliwy jest dostęp do pełnego zbioru danych bez nadmiernego przeciążania łączy i przy zapewnieniu redundancji dodatnio wpływającej na jej niezawodność.
Uruchomienie własnego węzła wyszukiwarki wymaga jedynie przeznaczenia dlań przeciętnego komputera PC, ale dla „Maliny" jest to zbyt duże obciążenie.

6. Łączności głosowe przez „Mumble” i „Allstar”

„Mumble” jest oprogramowaniem serwera VoIP do prowadzenia łączności głosowych (rozmów) podobnie jak w „Skypie” czy „TeamSpeak” i dającym się łatwo dostosować do potrzeb krótkofalarskich. Pozwala on na pracę simpleksową z przełączaniem na nadawanie podobnie jak w radiostacjach i rozmowy indywidualne z wybranym partnerem. Jego dużym plusem jest łatwość obsługi. Do pracy klienta „Mumble” konieczna jest instalacja odtwarzacza „Macromedia Flash Player” w wersji 10 lub wyższej.

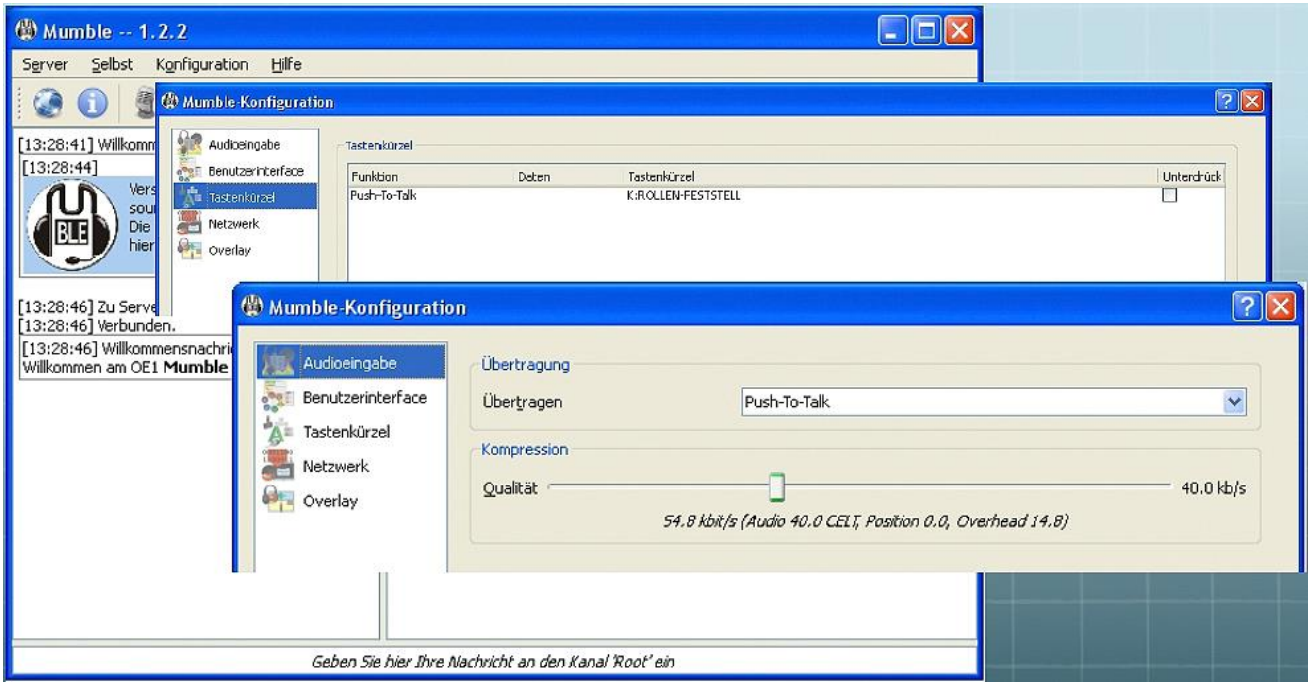
Program w wersjach dla Windows, Linuksa i macOS jest dostępny bezpłatnie w Internecie (*www.mumble.info*) i w wielu wypadkach także „Hamnecie”. Dla „Androida” i iOS dostępne są programy klientów o zbliżonych właściwościach j.np. *Plumbie*.

Rys. 6.1. Okno klienta Mumble

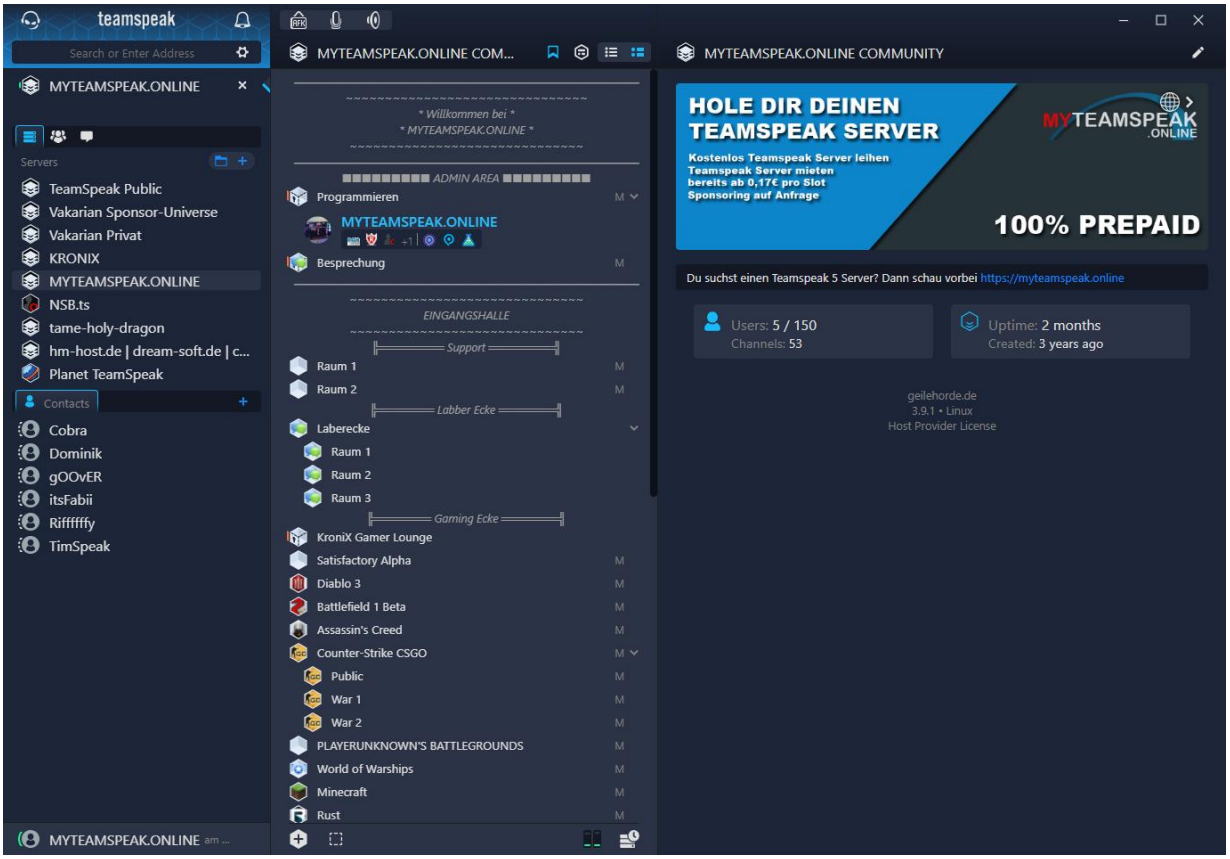


Rys. 6.2. Przykład konfiguracji dla dostępu do serwera „Mumble” OE1XRU

Serwer „Mumble”, którego dotyczy przykład z rys. 6.2 jest dostępny w „Hamnecie” pod adresem *web.oe1.ampr.at* (44.143.10.90), standardowo w kanale logicznym 64738. Jako nazwa użytkownika służy pokazana na ilustracji kombinacja znaku wywoławczego i imienia, nie wymagane jest natomiast hasło dostępu.



Rys. 6.3. Konfiguracja do przełączania nadawanie-odbiór. Zamiast automatycznego przełączania głosem należy wybrać z rozwijanej listy pozycję”Push-to Talk”



Rys.6.4. Okno TS5

Do prowadzenia łączności fonicznych przeznaczona jest także sieć „Allstar”, do której podłączonych jest już wiele przemienników FM (ale nie dorównująca rozpowszechnieniem „Echolinkowi”). „Allstar”

pozwala na dynamiczne łączenie się z przemiennikami, uruchamianie stałych łączy na wybranych trasach, zdalne sterowanie przemienników przez ich operatorów, „telefonowanie" przez sieć „Hamnetu", prowadzenie telekonferencji i uruchamianie skrzynek głosowych, a także wideotelefonia. Oprócz oprogramowania klienta dla Windows istnieje także wersja dla Androida.
System telefonii „Allstar" korzysta standardowo z kanału logicznego UDP (ang. *port*) 5060 i protokółu SIP (ang. *Session Initiation Protocol*).

TeamSpeak jest oprogramowaniem VoIP pozwalającym na prowadzenie dialogów i łączności w kółeczkach konferencyjnych. Do dyspozycji użytkowników są kanały publiczne i prywatne. Oprogramowanie korzysta z własnego protokółu będącego tajemnicą firmową producenta. Jego klient dla Windows, Linuksa i Mac jest dostępny bezpłatnie w witrynach *www.teamspeak.com* i *www.teamspeak.de*.

Skype zapewnia wizyjne łączności telefoniczne, konferencje wizyjne, telefonię IP, wymianę komunikatów „Instatn Messaging", transmisję plików i ujęć ekranowych. Program jest zasadniczo znany wśród użytkowników telefonów komórkowych i komputerów tabliczkowych (ang. *tablet*) i dzięki temu nie wymaga dłuższego omówienia. Program pracuje bezproblemowo na komputerach znajdujących się za zaporami przeciwwłamaniowymi (ang. *firewall*) i punktami dostępowymi NAT. Korzysta on z kanałów logicznych TCP 80 i 443. Oprócz wydania dla Windows istnieją także wersje dla Linuksa, macOS, Androida i iOS.

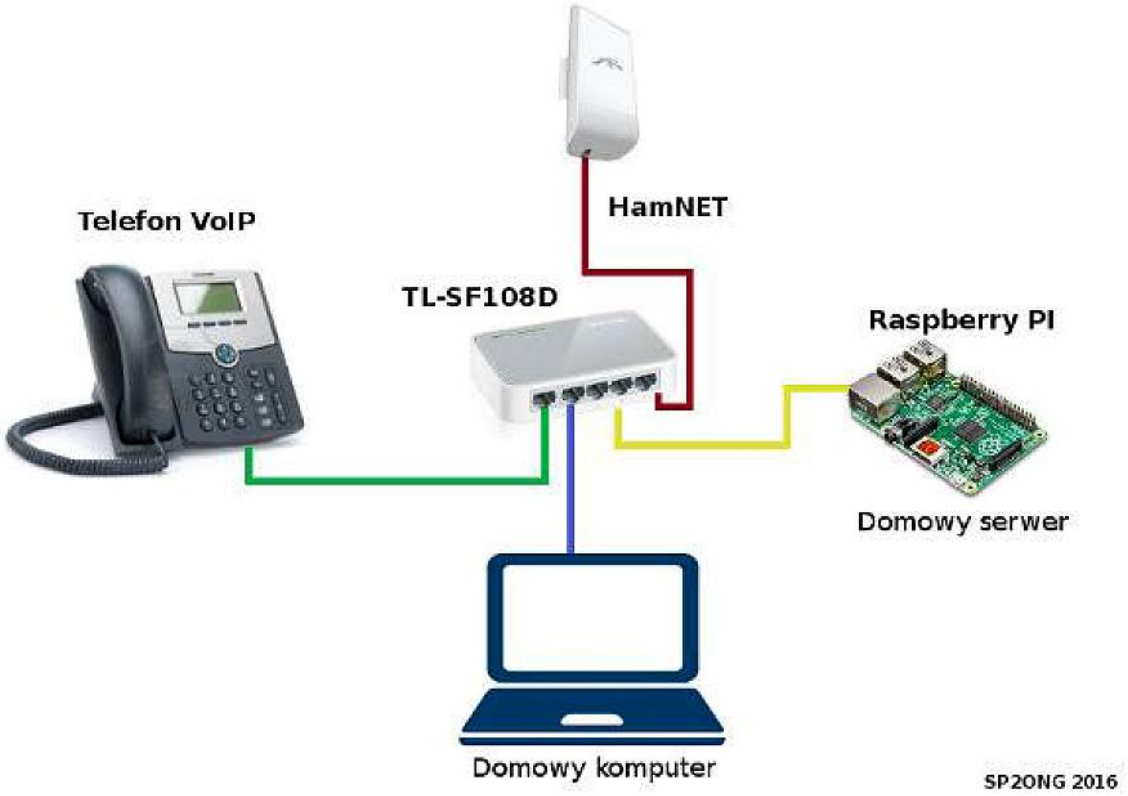
7. Telefonia SIP

Telefonia SIP (oparta o protokół o tej samej nazwie, ang. *Session Initiation Protocol*) zapewnia komfort sieci stacjonarej w Hamnecie. Numery telefonów są jednoznacznie przypisane do znaków wywoławczych użytkowników. Możliwe jest prowadzenie konferencji telefonicznych i korzystanie z automatycznej sekretarki. Sieć połączonych ze sobą serwerów korzysta z bazy danych użytkowników (abonentów) skopiowanej na każdy z nich. Abonenci meldują się na jednym z nich, a on łączy w miarę potrzeby rozmowę dalej. Sieć serwerów nie musi mieć pełnej topologii siatki.
Protokół SIP, będący najszerzej stosowanym porotokółem połączeniowym w telefonii VoIP, służy tylko do nawiązania połączenia między abonentami, jego funkcja odpowiada więc podniesieniu słuchawki w telefonach analogowych i ISDN. Jest to protokół tekstowy podobny do służącego do transmisji witryn WWW protokółu HTTP. Ułatwia to jego integrację w przeglądarkach internetowych i programach związanych z siecią WEB. Może on byc stosowany zarówno w sieciach lokalnych jak i w połączeniach internetowych. Po pierwszej fazie – nawiązania połączenia – następuje faza rozmowy i na zakończenie – przerwanie połączenia. Rozmowa VoIP (transmisja zakodowanych pakietów dźwiękowych) przebiega pod kontrolą protokółu RTP z użyciem datagramów UDP, a SIP już w niej nie uczestniczy (patrz rys. 7.4). Faza trzecia – przerwanie połączenia odbywa się znowu z użyciem protokółu SIP. Pozwala on nie tylko na nawiązanie połączeń dwustronnych, ale także i konferencyjnych. Protokół SIP stał się standardem światowym i może być używany przez wiele modeli telefonów.
Serwery telefoniczne (oznaczane również skrótem PBX – ang. *Private Branch Exchange*) pracują na bazie bezpłatnego linuksowego oprogramowania *Asterisk*. Istnieją również wersje *Asteriska* dla „Maliny", systemu Mac OSX i Windows i różne dystrybucje jak bezpłatna *FreePBX* (*www.freepbx.org*). Łączy ona serwer *Asterisk* z internetową powierzchnią obsługi i pracuje pod Linuksem Centos 7. W mniejszych sieciach (domowych hamnetowych itp.) wystarczy także „Malina".
Po zainstalowaniu i pierwszym uruchomieniu serwera konieczne jest założenie konta administratora wybranie jego nazwy i hasła dostępu. Wszelkie akcje dokonywane są w oknie przeglądarki internetowej połączonej z adresem IP serwera. W oknie administratora modułów („Module Admin") należy pozostawić włączone wszytkie moduły włączone domyślnie. Modułów dodatkowych przeznaczonych dla użytkowników profesjonalnych („EXTENDED", „COMMERCIAL") nie trzeba uruchamiać.
W oknie managera aparatów telefonicznych („Endpoint Manager") należy wybrać typ aparatu i wprowadzić dane konfiguracyjne. Pomocne w tym mogą być przykłady podane poniżej. W zależności od oprogramowania i jego wersji wygląd okien może się w pewnym stopniu różnić od podanych.
Zależnie od potrzeb można też uruchomić takie dodatkowe usługi jak skrzynka głosowa, nagrywanie itp.

1-sza cyfra ↓	2-ga cyfra				
	0	1	2	3	4
1	1				
2	2	A	B	C	
3	3	D	E	F	
4	4	G	H	I	
5	5	J	K	L	
6	6	M	N	O	
7	7	P	Q	R	S
8	8	T	U	V	
9	9	W	X	Y	Z
0	0				

Rys. 7.1. Kodowanie znaków wywoławczych na klawiaturze telefonu

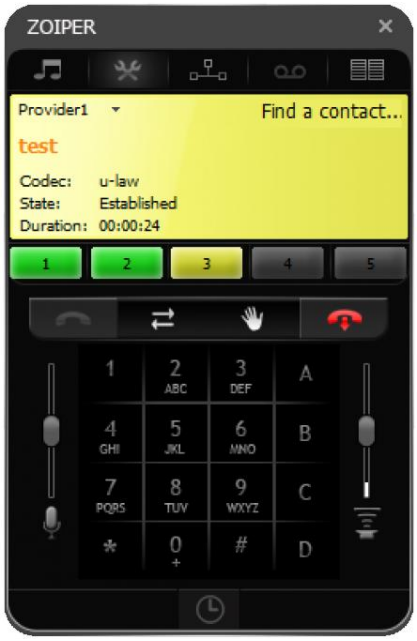
Abonenci muszą mieć na jednym z węzłów konto z numerem założone przez jego operatora. Dzięki połączeniu serwerów ze sobą użytkownicy mogą być dostępni na całym obszarze kraju albo i nie tylko. Abonenci są wpisani do centralnej bazy danych. Abonenci mogą prowadzić rozmowy ze stacjami połączonymi z tym samym serwerem oraz z innym serwerami sieci. W łącznościach między serwerami stosowany jest protokół AIX i system wybierania numerów Dundi.
Operatorzy serwerów mogą udostępnić lokalnie dodatkowe usługi w rodzaju zegarynki, echa, kółeczek konferencyjnych, wywoływania komunikatów krótkofalarskich itp.
W systemie telefonii hamnetowej SIP numer abonenta odpowiada jego znakowi wywoławczemu wprowadzanemu na klawiaturze telefonu. Zasada jest identyczna ze stosowaną w „Echolinku" – każdej z liter znaku odpowiadają dwie cyfry – cyfra na klawiszu zawierającym daną literę i pozycja litery w trzyliterowym ciągu, przykładowo literze E odpowiada ciąg cyfr 33, a literze Y – 93. W odróżnieniu od przyporządkowania stosowanego w Echolinku litery Q i Z nie są przeniesione na klawisz „1", a więc klawiszom „7" i „9" są przypisane ciągi czterech liter (rys. 7.1).
Znakowi OE1KDA odpowiadałby więc ciąg cyfr:
633210 (= OE1 jako człon kierunkowy) i 523121 (=KDA jako numer idywidualny). Człon kierunkowy jest używany tylko w trakcie wywołania stacji z innego okręgu, a więc stacja z okręgu OE1 musi podać tylko indywidualny człon numeru 523121, natomiast stacja z innych okolic podaje całość: 633210523121. Kalkulator numerów jest dostępny w Internecie pod adresem
https://www.oe2wnl.at/calltodtmf-voip.php.
W przypadku gdy stacja jest wyposażona w kilka aparatów telefonicznych jej operator musi sam wprowadzić w konfiguracji numery wewnętrzne.
Abonenci mają do wyboru różne modele aparatów telefonicznych VoIP, w tym także aparatów wycofanych z użytku profesjonalnego. Wśród nich są m.in. modele snom320, snom370, firmy Cisco itp. Oprócz tego można korzystać z aparatów analogowych z przystawką-konwerterem. Można korzystać także z inteligentnych telefonów (ang. *smartphone*) i komputerów z telefonem programowym.



Rys. 7.2. Telefon w sieci Hamnetu

Przy zakładaniu konta na serwerze *Asteriska* konieczne jest podanie jako najważniejszych parametrów (należy podać własny znak wywoławczy i dane od niego pochodzące):

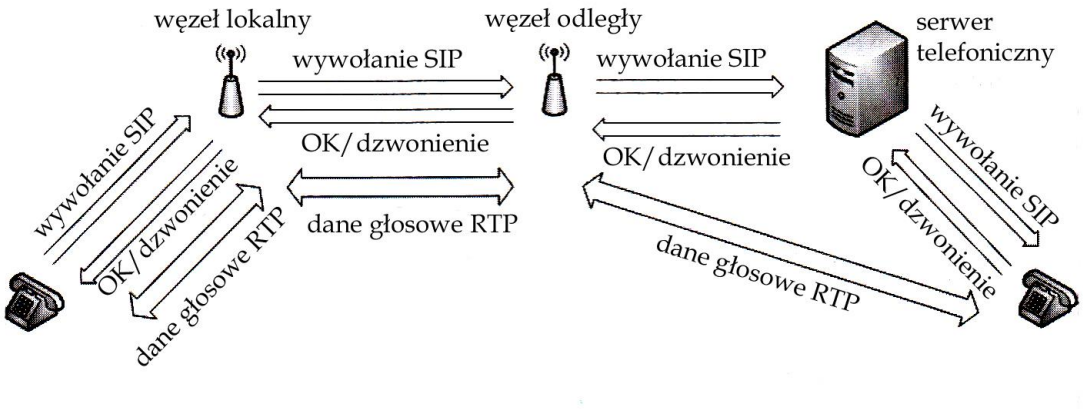
- Nazwy konta („Account name") – znaku wywoławczego, np. SP5XXX
- Domeny – 44.xx.xx.xx,
- Nazwy użytkownika („User Name") – w tym przykładzie użyto indywidualnej części znaku XXX, której odpowiada po przekodowaniu numer 929292,
- Hasła dostępu („Password") – w tym przykładzie również 929292, może być dowolne,
- Identyfikatora abonenta („User ID") – w tym przykładzie także 929292.



Dane te wystarczają także do korzystania w sieci telefonii hamnetowej z klienta *Zoiper* (obecnie w bezpłatnej wersji 5 i w płatnej 5 PRO) pozwalającego na telefonowanie za pomocą iPhona, telefonów androidowych, komputerów z Windows, Linuksem albo komputerów *Mac Book Pro* zamiast aparatów telefonicznych VoIP. Dla Androida istnieje również program *CSipSimple https://apkpure.com*).
Możliwości Zoipera nie są oczywiście ograniczone do Hamnetu. Można korzystać z niego również w Internecie za pośrednictwem dostawcy usług VoIP lub PBX. Program jest dostępny w Internecie w witrynie
https://www.zoiper.com/en/voip-softphone/download/current.

Rys. 7.3. Okno Zoipera

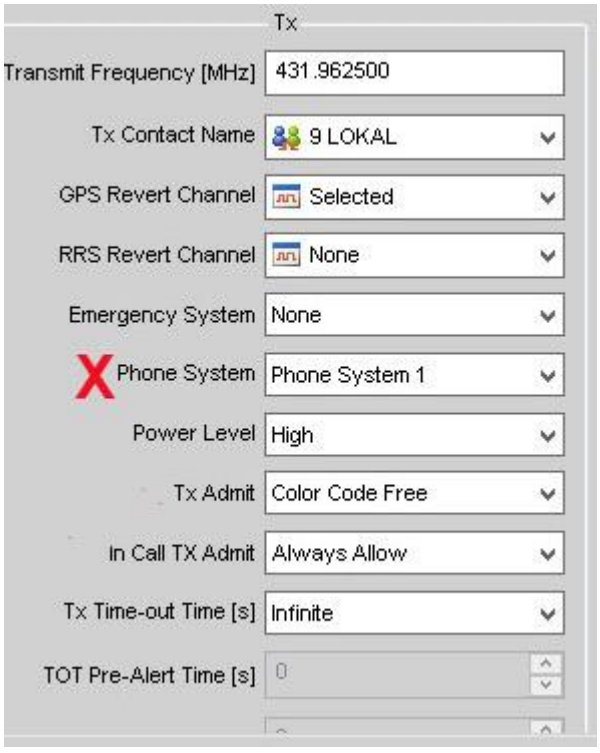
Szyfrowanie nie jest dozwolone w sieciach krótkofalarskich i tam gdzie jest ono technicznie możliwe należy je wyłączyć w konfiguracji.



Rys. 7.4. Przebieg połączenia telefonicznego

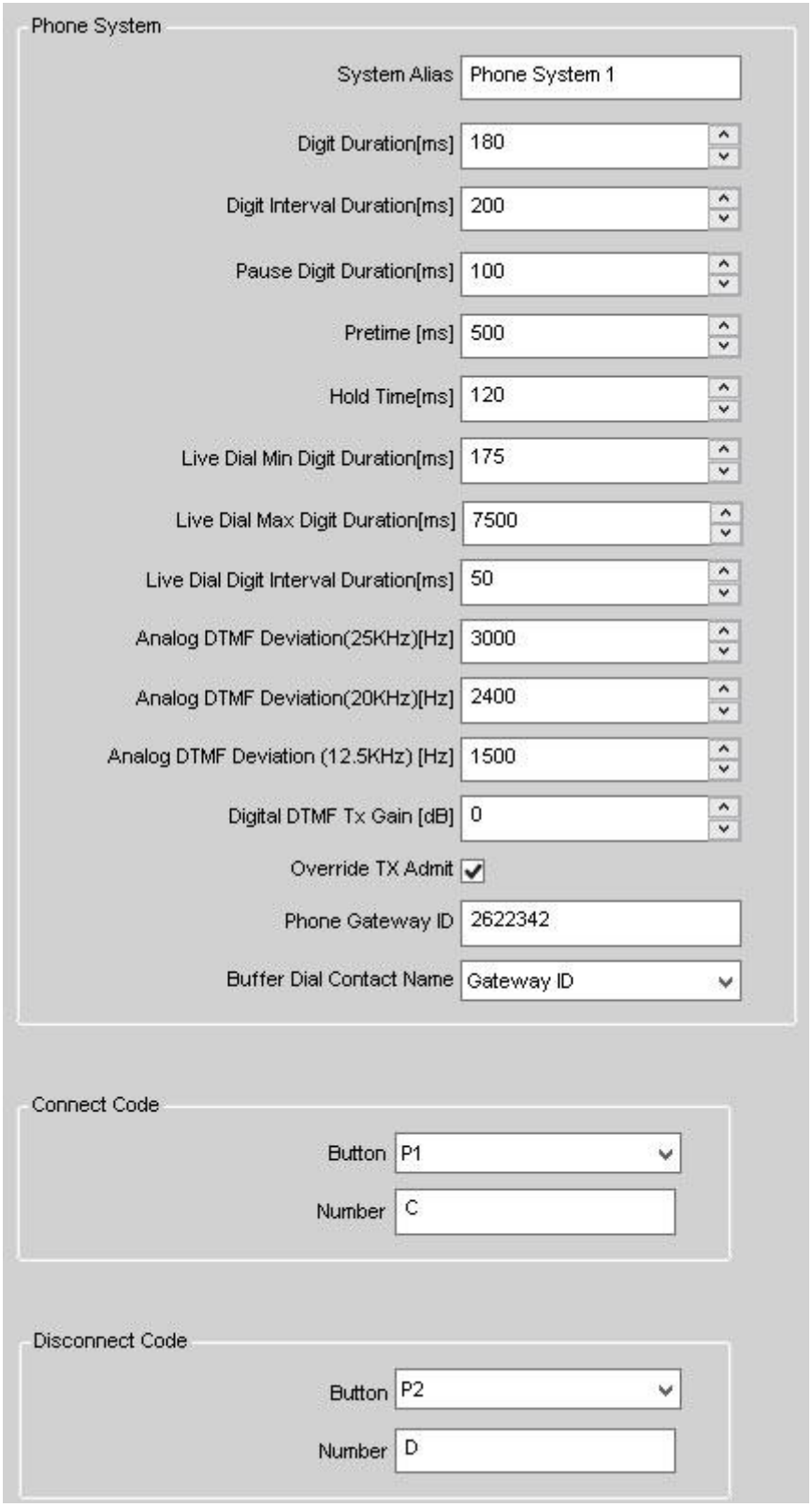
7.0.1. Rozmowy DMR-SIP

Niektóre z serwerów telefonicznych pozwalają nawet na prowadzenie rozmów między telefonami hamnetowymi SIP, a użytkownikowi sieci Brandmeistra DMR.
Przykładowo przemiennik DMR DB0FS w Hamburgu ma skonfigurowane dwa połączenia z grupami DMR dostępnymi pod numerami telegonicznymi:
nr 262220 – grupa lokalna TG9 w szczelinie TS2,
nr 2622 – grupa regionalna Hamburga i okolicy.
Oprócz tego możliwe są prywatne wywołania z telefonu SIP do radiostacji użytkowników osiągalnych przez ten przemiennik. Jako numer telefonu wybierany jest w tym przypadku identyfikator DMR stacji. Stacje indywidualne DMR, które mają być osiągalne w ten sposób muszą się zarejestrować u operatora przemiennika. W przypadku gdy radiostacja DMR jest wyłączona, nieosiągalna w szczelinie 2 albo połączona z inną siecią abonent SIP otrzymuje sygnał zajętości.
W trakcie rozmowy abonent SIP jest stale na nadawaniu, aż do czasu naciśnięcia przez jego korespondenta przycisku nadawania. Po naciśnięciu przycisku abonent SIP jest przełączany na odbiór. Kierunek nadawania i odbioru jest więc sterowany przez stację DMR za pomocą jej przycisku nadawania. Abonent telefoniczny otrzymuje sygnał dźwiękowy w momencie przełączenia. Użytkownik DMR musi co 45 sekund naciskać na krótko przycisk nadawania dla podtrzymania połączenia. Użytkownicy DMR zarejestrowani na serwerze SIP
Wyposażenie DB0FS w Hamburgu składa się z przemiennika Hytery RD985 połączonego z „Maliną”, na której pracuje serwer SIP – *Asterisk*.
Radiostacje użytkowników DMR wymagają dopasowania kofiguracji, aby możliwe było inicjowanie i kończenie połączeń telefonicznych. Konieczne zmiany w konfiguracji dla kanału cyfrowego DMR przedstawiamy na przykładzie radiostacji Hytery.



Rys. 7.0.1.1. Do kanału lokalnego DMR (TG9) dla przemiennika bramki DMR-SIP przypisana jest konfiguracja telefoniczna, tutaj pod nazwą „Phone System 1”

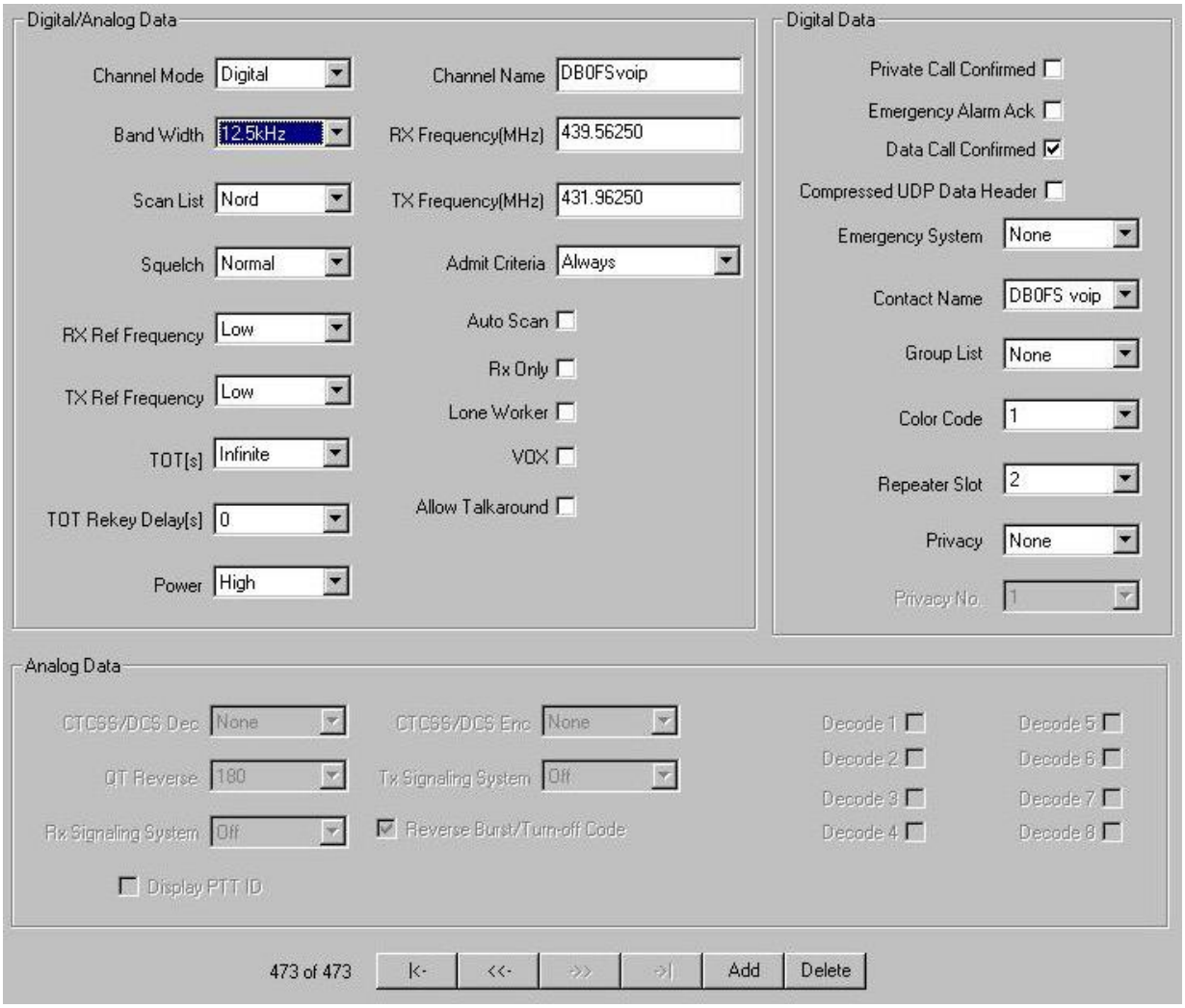
Na rysunku 7.0.1.1 przedstawiony jest fragment okna konfiguracyjnego dla kanału DMR dla przemiennika oferującego połączenie telefoniczne z Hamnetem. Konieczne jest zupełnienie jej o przypisanie systemu telefonicznego. Następnym krokiem jest konfiguracja funkcji telefonicznej w oknie „Phone” -> „Phone System” -> „Phone System 1”, jak to pokazano na ilustracji 7.0.1.2.



Rys. 7.0.1.2. Konfiguracja funkcji telefonicznej

Konfiguracja funkcji telefonicznej ma na celu umożliwienie korzystania z tonów DTMF do wybierania numeru telefonicznego. W przykładzie podano identyfikator bramki DMR-SIP DB0FS w Hamburgu. W menu „Phone List” („Spis telefonów”) można wpisać książkę telefoniczną.

Przebieg rozmowy:
– Rozmowa przychodząca jest sygnalizowania dźwiękowo przez radiostację. W celu jej odebrania należy nacisnąć przycisk nadawania i trzymając go nacisnąć zielony klawisz (P1 na rys. 7.0.1.2). Rozmowę można rozpocząć po puszczeniu przycisku nadawania. Dla zakończenia połączenia należy przy naciśniętym przycisku nadawania nacisnąć czerwony klawisz (P2 na rys. 7.0.1.2), a następnie puścić przycisk nadawania.
– Dla zatelefonowania do korespondenta można wybrać jego numer w książce telefonicznej, zaznaczyć go o nacisnąć na krótko przycisk nadawania. Po jego puszczeniu radiostacja wybiera wskazany numer. Numer można także wybrać ręcznie na klawiaturze po wejściu w tryb ręcznego wpisywania. Potem trzeba tylko nacinąć krótko przycisk nadawania i puścić go. Na zakończenie połączenia w obu przypadkach należy nacisnąć czerwony klawisz P2 przy naciśniętym przycisku nadawania. Po jego puszczeniu połączenie zostanie przerwane.

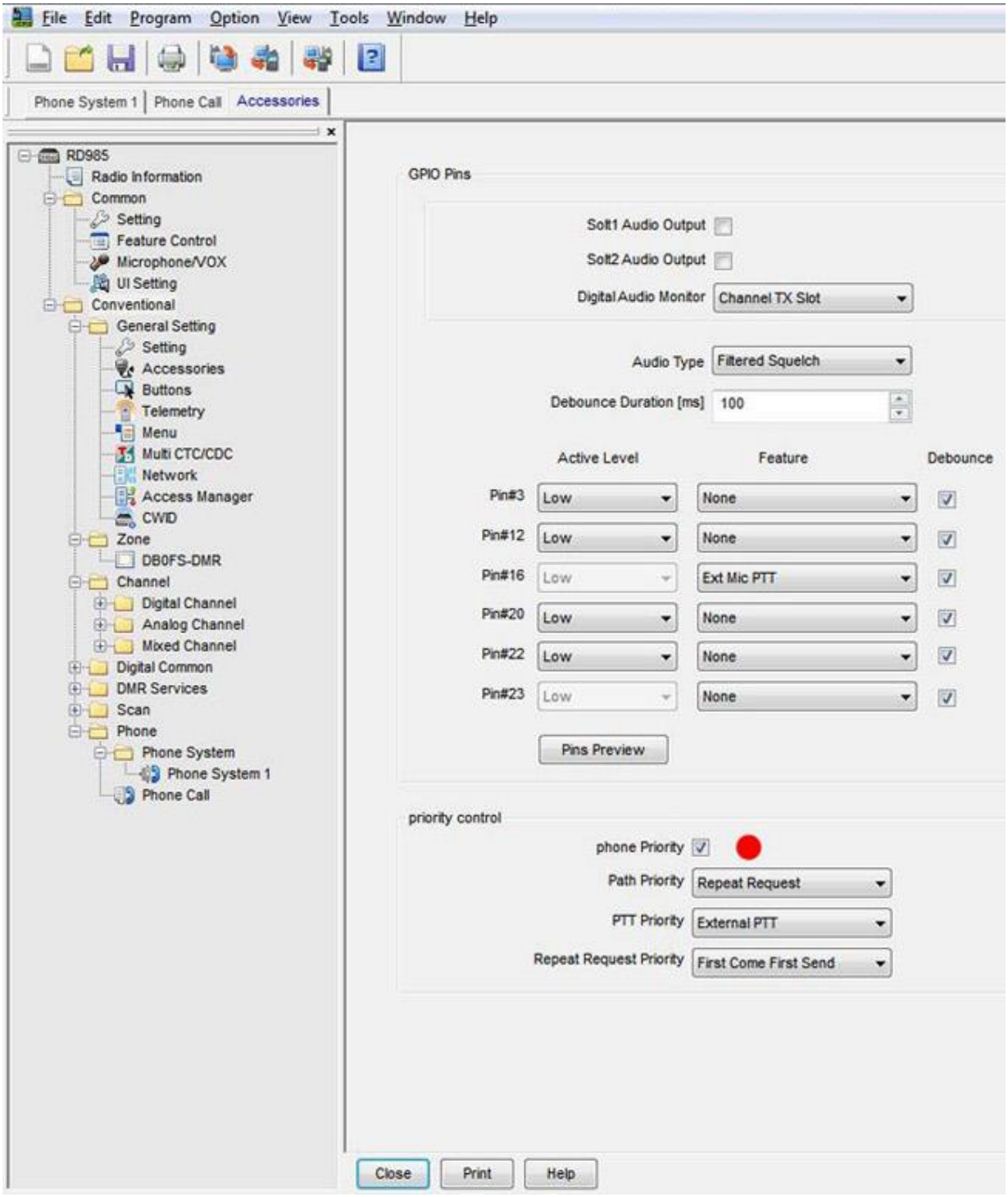


Rys. 7.0.1.3. Konfiguracja kanału dla Retevisa RT3

Dla skonfigurowania kanału DMR dla przemiennika-bramki w sposób pokazany na rysunku 7.0.1.3 w radiostacjach Tytery i Retevisa konieczne jest wpisanie najpierw prywatnego kontaktu (prywatnego wywołania) identyfikatora w spisie kontaktów. W pokazanym przykładzie jest to wywołanie identyfikatora 2622342 dla bramki SIP na DB0FS. Kontakt ten w przykładzie nosi nazwę *DB0FS voip*. Kontakt ten jest wpisywany w miejscu grupy w konfiguracji kanału. Odebranie rozmowy polega na naciśnięciu zielonego klawisza przy naciśniętym przycisku nadawania, a rozłączenie na naciśnięciu czerwonego klawisza. Funkcje klawiszy są skonfigurowane standardowo w radiostacji.
Zatelefonowanie do korespondenta w Hamnecie wymaga nastawienia kanału skonfigurowanego jak na rysunku powyżej, naciśnięcia przycisku nadawania i wpisaniu numeru na klawiaturze radiostacji.

Nawiązanie połączenia następuje po puszczeniu przycisku nadawania. Na zakończenie konieczne jest naciśnięcie czerwonego klawisza przy naciśniętym przycisku nadawania, i następnie puszczeniu przycisku nadawania.

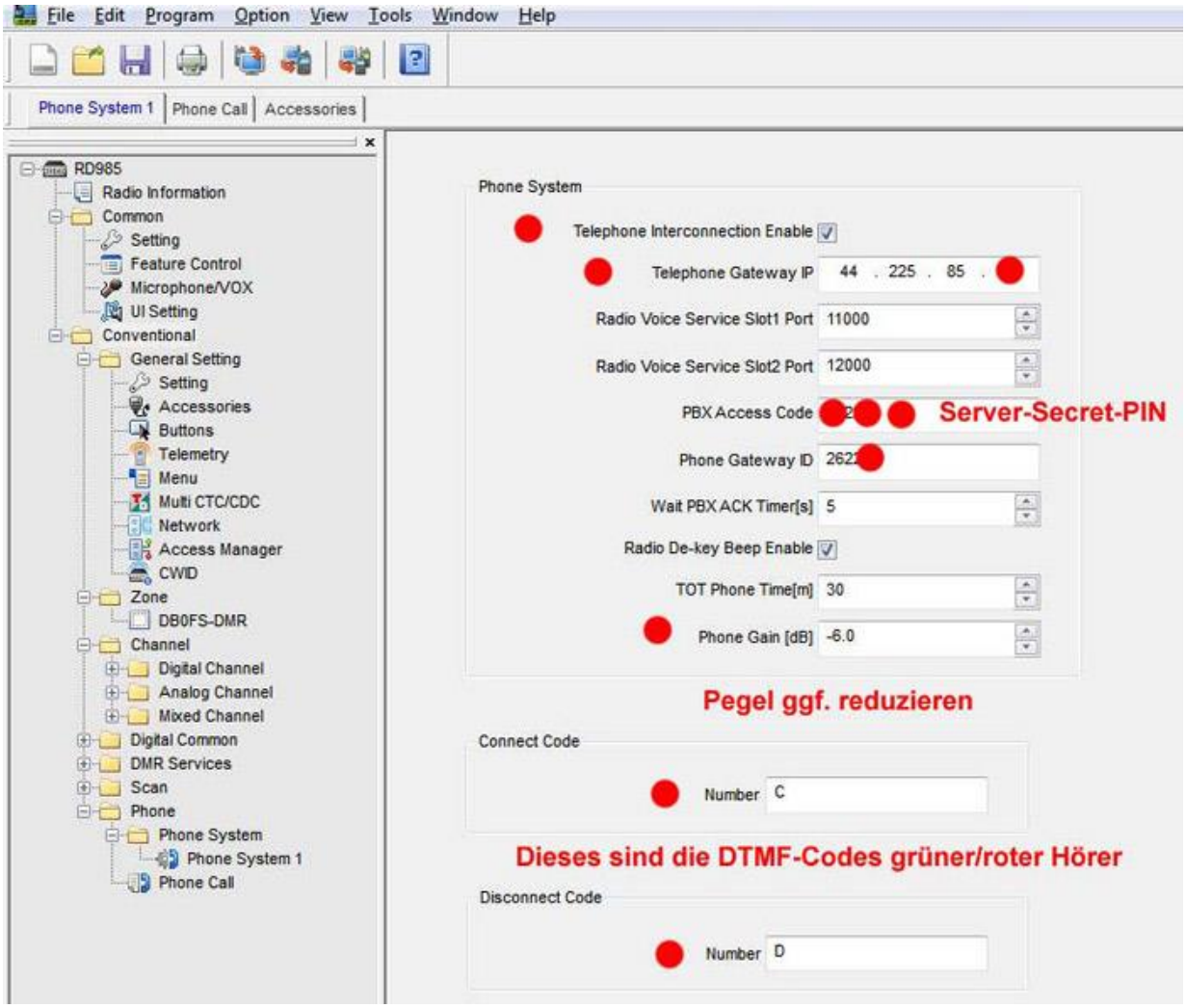
7.0.2. Konfiguracja przemiennika DMR



Rys. 7.0.2.1

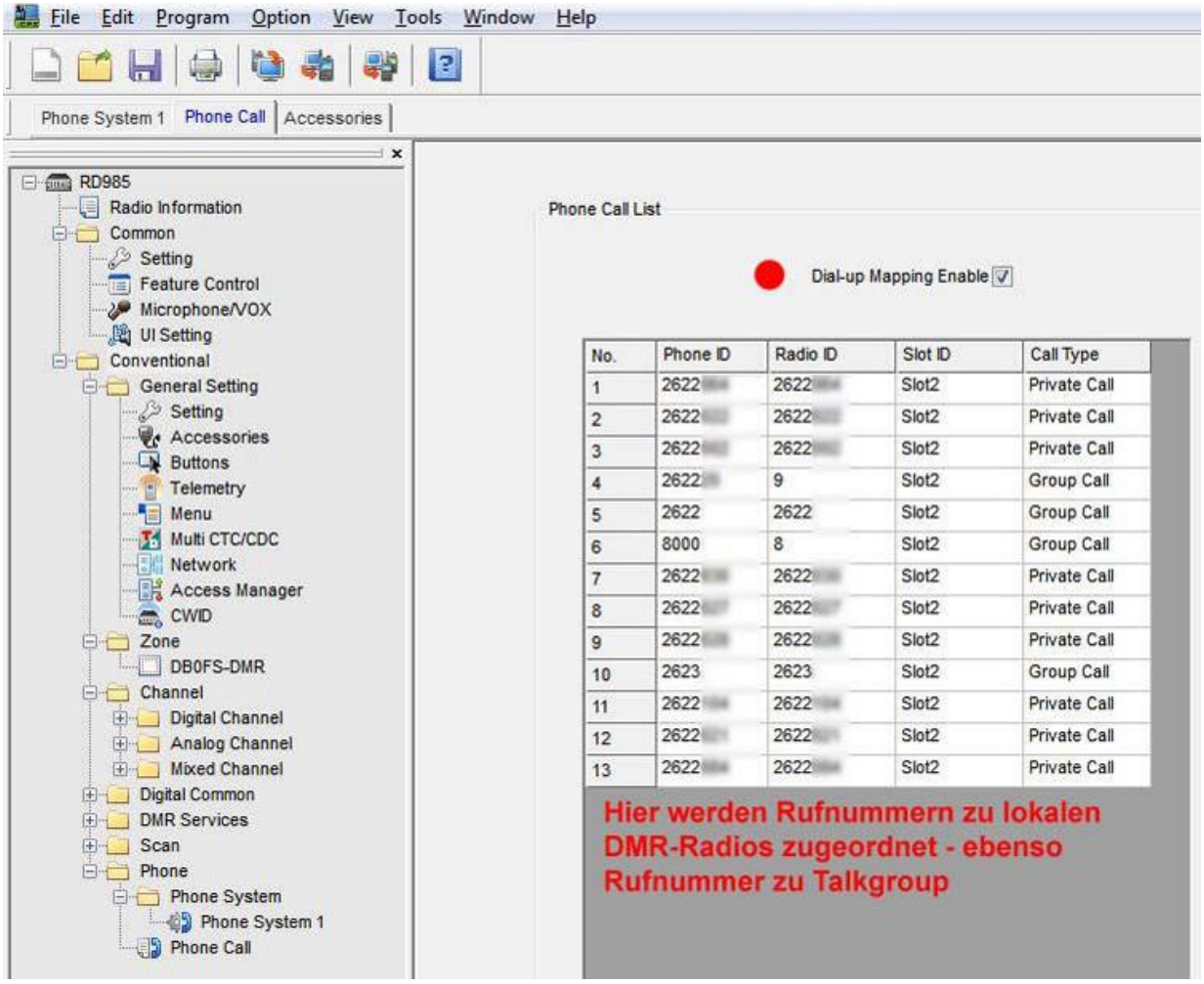
Służący jako bramka DMR-SIP przemiennik DMR Hytery jest połączony przez sieć z serwerem telefonicznym SIP (np. *FreePBX*). Konfiguracja jest na tyle łatwa, że do jej przedstawienia wystarczą poniższe ilustracje. Dodatkowo konieczne może być dobranie dalszych parametrów takich jak

ograniczenie czasu nadawania, czasu TOT itd. Bramka musi posiadać własny identyfikator DMR. W przykładzie dla DB0FS jest to 2622342. Pozwala on na rozpoznanie nadchodzących rozmów i przekierowanie ich do serwera SIP. Połączenia SIP są kierowane do sieci Brandmeistra. Bramka pozwala na łączenie się z nią przemienników DMR, ale nie mogą korzystać z niej mikroprzemienniki w rodzaju DV4mini itd. Maksymalna liczba zarejestrowanych użytkowników telefonii DMR-SIP jest ograniczona w pliku konfiguracyjnym. Z tego też powodu zalecane jest, aby byli to aboneneci regionalni.



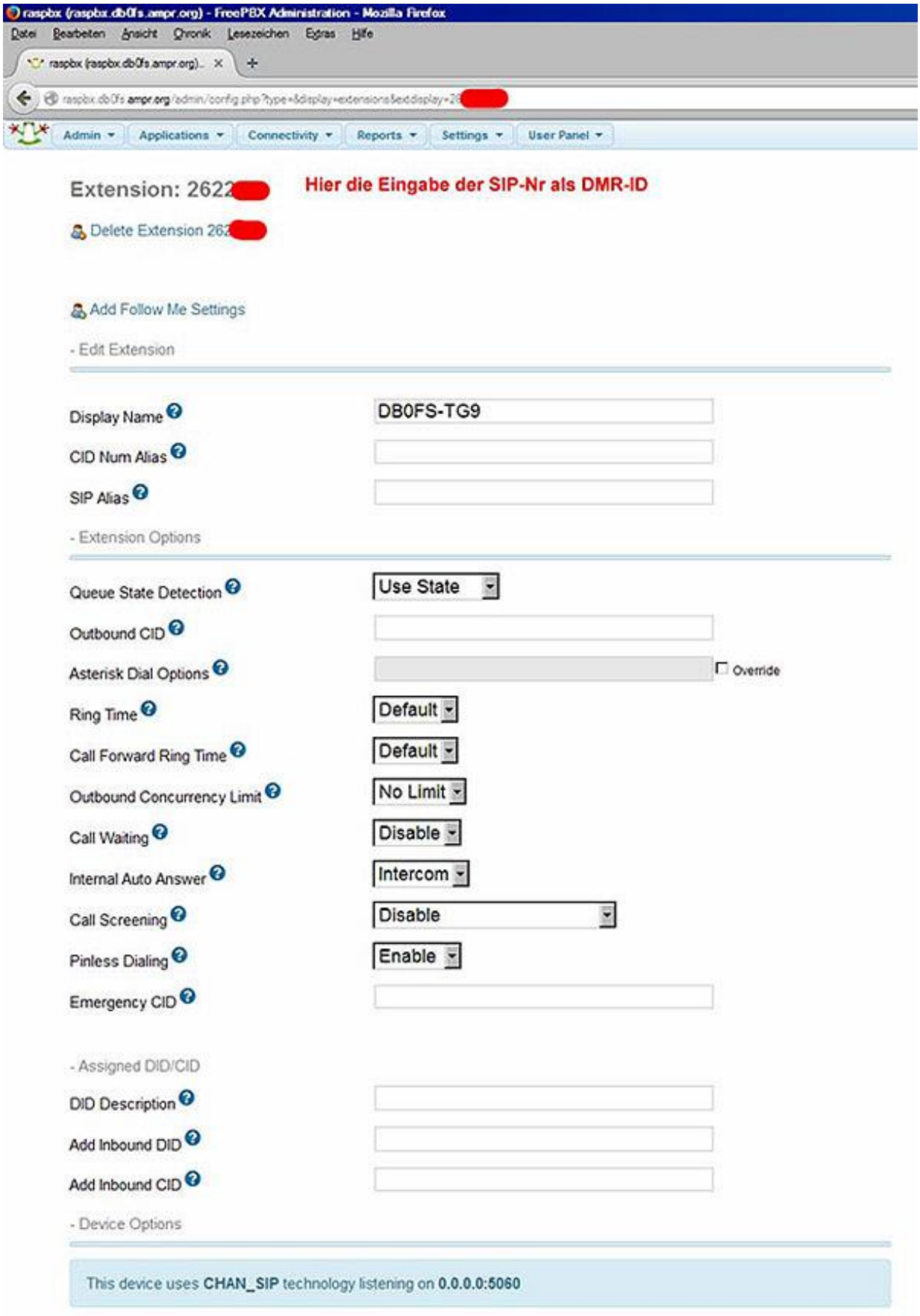
Rys. 7.0.2.2

W polu „Telephone Interconnection Enable” na rysunku 7.0.2.2 włączana jest usługa telefoniczna, w polu „Telephone Gateway” wprowadzany jest adres IP bramki, w polu „PBX Access Code” – hasło dostępu, a w polu „Phone Gateway ID” – identyfikator DMR-owy bramki. Pole „Phone Gain” umożliwia regulację siły głosu, a poniżej znajdują się pola kodów DTMF połączenia i rozłączenia, odpowiednio dla zielonego i czerwonego klawisza.

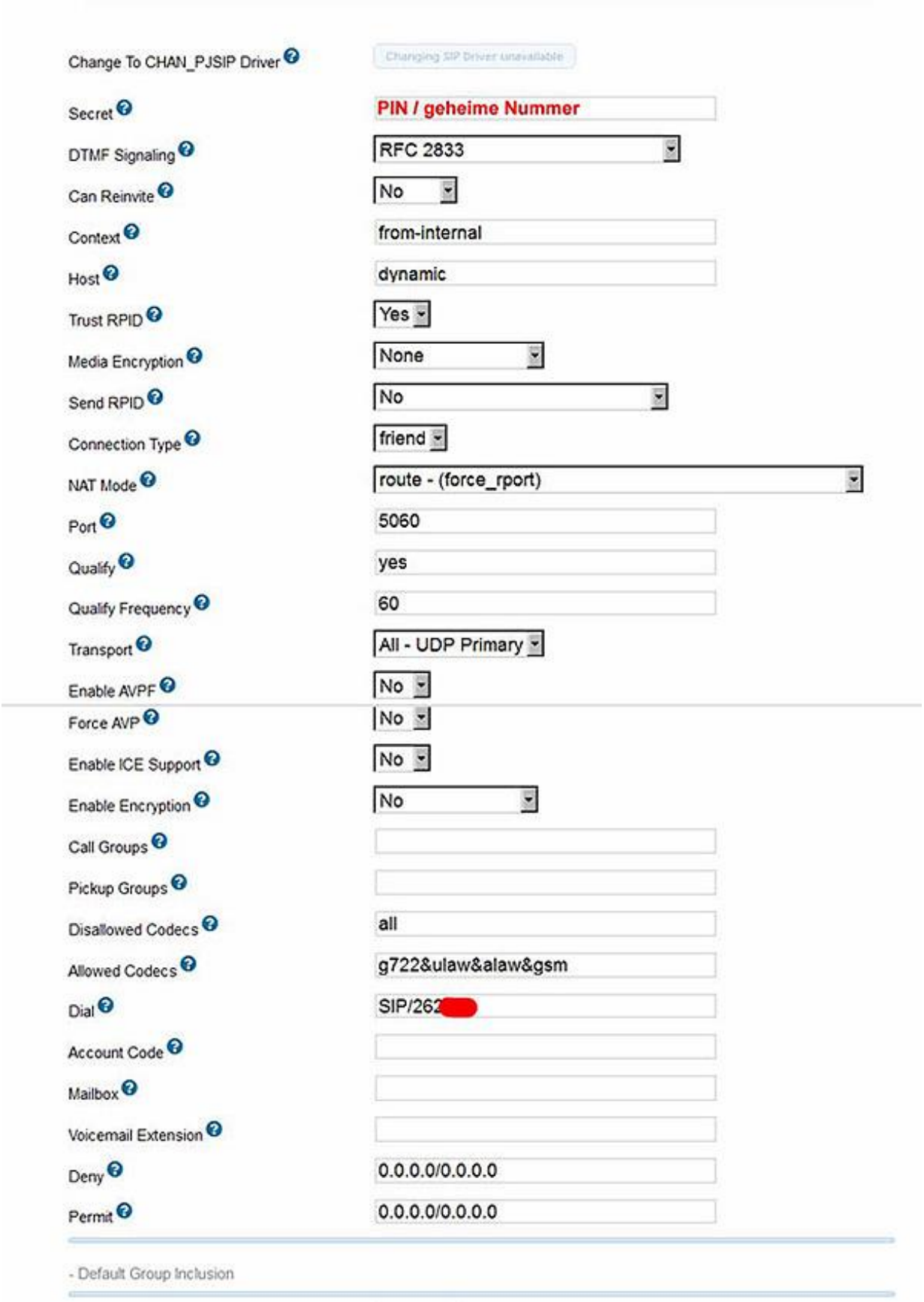


Rys. 7.0.2.3. Książka telefoniczna numerów stacji DMR i grup DMR

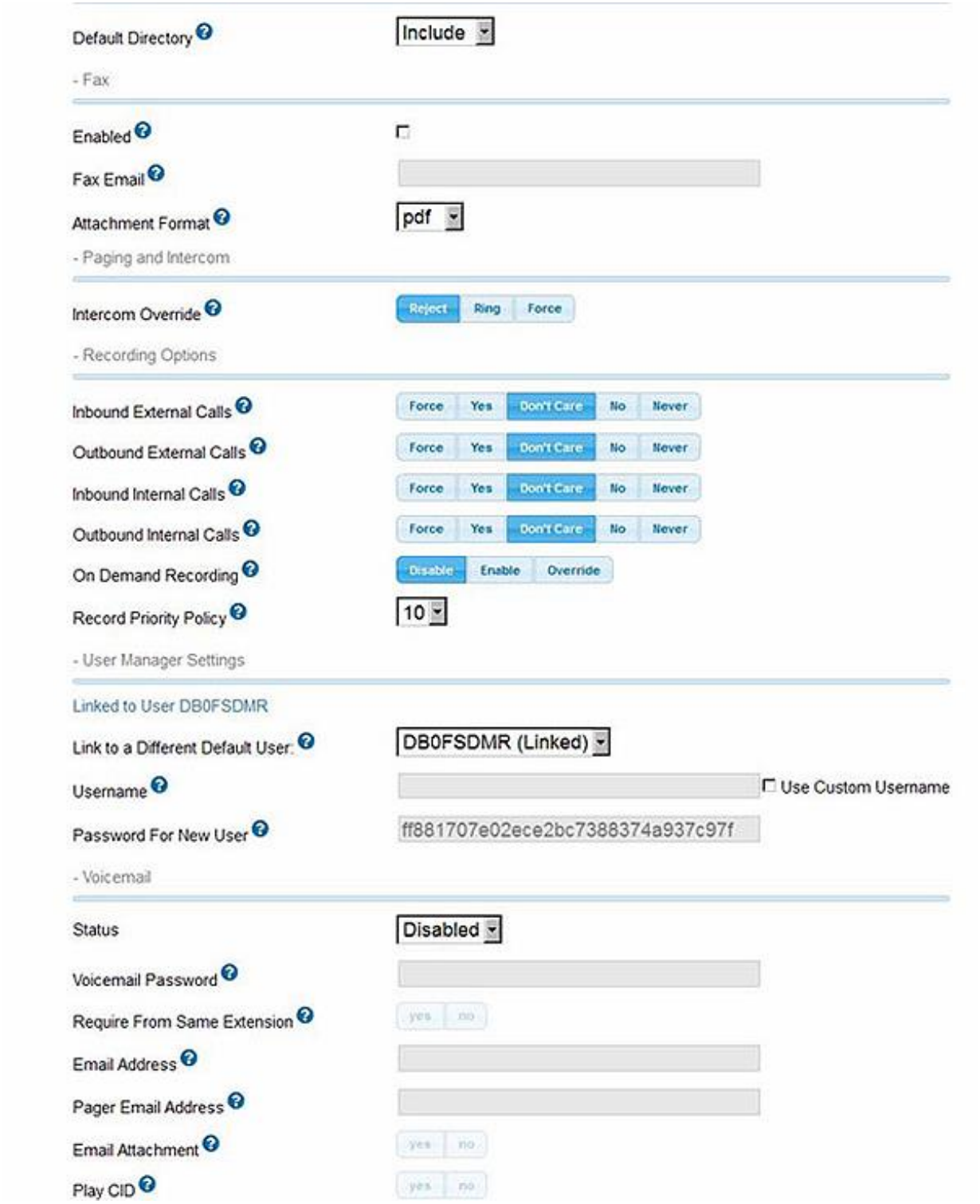
Na ilustracjach 7.0.2.4a – c przedstawiono przykład konfiguracji serwera *FreePBX* do łączności SIP-DMR dla grupy TG9 (pole „Display Name” na rys. 7.0.2.4a). Oprogramowanie serwera pracuje na *Malinie* połączonej z siecią Hamnetu 44. Prowadzenie łaczności telefonicznej wymaga dwóch różnych rejestracji: SIP i DMR. Abonent posiada więc konto pod swoim numeren SIP wywodzącym się ze znaku wywoławczego i wpis identyfikatora DMR jako numeru telefonicznego w konfiguracji przemiennika. Przemiennik otrzymuje kilka numerów dla wybranych grup rozmówców.
Ze względu na to, że przemiennik posiada tylko jedno hasło dostępu do wszystkich konfiguracji SIP konieczne jest jego użycie wszędzie na serwerze SIP.
Po przeprowadzeniu prawidłowej konfiguracji przemiennika i serwera należy upewnić się, że są one widoczne nawzajem dla siebie przez łącze IP w odpowiednich kanałach logicznych.
W polu „Extention” u góry na rys. 7.0.2.4a i w polu „Dial” w dolnej części rys. 7.0.2.4b podawany jest identyfikator DMR jako numer SIP. W polu „Secret” u góry na rys. 7.0.2.4b podawane jest hasło dostępu.


raspbx (raspbx.db0fs.ampr.org) - FreePBX Administration - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Admin Applications Connectivity Reports Settings User Panel
Extension: 2622
Hier die Eingabe der SIP-Nr als DMR-ID
Delete Extension 262
Add Follow Me Settings
- Edit Extension
Display Name
DB0FS-TG9
CID Num Alias
SIP Alias
- Extension Options
Queue State Detection
Use State
Outbound CID
Asterisk Dial Options
Override
Ring Time
Default
Call Forward Ring Time
Default
Outbound Concurrency Limit
No Limit
Call Waiting
Disable
Internal Auto Answer
Intercom
Call Screening
Disable
Pinless Dialing
Enable
Emergency CID
- Assigned DID/CID
DID Description
Add Inbound DID
Add Inbound CID
- Device Options
This device uses CHAN_SIP technology listening on 0.0.0.0:5060

Rys. 7.0.2.4a


Change To CHAN_PJSIP Driver
Changing SIP Driver unavailable
Secret
PIN / geheime Nummer
DTMF Signaling
RFC 2833
Can Reinvite
No
Context
from-internal
Host
dynamic
Trust RPID
Yes
Media Encryption
None
Send RPID
No
Connection Type
friend
NAT Mode
route - (force_rport)
Port
5060
Qualify
yes
Qualify Frequency
60
Transport
All - UDP Primary
Enable AVPF
No
Force AVP
No
Enable ICE Support
No
Enable Encryption
No
Call Groups
Pickup Groups
Disallowed Codecs
all
Allowed Codecs
g722&ulaw&alaw&gsm
Dial
SIP/262
Account Code
Mailbox
Voicemail Extension
Deny
0.0.0.0/0.0.0.0
Permit
0.0.0.0/0.0.0.0
- Default Group Inclusion

Rys. 7.0.2.4b


Default Directory
Include
- Fax
Enabled
Fax Email
Attachment Format
pdf
- Paging and Intercom
Intercom Override
Reject
Ring
Force
- Recording Options
Inbound External Calls
Outbound External Calls
Inbound Internal Calls
Outbound Internal Calls
Force
Yes
Don't Care
No
Never
On Demand Recording
Disable
Enable
Override
Record Priority Policy
10
- User Manager Settings
Linked to User DB0FSDMR
Link to a Different Default User:
DB0FSDMR (Linked)
Username
Use Custom Username
Password For New User
ff881707e02ece2bc7388374a937c97f
- Voicemail
Status
Disabled
Voicemail Password
Require From Same Extension
Email Address
Pager Email Address
Email Attachment
Play CID
yes
no

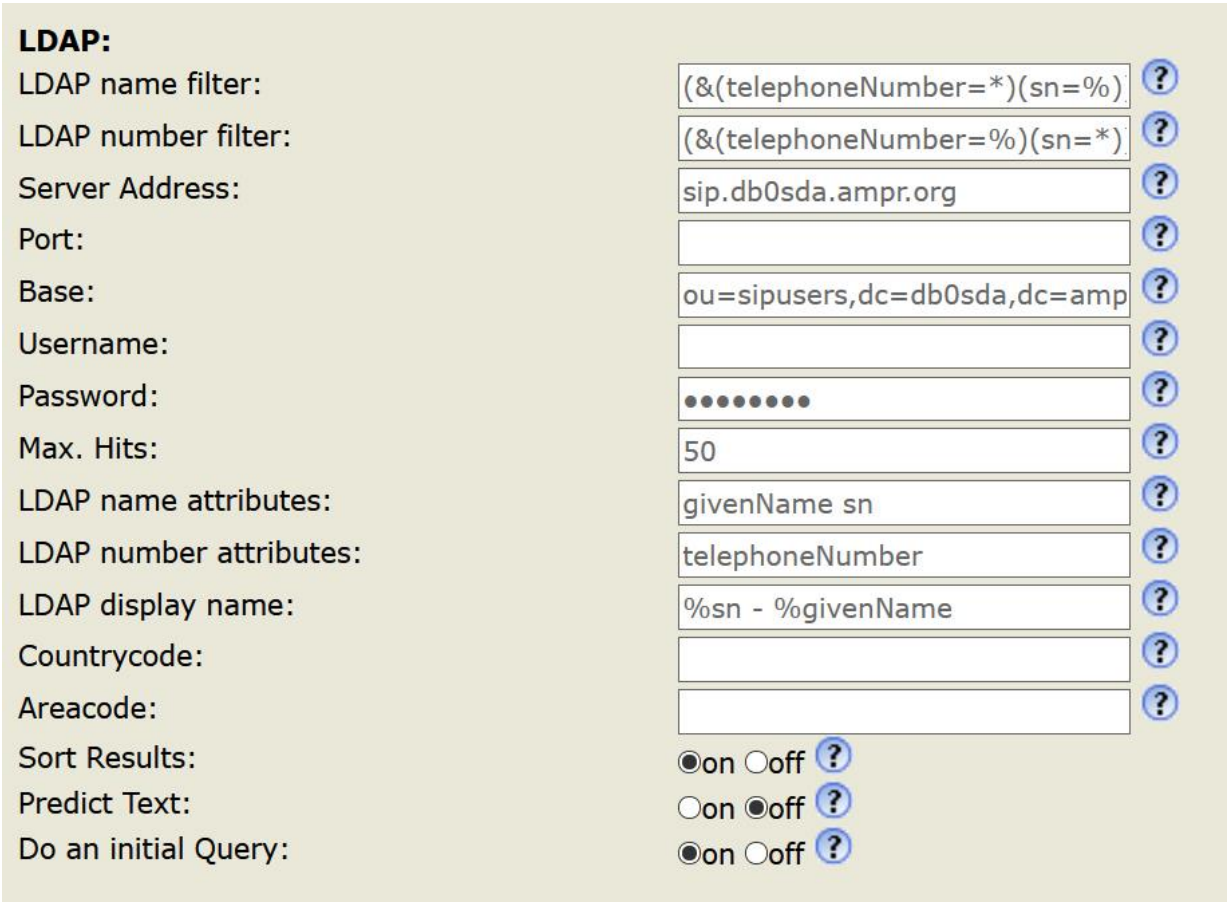
Rys. 7.0.2.4c

7.1. Konfiguracja telefonu SNOM300

Rys. 7.1.1. Zakładka dostępu („Login”)

Rys. 7.1.2. Zakładka „RTP”

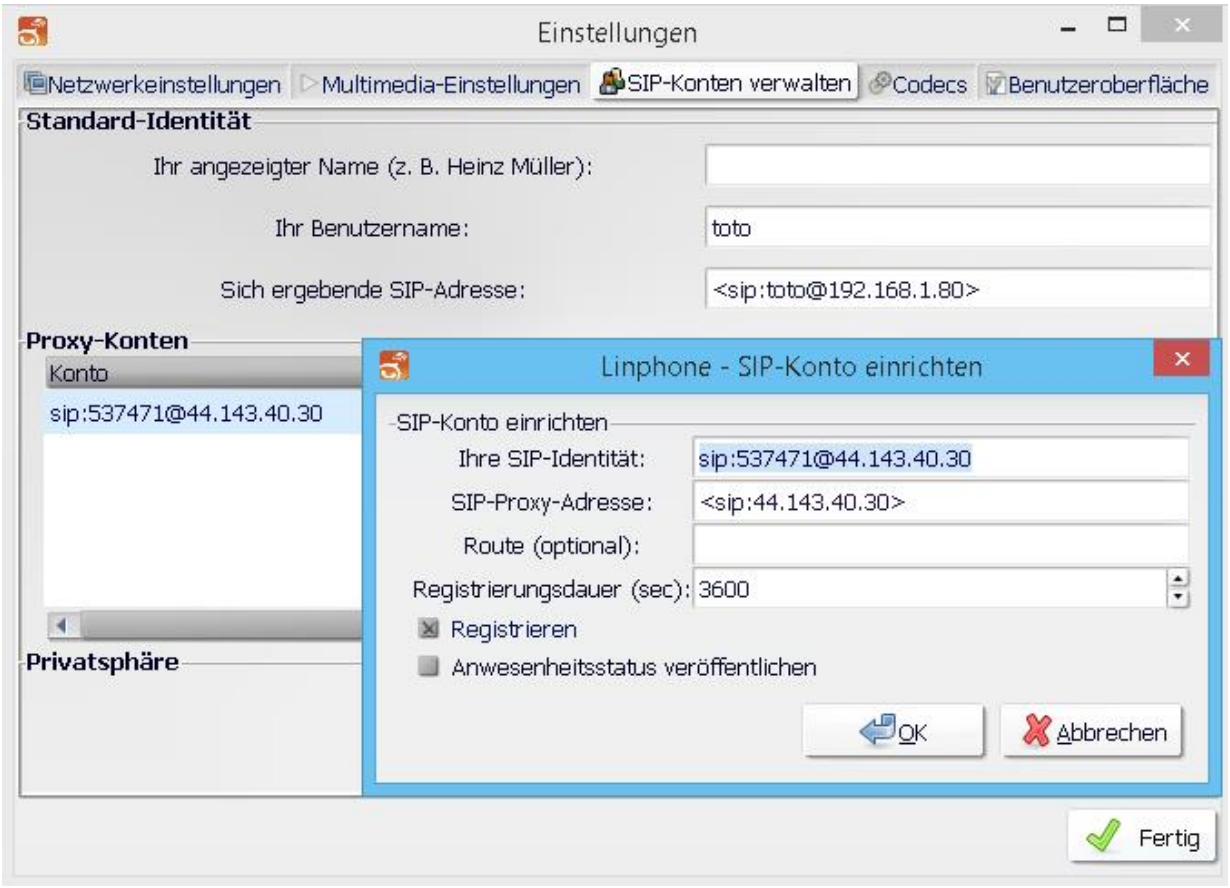
W przykładzie przygotowanym przez kolegów z OE nazwa konta 916123 jest przekodowaną częścią indywidualnego znaku wywoławczego OE2WAO, a adres serwera jest podany w polu „Registrar” – *voip.oe2xzr.ampr.org*. Występujące tutaj i w konfiguracjach niektórych urządzeń pole „Proxy” pozostaje puste.
Konfiguracja aparatu SNOM870 wygląda identycznie, należy jedynie pozostawić puste pole hasła dostępu.
Wiele telefonów SIP pozwala także na korzystanie z censtralnego spisu numerów (abonentów). Aparaty telefoniczne marki snom korzystają w tym celu z protokółu LDAP. Na węzłach sieci musi być uruchomiony serwer LDAP udostępniający spis.
Przykład konfiguracji dla aparatu snom360 przedstawiono na ilustracji 7.1.3. Dla innych typów telefonów konfiguracja wygląda podobnie.



Rys. 7.1.3. Przykład konfiguracji LDAP

W polu „Server Address” podawany jest hamnetowy adres serwera SIP jako adres IP lub w postaci symbolicznej jak na ilustracji. W polu „Base” jest on rozbity na części (przykładowo dla DB0SDA:
ou=sipusers,dc=db0sda,dc=ampr,dc=org).
Pól nazwy użytkownika („User Name”) i hasła dostępu („Password”) nie należy wypełniać. Pole hasła zostanie wypełnione automatycznie. Przyjęto następujace przyporządkowanie dla imienia i znaku wywoławczego:
givenName -> imię operatora,
sn -> givenName.

7.2. Konfiguracja klienta „Linphone”

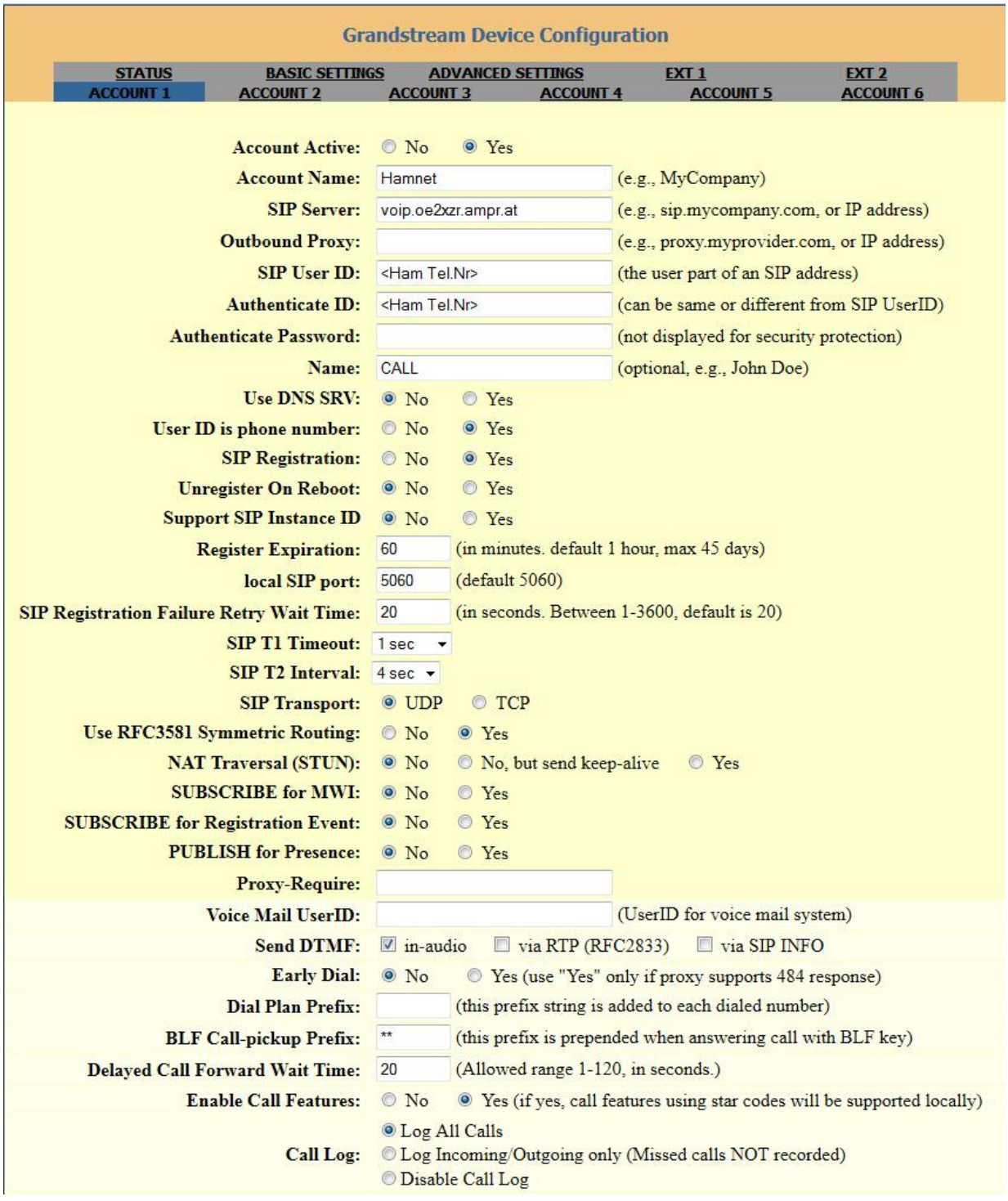


Rys. 7.2.1

W zakładce kodeków („Codecs”) należy sprawdzić czy włączone są kodeki (wokodery) GSM, PCMA (charakterystyka a) i PCMU (charakterystyka μ).

7.3. Konfiguracja telefonu „Grandstream 2020”

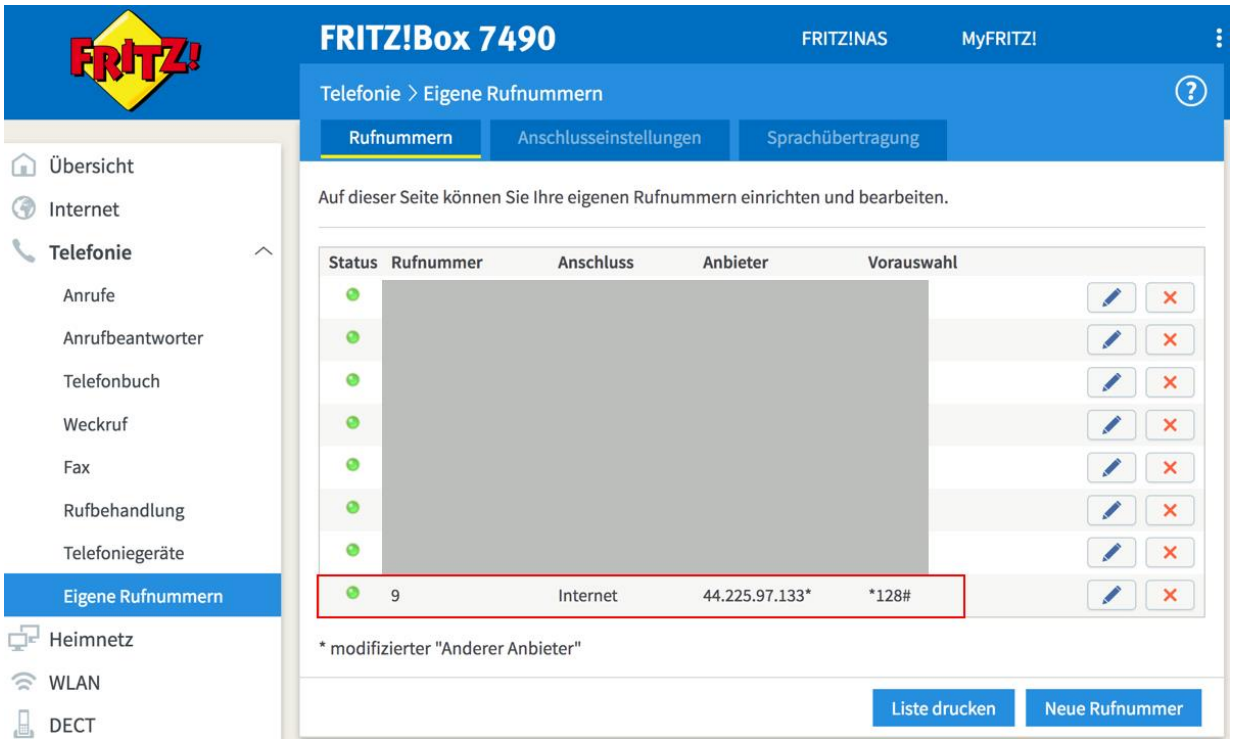
Konfiguracja aparatu dokonywana przez internetową powierzchnię obsługi powinien wyglądać jak w przykładzie z rysunku 7.3.1. Ważną sprawą jest włączenie we wszystkich ośmiu pozycjach u dołu okna kodeka GSM.
Pole „SIP Server” zawiera adres serwera i odpowiada polu „Registar” w poprzednich konfiguracjach. Pole „Outbound Proxy” pozostaje puste. W polach poniżej podawany jest hamnetowy nr telefonu.



Rys. 7.3.1. Okno konfiguracyjne

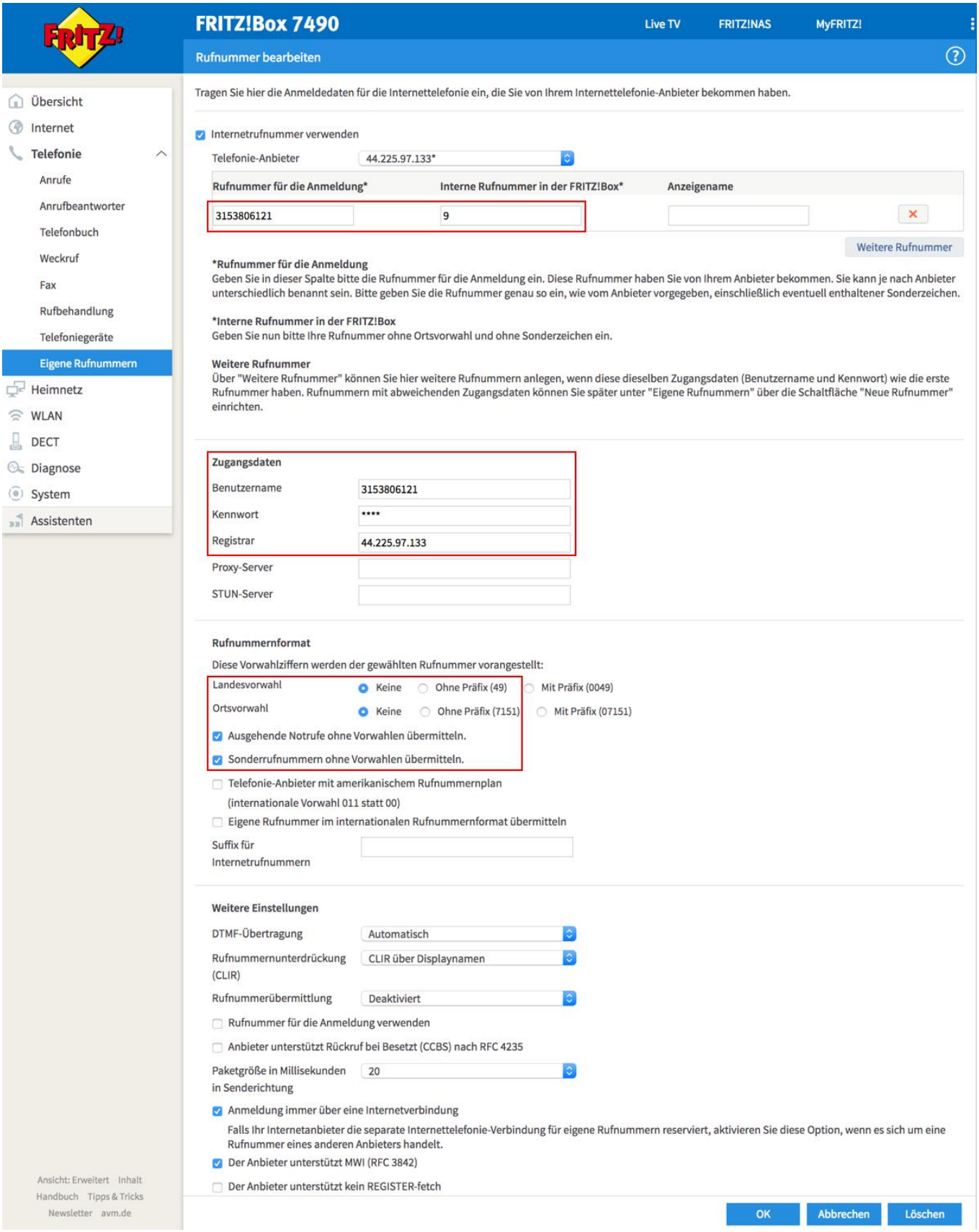
7.4. „FritzBox” 7490

Punkt dostępowy „FritzBox” pracujący jako lokalna asteriskowa centralka telefoniczna należy skonfigurować tak, aby łączność z adresami 44.xx.xx.xx była kierowana do sieci Hamnetu. Łącza do Hamnetu mogą przebiegać drogą radiową albo internetowo przez tunel VPN (z węzłami, które na to pozwalają). Konfiguracja z poniższego przykładu powinna funkcjonować i na innych modelach jeśli pozwalają one na korzystanie z transmisji głosu przez IP (VoIP). Zależnie od modelu konieczne może być umieszczenie oprogramowania serwera na dysku (paluszku lub twardym dysku) USB podłączonym do złącza USB. Do celów hamnetowych w zupełności wystarczą starsze modele „FritzBoxa” np. 7170, 7312 itd.
Następnie należy wpisać numer telefonu SIP jako dalszy własny numer telefoniczny (rys. 7.4.1). Dane dostępowe uzyskuje się od operatora węzła SIP w sieci Hamnetu. W ramach integracji z domową siecią mogą one być włączone do niej za głównym punktem dostępowym do Internetu i służyć tylko jako serwer SIP stanowiący domową centralkę telefoniczną dla większej liczby aparatów telefonicznych, analogowych, bezprzewodowych DECT i VoIP (w tym także telefonów programowych). Można także korzystać z serwera SIP połączonego tylko z Hamnetem.



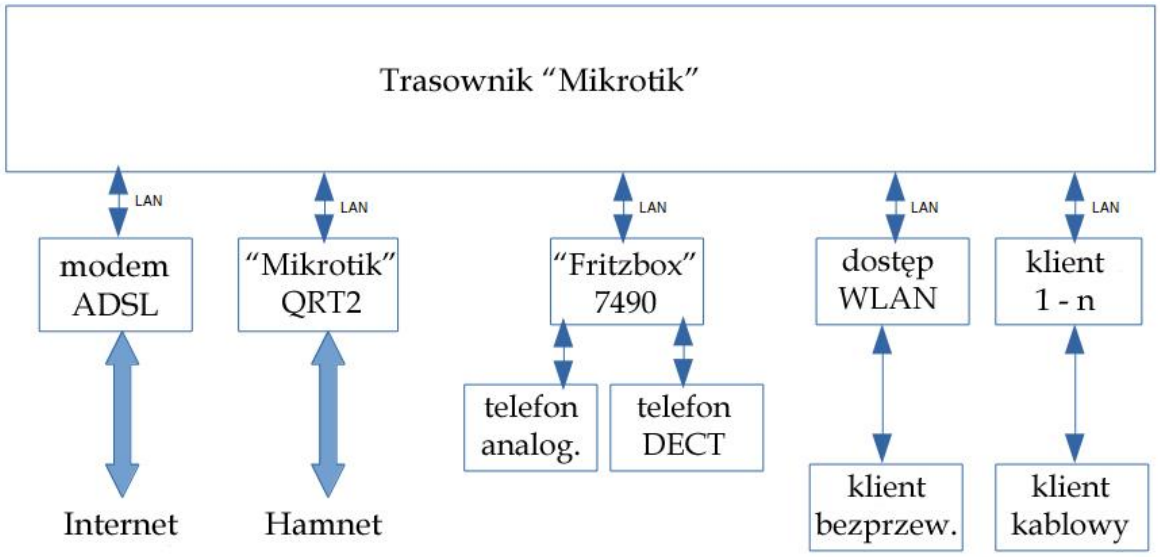
Rys. 7.4.1. Wpisanie numeru telefonu SIP

W górnym obwiedzionym na czerwono obszarze okna z rysunku 7.4.2 wpisywany jest numer abonenta w polu po lewej stronie otrzymany od internetowego dostawcy VoIP i wewnętrzny numer w domowej sieci. Dla telefonii w sieci Hamnetu istotne jest dodanie dalszych numerów.
W drugiej od góry ramce wprowadzany jest numer hamnetowy telefonu SIP zakodowany w podany powyżej sposób w oparciu o znak wywoławczy użytkownika. Poniżej podawane jest hasło dostępu i adres serwera VoIP w polu „Registrar” u dołu czerwonej ramki.
W trzeciej od góry czerwonej ramce ustalany jest format numeru. Pierwsze dwa pola od góry w podanym przykładzie ustalają podawanie numerów bez poprzedzającego je numeru kierunkowego krajowego i miejscowego. Dwa kolejne decydują o pomijaniu numeru kierunkego w numerach ratunkowych i specjalnych.
Przy podanych ustawienia wszystkie telefony z sieci Hamnetu są sygnalizowane wszystkim urządzeniom podłączonym do „FritzBoxu” i kierowane do nich.


FRITZ!Box 7490
Live TV
FRITZ!NAS
MyFRITZ!
Rufnummer bearbeiten
Übersicht
Internet
Telefonie
Anrufe
Anrufbeantworter
Telefonbuch
Weckruf
Fax
Rufbehandlung
Telefoniegeräte
Eigene Rufnummern
Heimnetz
WLAN
DECT
Diagnose
System
Assistenten
Tragen Sie hier die Anmeldedaten für die Internettelefonie ein, die Sie von Ihrem Internettelefonie-Anbieter bekommen haben.
Internetrufnummer verwenden
Telefonie-Anbieter
44.225.97.133*
Rufnummer für die Anmeldung*
Interne Rufnummer in der FRITZ!Box*
Anzeigename
3153806121
9
Weitere Rufnummer
*Rufnummer für die Anmeldung
Geben Sie in dieser Spalte bitte die Rufnummer für die Anmeldung ein. Diese Rufnummer haben Sie von Ihrem Anbieter bekommen. Sie kann je nach Anbieter unterschiedlich benannt sein. Bitte geben Sie die Rufnummer genau so ein, wie vom Anbieter vorgegeben, einschließlich eventuell enthaltener Sonderzeichen.
*Interne Rufnummer in der FRITZ!Box
Geben Sie nun bitte Ihre Rufnummer ohne Ortsvorwahl und ohne Sonderzeichen ein.
Weitere Rufnummer
Über "Weitere Rufnummer" können Sie hier weitere Rufnummern anlegen, wenn diese dieselben Zugangsdaten (Benutzername und Kennwort) wie die erste Rufnummer haben. Rufnummern mit abweichenden Zugangsdaten können Sie später unter "Eigene Rufnummern" über die Schaltfläche "Neue Rufnummer" einrichten.
Zugangsdaten
Benutzername
3153806121
Kennwort
****
Registrar
44.225.97.133
Proxy-Server
STUN-Server
Rufnummernformat
Diese Vorwahlziffern werden der gewählten Rufnummer vorangestellt:
Landesvorwahl
Keine
Ohne Präfix (49)
Mit Präfix (0049)
Ortsvorwahl
Keine
Ohne Präfix (7151)
Mit Präfix (07151)
Ausgehende Notrufe ohne Vorwahlen übermitteln.
Sonderrufnummern ohne Vorwahlen übermitteln.
Telefonie-Anbieter mit amerikanischem Rufnummernplan
(internationale Vorwahl 011 statt 00)
Eigene Rufnummer im internationalen Rufnummernformat übermitteln
Suffix für Internetrufnummern
Weitere Einstellungen
DTMF-Übertragung
Automatisch
Rufnummernunterdrückung (CLIR)
CLIR über Displaynamen
Rufnummerübermittlung
Deaktiviert
Rufnummer für die Anmeldung verwenden
Anbieter unterstützt Rückruf bei Besetzt (CCBS) nach RFC 4235
Paketgröße in Millisekunden in Senderichtung
20
Anmeldung immer über eine Internetverbindung
Falls Ihr Internetanbieter die separate Internettelefonie-Verbindung für eigene Rufnummern reserviert, aktivieren Sie diese Option, wenn es sich um eine Rufnummer eines anderen Anbieters handelt.
Der Anbieter unterstützt MWI (RFC 3842)
Der Anbieter unterstützt kein REGISTER-fetch
Ansicht: Erweitert Inhalt
Handbuch Tipps & Tricks
Newsletter avm.de
OK
Abbrechen
Löschen

Rys. 7.4.2

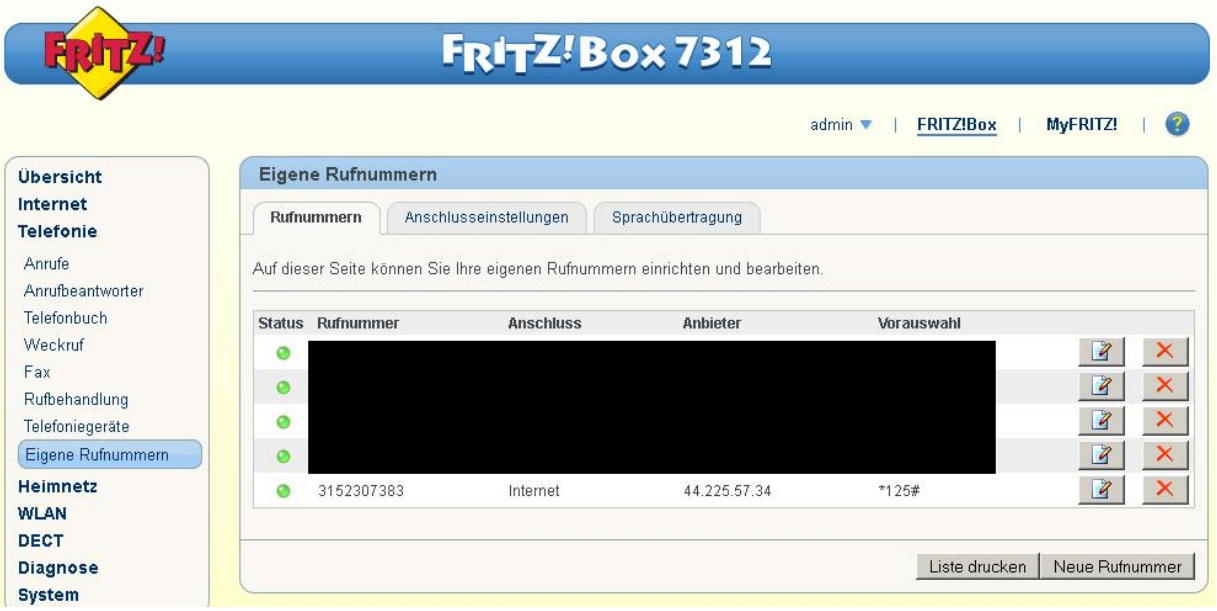
Wywołania wychodzące są przy podanych ustawieniach poprzedzone prefiksem *128#. Rozmowy telefoniczne w Hamnecie możliwe są jedynie między licencjonowanymi nadawcami. Rozmowa przebiega identycznie jak zwykła rozmowa telefoniczna.



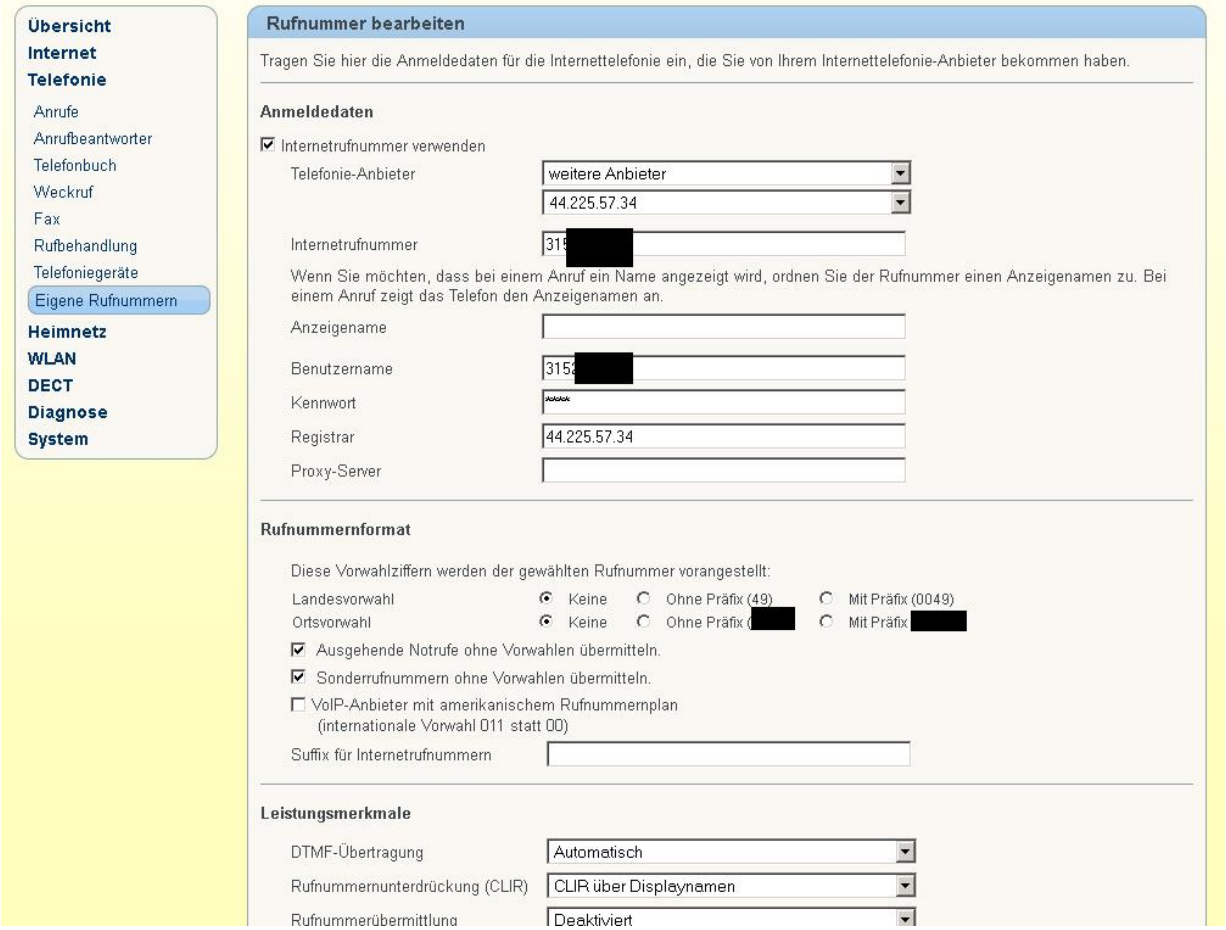
Rys. 7.4.3. Przykład domowej sieci z dostępem do Internetu i Hamnetu i centralką telefoniczną na „FritzBoxie"

W konfiguracji sieci z rysunku 7.4.3 przewidziany jest dostęp zarówno do Hamnetu jak i do Internetu, pokazano również sposób podłączenia telefonów cyfrowych i analogowych, a także klientów komputerowych i telefonicznych kablowo albo bezprzewodowo przez WLAN. „FritzBox" 7490 służy jako bramka VoIP.
– W modemie ADSL trasownik (ang. *router*) Mikrotik jest zadeklarowany jako DMZ (z ang. „strefa zdemilitaryzowana") – podsieć zwierająca usługi dostępne z zewnątrz (np. serwer poczty elektronicznej, FTP, serwer HTTP, serwer DNS itd.). Chroni ona pozostałą część sieci lokalnej przed zagrożeniami z zewnątrz.
– W trasowniku „Mikrotik" jako domyślna trasa podany jest adres IP modemu ADSL.
– W trasowniku „Mikrotik" jako statyczna trasa dostępu do Hamnetu (44.0.0.0/8) podany jest adres IP QRT2.
– Własny punkt dostępowy jest połączony kablowo z „Mikrotikiem",
– Standardowo adresem IP „Fritzboxa" jest 192.168.178.1. Dla uniknięcia konfliktów adresy PC w sieci muszą więc leżeć w zakresie 192.168.171.2 – 253. Maską sieci jest 255.255.255.0. Można także korzystać z serwera DHCP „Fritzboxa".
Każdy z klientów w sieci LAN ma w ten sposób dostęp zarówno do Internetu jak i do Hamnetu. Zapora przeciwwłamaniowa (ang. *firewall*) musi dopuszczać dostęp do sieci 44 tylko dla wybranych klientów. W konfiguracji sieci z rys. 7.4.3 konieczne jest przełączenie „Fritzboxa" w tryb klienta IP (patrz instrukcja obsługi).
W prostszych konfiguracjach „FritzBox" może zapewniać także dostęp do Internetu przez ADSL bez pomocy dalszych urządzeń. Możliwe jest także wykorzystanie „FritzBoxa" tylko w sieci połączonej z Hamnetem. W tych przypadkach nie trzeba przełączać go w tryb klienta IP.

7.5. „FritzBox” 7312



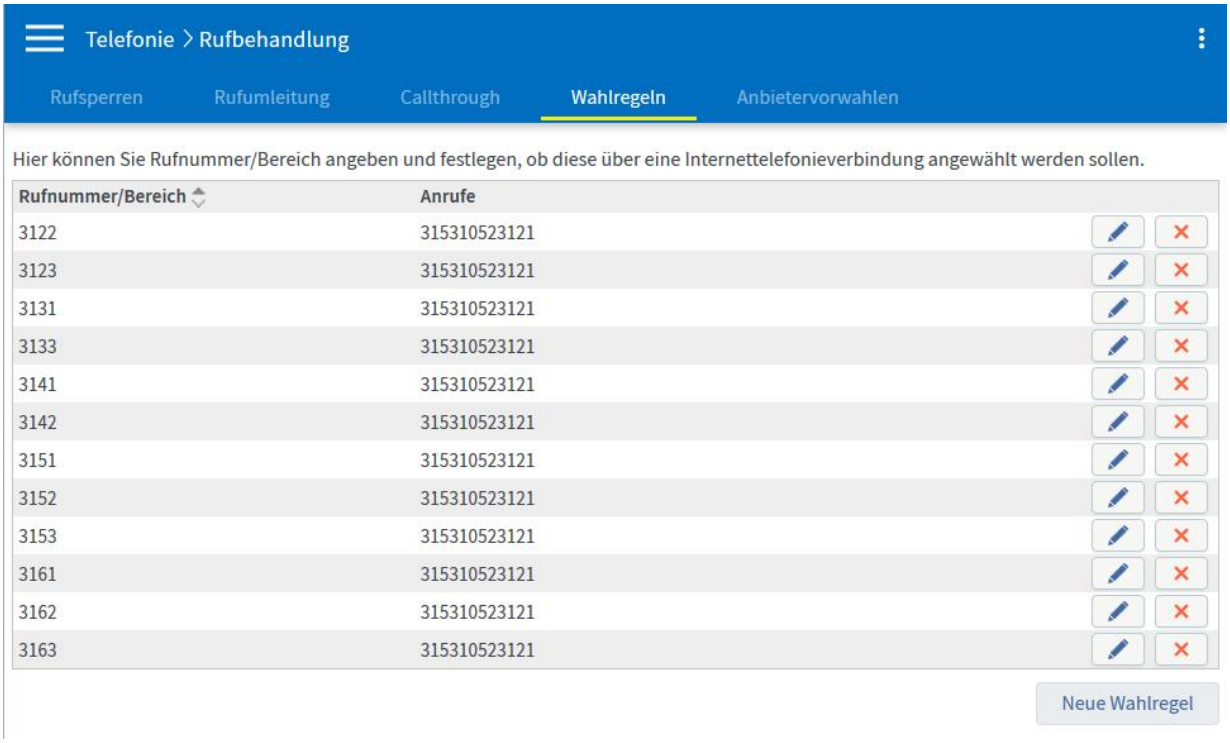
Rys. 7.5.1



Rys. 7.5.2

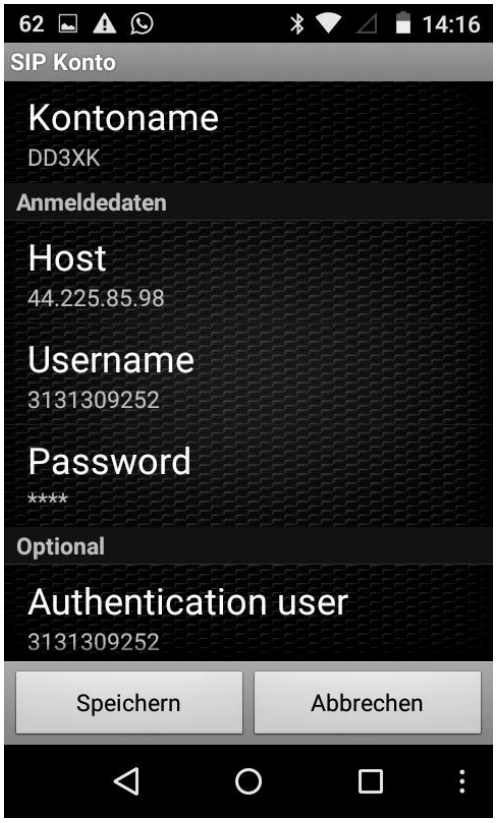
Konfiguracja centralki telefonicznej jest podobna do podanej w poprzednim punkcie dla modelu 7490. Numery w tym przykładzie są poprzedzone prefiksem *125#.

„FritzBox” pozwala także na ustalenie zasad kierowania rozmów: do Internetu lub do Hamnetu w zależności od numeru wywoływanego abonenta (rys. 7.5.3).

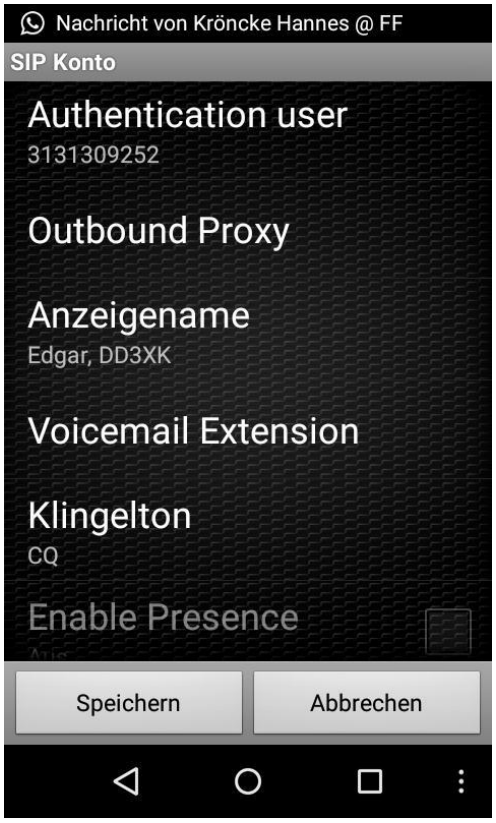


Rys. 7.5.3. Okno „Telefonia”|„Rozmowy”|„Zasady wybierania numeru”

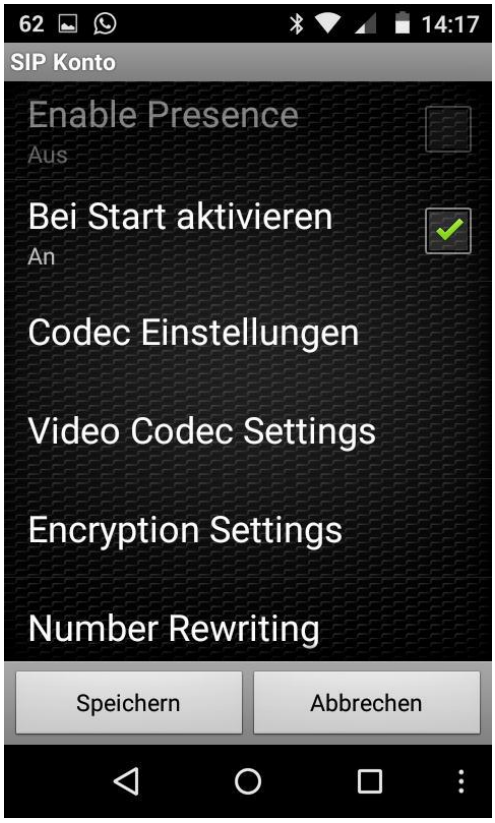
7.6. Konfiguracja „Zoipera”



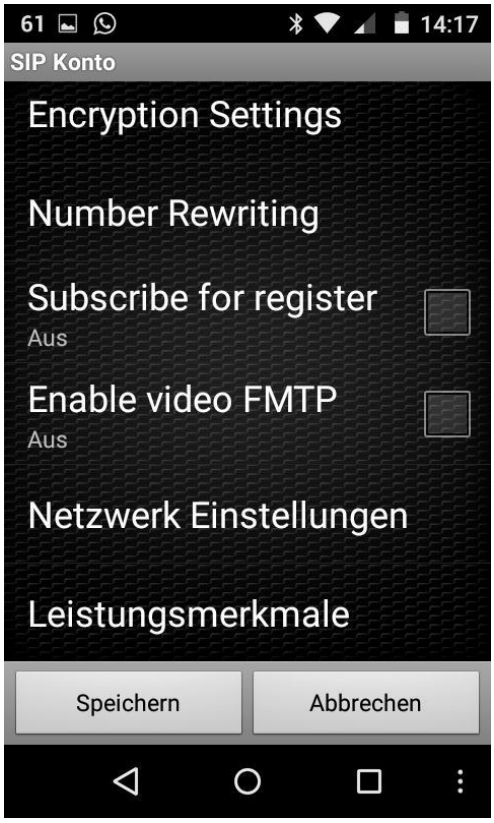
Rys. 7.6.1



Rys. 7.6.2



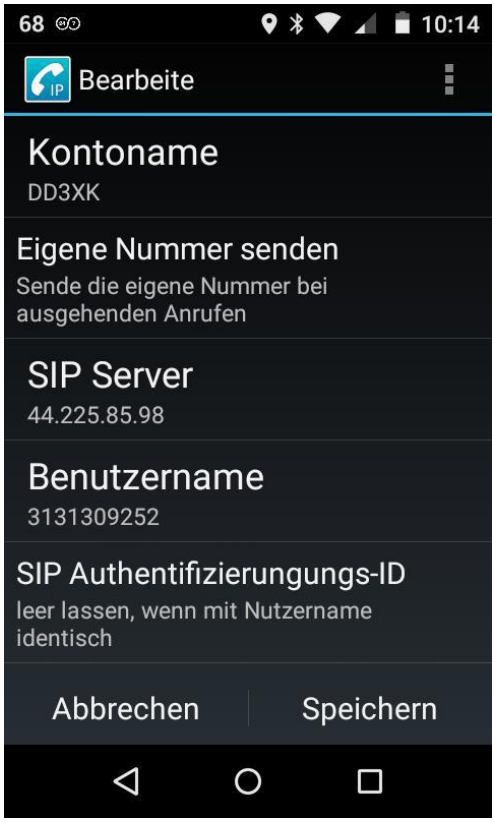
Rys. 7.6.3

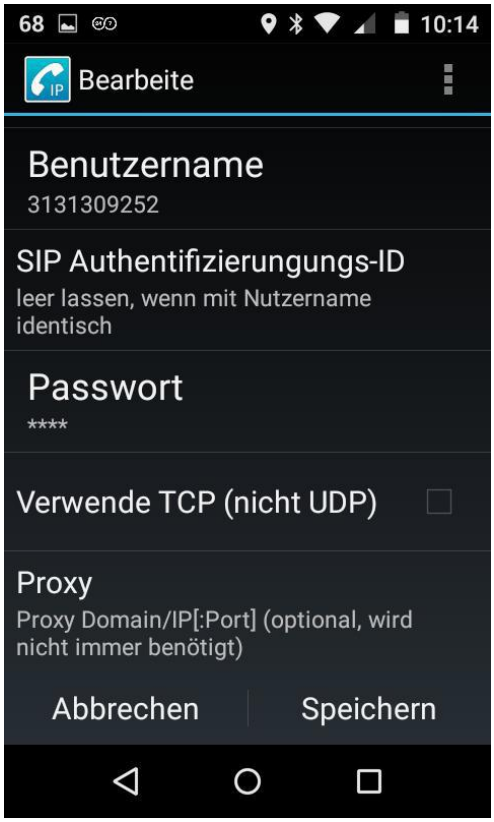


Rys. 7.6.4

W polu nazwy konta „Kontoname” na rys. 7.6.1 podawany jest znak wywoławczy stacji, a w polach nazwy użytkownika „Username” i uwierzytelnienie „Authentification user” na rysunkach 7.6.1 i 7.6.2 podawany jest numer telefonu obliczony na podstawie znaku wywoławczego w sposób wyjaśniony wcześniej. Hasło dostępu otrzymuje się od operatora przemiennika. Pozycja automatycznego startu („Beim start aktivieren”) może być zaznaczona, ale nie jest to konieczne. Wybrane ustawienia należy zapisać naciskając prawy przycisk ekranowy (na ilustracjach „Speichern”).

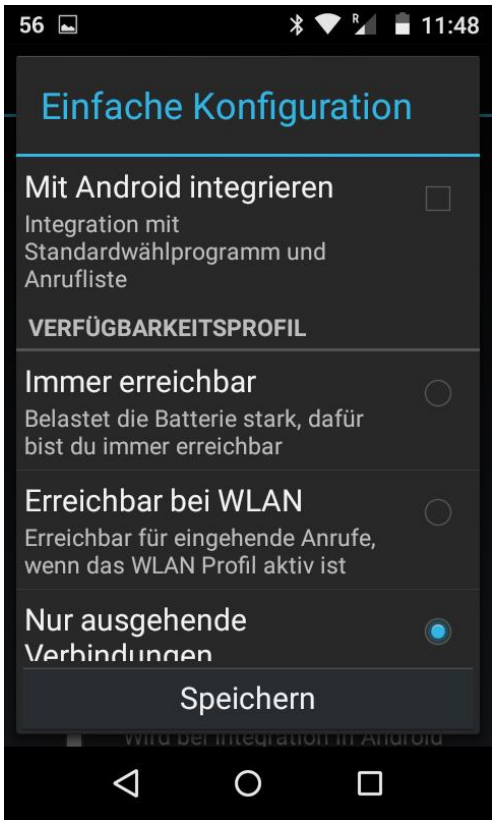
7.7. Konfiguracja „CSipSimple”



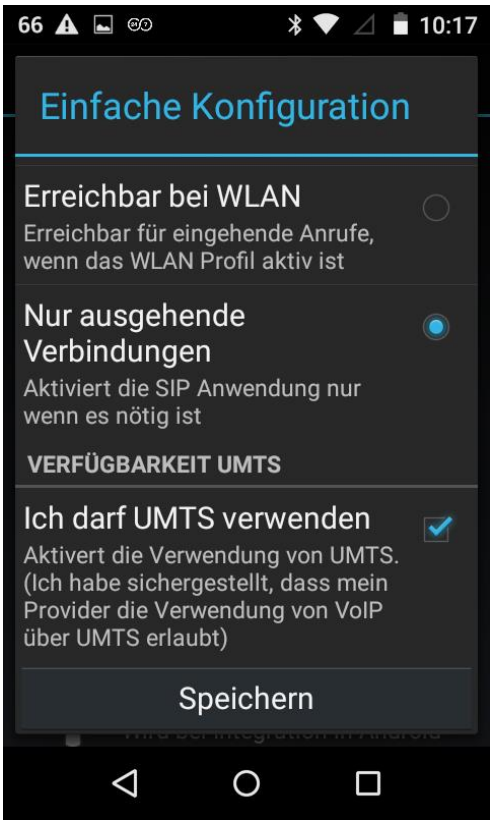


Rys. 7.7.1 Rys. 7.7.2

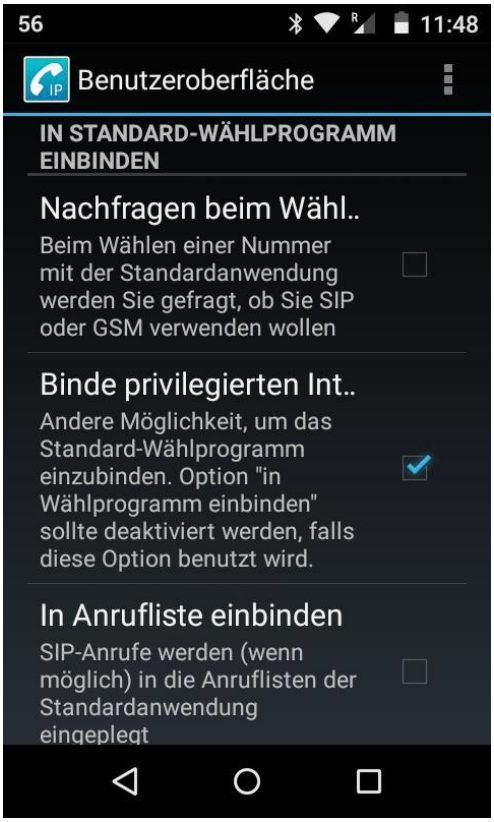
W polu nazwy konta „Kontoname” z rys. 7.7.1 wpisywany jest znak wywoławczy, a w polu nazwy użytkownika „Benutzername” na rysunkach 7.7.1 i 7.7.2 – numer telefonu obliczony na podstawie znaku. Hasło dostępu otrzymuje się od operatora przemiennika. Pole uwierzytelnienia „SIP Authentifizierungs-ID” pozostaje puste, jeżeli jest identyczne z nazwą użytkownika. Pole serwera buforowego „Proxy” z rys.7.7.2 też przeważnie może pozostać puste.
Pola integracji z Androidem (u góry na rys. 7.7.3) nie powinno być zaznaczone, ponieważ mogą wystąpić problemy przy korzystaniu ze standardowej funkcji telefonu.
W podanym przykładzie telefonia SIP jest aktywowania tylko dla rozmów wychodzących („Nur ausgehende Verbindungen” na rys. 7.7.3 i 7.7.4). Pole korzystania z UMTS przydaje się natomiast poza domem. Można także korzystać z dostępu przez WLAN. Ciągła osiągalność – pole „Immer erreichbar” na rys. 7.7.3 – oznacza duże obciążenie akumulatora.
Zapytania o to czy korzystać z SIP (pole „Nachfragen beim Wählen”) niepotrzebnie utrudnią wybieranie numerów z kontaktów dla sieci telefonicznej – pole powinno pozostać nie zaznaczone.



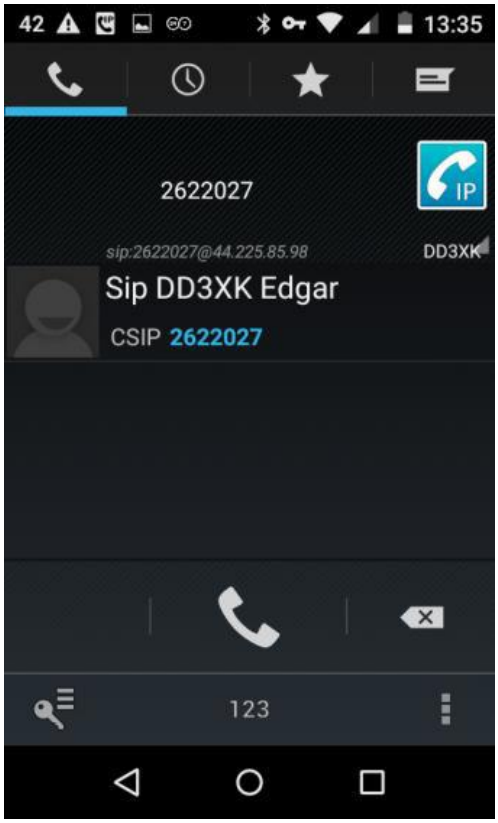
Rys. 7.7.3



Rys. 7.7.4

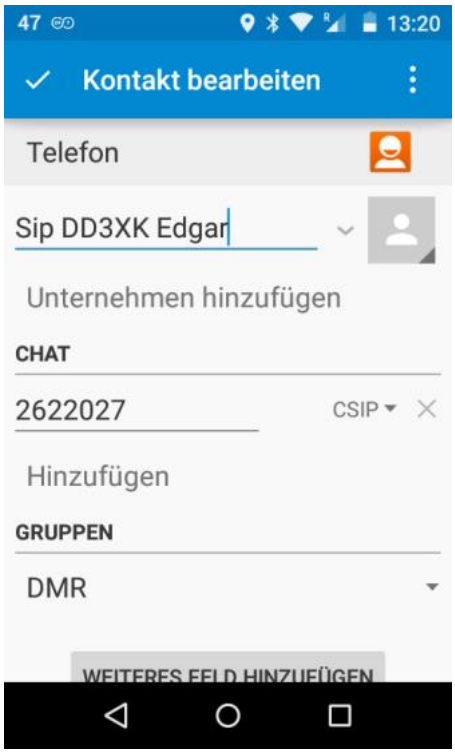


Rys. 7.7.5



Rys. 7.7.6

Przebieg rozmów telefonicznych SIP:
– po wybraniu kontaktu SIP ze spisu kontaktów automatycznie wywoływany jest program *CSipSimple*,
– numer abonenta jest wyświetlany na ekranie,
– po naciśnięciu symbolu słuchawki (w dolnej części ekranu na rys. 7.7.6) rozpoczyna się wybieranie numeru, w przypadku zaznaczenia pola „Mit Android integrieren” w konfiguracji po wybraniu kontektu z publicznej sieci telefonicznej następuje, niepotrzebnie, zapytanie czy korzystać z SIP czy telefonii komórkowej.



Rys. 7.7.7. Kontakt dla SIP – przykład

Przy zakładaniu nowego kontaktu, jak w przykładzie z rys. 7.7.7 trzeba wybrać typ CHAT albo IM, a dla lepszej orientacji dobrze jest podać w nazwie skrót SIP. W polu poniżej napisu CHAT podawany jest numer abonenta. W nazwie etykiety po prawej stronie numeru trzeba podać CSIP.
Przykładowo numerem grupy TG9 jest na przemienniku DMR-owym DB0FS – 262220, grupy regionu – 2622, a prywatny numer abonenta DD3XK wynosi 2622027.

7.8. Usługa „Hamshack Hotline”

„Hamshack Hotline” (HH) – *www.hamshackhotline.com* – jest bezpłatną usługą telefoniczną dla krótkofalowców korzystająca z tego samego wyposażenia co telefonia SIP w Hamnecie. Połączenia odbywają się jednak przez Internet i jedynie inna możliwość wykorzystania tego wyposażenia spowodował dodanie do skryptu tego punktu. „Hamshack Hotline” jest wykorzystywana przez indywidualnych krótkofalowców, kluby i organizacje krótkofalarskie na świecie. Sieć HH jest pozielona na trzy części HHUS (dla Ameryki Północnej), HHEU (dla Europy), HHAP (dla Azji i Oceanii) i sieć eksperymentalną HHX.
Jest ona pomyślana jako uzupełnienie sieci łączności radiowych, a nie jako jej zastępstwo (zwłaszcza w przypadku łączności kryzysowych). Oprócz rozmów telefonicznych, także konferencyjnych, i skrzynki głosowej możliwe jest korzystanie z faksymile, pod warunkiem posiadania potrzebnego wyposażenia.

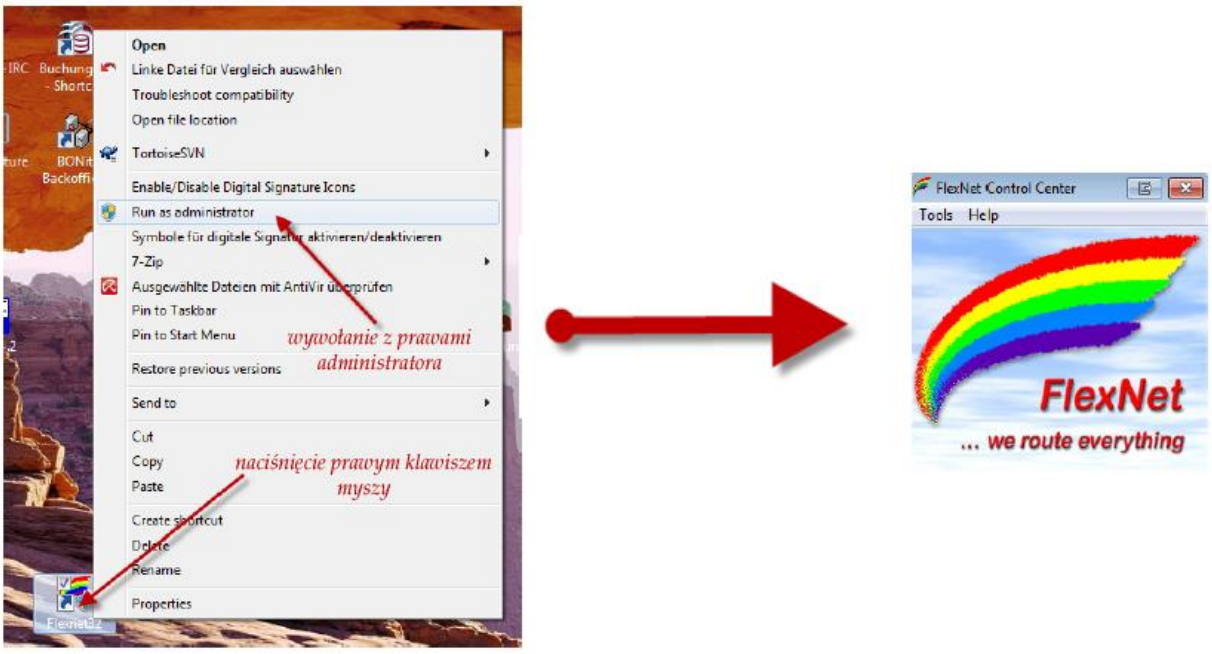
„Hamshack Hotline” może być przykładowo wykorzystywana jako dodatkowy kanał w przypadku prób i napraw wyposażenia albo w niekorzystnych warunkach propagacji.
Abonenci korzystają z telefonów SIP firm *Cisco*, *Fanvil*, telefonów programowych *Zoiper* itd., oprogramowania *Asterisk* (*FreePBX*) itd. identycznie jak w Hamnecie. Jednym z alternatywnych rozwiązań dla telefonów komórkowych może być zainstalowanie oprogramowania 3CX na „Malinie” i telefonu programowego 3CX na telefonie.
Przed rozpoczęcierm pracy w sieci konieczne jest założenie własnego konta – analogicznie jak na serwerze Hamnetu – w witrynie podanej na początku.

8. Łączności Packet-Radio

Przez długi czas sieć packet-radio składała się z węzłów, pomocniczych stacji przekaźnikowych i skrzynek elektronicznych dostępnych dla użytkowników w pasmach 2 m – 23 cm przeważnie z szybkościami transmisji 1200 – 9600 bit/s. Łącza między stacjami sieci AX.25 pracowały często też z niewiele większymi szybkościami transmisji od 19200 do (w najlepszych przypadkach) 76800 bit/s. Sieć wystarczała zasadniczo do prowadzenia łączności pisanych (dialogów), wymiany poczty elektronicznej, plików i ilustracji o niezbyt dużej objętości. W miarę rozpowszechniania się Internetu i przyzwyczajania się użytkowników do typowych tam szybkości transmisji sieć packet-radio zaczęła wydawać się coraz mniej interesująca i powoli w wielu krajach zaczęła podupadać. Tam gdzie istnieje jeszcze dobrze funkcjonująca infrastruktura coraz trudniej niestety znaleźć korespondenta. Wywołanie w sieci packet-radio coraz bardziej przypomina wołanie na puszczy nawet jeżeli bramka wyjściowa znajduje się w tak dużym mieście jak Kraków. Rozbudowa sieci „Hamnetu" może, dzięki znacznie większym szybkościom transmisji, stać się drugą szansą dla systemu packet-radio, szansą na którą sobie w pełni zasługuje. Zastosowane w protokóle AX.25 mechanizmy korekcji przekłamań umożliwiają praktycznie prawie bezbłędną transmisję danych pisanych i obrazów, wyposażenie jest niekosztowne i może być używane także w łącznościach ratunkowych i kryzysowych. Rozbudowując sieć "Hamnetu" warto o tym pamiętać. Niektóre z węzłów austriackich oferują dostęp do sieci packet-radio przez Hamnet za pomocą „Flexnetu" i „Paxona". Wykorzystywany jest protokół AXUDP transportujący pakiety AX.25 w datagramach UDP i dalej w pakietach IP.
Na potrzeby APRS zostało opracowane oprogramowanie serwera APRS4R dla OpenWRT.

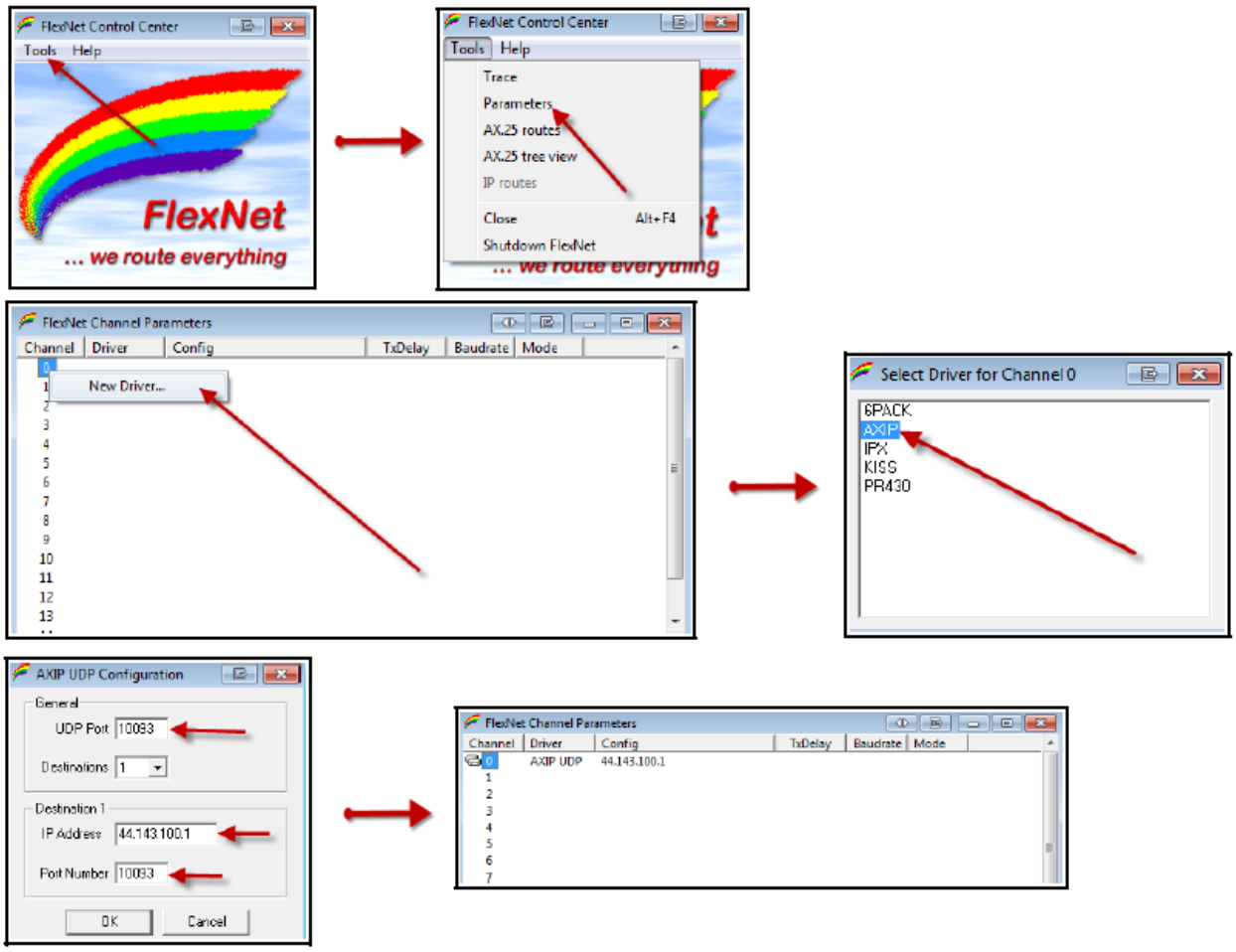
8.1. Dostęp przez „Flexnet" i „Paxona"

System „Packet Radio" i używane w łącznościach programy, w tym „Flexnet" i „Paxon" omówiono szczegółowo w tomie 7 niniejszej serii dlatego też w bieżącym rozdziale zostanie poruszona jedynie konfiguracja „Flexnetu" i „Paxona" do łączności „Packet-Radio" w sieci „Hamnetu" z pominięciem wszystkich pozostałych aspektów, w tym ich instalacji i podstawowej konfiguracji.
Podany poniżej przykład konfiguracji dotyczy wprawdzie węzła OE5XBL [3] ale bez trudu daje się dostosować do dostępu przez inne węzły hamnetowe „Packet-Radio" (patrz też [7]). Dostęp do sieci Packet-Radio przez Hamnet umożliwia prowadzenie łączności z szybkościami typowymi dla niej i znacznie przekraczającymi dotychczasowe typowe szybkości dostępu 1200 lub 9600 bit/s.



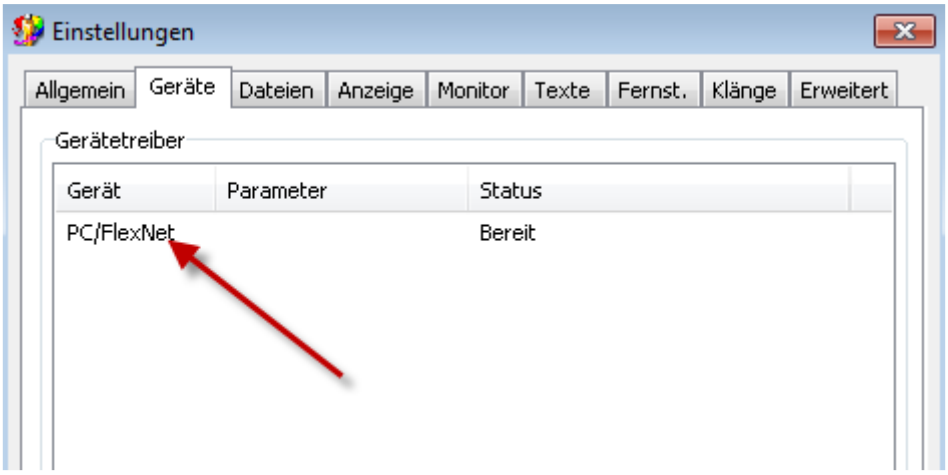
Rys. 8.1.1. Uruchomienie „Flexnetu"

Przed skonfigurowaniem dostępu przez „Hamnet” należy najpierw wywołać „Flexnet”, który służy praktycznie jako uniwersalny sterownik warstwy 2.
Po uruchomieniu „Flexnetu” należy skonfigurować (wybrać lub dodać) jako nowy sterownik AXIP i przypisać do niego kanał logiczny UDP, w tym przykładzie o numerze 10093. Numer kanału i widoczny w okienku po lewej stronie u dołu rysunku 8.1.2 adres z serii 44 dotyczą konkretnego przemiennika dostępowego „Hamnetu” i dla każdego z nich będą różne (oczywiście przynajmniej adres IP, kanał logiczny UDP może mieć taki sam lub inny numer). W dostępie przez OE2XZR jest to przykładowo kanał 93 lub 10094 a przez DB0RES – kanał 8093. Oczywiście w lokalnej sytuacji może on się różnić od podanych przykładów.
Węzły packet-radio pracują najczęściej pod oprogramowaniem X-NET i dla dostępu do packet-radio przez „Hamnet” korzystają z własnego rozszerzenia j.np. OE2XZR-15. W skrzynkach elektronicznych stosowane jest bardzo często oprogramowanie „Open Baycom”.
Przed rozpoczęciem konfiguracji i prób połączeń należy się oczywiście poinformować o tych parametrach. Oczywistym jest też, że nie każdy z przemienników dostępowych do „Hamnetu” umożliwia także dostęp do sieci „Packet-Radio”.



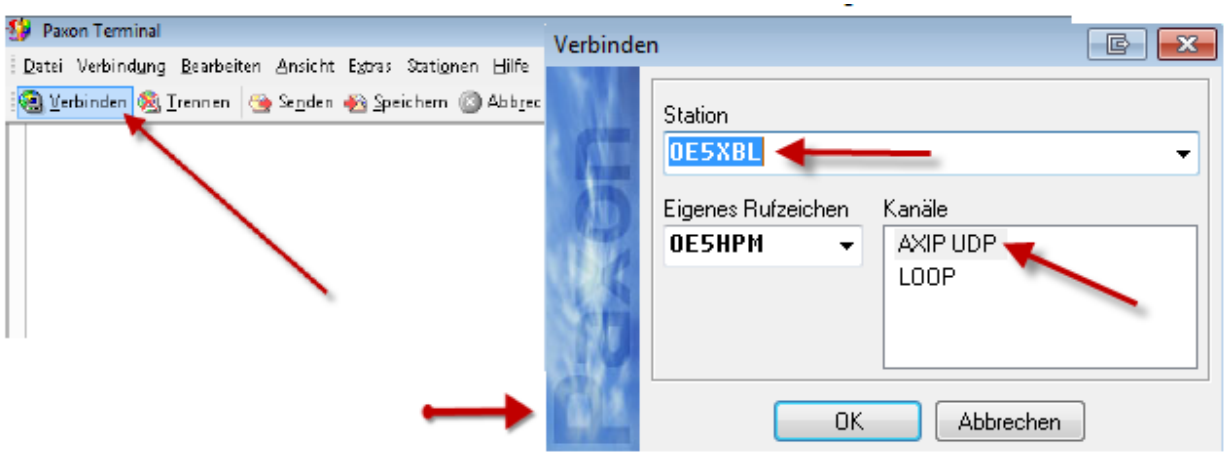
Rys. 8.1.2. Konfiguracja „Flexnetu” jako sterownik AXIP

Przeprowadzona w ten sposób konfiguracja „Flexnetu” jest automatycznie zapisywana na dysku i pozostaje aktywna także po każdym następnym wywołaniu „Flexnetu”.
Następnym krokiem jest konfiguracja „Paxonu” (zakładając, że został on już zainstalowany i uruchomiony w sposób opisany w tomie 7).
Po wywołaniu „Paxonu” należy w zakładce „Urządzenia” („Geräte”) sprawdzić, czy jest w niej widoczny „Flexnet” (rys. 8.1.3).



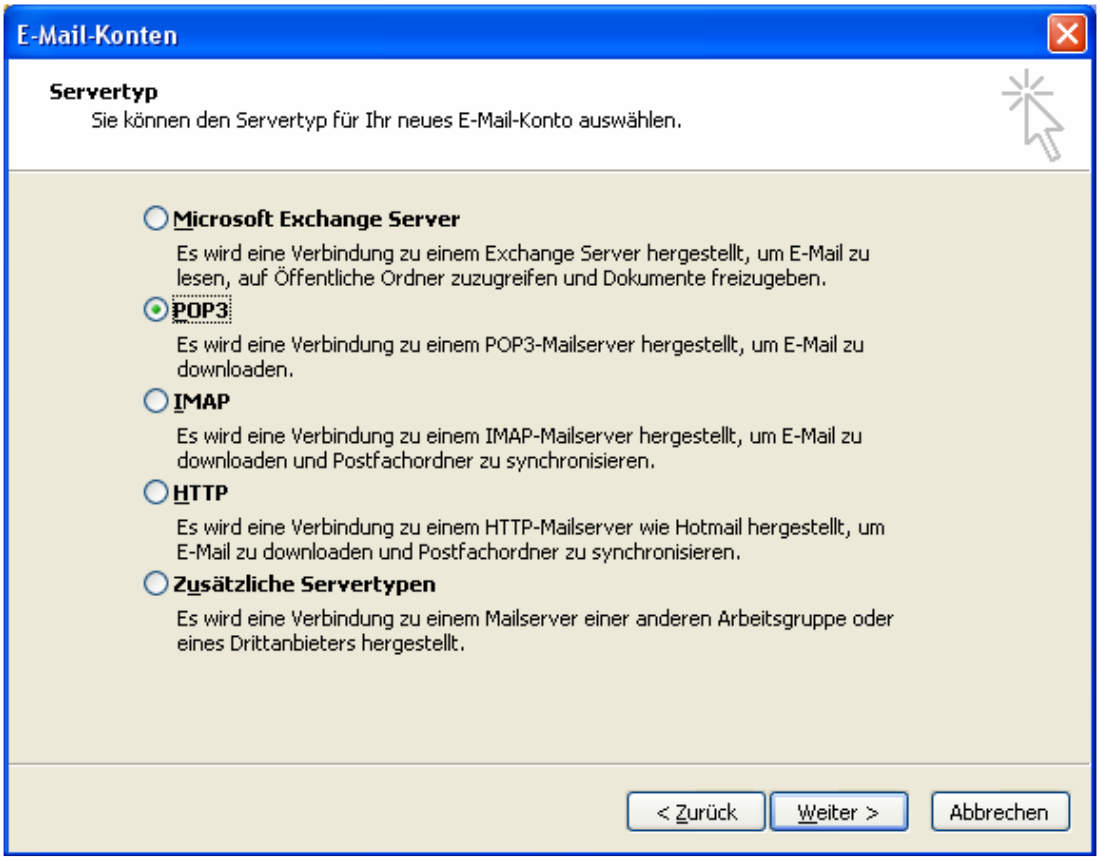
Rys. 8.1.3. Zakładka urządzeń

Jeśli wszystko jest w porządku można przystąpić do nawiązania połączenia przy wykorzystaniu protokółu AXIP przez UDP. Przykład dla połączenia z OE5XBL przedstawia rys. 8.1.4. W zależności od wyposażenia węzła packet-radio możliwe jest korzystanie z elektronicznej skrzynki pocztowej (ang. *mailbox*, *BBS*) nawiązywanie połączeń z dalszymi węzłami itd.



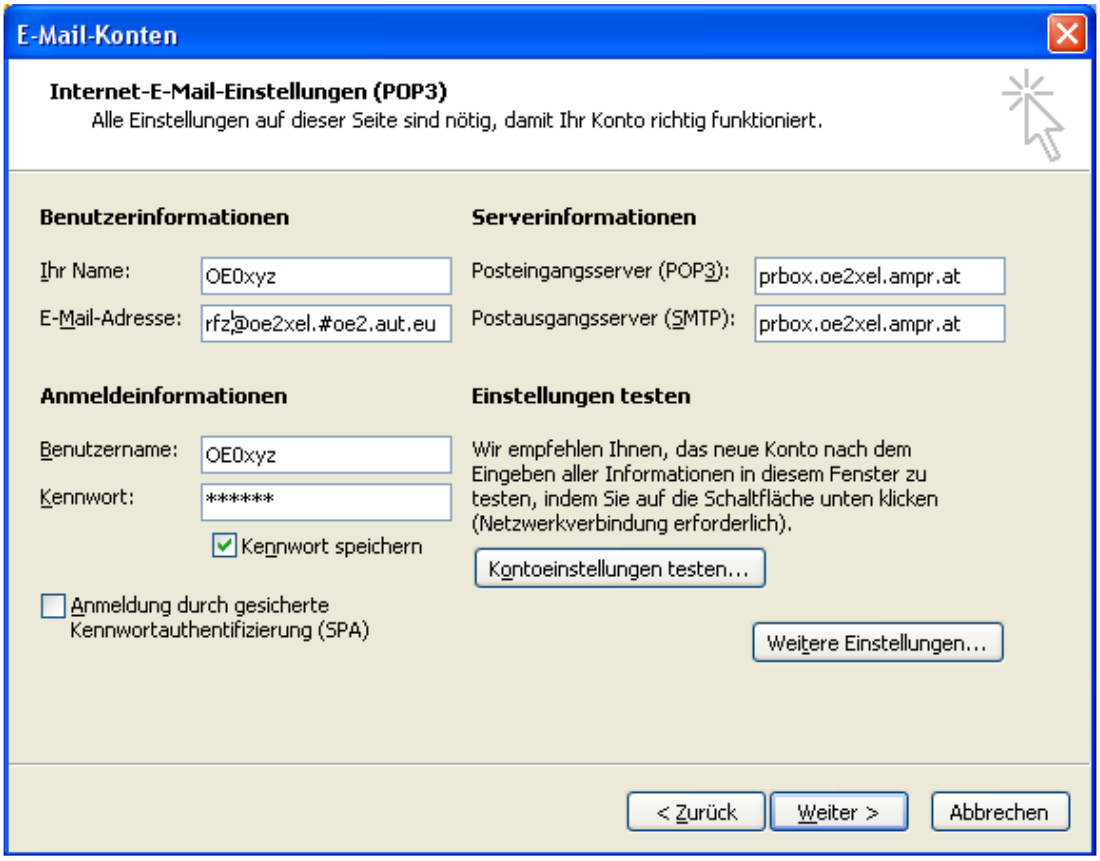
Rys. 8.1.4. Połączenie packet-radio przez AXIP UDP

8.2. Dostęp do skrzynek elektronicznych przez „Outlook”

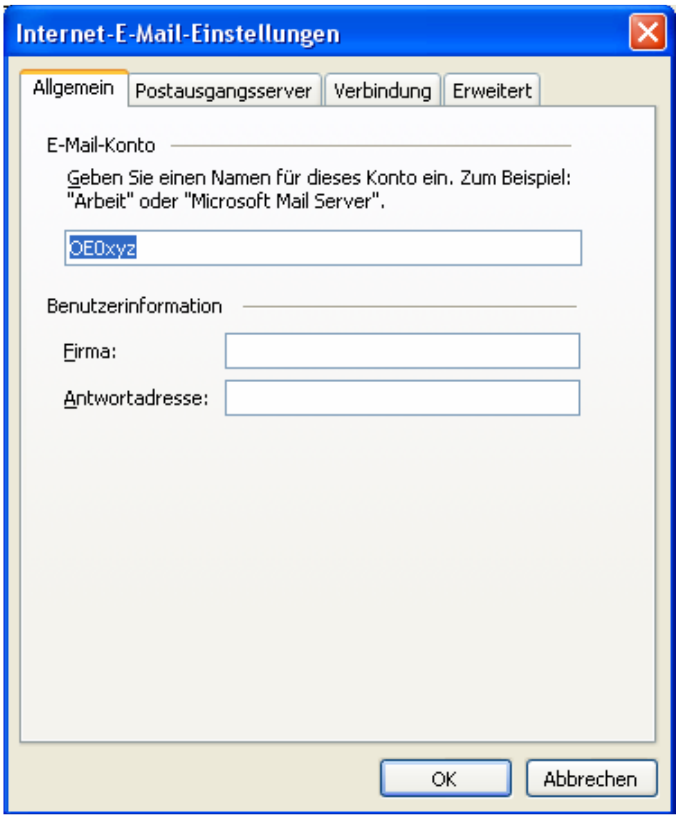


Rys. 8.2.1. Zakładanie konta pocztowego w „Outlooku”

Niektóre ze skrzynek elektronicznych packet-radio pozwalają także na wymianę poczty za pomocą rozpowszechnionych programów pocztowych takich jak „MS Outlook”. Wymaga to otrzymania od operatora skrzynki hasła dostępu TTY. Sposób korzystania ze skrzynki packet-radio przez „MS Outlook” przedstawimy na przykładzie skrzynki OE2XZR [6].
W tym przypadku konieczne jest wejście na dostępną w „Hamnecie” stronę *http://prbox.oe2xel.ampr.at:8080* (rys. 8.2.5) i wysłanie stamtąd wiadomości do operatora skrzynki. Jest to oczywiście jadna z możliwości – w innych instalacjach sprawa może wyglądać zupełnie inaczej.
Hasło to moża w wielu skrzynkac ustawić także samodzielnie łącząc się z nimi przez packet-radio i posługując poleceniem „A TTYPW xxxxx”, gdzie w miejscu ciągu xxxx podawane jest rzeczywiste hasło.
Po uruchomieniu „Outlooka” należy poprzez menu wywołać okno służące do dodania nowego konta pocztowego i wybrać w nim typ POP3 jak to pokazano na ilustracji 8.2.1.
W następnym oknie (rys. 8.2.2) należy podać w polu nazwiska własny znak wywoławczy, a w polu poniżej adres poczty elektronicznej w sieci packet-radio (podobnie jak w przykładach poniżej:
OE0xyz i **<znak>@oe2xel.#oe2.aut.eu**
A następnie nazwę (lub nazwy) serwera pośredniczącego w wymianie poczty w obu kierunkach, w tym przykładzie **prbox.oe2xel.ampr.at**.
Po naciśnięciu na ekranie przycisku konfiguracji rozszerzonej (na ilustracji „Weitere Einstellungen...”) otwierane jest okno przedstawione na ilustracjach 8.2.3 i 8.2.4. Zawiera ono cztery zakładki, ale tylko w dwóch z nich konieczne jest wprowadzenie własnych danych.

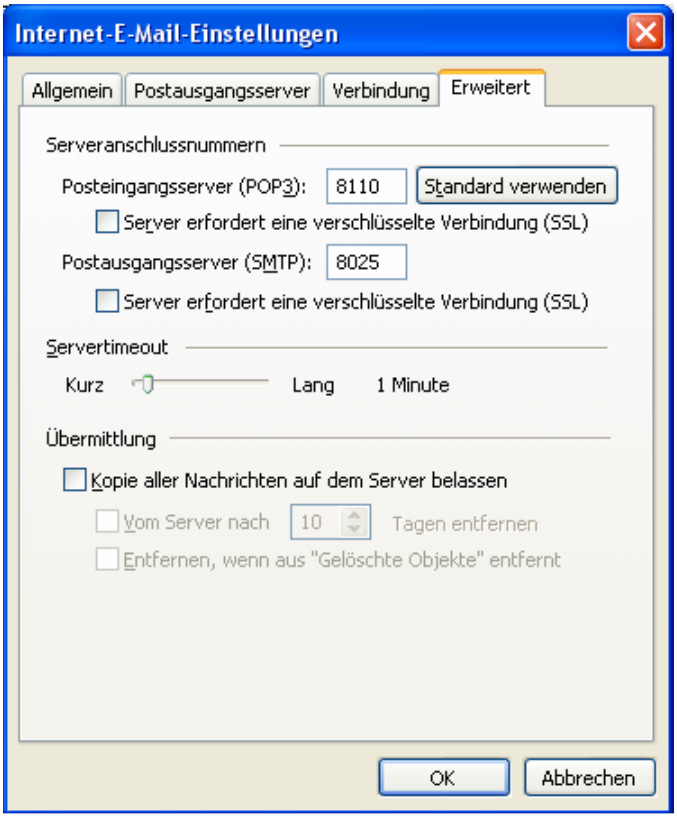


Rys. 8.2.2. Przykład wprowadzonych danych dostępowych

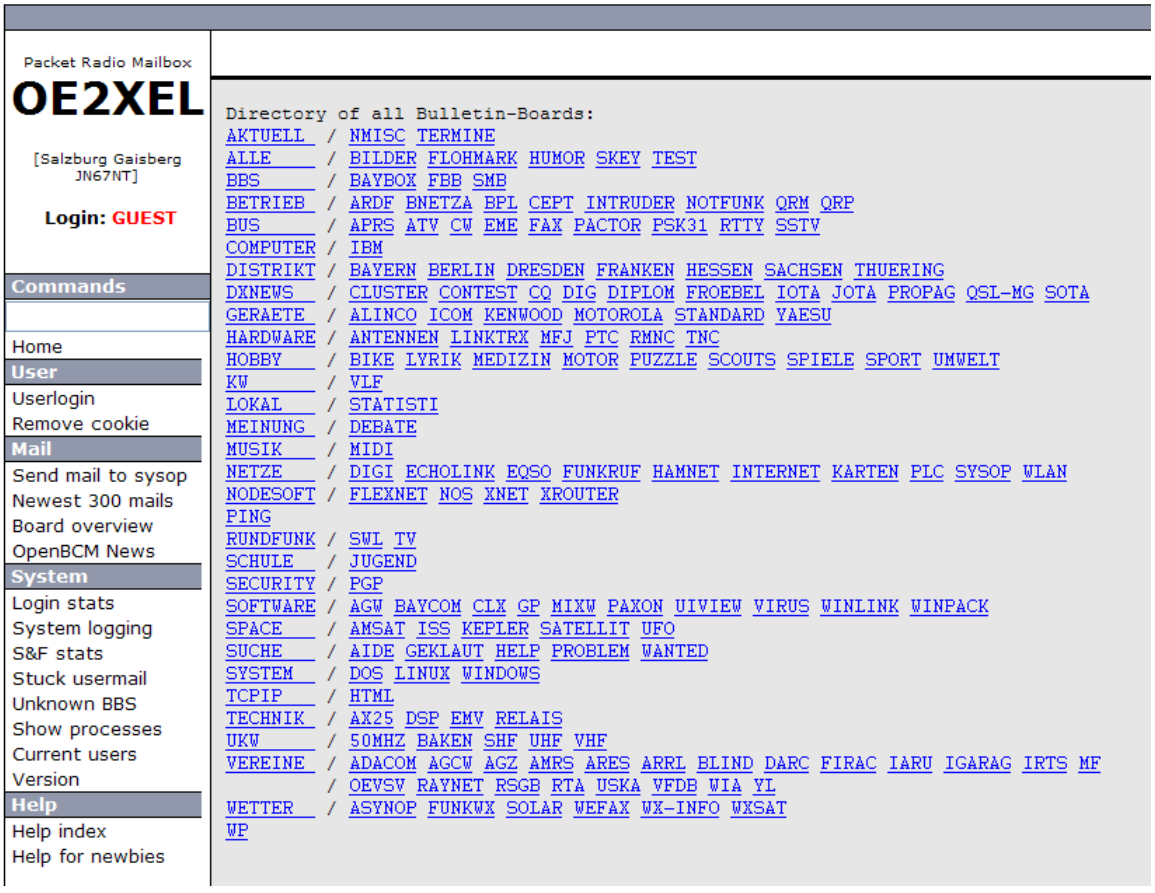


W zakładce pierwszej (danych ogólnych, rys. 8.2.3) należy podać dowolną nazwę konta. Praktycznie jest użyć tutaj własnego znaku wywoławczego (na ilustracji na niebieskim tle).
W ostatniej karcie konfiguracji rozszerzonej (rys. 8.2.4) należy, po zasięgnięciu informacji u operatora skrzynki, wprowadzić używane w dostępie do niej kanały logiczne. W podanym przykładzie różnią się one od używanych standardowo do tego celu i w każdej innej instalacji mogą być też różne od pokazanych w przykładzie: POP3 – 8110, SMTP – 8025, ew. też NNTP – 8119.
W oknie z rysunku 8.2.4 możliwe jest także zaznaczenie pola powodującego pozostawienie kopii wiadomości w skrzynce na serwerze. W przeciwnym przypadku są one kasowane w skrzynce automatycznie po ich odebraniu.

Rys. 8.2.3. Konfiguracja konta pocztowego



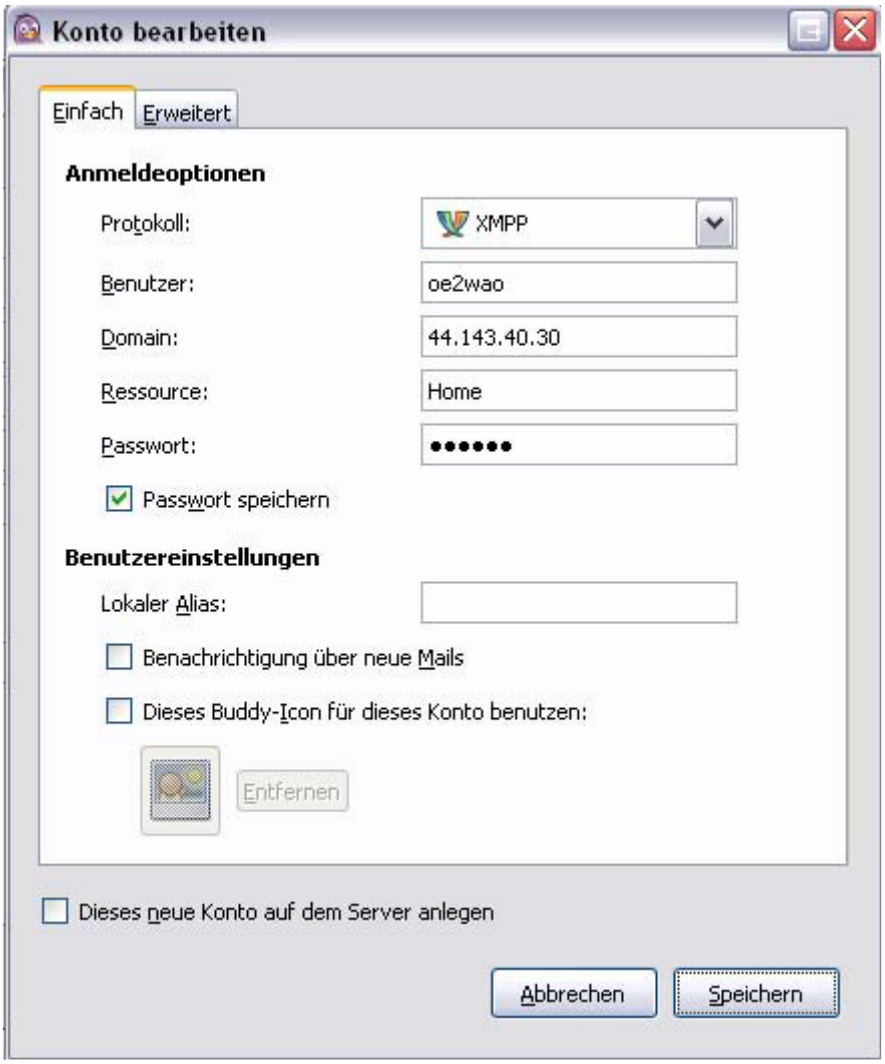
Rys. 8.2.4. Dalsza konfiguracja



Rys. 8.2.5. Dostęp do skrzynki elektronicznej packet-radio OE2XEL przez przeglądarkę internetową

9. Wymiana komunikatów „Instant Messagigng”

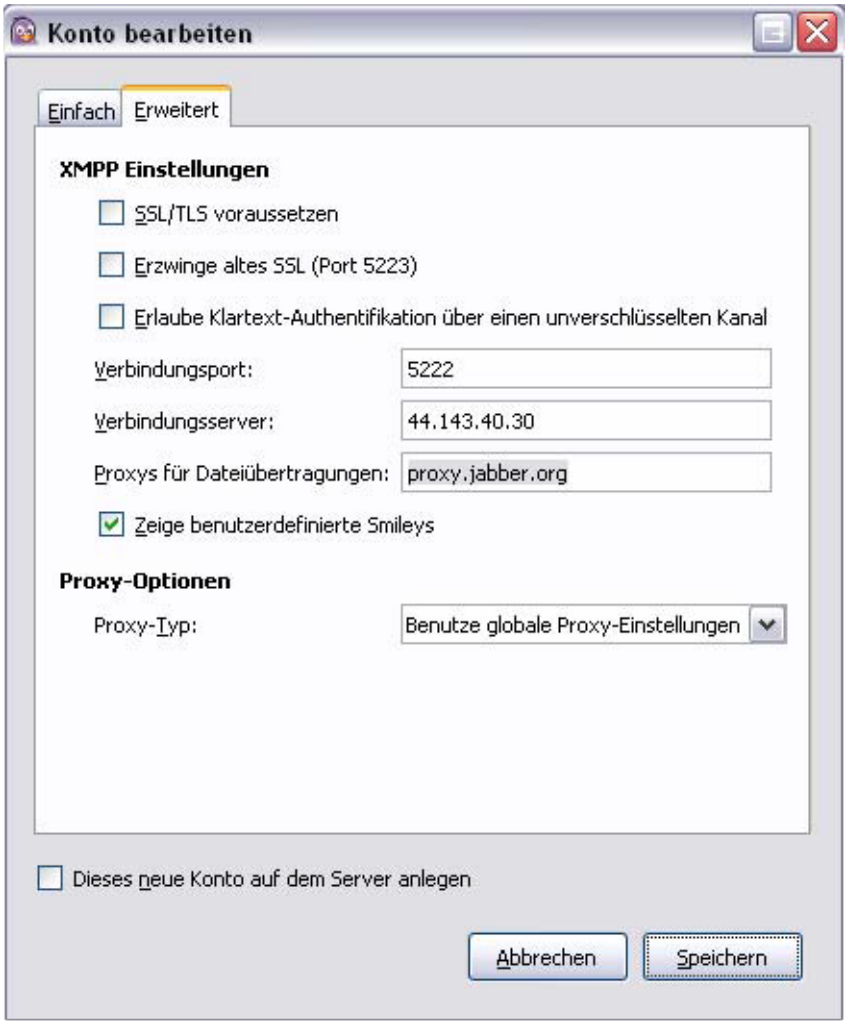
Usługa „Instant Messaging” pozwala na wymianę wiadomości tekstowych i prowadzenie dzięki temu dialogów (ang. *chat*) w Hamnecie. Systemy komunikacji tego rodzaju są oparte przeważnie na protokóle IRC (ang. *Internet Relay Chat*). Możliwa jest w nich zarówno komunikacja między dwoma osobami jak i w kółeczkach konferencyjnych. Klienci IRC komunikują się z serwerem, który rozsyła do adresatów otrzymane wiadomości. Do programów używanych w Hamnecie należą m.in. *HamChat*, *Openfire* i *Pidgin*.
Konfiguracja *Pidgin*, klienta komunikatów i dialogów „Instant Messaging”, jest przedstawiona na przykładzie hamnetowego dostępu przez przemiennik OE2XZR.
Aktualna wersja klienta *Pidgin* dla systemów operacyjnych Windows, Linuks (Debiana i Ubuntu) jest dostępna w Internecie m.in. pod adresem *www.pidgin.im*. Można korzystać z niego nie tylko w „Hamnecie” ale również w dostępie do serwerów wymienionych usług internetowych i to równolegle.
Po zainstalowaniu programu klienta należy założyć w systemie własne konto poprzez KONTA – ZARZĄDZANIE – DODAJ. Otwierane jest okno widoczne na ilustracji 9.1.



Rys. 9.1. Zakładanie własnego konta – pierwsza zakładka

W przykładzie tym wybrany został protokół XMPP (ang. *Extensible Messaging and Presence Protocol*). Jako nazwę użytkownika podaje się pisany małymi literami własny znak wywoławczy, w polu „Ressource” – „Home”, a w polu „Domain” adres IP przemiennika dostępowego – w przykładzie przemiennika OE2XZR. Należy podać także własne hasło dostępu i zaznaczyć pole zapamiętania

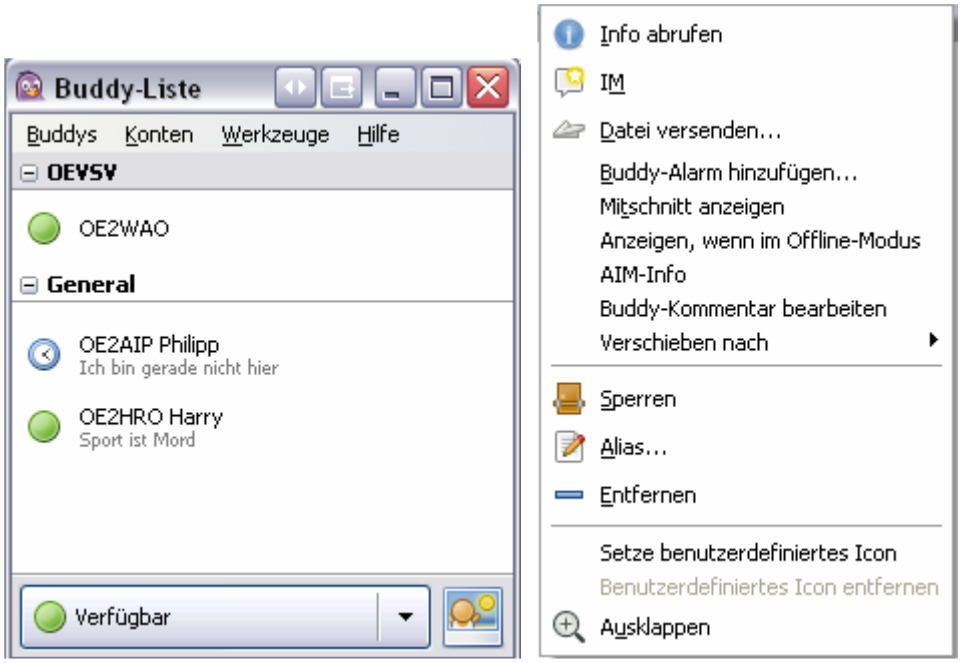
go przez program. Należy też zaznaczyć znajdujące się całkiem na dole pole decydujące, że konto jest zakładane na serwerze.



Rys. 9.2. Zakładanie konta – zakładka danych serwera

Rys. 9.3. Rejestracja

W zakładce danych rozszerzonych (rys. 9.2) wprowadzane są dane serwera: jego adres IP w sieci Hamnetu, kanał logiczny (tutaj 5222) i nazwę pomocniczego serwera „proxy”. Po wpisaniu wszystkich danych należy je zapisać naciskając przycisk „Speichern”.
Program klienta nawiązuje następnie połączenie z serwerem. Może zdarzyć się także zapytanie o akceptację certyfikatu – co należy potwierdzić. Po nawiązaniu połączenia z serwerem należy w oknie rejestracji klienta podać własne dane analogicznie jak w przykładzie z rys. 9.3. Dane te są wykorzystywane wyłącznie przez system. Po ich wpisaniu należy nacisnąć przycisk „OK”.
W otwartym oknie klienta (rys. 9.4) wyświetlany jest spis wszystkich aktualnie połączonych użytkowników.



Rys. 9.4. (po lewej) Spis połączonych użytkowników
Rys. 8.5. (po prawej) Menu kontekstowe

Po naciśnięciu prawym klawiszem myszy w spisie na wybranego użytkownika otwierane jest menu kontekstowe pozwalające na nawiązanie dialogu (punkt IM), wymianę plików, alarmowanie wybranych korespondentów, wywołanie dodatkowych informacji i skorygowanie niektórych danych.
HamChat jest prostym programem przeznaczonym do komunikacji tekstowej. Pracuje w sprzęcie firm *Linksys* i *Ubiquiti*.
OpenFire pozwala natomiast dodatkowo na przesyłanie plików i zdjęć. Pod systemem Windows możliwe jest ustawienie jego startu automatycznie jako usługi, ale możliwe jest także ręczne uruchamianie po włączeniu komputera. W celu zainstalowania programu jako usługi pod Windows należy otworzy okno wiersza poleceń i przejść w nim do katalogu (folderu) programu. Przeważnie jest to katalog *C:\Program Files (x86)\Openfire\bin*. W oknie wiersza poleceń należy kolejno podać polecenia:
Openfire-service /install i *Openfire-service /start*. Konfiguracja serwera odbywa się w oknie przeglądarki internetowej pod jego adresem IP z użyciem kanału logicznego 9000, a więc np. 10.0.0.20:9000. Użykowników dodaje się w oknie administratora. Do współpracy z serwerem *OpenFire* zalecany jest klient *Spark*. Umożliwia on przesyłanie plików i ujęć ekranowych bez konieczności korzystania z FTP.

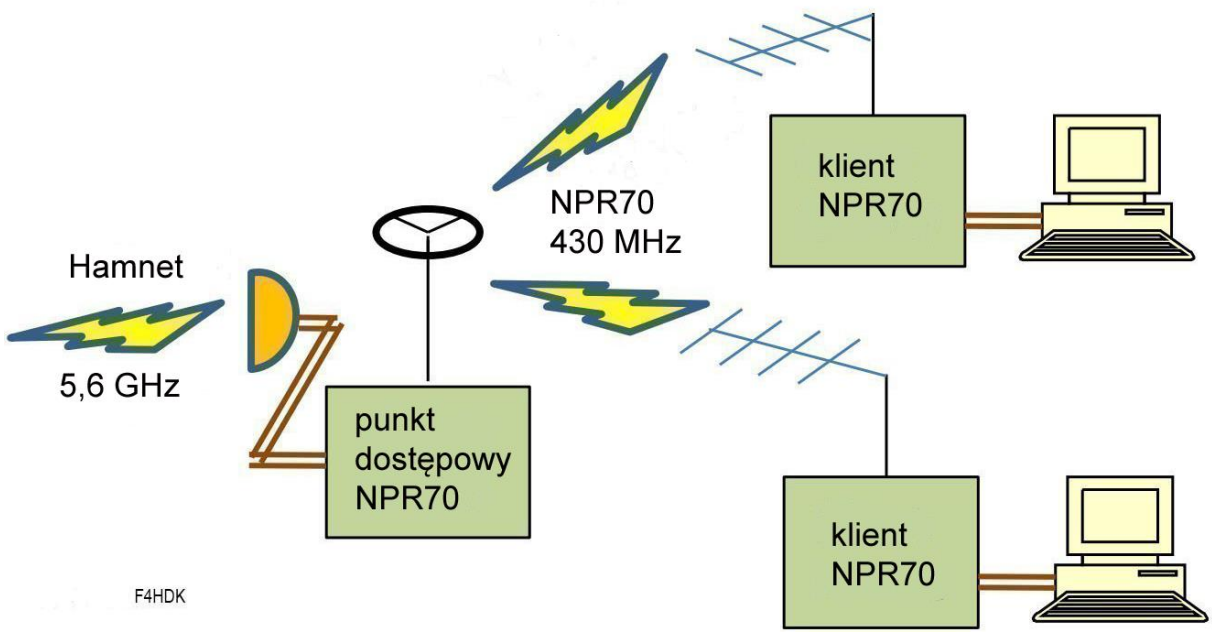
10. Dostęp w niższych pasmach

Punty dostępowe w niższych pasmach UKF od 6 m do 70 cm pozwalają na uzyskanie większych zasięgów aniżeli w zakresach mikrofalowych, ale odbywa się to kosztem zmniejszenia przepustowości.

10.1. NPR-70

Nowe wcielenie „Packet Radio" NPR70 jest rozwiązaniem pośrednim między dobrze znaną wersją „Packet Radio" opartą o protokół AX.25 i stosowanym w sieci Hamnetu systemem opartym o WiFi. W założeniu ma ono ułatwić dostęp do Hamnetu użytkownikom znajdującym się w większych odległościach od węzłów sieci przez wykorzystanie pasma 70 cm. Osiągane szybkości transmisji leżą w zakresie 110 kbit/s – 1 Mbit/s, a więc znacznie poniżej hamnetowych szybkości rzędu 10 Mbit/s.

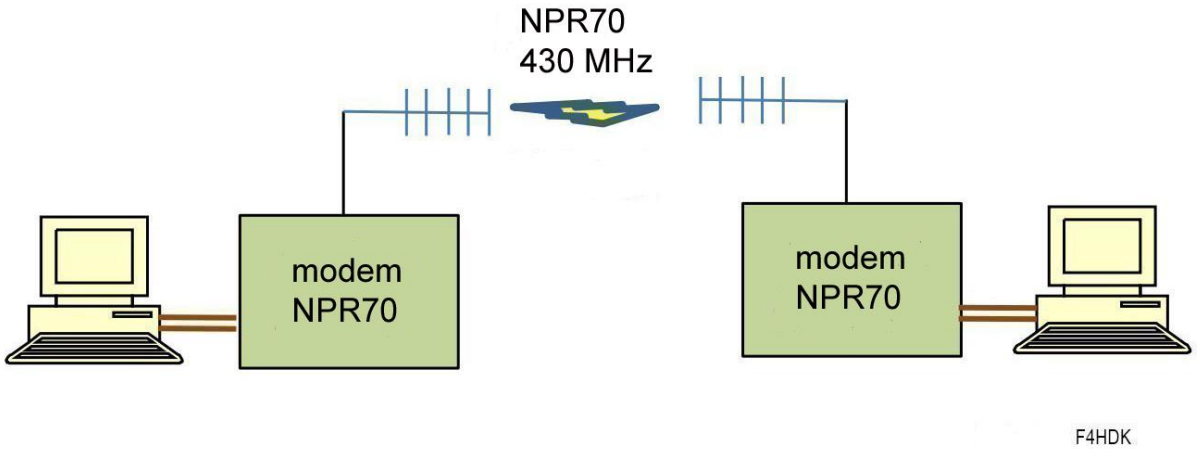
Protokół NPR został opracowany (przez F4HDK) dla zapewnienia dwukierunkowych łączności radiowych w amatorskich sieciach IP. Jest to rozwiązanie w pełni amatorskie nie ukrywające swoich tajemnic przed zainteresowanymi, ale nie jest ono oparte o protokół AX.25. Protokół z podziałem na szczeliny czasowe (TDMA) obsługuje łączności w topologii gwiazdowej – między punktem centralnym (serwerem) i stacjami użytkowników (klientami). Przydziałem szczelin czasowych zarządza stacja centralna, dzięki czemu unika się kolizji pakietów nadawanych przez użytkowników. Głównym zastosowaniem protokółu NPR jest rozszerzenie istniejącej sieci hamnetowej o punkty dostępowe pracujące w paśmie 70 cm (rys. 10.1.1). Pasmo 70 cm zapewnia dalsze zasięgi aniżeli przy bezpośrednim dostępie do Hamnetu w pasmach 13 lub 6 cm. NPR70 jest wyposażony w prosty mechanizm wyprzedzającej korekty przekłamań (FEC) chroniący tylko najważniejszą część pakietu danych. Protokół spełnia wymagania stawiane transmisjom amatorskim: regularnie nadawane są znaki wywoławcze stacji, a transmisja nie jest szyfrowana. Stacja centralna (punkt dostępowy) nadaje jedynie wówczas, gdy połączony jest z nią przynajmniej jeden użytkownik. W pozostałym czasie kanał jest wolny.



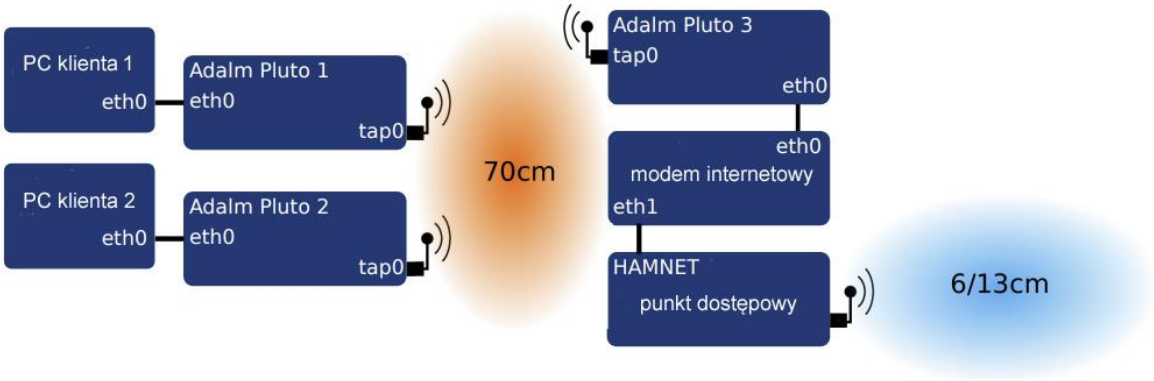
Rys. 10.1.1. Łączność w topologii gwiaździstej

Zalecane jest, aby w punktach dostępowych stosować anteny dookólne, a w stacjach użytkowników anteny kierunkowe dla uniknięcia ewentualnalnego zakłócania sąsiadujących sieci. Przypadkiem szczególnym jest łączność tylko dwóch stacji: możliwe jest wówczas stosowanie anten kierunkowych po obu stronach (rys. 10.1.2). Polaryzacja anten może być dowolnie wybrana przez operatora punktu dostępowego w zależności od lokalnej sytuacji. Anteny muszą charakteryzować się stosunkowo dużym zyskiem.

W Niemczech dla eksperymentalnej szybkiej transmisji danych przewidziane są dwa podzakresy o szerokości 200 kHz: 434,800 – 435,000 i 439,600 – 439,800 MHz, co pozwala na pracę półdupleksową z odstępem częstiwości 4,8 MHz (z wejściem w podzakresie dolnym) lub na pracę simpleksową (również w dolnym podzakresie), natomiast w Szwajcarii jest to podzakres o szerokości 600 kHz wokół częstotliwości 434,400 MHz. W Austrii być może zostanie zastosowane inne rozwiązanie.



Rys. 10.1.2. Połączenie pojedyńczej stacji z punktem dostępowym



Rys. 10.1.3. Sieć oparta na radiostacjach „Adalm Pluto”

Modemy użytkowników nadają cyklicznie (co 2 – 6 sekund) swoje znaki wywoławcze, a punkt dostępowy nadaje identyfikator własnej sieci. W obecnej wersji systemu punkt dostępowy może obsługiwać do siedmiu użytkowników równolegle, ale w przyszłości ich liczba ma wzrosnąć do 15. Protokół NPR nie jest przewidziany dla stacji ruchomych, gdyż nie jest dostatecznie odporny na przekłamania występujące wskutek odbioru wielodrożnego. Dla stacji stałych teoretyczny zasięg wynikający ze stosunku długości ramki do czasu propagacji wynosi 300 km. Protokół jest przeznaczony dla sieci o topologii gwiaździstej i nie pozwala na bezpośrednią komunikację stacji użytkowników między sobą – nie obsługuje więc topologii siatki. Każda ze stacji klientów otrzymuje od stacji centralnej (punktu dostępowego) szczelinę czasową, przyznawaną w taki sposób, aby umożliwić dostęp wszystkim nawet jeżeli jeden z użytkowników ma potrzeby większe od pozostałych. W zależności od potrzeb użytkownika stacja centralna przyznaje dostęp szybki lub wolniejszy – czyli większą lub mniejszą liczbę szczelin w ciągu sekundy. Liczba szczelin jest w trybie szybkim 5 – 10-krotnie większa, zależnie od rodzaju modulacji (patrz tab. 10.1.1). W danym momencie użytkownicy mogą być połączeni tylko z jedną siecią – z jedną stacją dostępową. Stacja dostępowa odmawia połączenia z użytkownikiem jeżeli obsługuje już ich maksymalnie dopuszczalną liczbę lub gdy wszystkie adresy IP z jej puli są już wykorzystane (pula obejmuje nie tylko adresy dla użytkowników, ale również i dla dalszych łączy w sieci).

W przypadku przekraczającego 30 sekund braku aktywności punkt dostępowy przechodzi w tryb czuwania (nasłuchu) i wraca do trybu czynnego po odebraniu sygnału użytkownika. Szerokości kanału w.cz. w zależności od typu modulacji podano w tabeli 10.1.1.

Fot. 10.1.4. Modem F4HDK

Najważniejszym elementem wyposażenia stacji użytkowników są modemy NPR. Konstrukcje modemów F4HDK (fot. 10.1.4) są dostępne m.in. w sklepie internetowym [10.1.2]. W ich części radiowej pracuje moduł TRX z cyfrową obróbką sygnałów typu SI4463F30. W chwili obecnej charakteryzują się one stosunkowo niską czułością – dla uzyskania możliwej do przyjęcia stopy błędów (BER) wymagany jest poziom sygnału odbieranego rzędu -87 dBm (S9 + 6 dB) przy modulacji typu 21. Ewentualne dodatkowe wzmacniacze mocy muszą zapewnić czas przełączania nadawanie-odbiór poniżej 1 ms (moce wyjściowe modemów NPR-70 F4HDK wynoszą w przybliżeniu 500 mW – 27 dBm). Wymagania te spełniają wzmacniacze dla radiostacji DMR. Modemy te stosują dwu- lub 4-stanowe gaussowskie kluczowanie częstotliwości (2GFSK lub 4GFSK) z szybkościami transmisji dochodzącymi do 500 kbit/s. Konfiguracja modemu wymaga połączenia go z komputerem PC przez złącze USB lub za pomocą protokółu *Telnet*. Jeżeli modem ma pracować w trybie zdalnego nadzoru musi on pozostać stale połączony z PC albo z mikrokomputerem w rodzaju „Maliny”. Oprócz toru radiowego modem zawiera mikrokomputer sterujący STM32L432KC i złącze ethernetowe.
W rozwiązaniu alternatywnym [10.1.3 – 10.1.5] opartym o protokół dostępowy HNAP zastosowano modulację ortogonalną z 40 podnośnymi odległymi od siebie o 4 kHz. Całkowita szerokość zajmowanego pasma wynosi więc 160 kHz. Podnośne są zmodulowane na jeden z siedmiu sposobów od QPSK począwszy a na QAM256 skończywszy (z różniącymi się współczynnikami FEC 1/2 albo 3/4). Zarówno w stacjach użytkowników jak i w stacji dostępowej jako wyposażenie radiowe pracuje radiostacja „Adalm Pluto” ze specjalnie opracowanym oprogramowaniem. Stabilność zamontowanego w niej fabrycznie generatora TCXO jest niewystarczająca, dlatego też konieczna jest jego wymiana na generator zapewniający stabilność 0,5 x 10^{-6}. W obecnej wersji osiągane są szybkości transmisji 80 – ~350 kbit/s. Radiostacje „Adalm Pluto” są połączone z komputerem za pośrednictwem złącza ethernetowego (z ewentualnym wykorzystaniem przejściówki Ethernet/USB w przypadku gdy komputer nie posiada złącza Ethernet) – patrz fot. 10.1.5.
Krótkofalowcy austriaccy pracują natomiast, wspólnie z Politechniką Wiedeńską, nad opracowaniem szerokopasmowego rozwiązania dostępu do Hamnetu. Pod naukowym kierownictwem profesora politechniki OE1VMC opracowywany jest punkt dostępowy i modem dla użytkowników pracujące w paśmie 52 – 54 MHz z szerokością pasma 2 MHz [10.1.6]. Mają one pracować zgodnie ze standardem IEEE802.22 (WRAN). W przyszłości mogłyby powstać również analogiczne urządzenia dla pasma 70 cm. Dzięki temu krótkofalowcy austriaccy mogliby przeskoczyć etap NPR70.

Fot. 10.1.5. Łącze z wykorzystaniem radiostacji „Adalm Pluto”

Tabela 10.1.1
Warianty modulacji

Kluczowanie	Szybkość modulacji [kbod]	50	100	180	300	500
	Pasmo [kHz]	100	200	360	600	1000
2GFSK	Typ modulacji	---	11	12	13	14
	Przepływność brutto [kbit/s]	---	100	180	600	500
	Przepływność netto [kbit/s]	---	71	120	190	300
4GFSK	Typ modulacji	20	21	22	23	24
	Przepływność brutto [kbit/s]	100	200	360	600	1000
	Przepływność netto [kbit/s]	68	130	220	330	470

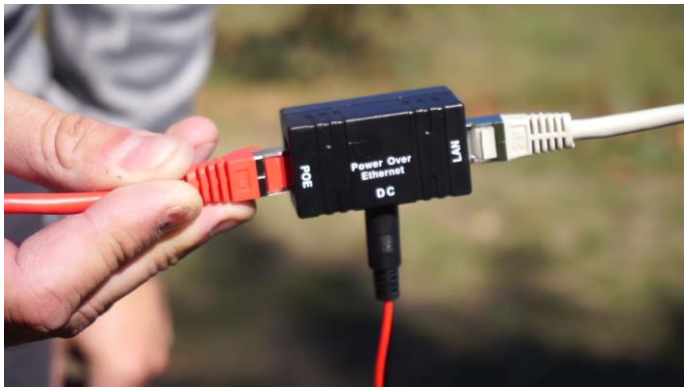
10.2. WRAN

Standard sieci WRAN (ang. *Wireless Regional Area Network*) jest zdefiniowany w normie IEEE 802.22 (zwanej również Super-WiFi). Klub Politechniki Wiedeńskiej (TU-Wien) wraz z pracownikami naukowymi i studentami uczelni (w ramach prac dyplomowych) prowadzi prace nad szerokopasmowym modemem OFDMA (ang. *Orthogonal Frequency Division Multiple Access*) przeznaczonym eksperymentalnie dla pasma 52 – 54 MHz i nad stacją bazową – węzłem. Węzły mają zapewnić dostęp dla kilkudziesięciu użytkowników. Stanowią one jądra dużych komórek o promieniu 50 – 80 km, przeznaczonych dla rzadziej zaludnionych terenów. Możliwe ma być także przenoszenie łączności między komórkami (ang. *rooming*).
Oprócz łączności w normie IEEE 802.22 używane mają być również spokrewnione z nią normy IEEE 802.11af i 802.11ah. Szerokość pasma pracy ma wynosić 2 MHz w paśmie 6 m, a w przyszłości również w paśmie 70 cm. Planowane jest też wykorzystanie modemu w paśmie 2 m.
Konstrukcja modemu opiera się na technice cyfrowej obróbki sygnałów i odbiorników programowalnych (ang. SDR). W rozwiązaniu prototypowym zastosowanie znalazły radiostacje LimeSDR i Ettus

z dodatkowymi układami uzupełniającymi: filtrami i wzmacniaczami w.cz. Moc wyjściowa prototypowego nadajnika ma wynosić 5 W. W prototypowym modemie przeznaczonym dla użytkowników pracuje LimeSDR mini i „Malina 4B". W ramach eksperymentów z modememi planowane jest także wypróbowanie dynamicznego zarządzania zasobami częstotliwościowymi – kanałami (ang. *cognitive radio*). Stanowi ono część standardu WRAN.

11. Sieć ratunkowa AREDN

AREDN (ang. *Amateur Radio Emergency Data Network*) jest hamnetową siecią o topologii siatki (ang. *mesh*) oferującą przepływność do 54 Mb/s. Jest ona oparta na wcześniejszych opracowaniach oprogramowania wewnętrznego BBHN (szerokopasmowy Hamnet; ang. *Broadband Hamnet*) dla Linuksowych urządzeń sieci WiFi i WISP (ang. *Wireless Internet Service Provider*).
W sieci AREDN fabryczne oprogramowanie wewnętrzne zostaje zastapione przez następujące moduły:
1) „OpenWRT" – otwarty system dla łączności bezprzewodowych, z którego mogą korzystać dalsze opracowania,
2) OLSR (ang. *Optimized Link State Routing Protocol*) – protokół trasowania oparty na IP i zoptymalizowany do użytku w dynamicznych sieciach *Ad-hoc*,
3) Internetową powierzchnie obsługi – służącą do konfiguracji,
4) Automatyczną konfigurację TCP/IP zależną od typu urządzenia i opierająca się na jego adresie MAC.
Sieć zapewnia znaczną przepustowość przy prostocie realizacji jako standardowego rozwiązania TCP-IP. Pracuje więc ona identycznie jak kablowa sieć domowa i zapewnia typowe usługi elefoniczne wymianę poczty elektronicznej, dostęp do witryn HTTP, do kamer, dyskusje itp.
W odróżnieniu od stacjonarnego Hamnetu, gdzie sieć i punkty węzłowe są zrealizowane według uprzednio opracowanego planu, przydziału częstotliwości i centralnego przydziału adresów IP, węzły sieci AREDN pracują na wspólnej częstotliwości i korzystają z alternatywnych częstotliwości tylko w szczególnych przypadkach i na niektórych odcinkach łączy. Każda ze stacji sieci widzi pozostałe i jest przez nie widziana. Może też połączyć się z dowolną inną. Wybór tras połączeń między stacjami i ich ocena odbywa się przy użyciu protokółu OLSR. W trakcie wymiany danych wykorzystywana jest „najkorzystniejsza" trasa. W przypadku niedostępności któregoś z odcinków lub węzłów poszukiwana jest trasa alternatywna.
W łącznościach kryzysowych pozwala to na szybsze uruchomienie sieci na standardowej częstotliwości. Po włączeniu urządzeń cała reszta odbywa się automatycznie. Usługi uruchomione na jednym z węzłów stają się automatycznie dostępne w całej sieci. Możliwe są połączenia pierścieniowe i skrótowe.
Oprogramowanie AREDN pracuje obecnie na różnych urządzeniach z serii „Ubiquiti M". Szczególnie przydatne są seria M3 i M5. Można także korzystać z punktów dostępowych firmy „Mikrotik".
Szczególnie interesujące są
– Ubiquiti Nanostation Loco M5 Loco, jako lokalne węzły o kącie pokrycia 60°,
– Ubiquiti M5, jako lokalne węzły i krótkie łącza, o kącie pokrycia 45°
– Ubiquiti Power Beam M5300 ISO i 400 jako łącza o większych długościach i w tunelach,
– urządzenia z serii M3 pracujące w paśmie 3,4 GHz (jego zaletą jest mniejsze obciążenie aniżeli na pozostałych dwóch pasmach),
– inne j.np. Bullet, Rocket, i AirGrid (przy węższym paśmie przenoszenia),
– Mikrotic hAP ac lite, (RB952Ui-5ac2nD) – w paśmie 2,4 GHz.
Urządzenia Ubiquiti są zasilane przez gniazdko PoE, przy czym dopuszczane napięcie leży w zakresie 10,5 – 24 V. Wygodnie jest skorzystać w tym celu z rozgałęźników (zwrotnic) PoE (ang. *PoE Injector*).



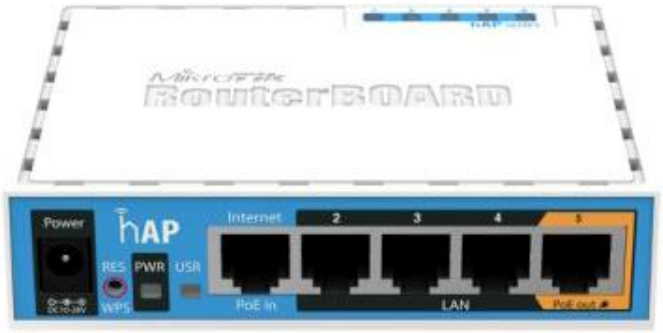
Rys. 11.1. Rozgałęźnik do zasilania przez PoE

W sieci 100 MB do zasilania służą przewody niebieski i brązowy. Nie wolno używać kabli skrzyżowanych.

Rys. 11.2. Połączenie punktu dostępowego Ubiquiti, komputera i zasilania

Rys. 11.3. Najprostszy sposób połączenia dwóch odcinków łączy – wyłącznie za pomocą kabla – dla węzłów przemiennikowych

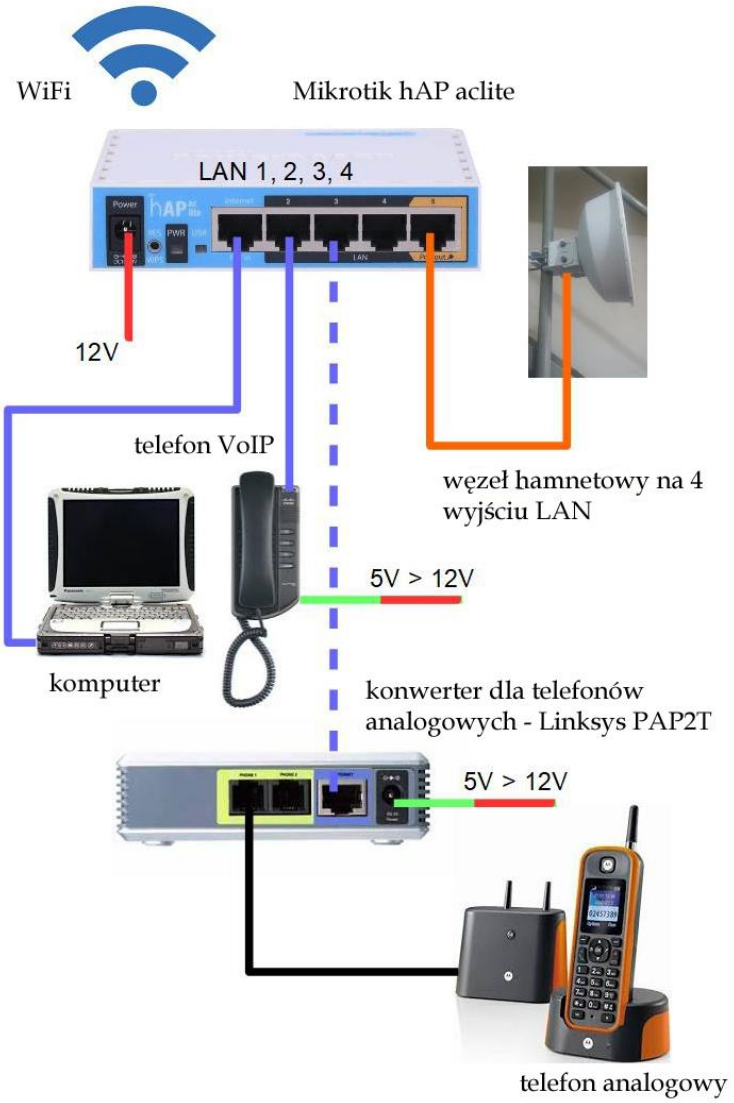
Dla połączenia ze sobą dwóch odcinków łączy hamnetowych nie potrzeba komputera PC. Wystarczy połączenie ich bezpośrednio kablem ethernetowym jak na rysunku 11.3. Komputer jest potrzebny tylko w fazie konfiguracji. W razie potrzeby punkty dostępowe mogą być zasilane z akumulatorów.



Rys. 11.4. *Mikrotik RB259Ui-5ac2nD* jako węzeł AREDN lub punkt dostępowy (ang. *hotspot*) ze standardowym oprogramowaniem wewnętrznym

Alternatywnym rozwiązaniem może być zastosowanie komutatora sieciowego (ang. *switch*) z funkcją zasilania przez PoE. Komutatory sieciowe pracują na poziomie warstwy 2 modelu ISO. Dla połączenia z Internetem musi być to inteligentny komutator (ang. *smart switch* lub *managed switch*) z funkcją zarządzania redundantnymi trasami w taki sposób, aby uniknąć powstania pętli w sieci (w oparciu o protokół STP – *Spanning Tree Protocol*). Protokół STP ma w małych indywidualnych sieciach krótkofalarskich mniejsze znaczenie, ale isotna jst możliwość korzystania z wirtualnych sieci lokalnych (VLAN). Musi on wówczas obsługiwać połączenie z Internetem (wirtualna sieć 1), sieć Hamnetową OLSR (wirtualna sieć 2 i lokalną sieć z DHCP (wirtualna sieć 3). Skonfigurowanie sieci wirtualnych pozwala na odizolowanie od siebie poszczególnych podsieci. Przykłady konfiguracji znajdują się

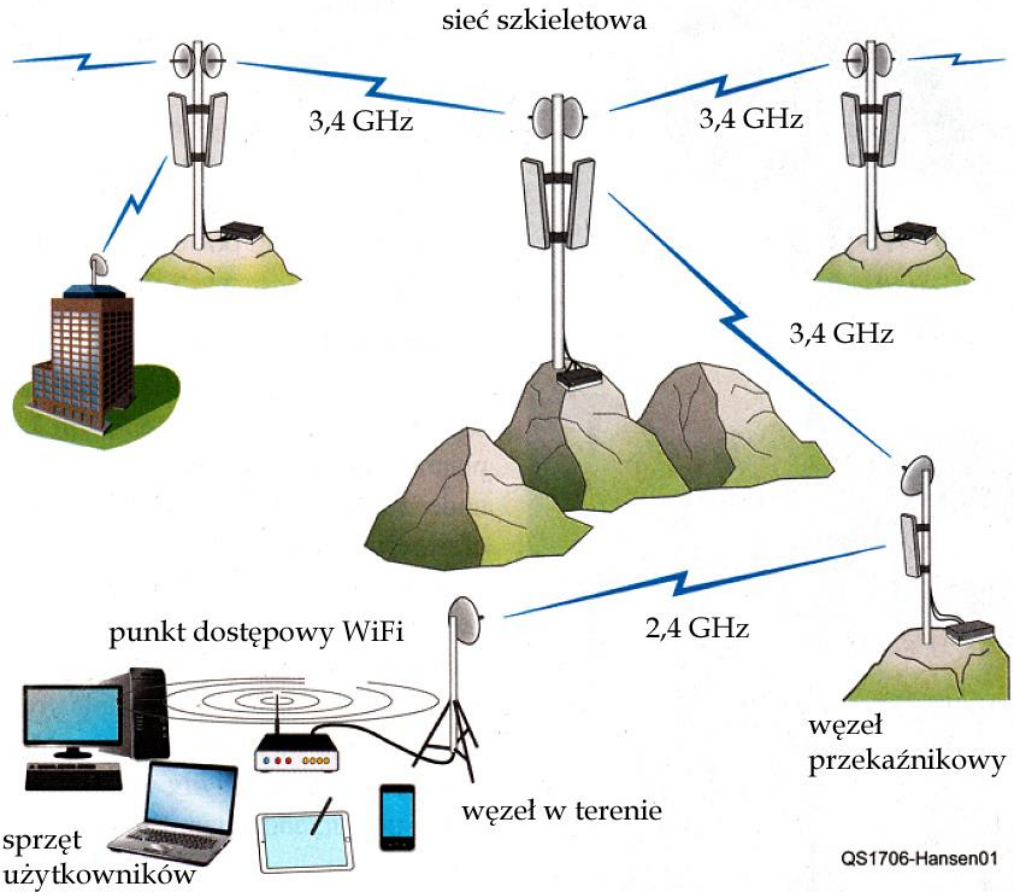
w internetowej witrynie AREDN. Zastosowanie zwykłych nieinteligentnych komutatorów grozi powstaniem konfliktów adresowych w sieci.
Jednym z zalecanych urządzeń jest „Mikrotek hAP aclite". Innym wchodzącym w grę urządzeniem jest „Toughswitch TSW-5" firmy Ubiquiti.



Rys. 11.5. Prosta stacja węzłowa

Rys. 11.6. Przenośna stacja walizkowa z akumulatorem 8 Ah, punktem dostępowym WLAN i telefonem VoIP

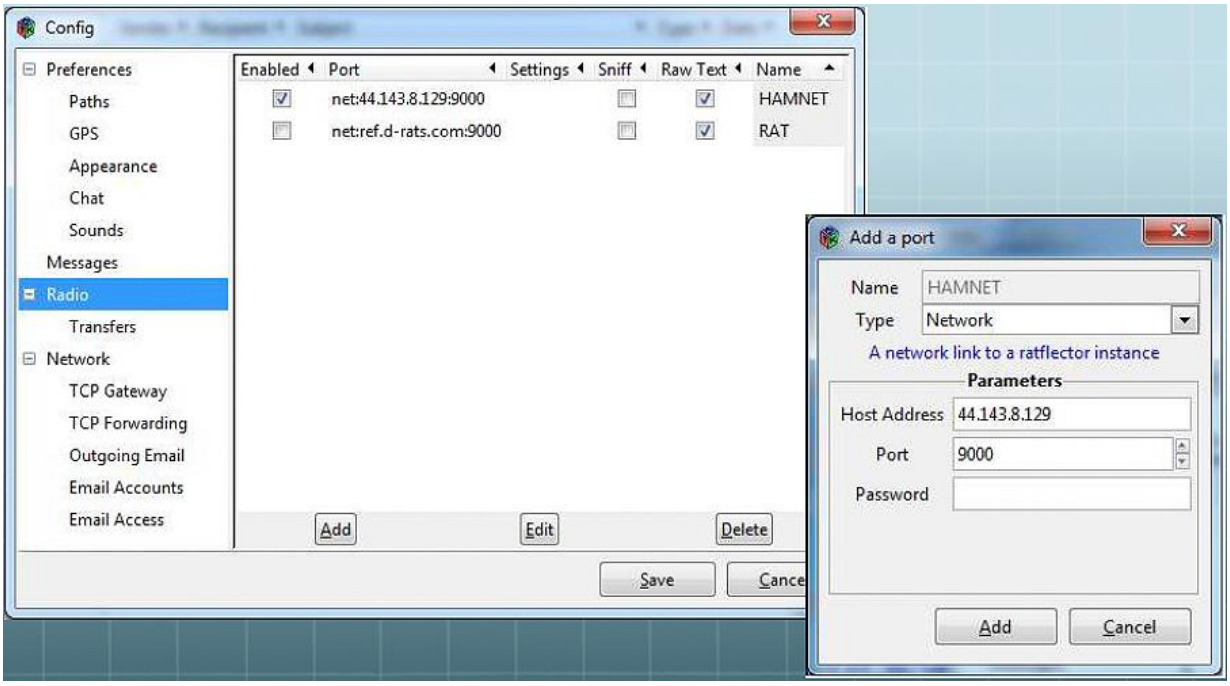
Na ilustracji 11.5 przedstawiony jest przykład typowego rozwiązania stacji węzłowej użytkownika sieci kryzysowej. Zastosowano tutaj zasilany napięciem 12 V „Mikrotik hAP aclite" z oryginalnym oprogramowaniem wewnętrznym. Przekazuje on adresy DHCP z punktu dostępowego do Hamnetu podłączonego do złącza 5 na złącza LAN. Użytkownicy lokalni mogą korzystać z sieci WiFi w pasmach 2,4 oraz 5 GHz. Użycie telefonu analogowego ma tą zaletę, że nie wymaga on dodatkowego zasilania. Proste telefony VoIP w rodzaju Cisco SPA301 albo konwerter Linksys PAP2T mogą być zasilane przez przetwornicę z napięcia 5 V. Dwuprzewodową linię telefoniczną można też łatwo przedłużyć w razie potrzeby. Telefony komórkowe i komputery tabliczkowe mogą korzystać z Hamnetu przez złącze WLAN. Punkt dostępowy do Hamnetu jest zasilany przez „Mikrotik" przez gniazdo PoE.



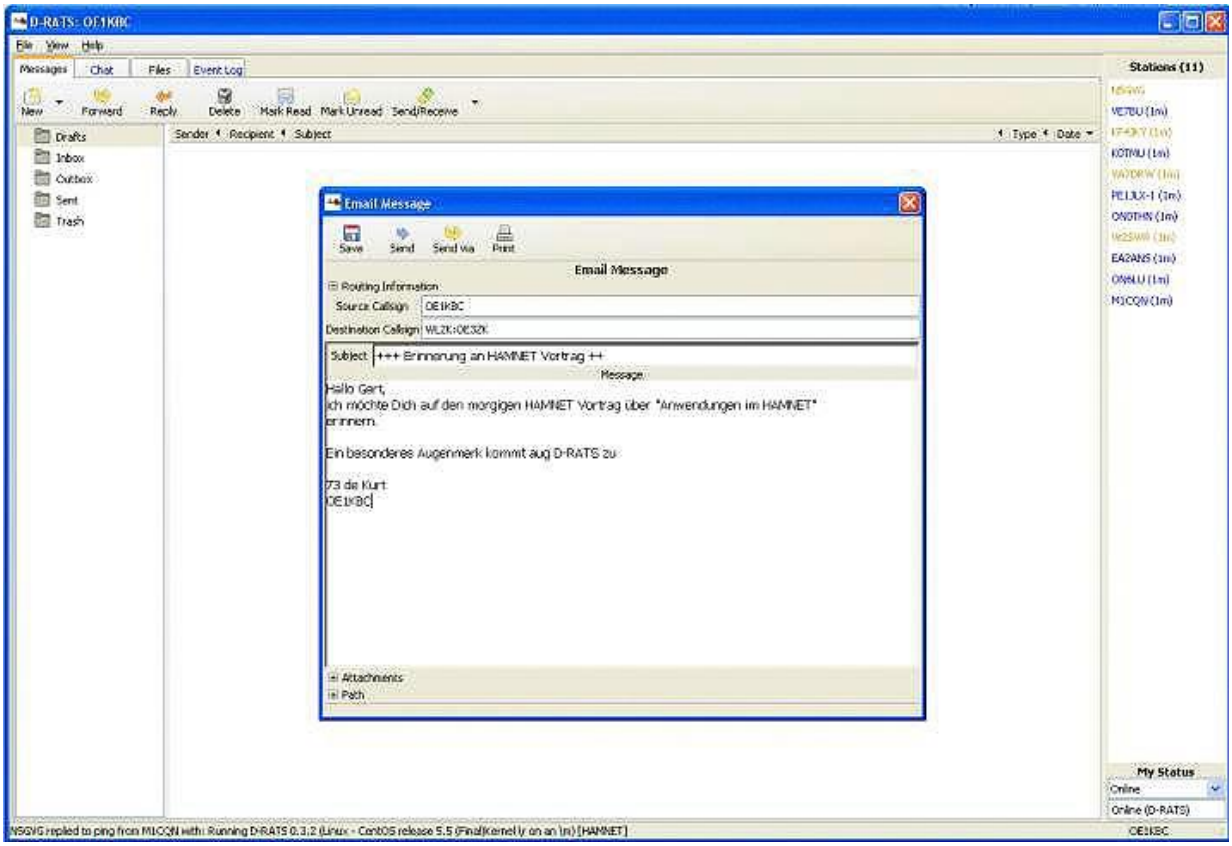
Rys. 11.7. Przykład fragmentu sieci AREDN (źródło QST), połączenie węzła terenowego przez przekaźnik z siecią szkieletową. Jej węzły są zainstalowane na stałe w dogodnych lokalizacjach

W planowaniu akcji ratunkowych konieczny jest dostęp do materiałów kartograficznych. W wielu węzłach hamnetowych w Niemczech pracują serwery udostępniające mapy oparte o standard „Open Street Map". Nie są to mapy pobrane z Internetu, a specjalnie przygotowane dla potrzeb użytkowników Hamnetu.

Dodatek A
Konfiguracja D-RATS



Rys. A.1. Konfiguracja programu D-RATS do połączenia z „Hamnetem”. Przykład z sieci austriackiej

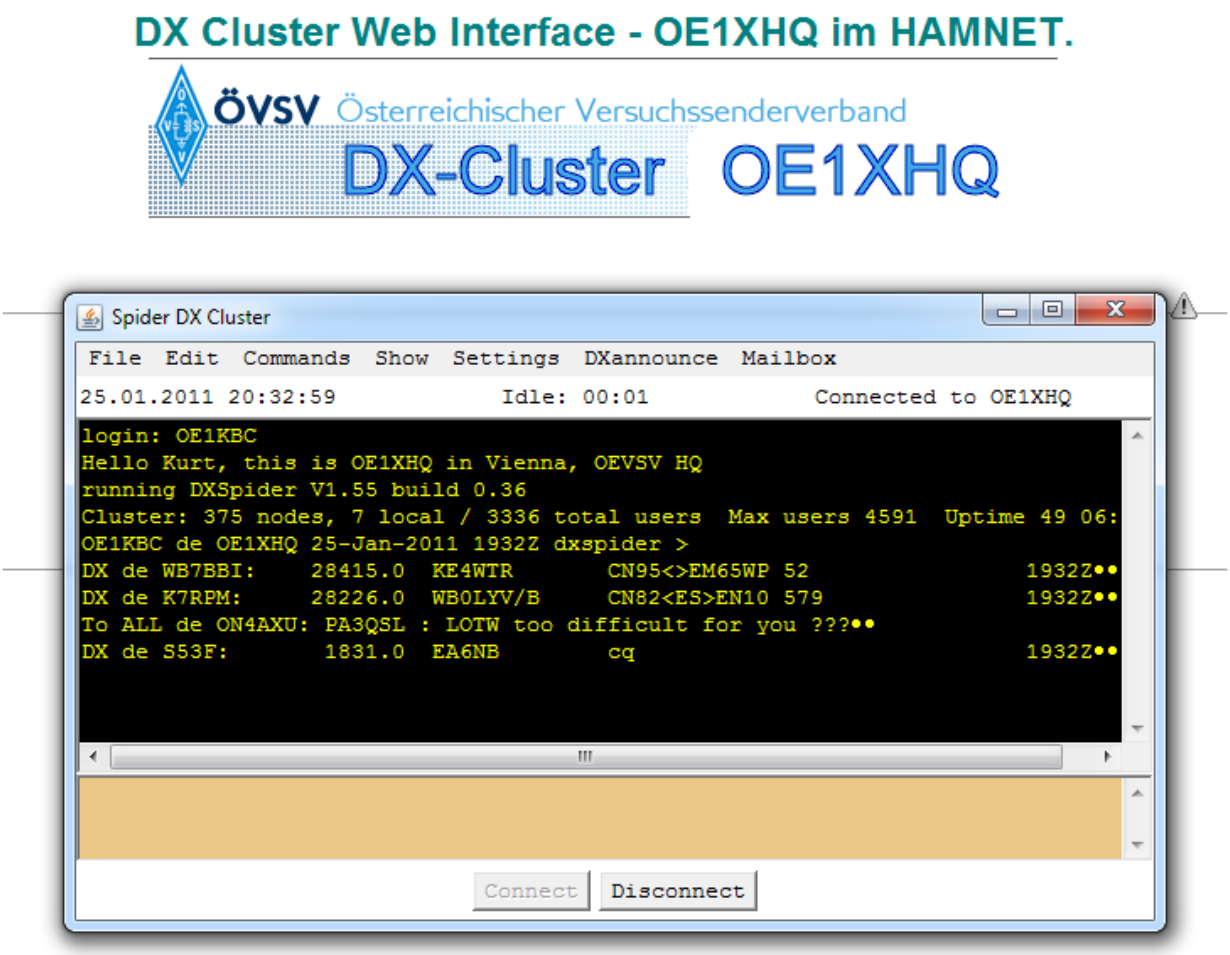


Rys. A.2. Odczyt poczty elektronicznej w programie D-RATS

W Austrii „Ratflector” hamnetowy jest przykładowo dostępny pod adresem IP 44.143.8.129 w kanale logicznym 9000, co odpowiada adresowi symbolicznemu *d-rats.oe1xhq.ampr.at*. Korzystanie z „Ratflectora” umożliwia szybką wymianę danych (tekstów, plików, formularzy przewidzianych na różne okazje, w tym także dla łączności ratunkowych) między użytkownikami sieci D-Starowej dodatkowo do wolnej (ale i tak wystarczająco szybkiej do wielu celów) transmisji drogą radiową za pomocą radiostacji D-Starowych.
D-RATS pozwala także na wymianę poczty elektronicznej przez Internet i dostęp do sieci „WinLinku” (patrz też: tom 15 „Biblioteki”). Do wymiany poczty elektronicznej przez Internet można korzystać z prywatnego konta użytkownika lub założyć oddzielne konto tylko w tym celu.

Dodatek B
Dostęp do skrzynki „DX Cluster”

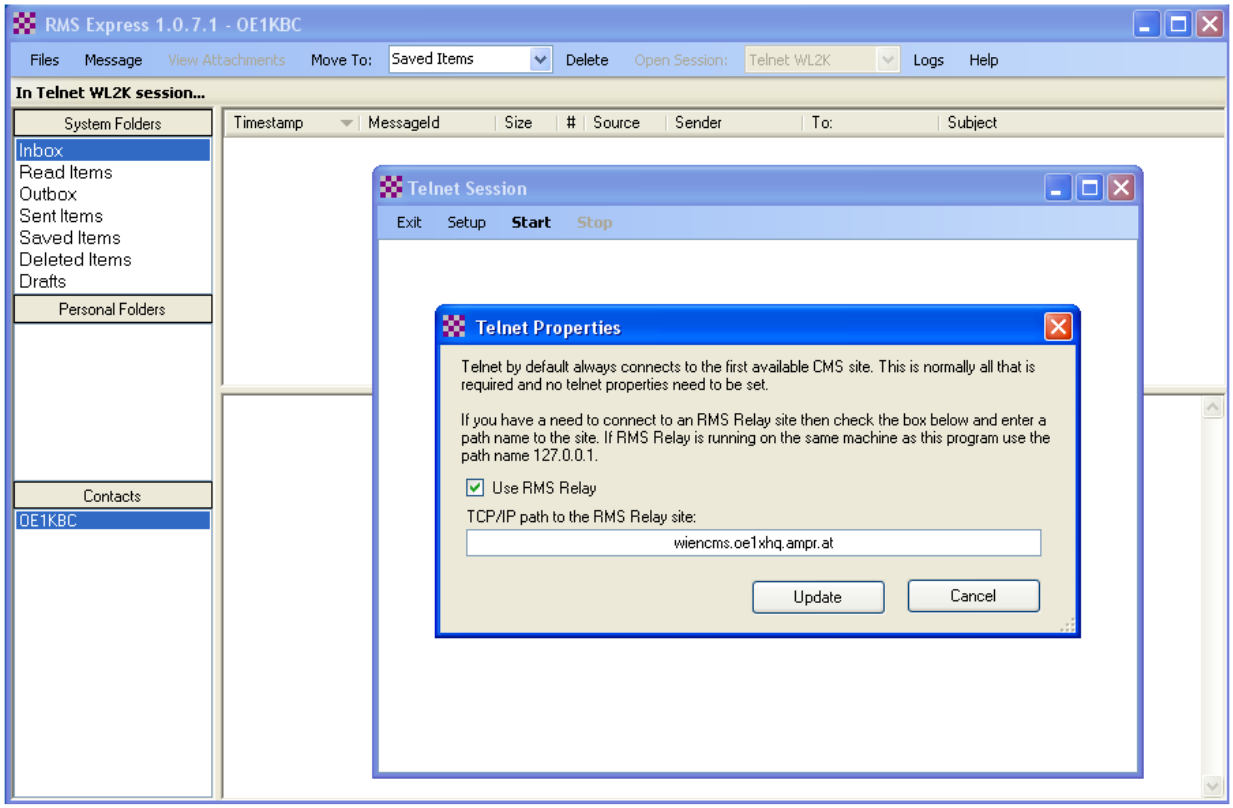
Przedstawiony poniżej przykład dostępu do skrzynki „DX Cluster” w sieci austriackiej ma stanowić dalszą ilustrację możliwości sieci „Hamnetu”. Nie oznacza to, że dostęp z polskiej sieci „Hamnetu” (tam gdzie już istnieje) jest również możliwy.



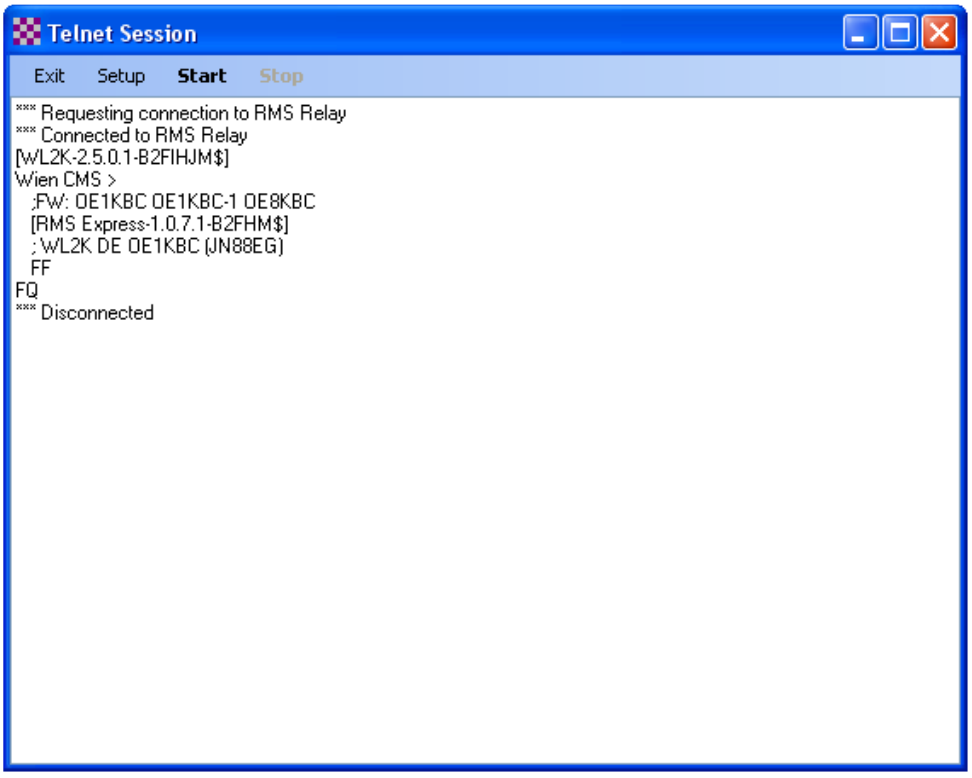
Rys. B.1. Przykład dostępu do skrzynki „DX Cluster”

Skrzynka OE1XHQ jest dostępna pod adresem *dxcluster.oe1xhaq.ampr.at* przez przeglądarkę internetową. Alternatywnie możliwy jest także dostęp przez „Telnet” pod tym samym adresem w kanale logicznym (ang. *port*) 41112. Numer kanału jest zależny od konfiguracji skrzynki i musi być podany do publicznej wiadomości. Korzystanie z przedstawionej w przykładzie skrzynki wymaga zainstalowania Javy na komputerze użytkownika, co przeważnie i tak zostało już dokonane przy innych okazjach.

Dodatek C
Dostęp do sieci „Winlinku”



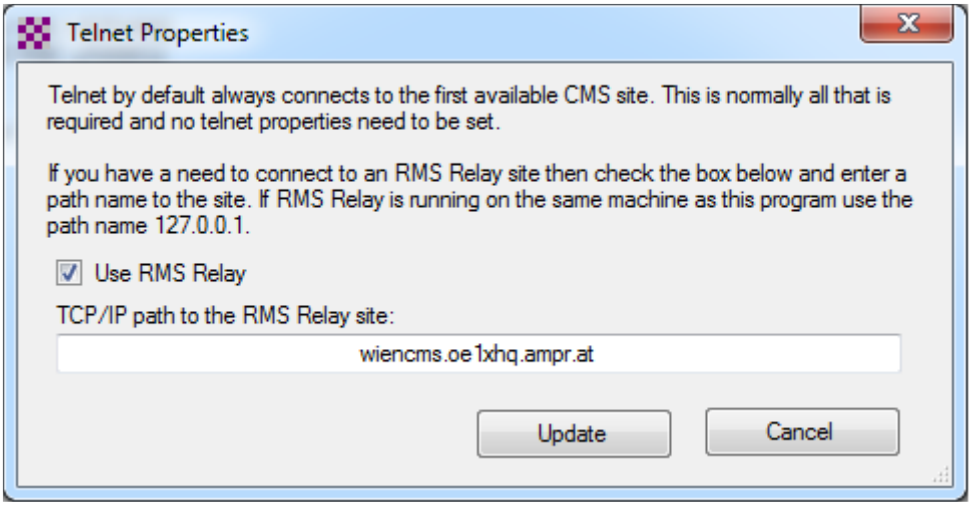
Rys. C.1. Sesja Telnetu w programie „RMS-Express”



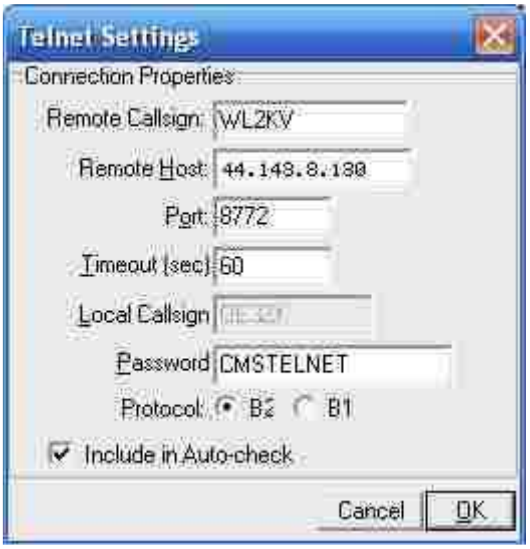
Rys. C.2. Przebieg sesji Telnetu w programie „RMS-Express”

Usytuowany w Wiedniu serwer CMS (patrz tom 9 „Biblioteki polskiego krótkofalowca") jest dostępny nie tylko internetowo, ale także przez Hamnet pod adresem *wiencms.oe1xhq.ampr.at* w kanale logicznym 8772 (adres IP 44.143.8.130). Jego znakiem dla dostępu zdalnego jest WL2KV, a hasłem dostępu CMSTELNET.

Użytkownicy mogą posługiwać się programami „AirMail", „RMS-Express" i „PacLink".

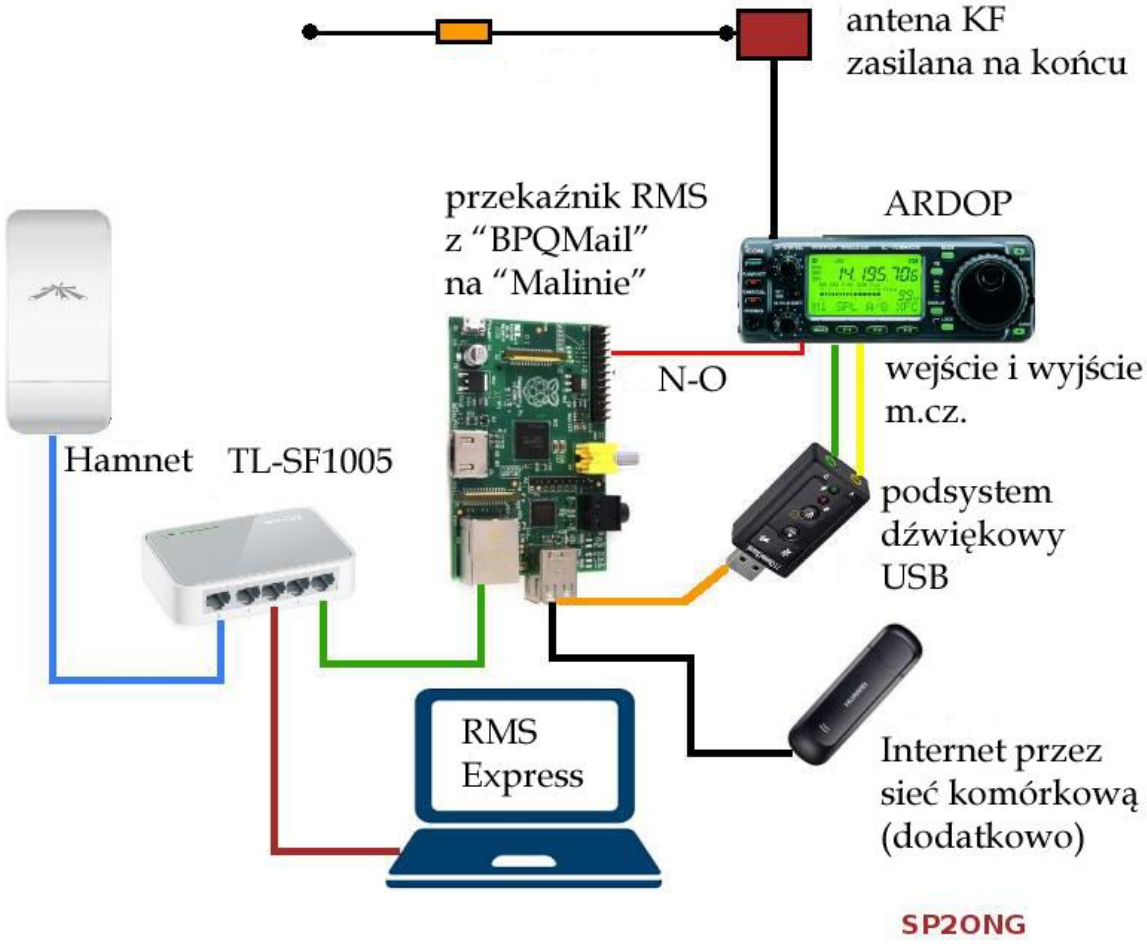


Rys. C.3. Konfiguracja dostępu do „Winlinku" przez wiedeński CMS w programie „RMS-Express"



Rys. C.4. Konfiguracja dostępu telnetowego w programie „AirMail"

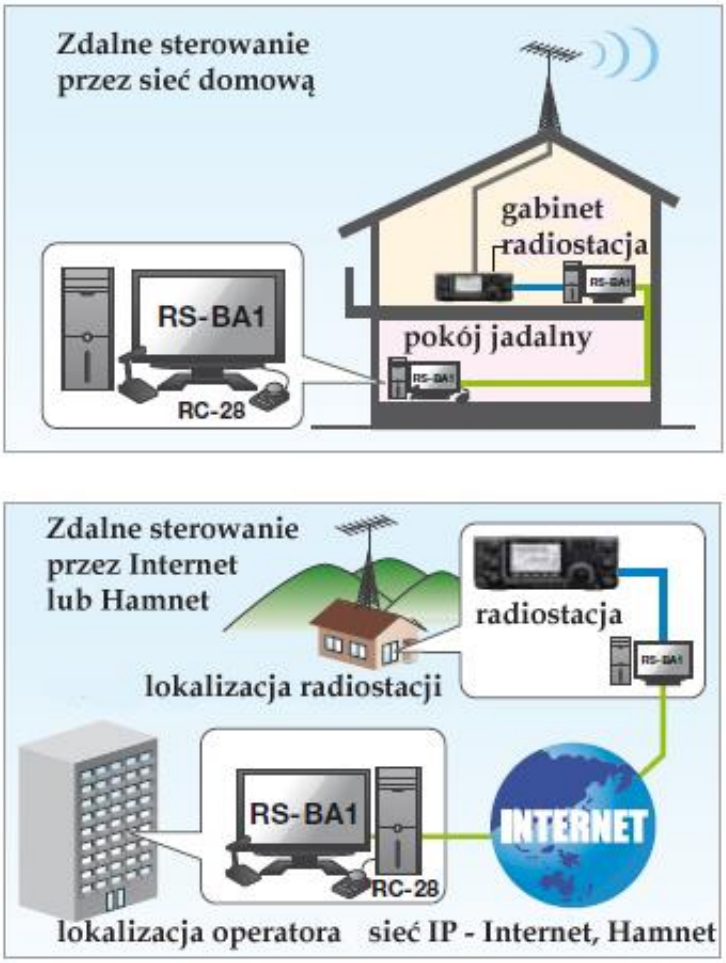
Oprócz tego sieć „WinLinku" posiada dostęp przez bramkę pakietową RMS OE1XIK-10 – osiągalną radiowo przez przemiennik cyfrowy OE1XAR z Bisambergu na częstotliwościach 144,925 i 433,675 MHz.
Poczcie elektronicznej na falach krótkich, Winlinkowi i innym programom poświęcone są tomy 9 i 10 „Biblioteki polskiego krótkofalowca".



Rys. C.5. Przykład wyposażenia stacji Hamnetowej pracującej w sieci Winlinku

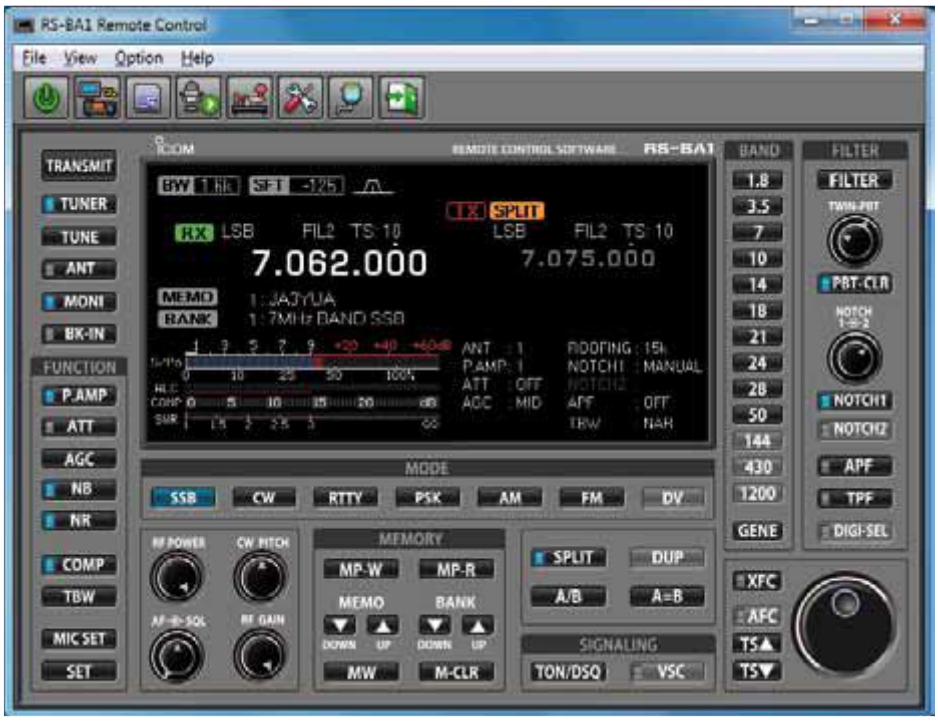
Dodatek D
Zdalne sterowanie radiostacji przez „Hamnet”

System zdalnej obsługi radiostacji przez „Hamnet” jest łatwiejszy do zainstalowania i uruchomienia ponieważ nie występują tu problemy z uzyskaniem stałego adresu IP, nie są używanie zapory przeciwwłamaniowe (ang. *firewall*) i łatwiej jest uzyskać odpowiednio krótkie czasy reakcji.
Sprzęt może być w razie potrzeby zasilany autonomicznie dzięki czemu można korzystać z niego w trakcie łączności kryzysowych i ratunkowych. Do sterowania nadają się takie ogólnie dostępne programy j.np. „Ham Radio Deluxe” lub programy fabryczne udostępniane przez producentów sprzętu, j.np. RS-BA1 firmy „ICOM”.
Program RS-BA1 pozwala na sterowanie niektórych radiostacji firmy „ICOM” zarówno przez lokalną sieć domową jak i przez Internet. W ten sam sposób możliwa jest zdalna praca na radiostacji przez „Hamnet”. Dla ułatwienia strojenia używana bywa dodatkowa gałka RC-28, ale nie jest ona konieczna. Przykładami modeli dostosowanych do zdalnej obsługi za jego pomocą są IC-9100, I-C7600, IC-7410, IC-7200, IC-7100, IC-7800, IC-7700, IC-9700 itd. Sposoby połączenia radiostacji z komputerem (przez złącze USB lub ACC i CI-V) podane są w dokumentacjach programu i radiostacji.



Rys. D.1. Zastosowania RS-BA1

Przedstawione na rys. D.1 rozwiązania mogą dotyczyć zarówno radiostacji indywidualnej jak i klubowej zainstalowanej w dogodnym radiowo miejscu. RS-BA1 nie posiada dostatecznie rozbudowanych mechanizmów regulujących prawa dostępu do radiostacji „publicznych” (j.np. ograniczenie czasu korzystania), ale w przypadku gdy użytkownicy korzystają z jednego komputera obsługującego lub też porozumieją się w inny sposób, może być to rozwiązanie atrakcyjne nie tylko dla osób prywatnych ale i dla niewielkich grup krótkofalowców.



Rys. D.2. Okno RS-BA1

Dla modeli innych firm stosowane jest oprogramowanie W4MQ („Remote Base"). Do transmisji głosu można stosować albo *IRBSound* z pakietu IRT (*Internet Remoting Toolkit*) tego samego autora albo skorzystać ze Skypa. Jeśli chodzi o dopasowanie anten to najprostszym i nie wymagającym instalowania dodatkowych programów (i układów) sterujących jest użycie automatycznej skrzynki antenowej wbudowanej do radiostacji lub oddzielnej. Podobnie rzecz ma się z przełączaniem anten, najlepiej aby radiostacja posiadała kilka przełączanych gniazd antenowych. Jeżeli nie ma tej możliwości to konieczne jest użycie zdalnie sterowanego przełącznika. Serwer W4MQ WEBXVCR zarządza również dostępem do stacji przez zarejestrowanych użytkowników.

Dla radiostacji Kenwooda do zdalnego sterowania stosowane są bezpłatne programy serwera i klienta oddzielne dla poszczególnych modeli. Są to odpowiednio ARHP-590G i ARCP-590G dla TS-590GS, ARHP-10 i ARCP-480 dla TS-480, ARHP-890 i ARCP-890 dla TS890S.

Sterowniki RRC-1258MkII firmy „Remoterig" pozwalają nie tylko na zdalne sterowanie radiostacjami, ale również obrotnicami antenowymi, dodatkowymi wzmacniaczami mocy, przełącznikami antenowymi itp. Sterownik jest połączony z jednej strony ze wszystkimi sterowanymi urządzeniami, a z drugiej za pomocą kabla ethernetowego z modemem dostępowym do sieci. Operator ma do wyboru albo program klienta „RRC-Micro" albo jeden z rozpowszechnionych uniwersalnych programów sterujących jak np. *Ham Radio Deluxe*.

Funkcję serwera dla stacji zdalnie dostępnej pełni także – oparty na „Malinie" – sterownik MFJ-1234 („RigPi Server"). Umożliwia on sterowanie zbaczną częścią modeli radiostacji (wyposażonych w złącze CAT) i pracę również emisjami cyfrowymi. Użytkownicy nie muszą instalować żadnych dodatkowych programów, wystarczy zwykła przeglądarka internetowa. Tematowi zdalnego sterowania radiostacji przez sieć jest poświęcona poz. [D.1] i większość z przedstawionych tam rozwiązań może pracować też w Hamnecie.

Jako inspiracja dla własnych hamnetowych rozwiązań zdalnego sterowania radiostacji, anten, telemetrii itd. może służyć opracowany przez OK1HRA serwer „Remote QTH" (*www.remoteqth.com*). Wyposażenie składa się z „Maliny" z dodatkami (zależnymi od indywidualnych potrzeb): płytki zawierającej przekaźniki, kamery, układu sterującego obrotnicę antenową na „Arduino", przetwornika analogowo-cyfrowego I2C, termometru I2C, układu kluczującego CW, układu kluczującego RTTY itd. Oprogramowanie pozwala na zdalne sterowanie własną stacją, przełączaniem i obracaniem anten, odczyt wartości pomiarowych (w tym temperatur), transmisję RTTY i CW, podgląd za pomocą kamery

Dodatek E
„HAMServerPi”

„HAMServerPi” jest pakietem oprogramowania przeznaczonym dla operatorów sieci „Hamnetu” pragnących szybko uruchomić dodatkowe usługi bez zbyt głębokiego wnikania w ich szczegóły i bez ponoszenia nadmiernych kosztów. Pakiet, od września 2021 r. w wersji V2, pracuje na mikrokomputerze „Raspberry Pi”, a więc nie tylko koszty inwestycji, ale i bieżące koszty eksploatacji są stosunkowo niskie. Wersja V2 oparta na „Debianie Buster” pracje nie tylko na „Malinie” 1 – 3 jak poprzednia, ale także na „Malinie” 4.
Instalacja pakietu wymaga skopiowania (np. z adresu [17]) obrazu pamięci, za pomocą programu „Win32DiskImager” na moduł pamięci SD i włożenia modułu do „Maliny”. Sama konfiguracja jest stosunkowo prosta.

W skład pakietu wchodzą:

- System operacyjny „Raspbian”,
- Serwer HTTP dla Hamnetu („Nginx”, PHP),
- System CMS dla tworzenia stron („GetSimple”),
- Sporządzanie i udostępnianie statystyki odwiedzin („HitCount”),
- Program do podłączenia wyszukiwarek („YaCy”),
- Serwer FTP do transmisji plików („ProFTPD”),
- Serwer pocztowy „Citadel” dla dostępu do poczty elektronicznej przez HTTP,
- Bramka radiowo-internetowa APRS – I-Gate korzystająca z odbiornika DVB-T („PyMultimonAPRS”),
- Serwer VOIP do prowadzenia konferencji słownych („Mumble”),
- Serwer „TeamTalk” dla konferencji audiowizualnych,
- „Prosody” – serwer dla komunikacji „Instant Messagigng”,
- Serwer telefoniczny VOIP „Asterisk”,
- Internetowa powierzchnia obsługi Asteriska („FreePBX”),
- Serwer dostępowy do APRS-IS („aprsc”),
- Sterowanie przemiennikiem lub bramką Echolinkową przez *SvxLink*,
- Echolinkowy serwer buforowy „proxy” („EcholinkProxy”),
- Serwer wizyjny dla ATV przez Hamnet („Icecast”),
- Klient VPN dla połączeń hamnetowych (PPTP),
- Bramka hamnetowa „Masquerade”,
- Ochrona przed atakami przez sieć,
- Graficzna powierzchnia obsługi pozwalająca na wykorzystanie mikrokomputera jako mini-PC dla programów APRSMAP, XASTIR, LoRa-APRS itd.,
- Serwer VNC,
- Kiwi-IRC,
- „The Net Node” (TNN) dla packet-radio z internetową powierzchnią obsługi,
- Elektroniczna skrzynka pocztowa z internetową powierzchnią obsługi („OpenBCM”),
- Program do zarządzania siecią z internetową powierzcchnią obsługi („Nagios”/ „Icingia”),
- ‘Team Talk 5 zamiast wersji 4,
- Serwer LDAP (slapd) z „phpPDAPadmin”,
- Obsługa 10 wyjść logicznych („gpio”) do sterowania sprzętem.

Usługi OpenWebRX, PymultimonAPRS, dxlAPRS i RemoteTRX korzystają z tego samego odbiornika programowalnego RTL i dlatego nie mogą być uruchomione razem. Możliwe jest jednak podłączenie dodatkowych odbiorników RTL i uruchomienie dalszych usług. Wszytkie usługi można włączać i wyłączać wygodnie przy użyciu myszy. Po skonfigurowaniu usługi GetSimple można korzystać z tego przez witrynę *http://myip/admin/load.php?id=hspcontrol*. Domyślnymi danymi dostępowymi są” użytkownik: – pi, hasło: hamsrvpi.

Pakiet został opracowany z myślą o wykorzystaniu w sieci Hamnetu, a nie w Internecie. Nie ma to zresztą większego sensu chociażby ze względów bezpieczeństwa. Jego ewentualne wykorzystanie w Internecie wymagałoby starannego doboru bezpiecznych haseł dostepu we wszystkich plikach konfiguracyjnych i umieszczenie serwera za zaporą przeciwwłamaniową (ang. *firewall*).

Literatura i adresy internetowe

Poniżej podano adresy i pozycje z literatury nie wymienione w poprzednich rozdziałach.

[1] „Hamnet Userzugang. Anhand der Musterkonfiguration Ubiquiti Bullet M5”, Kurt Baumann, OE1KBC, Wiedeń, 15 listopada 2010. Dokument dostępny w witrynie www.oevsv.at
[2] „Hamnet Userzugang. Anhand der Musterkonfiguration Ubiquiti Nanostation M5”, Kurt Baumann, OE1KBC, Wiedeń, 15 października 2010. Dokument dostępny w witrynie www.oevsv.at
[3] „Hamnet AXUDP PR Installation für OE5XBL”, autor OE5HPM. Dokument dostępny w witrynie www.oevsv.at
[4] „HAMNETmesh. Installation & Konfiguration”, Robert Kiendl, OE6RKE, 15 lipca 2009. Dokument dostępny w witrynie www.oevsv.at
[5] „Instant Messaging für Hamnet am OE2XZR Gaisberg konfigurieren. Beispiel anhand des Clients Pidgin“, OE2WAO. Dokument dostępny w witrynie www.oevsv.at
[6] „Packet-Radio via Mail-/Newsclient für Hamnet konfigurieren. Beispiel anhand MS Outlook unter Windows am OE2XZR Gaisberg“, OE5FHN. Dokument dostępny wwitrynie www.oevsv.at
[7] „Packet-Radio Client für Hamnet am OE2XZR Gaisberg konfigurieren. Beispiel anhand des Programs Paxon mit Flexnet unter Windows“, OE2WAO. Dokument dostępny w witrynie www.oevsv.at
[8] www.ubnt.com – witryna firmy Ubiquiti
[9] www.mikrotik.com – witryna firmy MikroTik
[10] www.ruhrlink.db0tv.org – archiwa programów „Mumble”, „Pidgin”, „Flexnet”, „Paxon”, „SDR-Radio”, „Win32DiskImager”, „Putty”
[11] www.mumble.com – witryna „Mumble”
[12] www.hamnet.ugu.pl – witryna polskiego „Hamnetu”
[13] www.qth.at/oe3nka_remote – witryna udostępniająca program „Webtransceiver”
[14] www.skype.com – witryna „Skypa”
[15] http://w4mq.com/remotebase.html – oprogramowanie klienta i serwera do zdalnej obsługi stacji internetowych „W4MQ Internet Remote Base”
[16] www.remoterig.com – witryna poświęcona zdalnej obsłudze radiostacji przez Internet
[17] https://db0gw-i.ampr.org/
[18] „High Speed Multimedia for Amateur Radio“, Glen Popiel, KW5GP, ARRL 2016, ISBN 978-1-62595-052-9

[1.3.1] „Hamnet – Zugang, Einstieg und Anwendungen“, Ralf Wilke, DH3WR

[10.1.1] „Packet Radio weiterentwickelt: New Packet Radio”, Jochen Berns, DL1YBL, „Funkamateur“ 9/2020, str. 797, 10/2020, str. 877, 11/2020, str. 962
[10.1.2] https://elekitsorparts.com – modemy F4HDK
[10.1.3] www.hnap.de – rozwiązanie oparte o TRX „Adalm Pluto”
[10.1.4] „Hamnet auf 70 cm mit dem PlutoSDR”, Jann Traschewski, DG8NDN, CQDL 7‘2020 i 8/2020
[10.1.5] „Design of a Radio Communication Protocol for Hamnet Access in the 70 cm Amateur Radio Band“, Lukas Ostendorf, praca dyplomowa, źródło: [3]
[10.1.6] „WRAN in HAMNET (via 6 m Breitband ins HAMNET)“ – www.oevsv.at

[11.1] AREDN_Grundlagen_V1.1.pdf, Timm Shunk, DL4FLY, 10/2018
[11.2] „AREDN – a high speed data network“, Andre Hansen, K6AH, QST 6/2017 str 36

[D.1] „Zdalnie sterowane radiostacje“, Krzysztof Dąbrowski, OE1KDA, Świat Radio 7/2020 str. 28

W serii „Biblioteka polskiego krótkofalowca” dotychczas ukazały się:

Nr 1 – „Poradnik D-STAR”, wydanie 1 (2011), 2 (2015), 3 (2019) i 4 (2021)
Nr 2 – „Instrukcja do programu D-RATS”
Nr 3 – „Technika słabych sygnałów” Tom 1
Nr 4 – „Technika słabych sygnałów” Tom 2
Nr 5 – „Łączności cyfrowe na falach krótkich” Tom 1
Nr 6 – „Łączności cyfrowe na falach krótkich” Tom 2
Nr 7 – „Packet radio”
Nr 8 – „APRS i D-PRS”
Nr 9 – „Poczta elektroniczna na falach krótkich” Tom 1
Nr 10 – „Poczta elektroniczna na falach krótkich” Tom 2
Nr 11 – „Słownik niemiecko-polski i angielsko-polski” Tom 1
Nr 12 – „Radiostacje i odbiorniki z cyfrową obróbką sygnałów” Tom 1
Nr 13 – „Radiostacje i odbiorniki z cyfrową obróbką sygnałów” Tom 2
Nr 14 – „Amatorska radioastronomia”
Nr 15 – „Transmisja danych w systemie D-STAR”
Nr 16 – „Amatorska radiometeorologia”, wydanie 1 (2013) i 2 (2017)
Nr 17 – „Radiolatarnie małej mocy”
Nr 18 – „Łączności na falach długich”
Nr 19 – „Poradnik Echolinku”
Nr 20 – „Arduino w krótkofalarstwie” Tom 1
Nr 21 – „Arduino w krótkofalarstwie” Tom 2
Nr 22 – „Protokół BGP w Hamnecie”
Nr 23 – „Technika słabych sygnałów” Tom 3, wydanie 1 (2014), 2 (2016) i 3 (2017)
Nr 24 – „Raspberry Pi w krótkofalarstwie”
Nr 25 – „Najpopularniejsze pasma mikrofalowe”, wydanie 1 (2015) i 2 (2019)
Nr 26 – „Poradnik DMR” wydanie 1 (2015), 2 (2016) i 3 (2019), nr 326 – wydanie skrócone (2016)
Nr 27 – „Poradnik Hamnetu” wydanie 1 (2015) i 2 (2021)
Nr 28 – „Budujemy Ilera” Tom 1
Nr 29 – „Budujemy Ilera” Tom 2
Nr 30 – „Konstrukcje D-Starowe”
Nr 31 – „Radiostacje i odbiorniki z cyfrową obróbką sygnałów” Tom 3
Nr 32 – „Anteny łatwe do ukrycia”
Nr 33 – „Amatorska telemetria”
Nr 34 – „Poradnik systemu C4FM”, wydanie 1 (2017), 2 (2019) i 3 (2021)
Nr 35 – „Licencja i co dalej” Tom 1
Nr 36 – „Cyfrowa Obróbka Sygnałów”
Nr 37 – „Telewizja amatorska”
Nr 38 – „Technika słabych sygnałów” Tom 4, wydanie 1 (2018) i 2 (2020)
Nr 39 – „Łączności świetlne”
Nr 40 – „Radiostacje i odbiorniki z cyfrową obróbką sygnałów” Tom 4
Nr 41 – „Licencja i co dalej” Tom 2
Nr 42 – „Miernictwo” Tom 1
Nr 43 – „Miernictwo” Tom 2
Nr 44 – „Miernictwo” Tom 3
Nr 45 – „Testy sprzętu” Tom 1
Nr 46 – „Testy sprzętu” Tom 2
Nr 47 – „Licencja i co dalej” Tom 3
Nr 48 – „Jonosfera i propagacja fal”
Nr 49 – „Anteny krótkofalowe” Tom 1
Nr 50 – „Anteny ultrakrótkofalowe” Tom 1
Nr 51 – „Anteny krótkofalowe” Tom 2
Nr 52 – „Anteny ultrakrótkofalowe” Tom 2
Nr 53 – „Anteny mikrofalowe”

Nr 54 – „Proste odbiorniki amatorskie” Tom 1
Nr 55 – „Proste odbiorniki amatorskie” Tom 2
Nr 56 – „Proste nadajniki amatorskie” Tom 1
Nr 57 – „Proste nadajniki amatorskie” Tom 2
Nr 58 – „Mini- i mikrokomputery w krótkofalarstwie” Tom 1
Nr 59 – „Mini- i mikrokomputery w krótkofalarstwie” Tom 2
Nr 60 – „DX-y w C4FM”
Nr 261 – „Poradnik DMR” Tom 1
Nr 262 – „Poradnik DMR” Tom 2