BIBLIOTEKA
POLSKIEGO KRÓTKOFALOWCA 22

Krzysztof Dąbrowski
OE1KDA

Protokół BGP w Hamnecie
Tłumaczenie instrukcji Bernharda Krölla OE7BKH i Markusa Fankhausera OE7FMI

Wiedeń 2013

Protokół BGP w krótkofalarstwie

Przekład i wstęp

Krzysztof Dąbrowski OE1KDA

Wydanie 1
Wiedeń, grudzień 2013

Spis treści

Wstęp

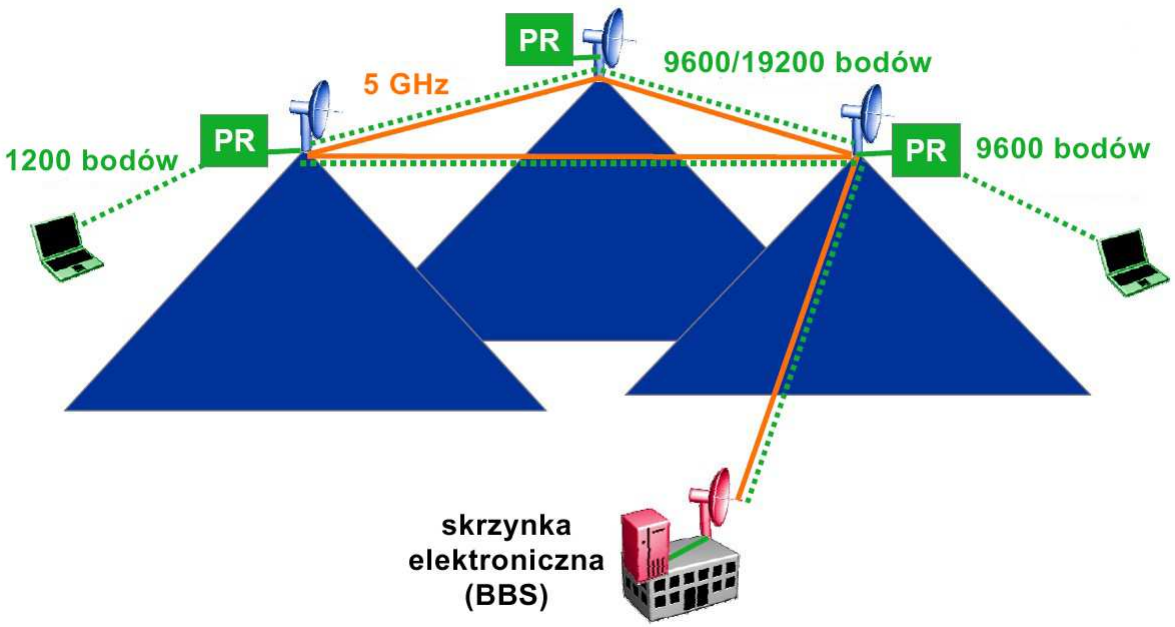
Hamnet jest szybką amatorską siecią TCP/IP czyli amatorskim bezprzewodowym odpowiednikiem internetu. Jej zadaniem nie jest jednak zastępowanie internetu ani też oferowanie krótkofalowcom dodatkowego radiowego dostępu do niego a treść dostępnych w Hamnecie informacji ma charakter czysto krótkofalarski. Jest ona siecią czysto radiową integrującą funkcje dotychczas dostępnych sieci amatorskich takich jak packet radio z usługami czysto internetowymi (poczta elektroniczna, dostęp do serwerów www) oraz oferuje dodatkowo łącza dla sieci przemienników echolinkowych, D-Star i telewizyjnych. W praktyce może ona służyć do transmisji dowolnego rodzaju danych, o ile nadają się one do transmisji za pośrednictwem pakietów IP. Jej zasadniczym zadaniem jest uniezależnienie (przynajmniej w pewnym stopniu) służby amatorskiej od komercyjnychj sieci kablowych. Projekt – noszący początkowo nazwę ALAN (Austria LAN) – został zainicjowany w 2005 roku przez krótkofalowców austriackich i do chwili obecnej rozrósł się na szereg krajów stając się najpoważniejszą akcją przebudowy cyfrowych sieci amatorskich w Europie Środkowej i nie tylko.

Sieć Hamnetu oparta jest na standardzie ethernetowym IEEE 802.11 i składa się z węzłów (bramek) połączonych za pośrednictwem linii radiowych pracujących głównie w paśmie 6 cm (standard IEEE 802.11a) a czasami również i w paśmie 13 cm. Sieć zapewnia w pierwszym rzędzie połączenie razem amatorskich przemienników fonicznych, echolinkowych i systemu D-Star, przemienników telewizyjnych oraz węzłów sieci packet-radio i przemienników APRS. Sposób korzystania z nich nie ulega w tym przypadku żadnej zmianie. Dodatkowo w miarę rozbudowy sieci udostępniane są bezpośrednie wejścia dla użytkowników indywidualnych pracujące najczęściej (w Austrii przyjęto to jako normę) w paśmie 13 cm (standard IEEE 802.11g). W paśmie 13 cm stosowana jest modulacja OFDM (*Orthogonal Frequency Division Multiplexing*) i ewentualnie także rozpraszanie widma z kluczowaniem fazy (DSSS) natomiast w paśmie 6 cm kluczowanie BPSK, QPSK lub wielostanowe QAM w-zależności od szybkości transmisji.

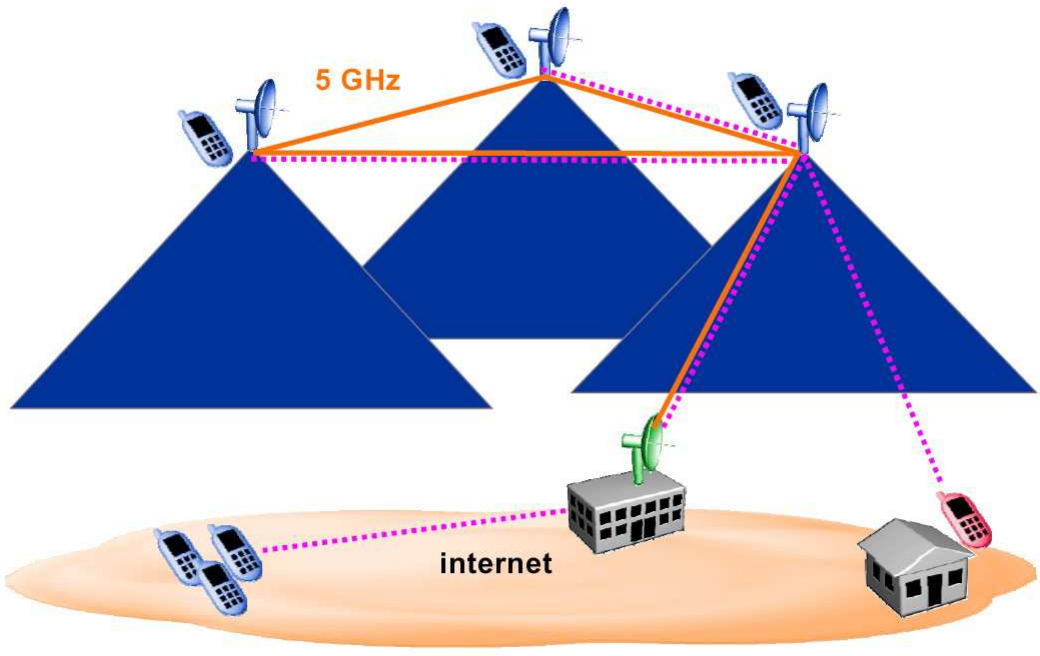
Do budowy sieci wykorzystano standardową aparaturę dla bezprzewodowych sieci komputerowych WLAN. Nadaje się ona do tego celu dzięki temu, że części pasm przemysłowych ISM 2,3 oraz 5,6 GHz pokrywają się z amatorskimi pasmami 6 i 13 cm co pozwala (po wybraniu odpowiednich kanałów i parametrów transmisji) na ich pracę zgodną z zasadami określonymi przez przepisy o służbie amatorskiej a nie w opraciu o przepisy regulujące pracę w pasmach nielicencjonowanych – dotyczy to w szczególności dozwolonej mocy nadajników. Szerokość pasma sygnałów jest przeważnie ograniczona do 5 MHz (w paśmie 2,4 GHz) lub 10 – 20 MHz (w paśmie 5,6 GHz) a szybkość transmisji wynosi najczęściej 1 – 17 Mb/s w zależności od długości trasy (jest to wielokrotnie więcej aniżeli najwyższe szybkości osiągane w dotychczasowej sieci Packet-Radio). Częstotliwości pracy w sieci podane są w tabelach na końcu rozdziału. Część z kanałów pasma 6 cm jest dostępna tylko w niektórych modelach syacji bazowych – punktów dostępowych – (ang. *router*) WLAN.
Transmisja danych w sieci Hamnetu odbywa się w oparciu o protokół IP przy czym stosowane są adresy z sieci amatorskiej 44.xx.xx.xx – w Austrii ampr.at.
W obecnym stanie realizacji sieć może zapewniać następujące usługi:

- Transmisję danych packet-radio z dużymi szybkościami, w tym transmisję danych APRS.
- Łącza echolinkowe.
- Łącza pomiędzy przemiennikami systemu D-Star.
- Transmisję poczty elektronicznej w systemie WinLink2000.
- Transmisję obrazów amatorskiej telewizji analogowej (ATV) i cyfrowej (DATV).
- Transmisję głosu – VOIP (np. „Skype” i podobne rozwiązania) przez serwer „Mumble”.
- Wymianę informacji w systemie „Instant messaging” lub innym podobnym („Jabber”, XMPP.
- Dostęp do amatorskich witryn WWW (wyłącznie tych umieszczonych w Hamnecie a nie internetowych) oraz dostęp przez przeglądarkę internetową do skrzynek *dxcluster*.
- Zastąpienie analogowych linii radiowych przez cyfrowe. Pozwala to na połączenie we wspólnej sieci również analogowych przemienników FM i skrzynek głosowych.
- Zdalny dostęp do odbiorników i radiostacji sterowanych internetowo.
- Zdalne sterowanie przemienników amatorskich.
- Od stosunkowo niedawnego czasu w austriackiej sieci Hamnetu występuja także serwery strumieniowe „BigBlueButton” rozprowadzające strumienie danych wizyjnych i dźwiękowych w sposób podobny jak w wideo-konferencjach.

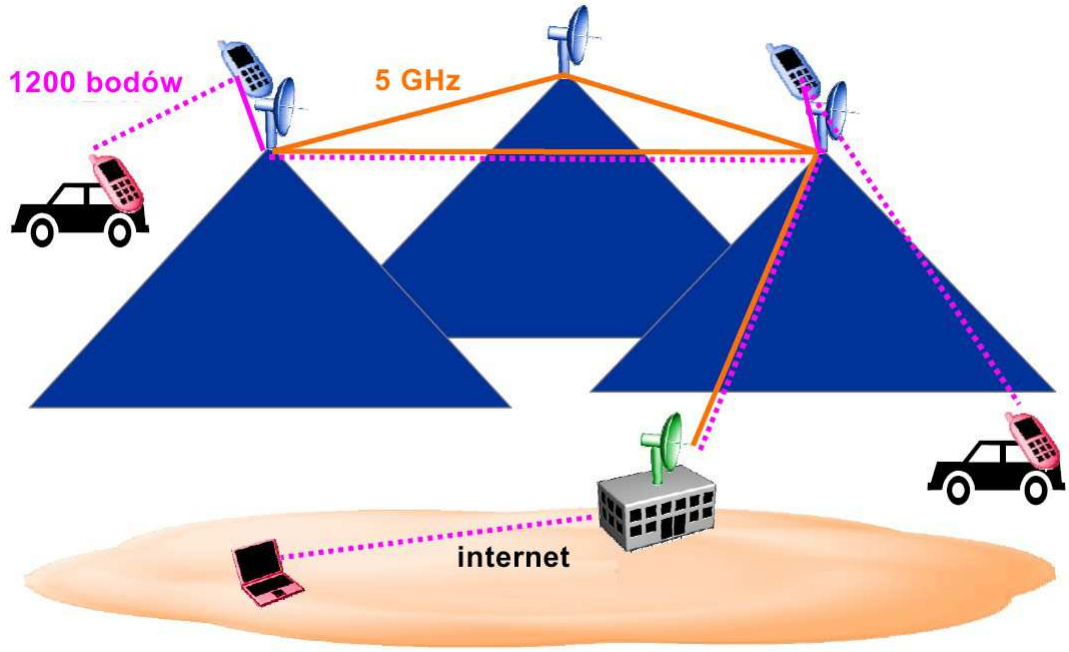
Ogólnie rzecz biorąc można wyróżnić dwa rodzaje dostępnych usług: usługi pośrednie oferowane przez Hamnet w ramach korzystania z systemów łączności na dotychczasowych zasadach i usługi wymagające bezpośredniego połączenia z siecią. Do grupy pierwszej można zaliczyć przykładowo szybką transmisję danych pomiędzy dostępnymi w zwykły sposób przemiennikami fonicznymi, telewizyjnymi albo cyfrowymi Packet-Radio i APRS a do grupy drugiej – bezpośredni szybki dostęp radiowy Packet-Radio, dostęp do sieci za pomocą przeglądarki internetowej, klienta poczty elektronicznej, klienta „*Instant messaging*" albo VOIP. Kilka przykładów wykorzystania sieci Hamnetu przedstawiają ilustracje 1 – 4.



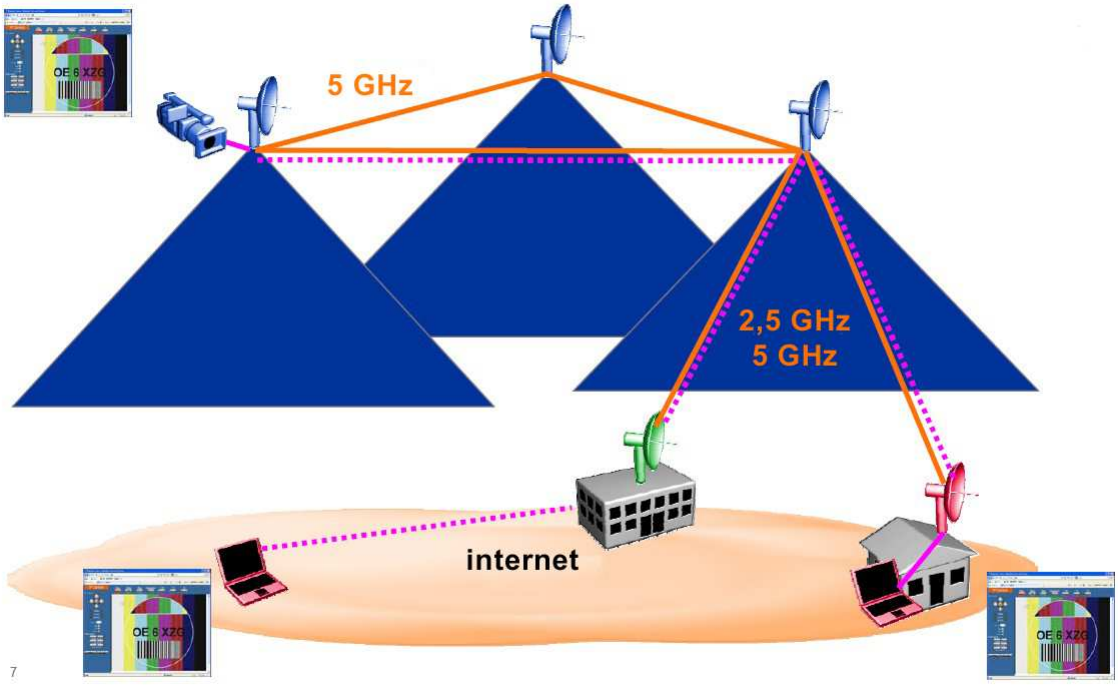
1. Sieć Hamnetu w łącznościach Packet Radio



2. Sieć Hamnetu w łącznościach fonicznych



3. APRS przez sieć Hamnetu



4. ATV przez Hamnet

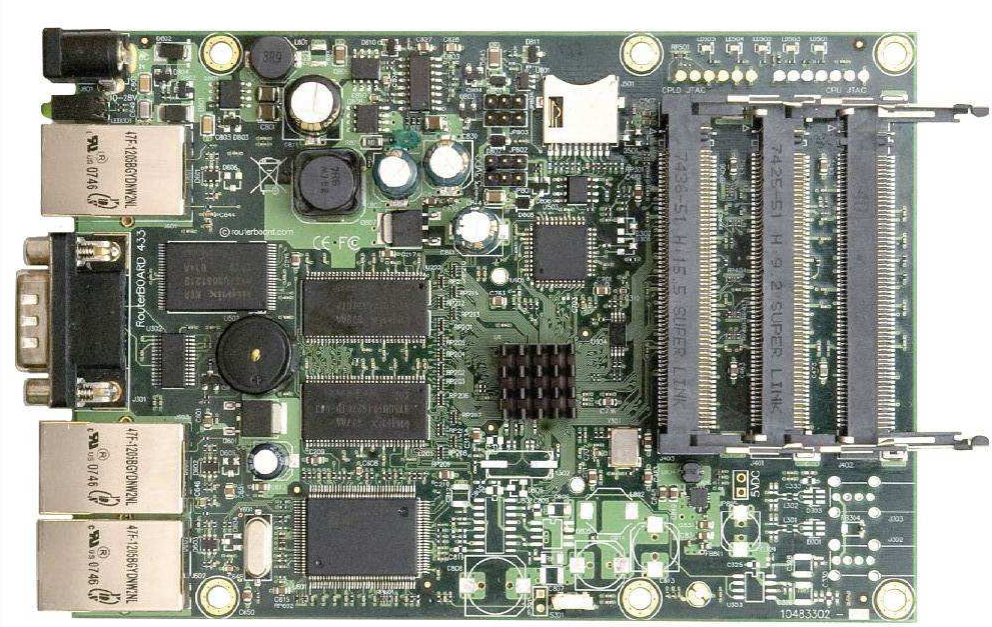
Łącza sieci

W łączach Hamnetu używane jest standardowe wyposażenie bezprzewodowych sieci WLAN – radiowe stacje bazowe (punkty dostępowe; ang. *router*) pracujące w segmentach pasm ogólnie dostępnych 6 i 13 cm pokrywających się z zakresami amatorskimi. Dzięki temu dopuszczalne są zarówno modyfikacje sprzętu jak i praca z mocami wyższymi aniżeli dozwolone dla sprzętu

nielicencjonowanego (oczywiście pod warunkiem, że tak zmodyfikowany sprzęt będzie pracował wyłącznie w pasmach amatorskich).

Przepisy o służbie amatorskiej nakładają jednak ograniczenia odnośnie szerokości pasma dlatego też szerokość pasma transmisji ograniczona jest przeważnie do 5 MHz w paśmie 13 cm i do 10 lub 20 MHz w paśmie 6 cm. Ma to jednakże tą zaletę, że zwykłe prywatne sieci komputerowe nie mogą nawiązać połączenia z siecią amatorską a ponadto węższe pasmo ułatwia uzyskanie większych zasięgów łączności. Dopuszczalne szerokości pasma transmisji amatorskich w Austrii podaje tab. 6.

Modelami najczęściej stosowanymi w obecnym stadium rozbudowy są stacje bazowe (punkty dostępowe) Mikrotik RB411(AH) i RB433(AH) łotewskiej firmy MikroTikls (fot. 5). Wymagają one dodatkowego wyposażenia w modemy radiowe (fot. 6), przy czym RB411(AH) posiada jedno gniazdo do podłączenia modemu natomiast RB433(AH) – trzy. Modele AH charakteryzują się większą mocą obliczeniową i są stosowane w węzłach o dużym natężeniu ruchu.



5. Stacja bazowa – punkt dostępowy – Mikrotik RB433

6. Modem radiowy R52

Oprócz modemów radiowych (*miniPCI WLAN*) typu Mikrotik R52, R52-350 i R52H można stosować także modemy DCMA82 firmy Wistron. Moce nadajników wynoszą przeważnie 100 – 200 mW, nadajnik R52-350 dysponuje mocą 350 mW a DCMA82 – 800 mW.

Jako anteny stosowane są najczęściej fabryczne anteny planarne lub sektorowe o zyskach rzędu 20 – 23 dBi. Z takim wyposażeniem uzyskiwane są zasięgi od kilkudziesięciu do ponad 100 km – przy stosunku sygnału do szumów równym co najmniej 30 dB – a rekordowy odcinek łącza (między Sardynią i Włochami) osiągnął długość 304 km.

Już w okresie planowania sieci wiadomo było, że będzie ona miała dość skomplikowaną i niejednorodną topologię dlatego też jako protokół wyboru tras (ang. *routing*) wybrano protokół BGP („*Border Gateway Protocol*") [18] – opisany szczegółowo w dokumencie RFC 4271. Zapewnia on prawidłowy transport pakietów danych w obie strony między korespondentami i automatycznie uwzględnia zmiany stanu sieci (przykładowo dostępność lub niedostępność poszczególnych odcinków łączy). Mówiąc krótko spełnia on to samo zadanie co protokół Flexnet w klasycznych sieciach Packet-Radio.

Oczywiście dokładna znajomość protokołu BGP i wogóle sposobu konfiguracji stacji węzłowej jest niezbędna tylko operatorom tych stacji. Użytkownicy indywidualni znajdują się w dużo dogodniejszej sytuacji i w najprostszym dla nich przypadku mogą korzystać tylko z dobrze im znanego wyposażenia Packet-Radio albo w zwykły sposób z innych systemów łączności np. przekaźników fonicznych, D-STAR czy Echolinku nie zaprzątając sobie głowy rodzajem łączącej je sieci.

Zasadniczą treść niniejszego skryptu stanowi tłumaczenie instrukcji wykorzystania protokółu BGP w sieci hamnetu napisanej przez austriackich Bernharda Krölla, OE7BKH i Markusa Fankhausera OE7FMI. Oryginał dokumentu w języku niemieckim jest dostępny w witrynie internetowej ÖVSV (*www.oevsv.at*). Skrypt ten jest przeznaczony zasadniczo dla operatorów węzłów sieci hamnetu oraz administratorów i koordynatorów tej sieci.

Dostęp dla stacji indywidualnych.

W zamyśle projektodawców Hamnet ma stanowić rozszerzenie dotychczasowej sieci Packet-Radio i w przyszłości zastąpić ją całkowicie. Dlatego też dotychczasowe stacje dostępowe (węzły) Packet-Radio pozostaną jeszcze przez dłuższy czas w użyciu. Miłośnicy Packet-Radio nie potrzebują więc w najbliższym czasie zmieniać wyposażenia a jedynie w sposób pozytywny odczują wzrost przepustowości łączy. Oczywiście w miarę rozbudowy sieci Hamnetu i uruchamiania wejść mikrofalowych będą mogli korzystać z nich bezpośrednio i to nie tylko w połączeniach Packet-Radio ale i w ramach wszystkich uprzednio wymienionych usług. Korzystanie z takich usług jak dostęp do witryn www czy „*Instant messaging*" wymaga ewentualnej instalacji dodatkowych programów i dokonania ich odpowiedniej konfiguracji.

Dotychczas uruchomione wejścia dla użytkowników pracują przeważnie w paśmie 13 cm ale ponieważ zakres ten jest w wielu rejonach poważnie obciążony pracującymi tam prywatnymi sieciami komputerowymi, kamerami bezprzewodowymi i transmisjami wielu innych urządzeń w przyszłości należy spodziewać się uruchamiania wejść do sieci także w paśmie 6 cm. W niektórych krajach j.np. w Austrii i Szwajcarii amatorskie pasmo 13 cm jest już w znacznym stopniu odebrane krótkofalowcom i w niektórych jego podzakresach nie wolno nawet uruchamiać stacji automatycznych a więc pasmo 6 cm powinno coraz bardziej zyskiwać na znaczeniu.

Wyposażenie stacji indywidualnej korzystającej z dostępu mikrofalowego różni się w znacznym stopniu od opisanego powyżej wyposażenia łączy sieci.

Ogólnie rzecz biorąc możemy rozróżnić dwa rodzaje dostępu do sieci, dostęp bezpośredni i pośredni. W pierwszym przypadku stacje indywidulane (zwane w definicji sieci *Poweruser*) znajdują się w bezpośrednim zasięgu węzła sieci natomiast w drugim (zwane *Meshuser*) korzystają z indywidualnych stacji innych użytkowników pośredniczących w kontakcie z węzłem sieci na zasadzie przemienników cyfrowych (analogicznie jak to było w pierwszym okresie rozwoju sieci AX.25). W tym drugim przypadku sieć lokalna sama uwzględnia zachodzące w jej ramach zmiany: dostępność lub wyłączenie stacji, konieczne dostosowanie tras transmisji danych do zmiennej sytuacji. Wyposażenie stacji indywidualnych w obu przypadkach znacznie się różni między sobą i nie jest wzajemnie kompatybilne.

Jako wyposażenie stacji indywidualnych z grupy pierwszej (mających bezpośredni dostęp do sieci) stosowane są najczęściej punkty dostępowe firmy Ubiquiti: Bullet2 (fot. 7), Bullet M2HP i Nanostation

M2. Zawierają one zarówno sam punkt dostępowy jak i modem bezprzewodowy WLAN a Nanostation posiada również wbudowaną antenę o zysku 10 dBi. Bullet2 i Bullet M2HP wymagają natomiast podłączenia anteny zewnętrznej, co zwiększa swobodę jej wyboru w zależności od warunków lokalnych i pozwala także na korzystanie z anten własnej konstrukcji. Urządzenia powinny być zainstalowane na zewnątrz w pobliżu anteny i są połączone z komputerem za pomocą kabla ethernetowego, który służy również do ich zasilania. Moc wyjściowa nadajników wynosi 16–20 dBm dla modelu Bullet2, 26 dBm dla Nanostation M2 i 28 dBm dla M2HP.

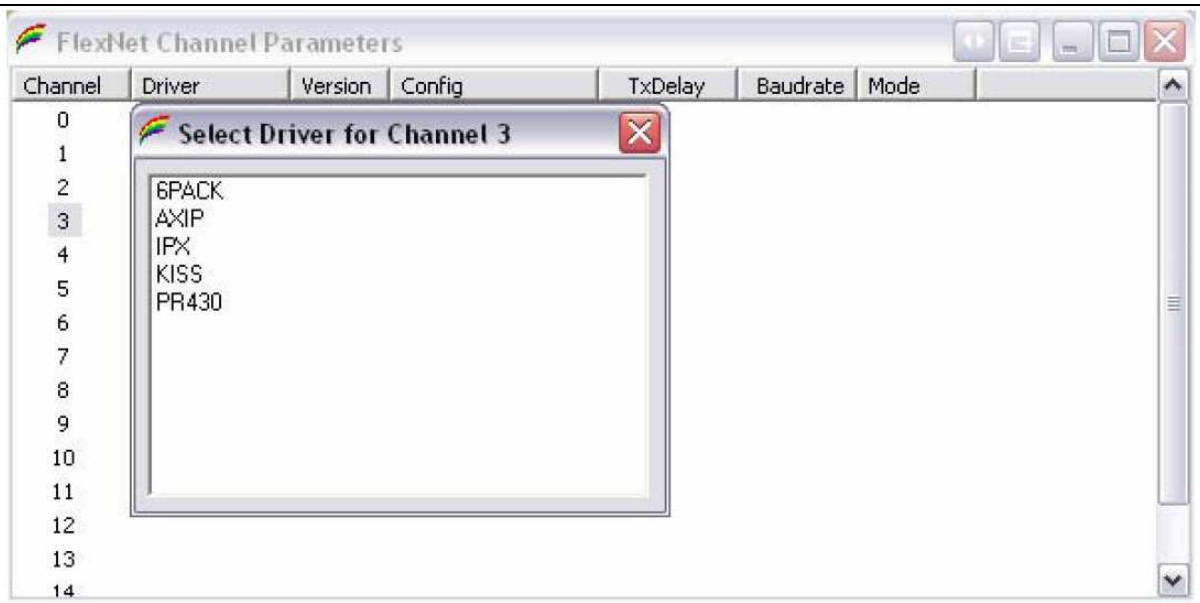
Oprogramowanie wszystkich trzech modeli pozwala na ograniczenie pasma nadawanego sygnału do 5 lub 10 MHz. Są one dostępne zarówno w wersjach 2,4 jak i 5,7 GHz (są to przykładowo modele Bullet M5HP lub Nanostation M5 – z anteną o zysku 13–14 dBi). Oferowany przez firmę Ubiquiti model Nanostation 3 pracujący w zakresie 3,4 – 3,65 GHz może znaleźć zastosowanie w krajach gdzie dostępne jest pasmo 9 cm. Jest on wyposażony w nadajnik o mocy 24 dBm i w antenę o zysku 13 dBi. Przykładowy sposób konfiguracji tego sprzętu zawiera dokument [13].

Wyposażeniem zalecanym dla użytkowników drugiej grupy jest zmodyfikowany punkt dostępowy Linksys WRT54GL (G, GS), ASUS WL500gp lub podobny (rys. 8), na którym można zainstalować oprogramowanie *Openwrt*. Po wymianie kwarcu generatora zegarowego z 20 MHz na 19,6608 MHz zmianie ulegają zarówno szerokość pasma (z 18 na 17,695 MHz dla standardu 802.11g) jak i odstępy podnośnych w kanale (z 200 na 196 kHz) co skutecznie zapobiega kontaktom między siecią amatorską a niezmodyfikowanym wyposażeniem użytkowników zwykłych lokalnych sieci komputerowych. Modyfikacja i konfiguracja sprzętu jest szczegółowo opisana w [11] a niezbędne oprogramowanie jest dostępne pod adresem [12]. Maksymalna użyteczna moc nadajnika WRT54GL wynosi około 170 mW. Nadajnik może wprawdzie dostarczyć większych mocy wyjściowych ale odbywa się to kosztem wzrostu poziomu szumów w nadawanym sygnale co utrudnia jego dekodowanie.

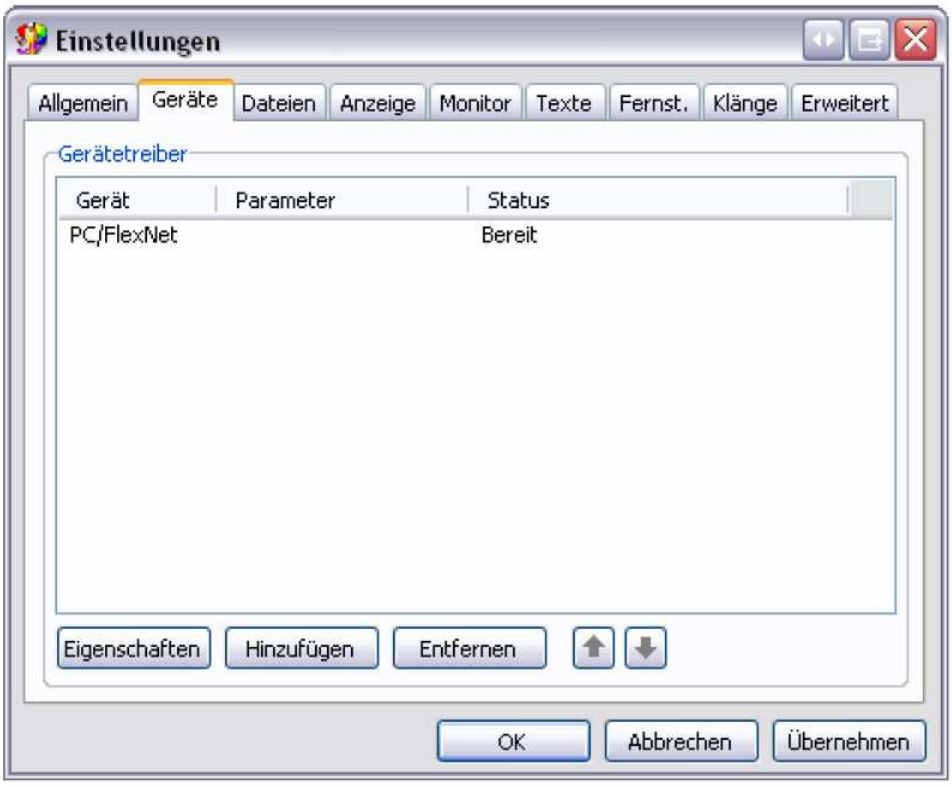
8. Punkt dostępowy Linksys WRT54GL na pasmo 2,4 GFHz

Bezpośrednie wykorzystanie sieci Hamnetu w łącznościach Packet-Radio wymaga zainstalowania Flexnetu [16] służącego jako sterownik sprzętowy oraz programu terminalowego Paxon [17] a następ-

nie skonfigurowanie obu programów [15]. W konfiguracji dla Hamnetu Flexnet pracuje jako sterownik AXIP natomiast Paxon korzysta z niego jako z kanału logicznego (modemu programowego).



9. Konfiguracja Flexnetu – wybór sterownika AXIP



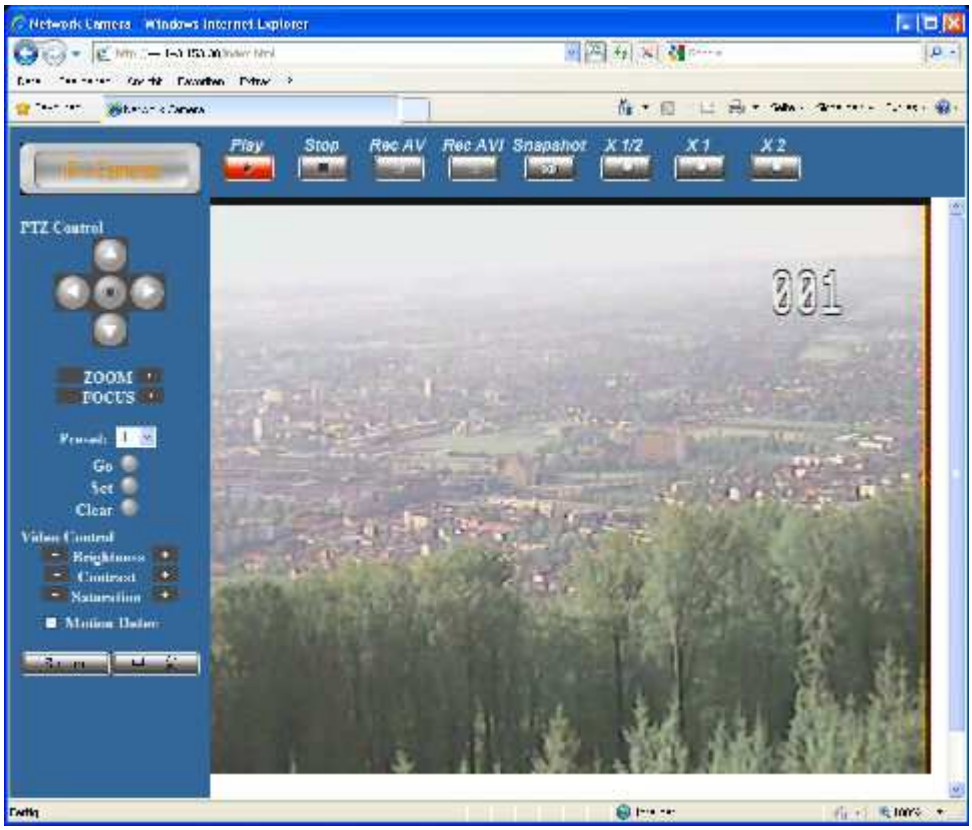
10. Konfiguracja Paxonu tak aby korzystał z Flexnetu

Przykładowa konstrukcja węzła sieci

Poniższa ilustracja przedstawia przykładowe minimalne wyposażenie węzła sieci z dwoma kanałami radiowymi.

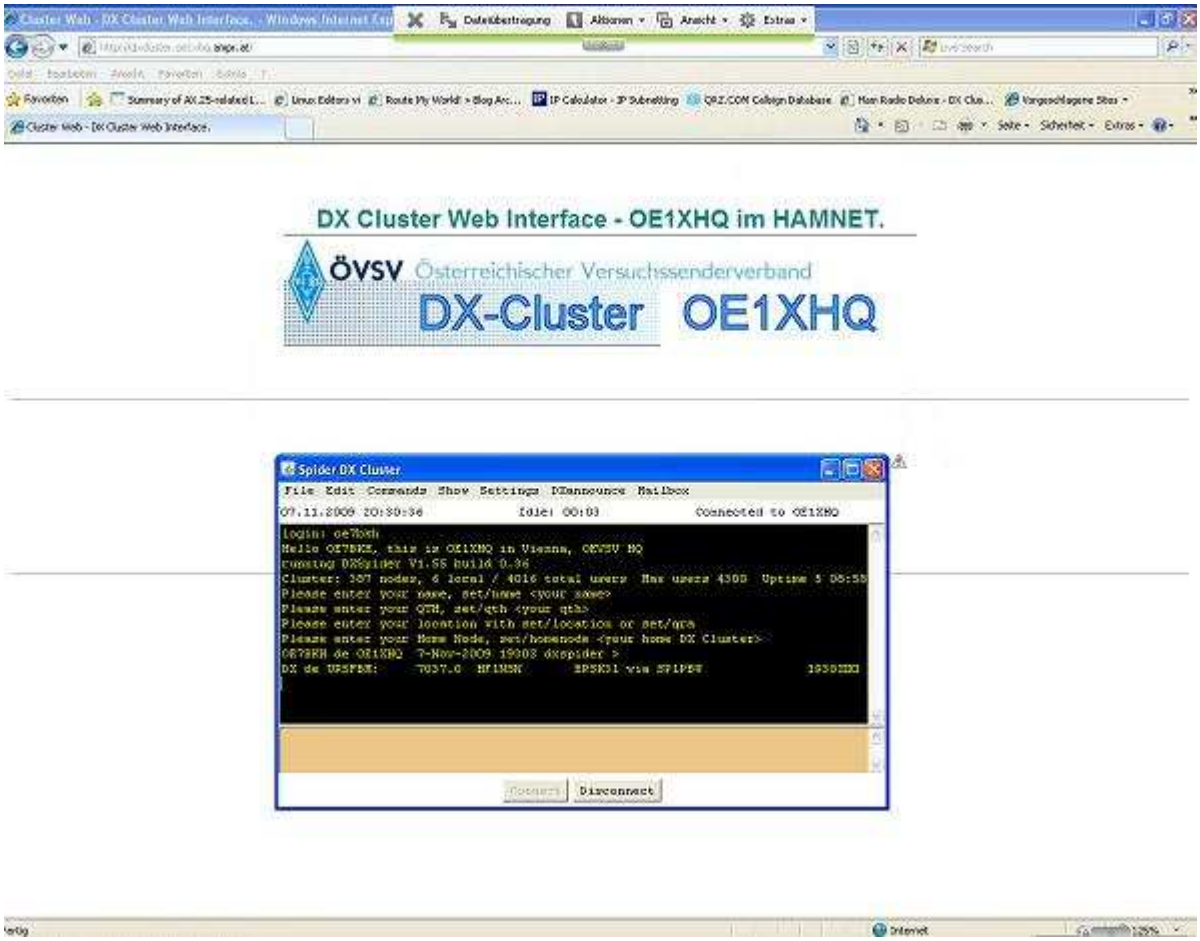
W skład wyposażenia wchodzą 1 egz. stacji bazowej „Mikrotik RB433AH“ (lub podobny model; **A**), 2 modemy radiowe „Wistron“ DCMA-82 (**B**) miniPCI, dwa kable antenowe (**C**), dwie anteny planarne (**D**) na pasmo 5 GHz, zasilacz (**E**) i ewentualnie kabel CAT6 SFTP (**F**).

Przykłady wykorzystania Hamnetu (dostępnych usług)

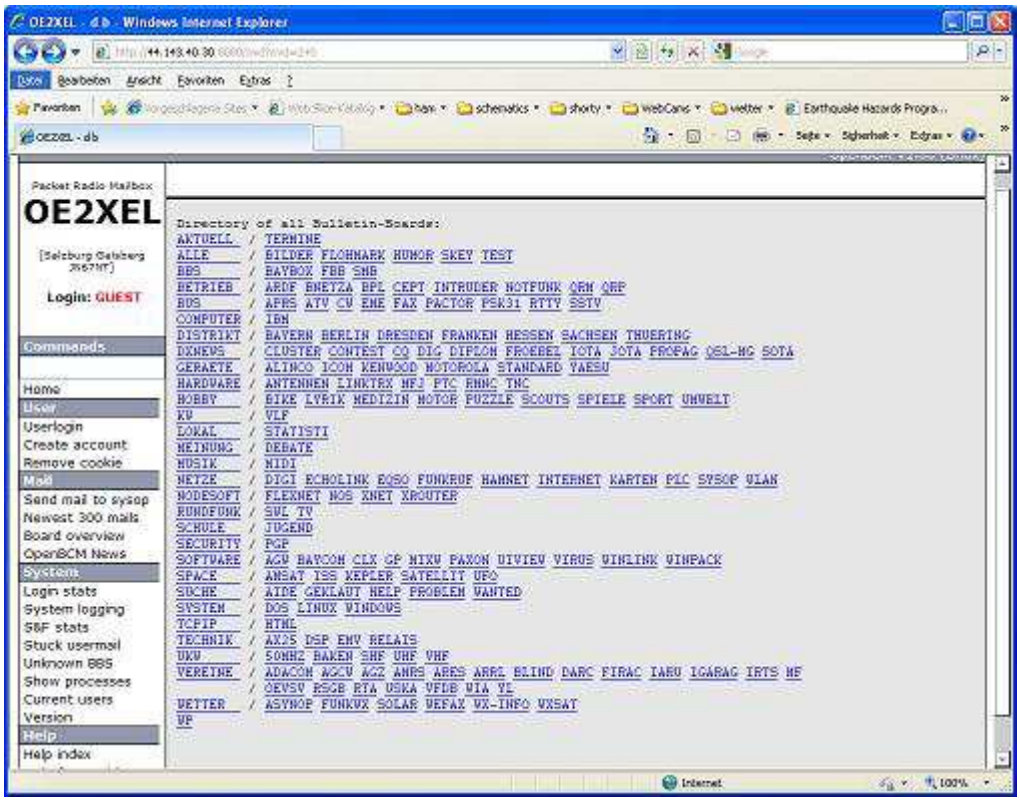


Okno stacji ATV OE6XRR

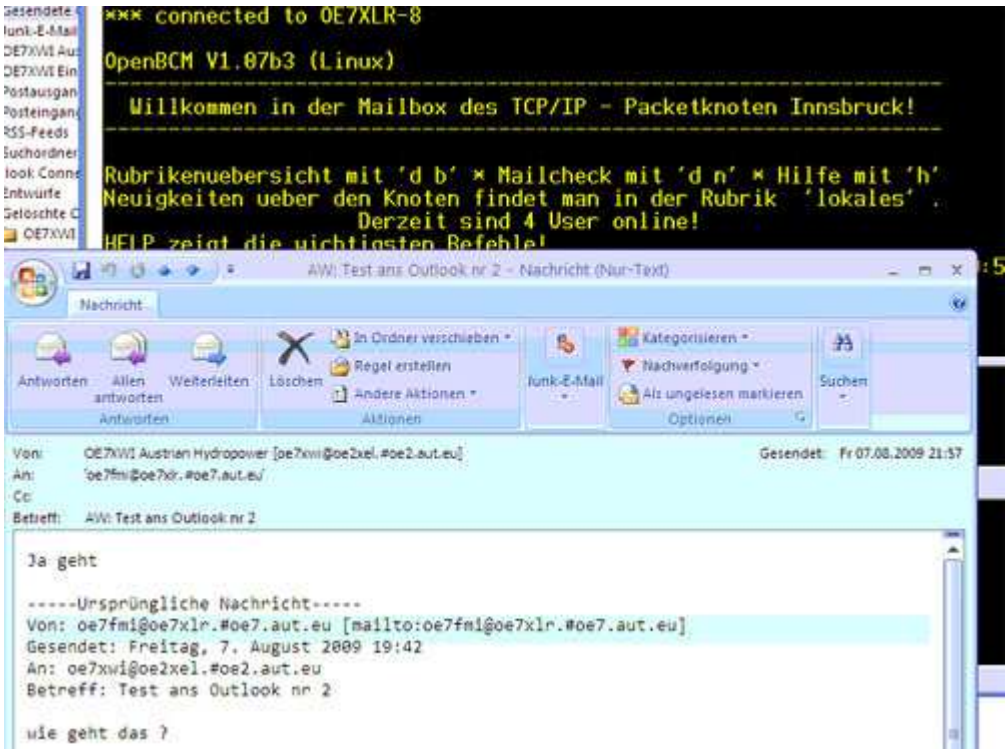
Serwer UI-View dla APRS w Hamnecie



DX-Cluster OE1XHQ



Dostęp do skrzynki elektronicznej Packet radio



Dostęp do poczty elektronicznej

Standardy IEEE 802.11

Standard 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 miedzy soba. W zależności od jakości połączenia (stopy błędów) wybierana jest automatycznie mniejsza lub większa szybkość transmisji. Stosowaną modulacja jest OFDM.
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 sybkości 22 i 44 MBit/s. W tym trybie stosowane jest rozpraszanie widma z kluczowaniem fazy (DSSS).

Standard IEEE 802.11a

Standardowo stosowane są szybkości transmisji 6, 9, 12, 18, 24, 36, 48 i 54 Mbit/s a praca odbywa się w paśmie 6 cm. 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.

Standard 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 jed dodatkowo zależnie od warunków transmisji kluczowana fazowo 2-PSK albo 4-PSK lun anmplitudowo-fazowo 16-QAM albo 64-QAM.

Domena adresowa

Austriacka sieć Hamnetu należy do domeny ampr.at.
W zależności od rodzaju usług i zastosowań występują w niej (lub są przewidziane na przyszłość) przykładowo takie adresy jak:

- ns7.ampr.at – serwer DNS w okręgu 7,
- web.oe2xyz.ampr.at – serwer HTTP w okręgu 2,
- aprs.oe7xgr.ampr.at – serwer APRS na OE7XGR,
- video.oe5xyz.ampr.at – serwer wizyjny np. kamera internetowa,
- video-ctrl.oe5xyz.ampr.at – sterowanie kamerą,
- atv.oe4xyz.ampr.at – serwer telewizji amatoprskiej ATV,
- ax25.oe7xgr.ampr.at – dostęp AX.25 – AXUDP na OE7XGR,
- prbox.oe2xel.ampr.at – skrzynka elektroniczna packet radio na OE2XEL; także dostęp do poczty elektronicznej przez SMTP/POP,
- pcsag.oe6xyz.ampr.at – serwer przywoławczy POCSAG,
- echolink.oe1xyz.ampr.at – serwer echolinkowy,
- d-star.oe3xyz.ampr.at – D-STAR,
- winlink.oe3xyz.ampr.at – bramka Winlinku,
- ntp.oe6xyz.ampr.at – serwer czasu,
- wetter.oe6xyz.ampr.at – serwer meteorologiczny; jeżeli posiada własną witrynę HTTP – web.wetter.oe6xyz.ampr.at,
- wiki.oe6xaa.ampr.at – serwer amatorskiej wikipedii,
- mail.ampr.at – ogolnokrajowy serwer poczty elektronicznej.

Numery AS

Numery systemów autonomicznych (AS) w Austrii – regionalnych sieci Hamnetu – wymienione są w tłumaczonej instrukcji.
Poniżej podano zakresy numerów używane w różnych krajach lub dla nich zarezerwowane:

- Belgia: 64778 – 64788,
- Chorwacja: 64686 – 64690,
- Francja: 64742 – 64777,
- Hiszpania: 64708 – 64719,
- Holandia: 64691 – 64694,
- Liechtenstein: 64740 – 64741,
- Luksemburg: 64684 – 64685,
- Niemcy: 64620 – 64683,
- Polska: 64800 – 64839,
- Słowenia: 64695 – 64704,
- Szwajcaria: 64720–64739,
- Turcja: 64789 – 64799,
- Węgry: 64705 – 64707,
- Włochy: 64600 – 64619.

Do celów próbnych zarezerwowany jest zakres 64510 – 64539.

Dostęp przez VPN

Dla umożliwienia użytkownikom nie mającym w dostatecznie bliskiej odległości radiowego punktu dostępowego do Hamnetu a pragnących się wstępnie zapoznać z jego możliwościami przewidziano kilka próbnych wejść internetowych przez VPN.
Internetowymi adresami dostępowymi w chwili opracowywania niniejszego skryptu są:

- www.db0tv.de – DB0TV w Wuppertalu,
- www.dm0ha.de – w Hagen,
- db0fhn.efi.fh-nuernberg.de – w Norymberdze i
- www.db0res.de – DB0RES w Rees.

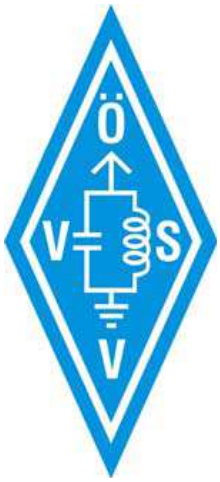
Skoryzstanie z dostępu do Hamnetu w ten sposób wymaga skonfugurowania połączenia VPN. Po uzyskaniu połączenia z jedną z wymienionych stacji komputer PC otrzymuje dynamicznie na czas sesji adres z domeny ampr (44.x.x.x) co pozwala mu na dostęp do adresów Hamnetowych w rodzaju db0tv.ampr.org, db0tv.ampr.org/wxnet, yacy.db0fhw.ampr.org, hambook.de.ampr.org, www.oe2xzr.ampr.at, 44.143.100.25:10080/weather itd. i uruchomionych tam usług.
Aktywne uczestnictwo w forach (np. hambook) itp. wymaga rejestracji z podaniem nazwiaska, adresu poczty elektronicznej i znaku wywoławczego.
Sposób uruchomienia połączenia VPN podano w literaturze poświęconej używanemu systemowi operacyjnemu.

Krzysztof Dąbrowski OE1KDA
Wiedeń
Grudzień 2013

Zastosowanie protokółu BGP w sieci Hamnetu

Wprowadzenie
Zasady
Przykładowe konfiguracje

Autorzy: Bernhard Kröll, OE7BKH
i Markus Fankhauser OE7FMI.



Tłumaczył Krzysztof Dąbrowski
OE1KDA

Spis treści

1 Wstęp

Dokument niniejszy opisuje metody wyboru tras transmisji (ang. *routing*) w amatorskiej sieci Hamnetu (**H**ighspeed **Am**ateur Radio **Net**work) i jej cyfrowej sieci szkieletowej (niem. *Digitale Backbone*).
Sieć Hamnetu stanowi połączenie dawnych i nowych technologii krótkofalarskich i łączności radiowej oraz protokółów transmisji danych. Jest ona siecią cyfrową pozwalającą na równoległe korzystanie z wielu usług i systemów. Zaliczają się do nich transmisje Packet-Radio, rozpowszechnianie komunikatów APRS z miejsc lokalizacji infrastruktury sieci, zdalny dostęp do odbiorników i radiostacji amatorskich, dostęp do własnych serwerów http, łącza telewizyjne (ATV) i wiele innych.
Hamnet stanowi niezależną od internetu sieć krótkofalarską składającą się z mikrofalowych łączy radiowych, radiowych punktów dostępu dla użytkowników oraz lokalnych łączy udestepniających poszczególne usługi.
Rozbudowa infrastruktury sieci i jej połączeń z poszczególnymi usługami rozpoczęła się [w Austrii – przyp. tłum.] w roku 2009. Sieć stanowi skomplikowaną strukturę opartą na szeregu szybkich łączy radiowych (sieci szkieletowej, ang. *backbone*) pomiędzy jej poszczególnymi węzłami.


HAMNET-stacja OE7XGR (łącza sieci szkieletowej)

Analogicznie jak w sieci Packet-Radio nadawane pakiety danych muszą niezawodnie dotrzeć do celu. W sieci Hamnetu spotykane są skomplikowane struktury mieszane (pierścieniowa, gwiazdowa), i należy uwzględnić ten fakt w trakcie planowania sieci pamiętając, że podobnie jak w sieci Packet-Radio konieczny jest dopasowany do potrzeb algorytm wyboru tras (ang. *routing*).
Przed dotarciem do ostatecznego celu pakiety muszą przebyć szereg odcinków trasy (ang. *hop*) i to naprzemian w obu kierunkach (łączność dupleksowa). Prawidłowe funkcjonowanie usług wymaga aby znalazły one potrzebne trasy transmisji w sieci.
Administracja tras transmisji przez operatorów jest praktycznie niemożliwa w dużych sieciach wymagających szybkiej reakcji na częste zmiany stanu i obciążenia łączy oraz dostępności adresatów.
W praktyce można ją przeprowadzać tylko automatyczne. W popularnej do niedawna sieci Packet-Radio zapewniał to m.in. protokół Flexnet.
Na podstawie zdobytych dotąd doświadczeń dla sieci Hamnetu został wybrany protokół BGP („*Border Gateway Protocol*“).
Następne rozdziały przedstawiają wstępnie i dokładnie ten właśnie algorytm wyboru tras wraz z przykładami konfiguracji węzłów sieci szkieletowej.
Instrukcja ta została uzupełniona o materiały dostępne w Internecie po ich częściowym dostosowaniu do specyfiki sieci Hamnetu.

Podane dalej przykłady konfiguracji i zalecenia są wynikiem doświadczeń praktycznych przeprowadzonych przez OE7BKH und OE7FMI.

OE7BKH Bernhard Kröll, OE7FMI Markus Fankhauser
Mayrhofen w Zillertal, maj 2009

2 Wprowadzenie ogólne do BGP

Rozdział ten jest poświęcony podstawom i zasadniczym definicjom związanym z wyborem tras i protokółem BGP.

2.1 Wybór tras

Do wyboru tras transmisji danych w dużych rozbudowanych sieciach konieczne jest zastosowanie automatycznego algorytmu wyboru tras (ang. *routing*). W sieciach pakietowych j.np. AX25 (Packet Radio) albo TCP/IP (Hamnet) należy przy tym rozróżnić procesy wyboru tras (ang. *routing*) i retransmisji pakietów (ang. *forwarding*). Pierwszy z nich decyduje o trasie transmisji danych w sieci, a drugi dotyczy autonomicznego podejmowania przez każdy z węzłów sieci decyzji o tym, do którego partenrów (sąsiadów) zostanie skierowana bieżąca wiadomość.
Oba te procesy są jednak często traktowane wspólnie i określane wspólną nazwą wyboru tras. Oznacza to wówczas zarówno wyszukiwanie tras transmisji jak i samą retransmisję danych w sieci.
Protokół IP („*Internet Protocol*“) jest obecnie najbardziej rozpowszechnionym rozwiązaniem tego typu i znalazł on również zastosowanie w sieci Hamnetu. Do jego najważniejszych zalet należy zdolność do do transmisji danych w dowolnych łączach fizycznych i systemach transmisji. Jego elastyczność jest jednak do pewnego stopnia przyćmiona przez stopień komplikacji w wyszukiwaniu tras transmisji (ang. *routing*) od nadawcy do adresata i z powrotem.

2.2 Bramki sieci

Określenie bramki sieci (ang. *router*) dotyczy urządzeń lub komputerów pośredniczących w wymianie danych pomiędzy różnymi sieciami komputerowymi. Bramki analizują adresy docelowe otrzymanych pakietów danych i w zależności od zaprogramowanych zasad pracy przekazują je odpowiednio dalej lub blokują dalszą retransmisję. Retransmitowane pakiety danych są przekazywane albo do znanej bramce sieci docelowej albo do sąsiedniej (w sensie sieciowym, logicznym) bramki. Dla zapewnienia sprawnej retransmisji bramki wymieniają między sobą dane tras korzystając z odpowiednich protokołów.

Bramka firmy „Mikrotik“ (RB433) używana w sieci szkieletowej Hanmetu

Płytki bramek z serii 600 firmy „Mikrotik“ wraz z modułami radiowymi zastosowane w bramce OE7XGX na *Hintertuxer Gletscher* na wysokości 3200 m n.p.m.

Wydajne bramki dla sieci firmowych albo połączeń z siecią szkieletową Internetu

2.3 Protokóły wyboru tras

Zadaniem protokółów wyboru tras jest wymiana informacji pomiędzy sieciami lub bramkami. Umożliwiają one złożenie i aktualizowanie przez bramki dynamicznych tabel tras zapewniających prawidłowe dotarcie do celu wszystkich otrzymanych danych. Protokóły wyboru tras uzupełniają dokonane ręcznie wpisy do tabel lub też zastępują je w zależności od sytuacji. Protokóły te i bramki sieci odpowiadają poziomowi warstwy 3 modelu ISO. Umiejscowionej poniżej warstwie 2 odpowiadają komutatory (and. *switch*) pakietów, w sieci amatorskiej występujące także wpod nazwą przekaźników cyfrowych (ang. *digipeater*). Wszystkie węzły sieci Hamnetu zawierają oprócz sprzętu radiowego także wy-

posażenie bramek sieci. Poniżej wymeniono kilka przykładów protokółów sieciowych warstwy 3 (protokółów wyboru tras):

Packet Radio

Protokół FLEXNET
Stanowi uzupełnienie protokółu AX.25 dla sieci Packet-Radio i jest stosowany zwłaszcza przez przekaźniki RMNC i podobne. Oprogramowanie węzła XNET (np. DLC7, Linksys dla openwrt) może również korzystać z Flexnetu.

Sieci IP

OSPF
Protokół OSPF jest dynamicznym protokółem wyboru tras w ramach systemów autonomicznych i w większości przypadków zastąpił RIP. Do oceny łączy OSPF korzysta z ich umownych „kosztów" a w przypadku równych „kosztów" może rozkładać obciążenie na poszczególne trasy.
RIP:
Protokół RIP – *Routing Information Protocol* – jest oparty o algorytm odstępu wektorowego w ramach systemu autonomicznego. Jest on wykorzystywany do dynamicznego tworzenia tabel tras w bramkach. Korzystają z niago protokóły IP i IPX.
OLSR:
OLSR jest zoptymalizowanym protokołem stanu łączy (niem. *Optimiertes Link-State-Routingprotokoll*) dostosowanym do potrzeb połączeń ad-hoc w sieciach mobilnych ale bywa stosowany także i w innych typach sieci.
BGP"
Protokół BGP – *Border Gateway Protocol* – definiuje sposób wymiany przez bramki informacji o dostępności łączy pomiędzy sieciami systemów autonomicznych (oznacznych dalej także skrótem AS). Znajduje on też zastosowanie w ramach systemów autonomicznych albo jako protokół nadrzędny dla OSPF.

2.4 Tabele tras

Tabela tras (ang. *routing table*; niem. *Routingtabelle*) jest konstrukcją znajdującą się w pamięci bramki lub komputera sieciowego. Zawiera ona trasy prowadzące do ustalonych sieci docelowych lub partnerów w sieciach. Zapisy te stanowią podstawę do rozstrzygnięć o kierunku nadania otrzymanego pakietu danych. Pakiet ten może być retransmitowany przez większą liczbę bramek (stacji).
Tabele tras mogą zawierać zarówno informacje wprowadzone ręcznie jak i automatycznie. Informacje o zakłóceniach na łączach lub zmianach w strukturze sieci muszą być wprowadzone automatycznie w dostatecznie krótkich odstępach czasu.
Również węzły Packet-Radio korzystają z tabeli tras wywoływanej przez użytkowników, najczęściej za pomocą polecenia „d" („*destinations*").
=>d db0
DB0OFG 0-0 7 DB0OFI 0-12 71 DB0PRT 0-15 5 DB0RTP 0-0 12
DB0SAU 0-12 7 DB0XSR 0-0 30
Powyższy przykład jest fragmentem tabeli tras węzła RMNC albo XNET utworzonej i aktualizowanej przez protokół Flexnet.

Kolejność analizy pakietów w protokóle IP (np. w sieci Hamnetu):

- W pierwszym rzędzie bramka (stacja) sprawdza czy pakiet jest dla niej przeznaczony. Pakiety o adresie docelowym identycznym z własnym są odpowiednio dalej przetwarzane (w sieci lokalnej, w tabeli ARP lub w rozgłaszaniu IP), jako że osiągnęły swój cel.
- W przypadku niezgodności adresów sprawdzane jest czy jest on przeznaczony dla jednej z bezpośrednio osiągalnych sieci (lokalnych). Adres docelowy jest wówczas kombinowany z maską sieci (lokalnej; podsieci). Pozostała część adresu pozwala na stwierdzenie czy jest on przezna-

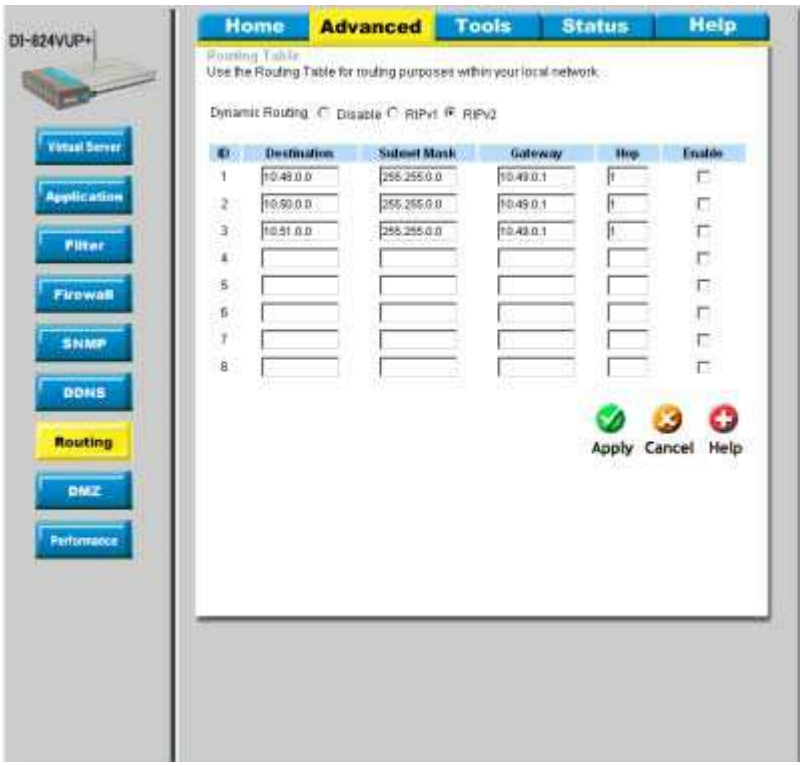
czony dla własnej sieci. Jeżeli tak, to w zależności od jej topologii jest on kierowany do odpowiedniej podsieci lub kasowany.

- Dopiero w trzeciej kolejności (po stwierdzeniu, że nie jest on przeznaczony dla bezpośrednio osiągalnej części sieci) bramka sprawdza, czy znana jest jej trasa prowadząca do adresata. W części przypadków trasy prowadzące do konkretnych adresów IP są zawarte w tabeli tras. Pakiety są wówczas kierowane dalej zgodnie z zawartością tabeli.
- Kolejny czwarty przypadek zachodzi gdy tabela tras nie zawiera trasy do danego celu. Bramka sprawdza wówczas czy istnieje wpis dla bramki lub trasy domyślnej – przewidzianej na takie przypadki. Bramka domyślna rozdziela otrzymane pakiety na swoje poszczególne wyjścia zgodnie z wpisami w swojej tabeli tras i zaprogramowanymi w niej zasadami.
- Brak wariantu domyślnego – niemożność dostarczenia danych do adresata – powoduje skasowanie pakietu danych.

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.10.1.1    10.10.1.100      20
          0.0.0.0          0.0.0.0     10.15.100.1   10.15.101.96      25
       10.10.1.0    255.255.255.0     10.10.1.100    10.10.1.100      20
     10.10.1.100  255.255.255.255       127.0.0.1      127.0.0.1      20
       10.10.2.0    255.255.255.0       10.10.1.1    10.10.1.100       1
       10.10.3.0    255.255.255.0       10.10.1.1    10.10.1.100       1
       10.10.4.0    255.255.255.0       10.10.1.1    10.10.1.100       1
       10.15.0.0      255.255.0.0    10.15.101.96   10.15.101.96      25
    10.15.101.96  255.255.255.255       127.0.0.1      127.0.0.1      25
  10.255.255.255  255.255.255.255     10.10.1.100    10.10.1.100      20
  10.255.255.255  255.255.255.255    10.15.101.96   10.15.101.96      25
       127.0.0.0        255.0.0.0       127.0.0.1      127.0.0.1       1
       224.0.0.0        240.0.0.0     10.10.1.100    10.10.1.100      20
       224.0.0.0        240.0.0.0    10.15.101.96   10.15.101.96      25
  255.255.255.255  255.255.255.255     10.10.1.100    10.10.1.100       1
  255.255.255.255  255.255.255.255    10.15.101.96   10.15.101.96       1
Default Gateway:       10.15.100.1
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
       10.10.2.0    255.255.255.0       10.10.1.1       1
       10.10.3.0    255.255.255.0       10.10.1.1       1
       10.10.4.0    255.255.255.0       10.10.1.1       1

C:\>_
```

Tabela tras wywołana za pomocą polecenia *netstat –r* w oknie konsoli w środowisku Windows



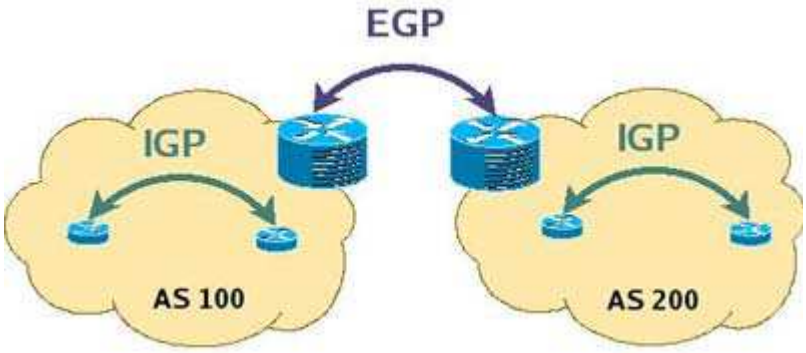
Ręczne wprowadzanie tras w domowej bramce dostępowej

2.5 System autonomiczny

System autonomiczny („AS“) jest siecią lub grupą sieci znajdujących się pod wspólną administracją i stosujących te same zasady wyboru tras (ang. *routing policy*). Podstawę systemu autonomicznego stanowią połączone weń komputery.
W Hamnecie austriackim każdy z krajów związkowych (ogolnie rzecz biorąc rejonów administracyjnych lub okręgów – przyp. tłum.) stanowi oddzielny system autonomiczny – a więc na terytorium Austrii istnieje 9 takich systemów.

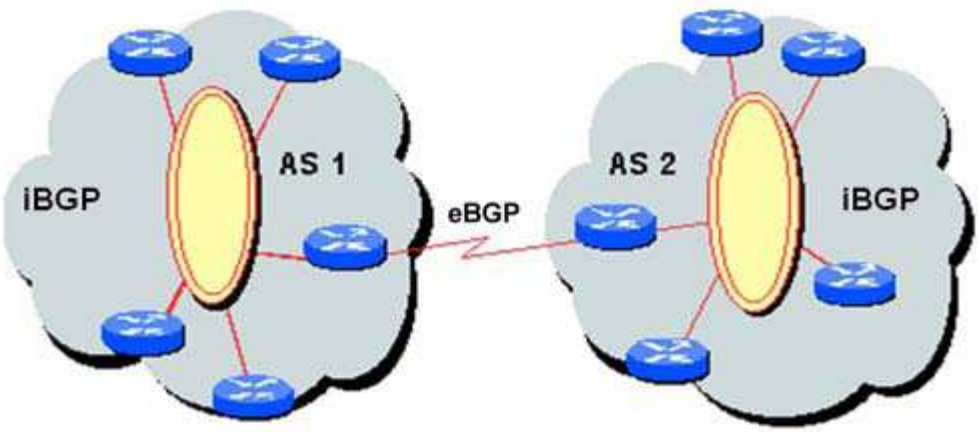
2.6 Trasy w ramach systemu autonomicznego / pomiędzy różnymi systemami

System autonomiczny składa się więc z pewnej liczby wspólnie zarządzanych bramek i przeważnie stosują one ten sam protokół IGP do wyboru tras. Systemy autonomiczne są natomiast połączone między sobą przy użyciu protokółu EGP.



IGP:
Protokóły stosowane wewnątrz sytemu autonomicznego (ang. „*Intra-AS-Routing*“) są również określane skrótem IGP (ang. „*Interior Gateway Protocol*“). Ich przykładami są *Routing Information Protocol* (RIP), *Open Shortest Path First Protocol* (OSPF) i *Intra Domain Intermediate System to Intermediate System Routing Protocol* (IS-IS).

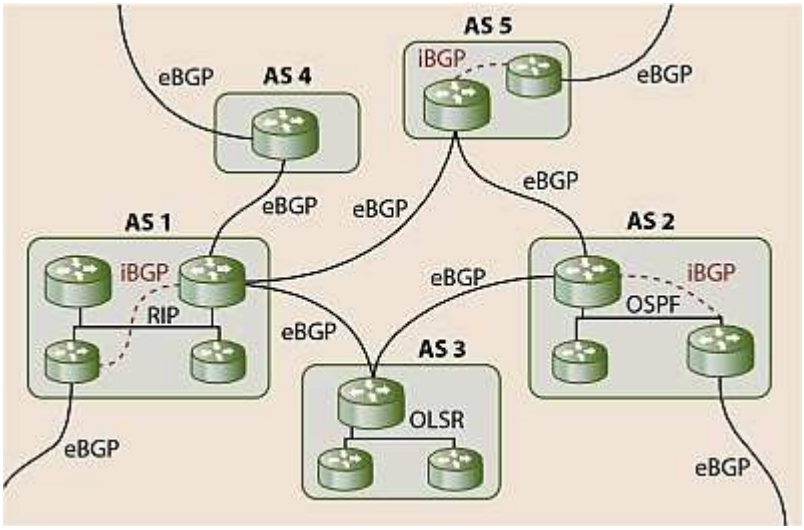
EGP:
Protokóły stosowane w transmisji między systemami autonomicznymi (ang. „*Inter-AS-Routing*“) noszą również nazwę EGP (ang. „*Exterior Gateway Protocol*“). Jedynym obecnie używanym w skali światowej protokółem z tej grupy jest *Border Gateway Protocol* (BGP). Protokół BGP (przeważnie występujący pod nazwą eBGP) wprowadza wybór tras oparty na z góry określonych zasadach.
Może on być także używany wewnątrz systemu autonomicznego a więc jako IGP. Zwykle stosowany jest po to aby otrzymane z zewnątrz (czyli przez eBGP) trasy udostępnić pozostałym bramkom wchodzącym w skład własnego systemu autonomicznego (upublicznić trasy). Mówimy wówczas o wewnętrznym BGP (iBGP). Rozróżnia się więc protokóły eBGP i iBGP.



Dwa systemy autonomiczne – iBGP jako „*Interior*-“ i eBGP jako „*Exterior Gateway Protocol*“

2.7 Protokół BGP („*Border Gateway Protocol*“) w cyfrowej sieci szkieletowej

Po przeprowadzeniu analizy przydziału adresów IP (podziału sieci szkieletowej na segmenty) oraz topologii sieci zdecydowano się na użycie w Hamniecie protokółu BGP zamiast OSPF.
BGP jest protokółem wyboru tras w sieciach IP. Do wymiany informacji służbowych wykorzystuje on protokół TCP. Informacje rozpowszechniane w ten sposób zawierają wszystkie występujące na trasie systemy autonomiczne („AS“) zamiast dokładnych adresów sieciowych bramek. Pozwalają one na śledzenie trasy pakietów bez konieczności wymiany nadmiernej ilości danych. Rozpowszechniane są jedynie informacje o trasie, którą wybrałby dany system autonomiczny.
Wymiana informacji między bramkami dokonuje się w ramach **sesji BGP**. Zawierają one kompletną trasę transmisji między systemami autonomicznymi. Na ich podstawie protokół wykreśla graf połączeń sieciowych pomiędzy systemami i zapobiega powstawaniu pętli transmisji.
Aktualizacja tras w oparciu o łączność z innymi systemami BGP odbywa się w ramach **sesji BGP**.
Ocena wartości tras, z której korzysta BGP, opiera się na danych wprowadzonych przez operatora w konfiguracji oraz na parametrach fizycznych i technicznych danego łącza.
W związku z tym, że każda z bramek BGP dysponuje danymi otrzymanymi od innych, a zwłaszcza od bramek sąsiadujących rozbudowuje ona sobie bazę danych o trasach prowadzących do wszystkich osiągalnych systemów autonomicznych.



Przykład wykorzystania BGP, możliwy także we współpracy z innimi oprotokółami IGP jak RIP, OSPF albo OLSR

Protokół BGP w obecnie używanej wersji 4 zawierającej również algorytm CIDR („*Classless Inter-Domain Routing*“) jest szczegółowo opisany w dokumencie RFC 4271. Może on współpracować również z OSPF.
Podstawowa zasada:
Protokół **eBGP** reguluje wymianę informacji o trasach transmisji pomiędzy bramkami **znajdującymi się w różnych systemach autonomicznych**.
Protokół **iBGP** reguluje wymianę informacji pomiędzy bramkami **należącymi do tego samego systemu autonomicznego**.

2.8 Różnice w pracy iBGP i eBGP

Rodzaj i treść wymienianych informacji o trasach są w obu protokółach (iBGP i eBGP) identyczne. Istotne różnice między nimi występują dopiero w upowszechnianu tych danych:

iBGP:
Informacje o sieci docelowej otrzymane od innej bramki iBGP nie są dalej rozpowszechniane wśród bramek iBGP.

Oznacza to, że trasa poznana przez iBGP nie jest rozpowszechniana dalej przez iBGP. Trasa iBGP jest używana dopiero gdy w IGP znana jest trasa do następnego odcinka (ang. „*hop*“). Zapobiega to powstawaniu pętli retransmisji.

eBGP:
W eBGP publikowane są również trasy poznane przez iBGP.
Sieć docelowa poznana przez bramkę w ramach sesji iBGP jest upubliczniana także wśród sąsiednich bramek eBGP.

Zasada:
Protokół eBGP jest używany w kontaktach pomiędzy systemami autonomicznymi. Protokół iBGP jest natomiast używany wewnątrz tych systemów autonomicznych. .
Zarówno w eBGP jak i w iBGP wymiana informacji odbywa się pomiędzy bramkami BGP kontaktującymi się między sobą w ramach **sesji BGP**.
Bramki mogące posługiwać się nadawczo i odbiorczo protokółem BGP i odpowiednio skonfigurowane do korzystania z niego nazywane są **„nadawcami BGP“** (ang. „*BGP-speaker*“).
Przy użyciu protokółu iBGP upubliczniane są w ramach własnego systemu autonomicznego informacje o celach zarówno wewnętrznych jak i na zewnętrznych.
Przy użyciu protokółu eBGP informacje o celach wewnętrznych i zewnętrznych są przekazywane do sąsiednich systemów autonomicznych. System sąsiedni przekazuje je z kolei dalej swoim sąsiadom.
W ten sposób dzięki współpracy obu protokółów możliwa jest szybka wymiana informacji o trasach w ramach bardzo dużych sieci.

2.9 Numery AS w BGP

Każdemu z systemów autonomicznych jest przypisany jednoznaczny numer tzw. numer AS leżący w zakresie od 0 do 65536 (16-bitowe liczby całkowite). Publiczne numery AS (ASN) leżą w podzakresie 1 – 64511.
Adresy prywatne używane wyłącznie w ramach danej organizacji leżą w podzakresie 64512 – 65535.
Do chwili obecnej w internecie zostało przyznanych ponad 37000 numerów. W związku z szybkim wzrostem zapotrzebowania planowane jest wprowadzenie w następnej wersji BGP adresów 32-bitowych.

Zasada: w Hamnecie wykorzystywane są wyłącznie prywatne numery AS nie wymagające przydziałów i koordynacji z zewnątrz..

Numer AS podawany jest przykładowo w konfiguracji punktu dostępowego (bramki) Mikrotik stosowanego powszechnie w Hamnecie i przyporządkowuje on w ten sposób jednoznacznie sprzęt do danego systemu autonomicznego. W Austrii oznacza to przyporządkowanie do sieci danego kraju związkowego:

OE1 64512 (-64519),
OE2 64520 (–64529),
OE3 64530 (–64539),
OE4 64540 (-64549),
OE5 64550 (-64559),
OE6 64560 (-64569),
OE7 64570 (-64579),
OE8 64580 (-64589),
OE9 64590 (-64599).

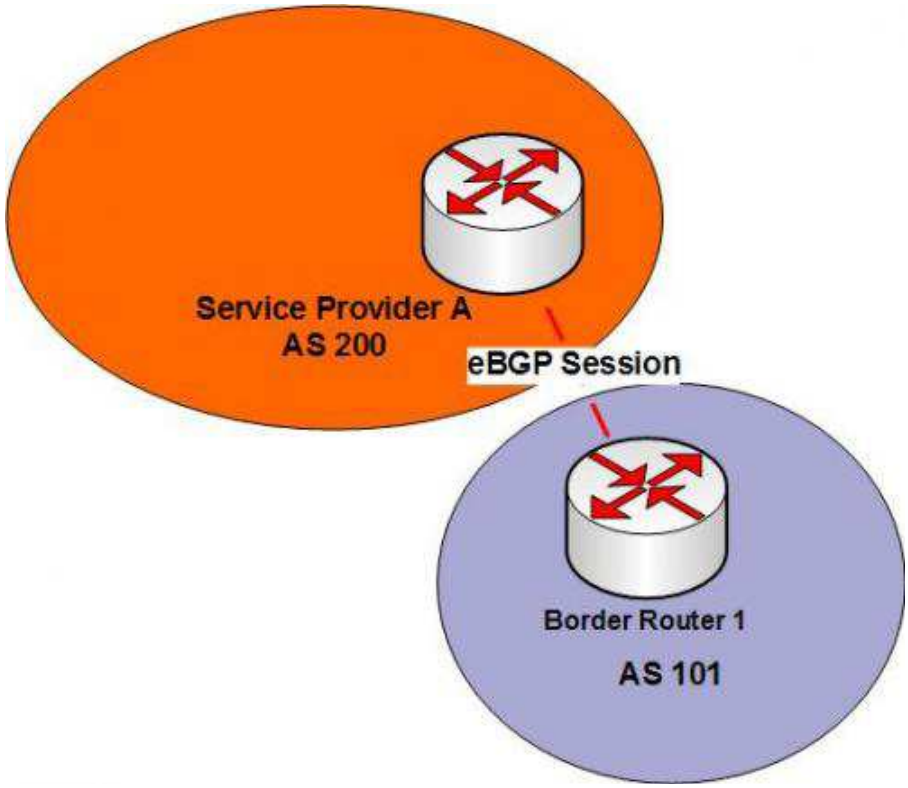
Zakresy obecnie nieużywane leżące pomiędzy numerami głównymi służą do prób i doświadczeń.

2.10 Sesja BGP
(sesja między równoważnymi partnerami, ang. *peer*)

2.10.1 Wyjaśnienie

W odróżnieniu od innych protokółów sieciowych (wyboru tras) rozgłaszających (ang. *broadcast*) swoje dane w sieciach lokalnych BGP korzysta z tzw. sesji BGP.
Są to sesje korzystające z kanału logicznego (ang. *port*) TCP o numerze 179. W ich ramach następuje wymiana informacji pomiędzy dwoma uczestniczącymi w niej bramkami (partnerami).
Dane tras i sieci znanych bramce A są w ramach sesji udostępniane bramce B i odwrotnie. W sesji uczestniczą zawsze dwie bramki posługujące się protokółem BGP.
Wraz ze zwiększaniem się liczby nadawców BGP konieczne jest skonfigurowanie większej liczby sesji.
Obie uczestniczące w sesji bramki są nazywane sąsiadami BGP (niem. *BGP-Nachbar*, ang. *BGP-Neigbour* lub *BGP-Peer*).
W oparciu o informacje otrzymywane w ramach sesji każda z bramek uzupełnia i aktualizuje swoją tabelę tras i na jej podstawie rozstrzyga o trasach retransmitowanych pakietów. W ogólności pakiety mogą w drodze od nadawcy do adresata przechodzić przez wiele bramek.

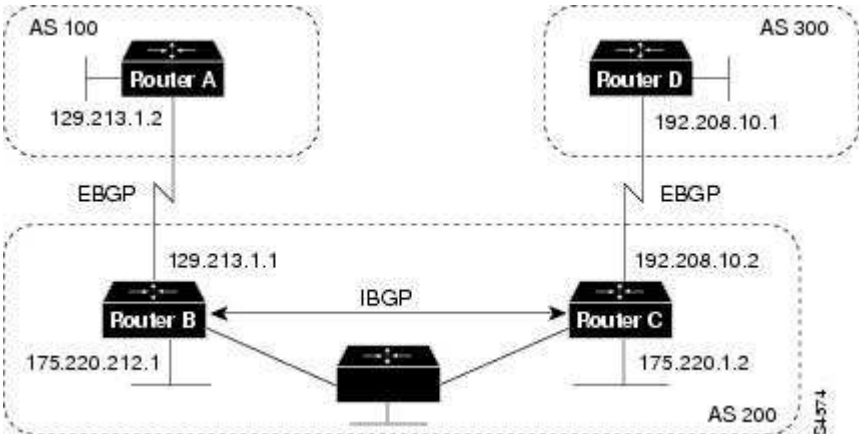
Uwaga odnośnie zapory przeciwwłamaniowej (ang. *firewall*): Prawidłowy przebieg sesji BGP wymaga otwarcia w zaporze kanału TCP 179 we wszystkich uczestniczących bramkach i komputerach.



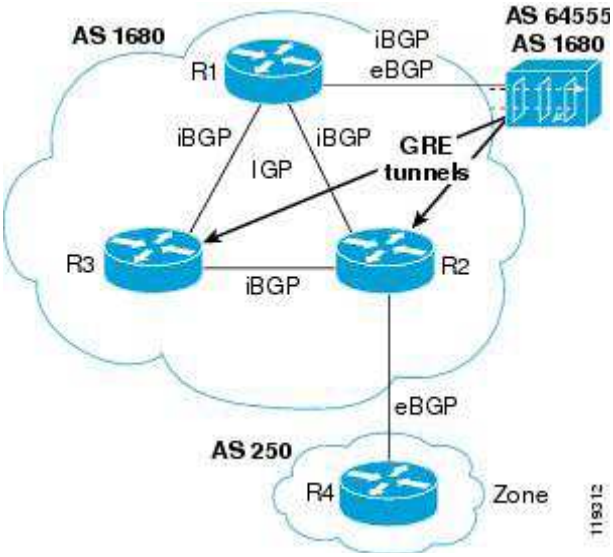
Sesja eBGP w kanale TCP 179 pomiędzy dwoma bramkami różnych systemów autonomicznych

2.10.2 Sesje iBGP i eBGP

W sesjach BGP mogą uczestniczyć bramki o identycznych numerach AS jak też i o różniących się między sobą. W zależności od tego sesje przebiegają zgodnie z protokółem iBGP lub eBGP.
Sesje BGP (TCP 179) między dwoma bramkami o różniących się numerach AS przebiegają automatycznie jako sesje eBGP.
Natomiast sesje BGP (TCP 179) pomiędzy dwoma urządzeniami o tym samym numerze AS przebiegają automatycznie jako sesje iBGP.



Przykład sesji eBGP i iBGP

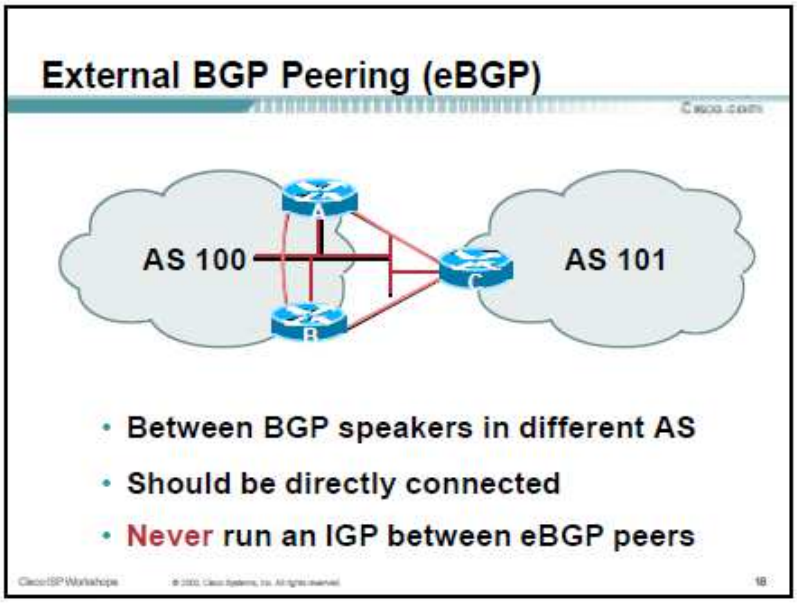


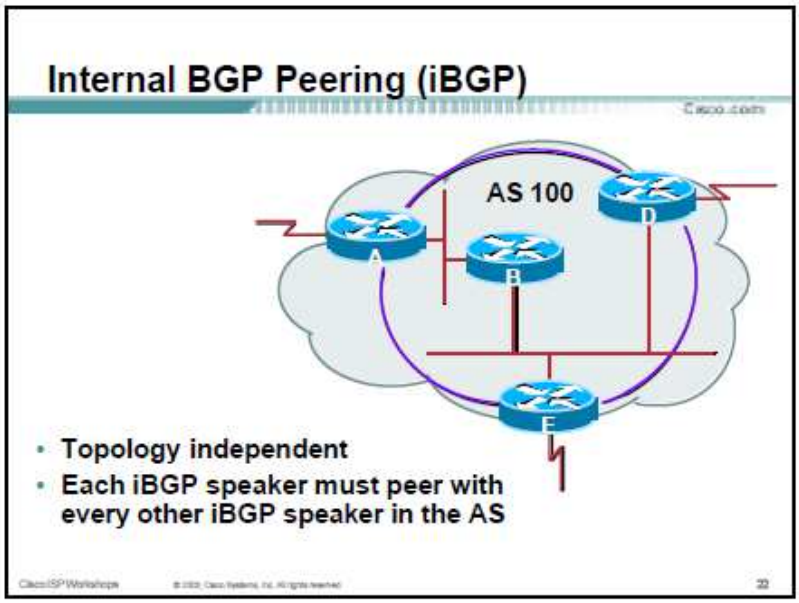
Kolejny przykład sesji eBGP i iBGP

2.10.3 Przebieg sesji BGP

Łączność odbywa się w kanale logicznym TCP nr 179 i połączenie jest aktywne w ciągu całej sesji. Sesja rozpoczyna się więc od nawiązania połączenia a jego potwierdzeniem jest nadanie pierwszego pakietu podtrzymującego (ang. „*Keep-Alive*“). Na zakończenie sesji połączenie TCP zostaje przerwane. Przebieg sesji jest identyczny dla iBGP i eBGP.

Otwarcie sesji: Sesja BGP rozpoczyna się od komunikatu „*Open*“ wysyłanego przez obu uczestnników do siebie nawzajem. Komunikat ten zawiera informację o wersji protokółu używanej przez daną bramkę, numer AS, maksymalny czas oczekiwania na dane w trakcie sesji (czas braku aktywności) i ewentualnie dodatkowe dane. Oprócz tego zawiera on identyfikator sąsiada – jeden z adresów IP złącza lub inny przydzielany automatycznie. Nie jest to parametr obowiązkowy i nie jest on używany w Hamnecie.
Komunikaty podtrzymujące połączenie („*Keep-alive*“): standardowo połączenie jest przerywane po upływie zadanego czasu braku aktywności na łączu (oczekiwania na dane) – ang. t*imeout*. Dla uniknięcia tej sytuacji partnerzy wymieniają w regularnych odstępach czasu komunikaty podtrzymujące połączenie (zastępujące rzeczywistą aktywność).
Komunikaty aktualizujące dane („*Update*“): ich treść stanowią zawartości tabel tras obu partnerów. Pełne tabele wymieniane są tylko bezpośrednio po nawiązaniu połączenia, a nastepnie – tylko zachodzące zmiany co pozwala na zmniejszenie obciążenia łączy.
Zawiadomienia („*Notification*“): komunikaty oznaczają zakończenie sesji BGP, np. po wystąpieniu poważnego błędu lub w przypadku jej zwykłego zakończenia.

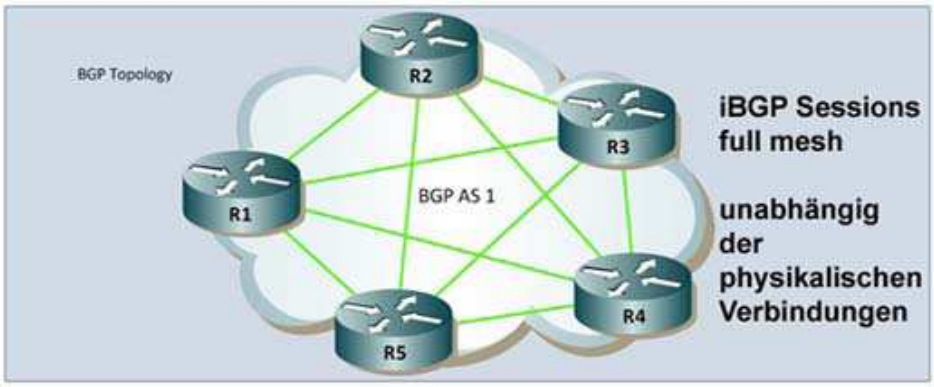




Sesja BGP dla eBGP (u góry) i iBGP (u dołu). Sesje eBGP odbywają się między bramkami BGP należącymi do różnych systemów i bezpośrednio połączonymi. Niedozwolone jest prowadzenie sesji IGP między różnymi systemami. Sesje iBGP muszą odbywać się między wszystkimi bramkami należącymi do danego systemu i zasad ta jest niezalezna od jego topologii.

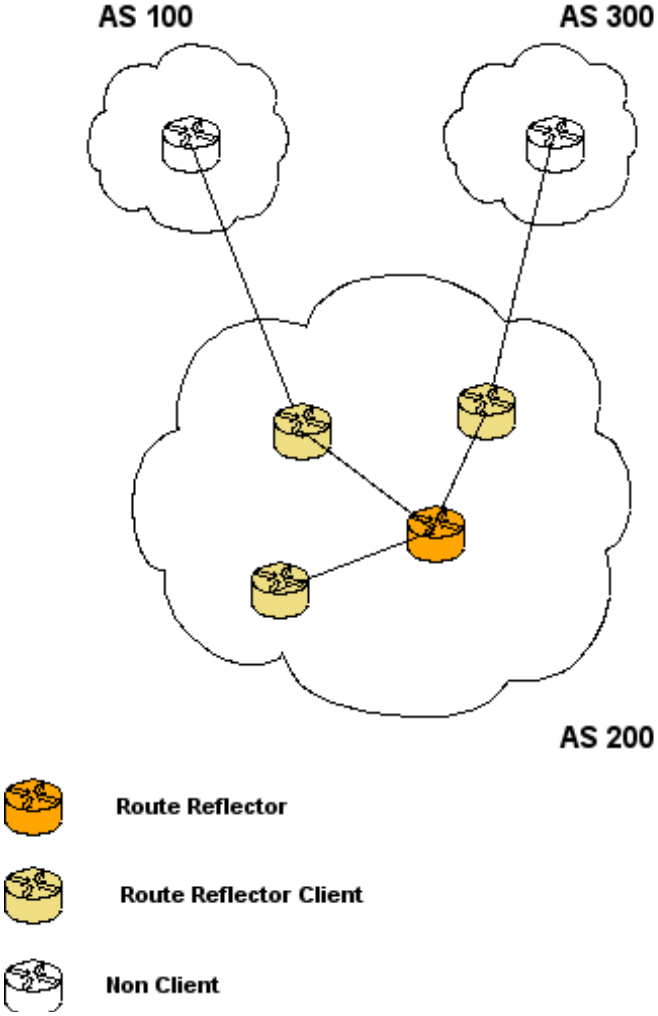
2.11 Całościowe sesje iBGP

Z dotychczasowych opisów pracy protokółu iBGP wynika, że trasy otrzymane w ramach sesji iBGP nie są przekazywane dalej do bramek sąsiednich. Zastosowanie protokółu iBGP w ramach systemu autonomicznego wymaga więc aby każda z bramek odbywała sesje BGP **ze wszystkimi pozostałymi należącymi do jej systemu autonomicznego** tak, że zapewniona jest kompletna wymiana informacji w sieci („*full mesh*“). Jest ona niezależna od tego czy wszyscy partnerzy są powiązani między sobą łączami fizycznymi (np. łączami radiowymi) – istotne są jedynie połączenia logiczne między bramkami czyli zdefiniowane sesje BGP pomiędzy nimi.



Całościowe sesje iBGP w kanale TCP 179 – konfiguracja partnerów. Liczą się połączenia logiczne a nie fizyczne.

Jak wynika z ilustracji dla każdej z bramek konieczne jest skonfigurowanie (zdefiniowanie) czterech sesji do pozostałych partnerów w sieci dla uzyskania całościowej wymiany informacji. W sieci austriackiej wszystkie bramki znajdują się na terytorium jednego i tego samego kraju związkowego.



Konfiguracja z reflektorem RR i sesjami iBGP między nim a bramkami (klientami). Bramki należące do innych systemów nie zaliczają się do klientów

Uwaga: dla sieci zawierającej n bramek liczba sesji rośnie w przyliżeniu proporcjonalnie do n^2 (dokładnie rzecz biorąc proporcjonalnie do n(n – 1)). W dużych sieciach ich liczba może być na tyle znaczna, że dla uproszczenia stosowane są reflektory tras (ang. *route reflector*; **RR**) zbierające dane od każdej

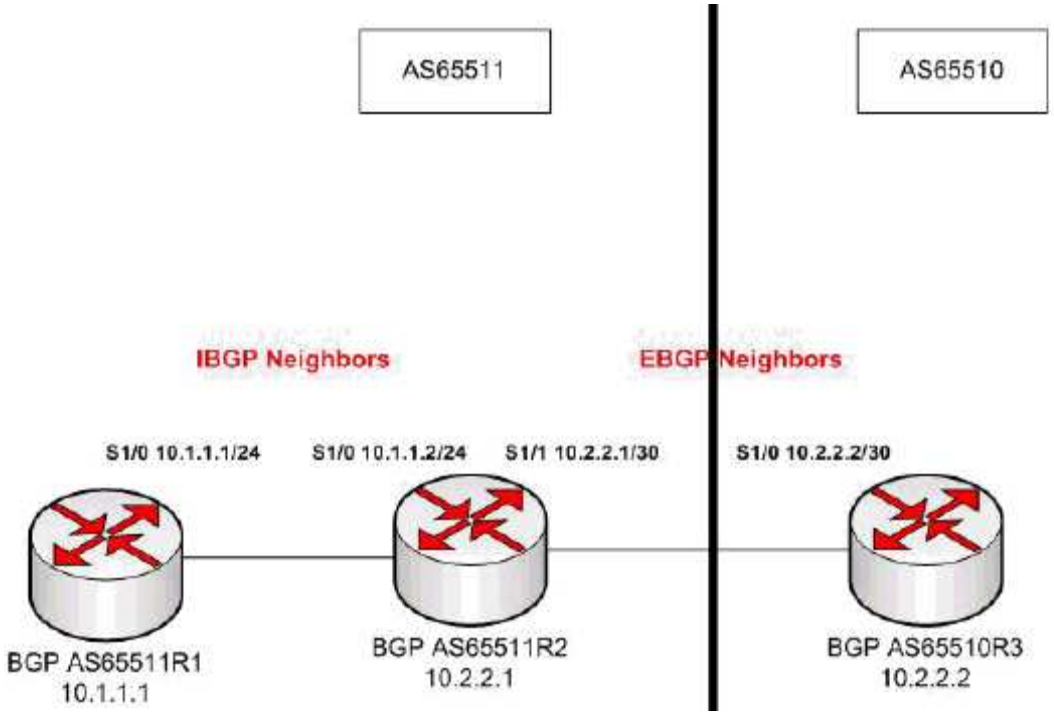
z bramek i udostępniające je pozostałym. Bramki firmy Mikrotik mogą być także skonfigurowane jako reflektory.
Każda z bramek eBGP przekazuje otrzymane z zewnątrz (z innych systemów autonomicznych) informacje o trasach przez iBGP do ustalonego reflektora tras (RR) we własnym systemie, który z kolei rozsyła je do pozostałych bramek. Liczba sesji maleje do n ponieważ każda z bramek musi utrzymywać połączenia jedynie z reflektorem. Odwrotną stroną medalu jest fakt, że defekt reflektora całkowicie paraliżuje wymianę informacji. Dlatego też większe systemy autonomiczne są wyposażone w reflektory rezerwowe.

W sieci Hamnetu przewidziane jest zadniczo przeprowadzanie **pełnej liczby sesji** dla każdego systemu autonomicznego (kraju związkowego w Austrii) bez korzystania z reflektora RR.

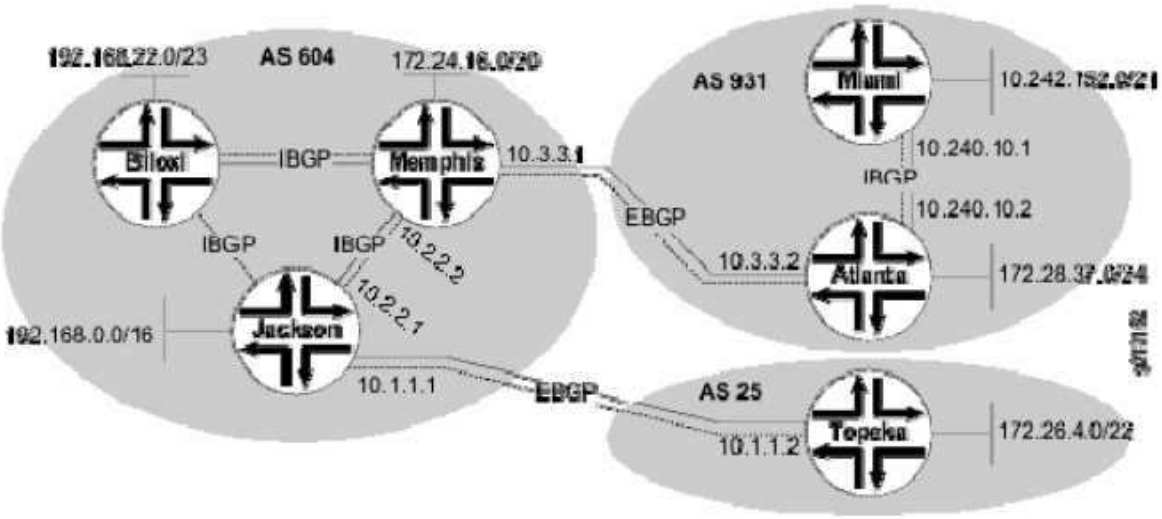
Wszystke dalsze przykłady dotyczą jedynie konfiguracji z sesjami całościowymi bez korzystania z reflektora tras. Doswiadczeni administratorzy mogą jednak w dowolnym czasie przejść na rozwiązanie reflektorowe w podległym im systemie autonomicznym. Konieczne jest wówczas zainstalowanie również reflektora rezerwowego. Początkującym administratorom zaleca się jednak zebranie doświadczeń z systemem bez reflektorowym.

2.12 Przykład iBGP i eBGP na styku systemów AS

Poniższe przykłady ilustrują zakresy wykorzystania iBGP i eBGP.



Przykład 1: Sesje iBGP i eBGP na styku systemów autonomicznych (na granicy AS) o różnych numerach AS. Bramki na granicy systemów AS65511 i 65512 sa sąsiadami eBGP a bramki wewnątrz systemu AS65511 – sąsiadami iBGP.



Przykład 2: iBGP i eBGP na styku systemów autonomicznych (na granicy AS) o różnych numerach AS

2.13 Atrybuty tras w BGP

W ramach sesji BGP przesyłane są **atrybuty (parametry) tras**. Najważniejsze z nich przedstawiono poniżej.

• Parametr **AS_PATH** (ścieżka transmisji) zawiera spis systemów autonomicznych leżących na trasie prowadzącej do celu. Do identyfikacji systemów służą ich numery AS. Na trasie AS nie dopuszczalne jest wprawdzie występowanie pętli ale systemy mogą być wymieniane wielokrotnie co sztucznie przedłuża te trasy. Trasa taka jest wprawdzie formalnie dostępna ale zmniejsza się jej atrakcyjność (ang. *AS-prepending*). Parametrami dodatkowymi są AS_SETS i AS_SEQUENCE. AS_SETS zawiera jeden lub więcej nieuporządkowanych numerów AS a AS_SEQUENCE – numery AS w kolejności ich przemierzenia.

• Parametr **IGP-Metrik** (ocena trasy) jest miarą (umownych) „kosztów“ ponoszonych przez własną sieć dla przekazania pakietu po danej trasie do punktu styku z następnym systemem autonomicznym.

• Parametr **Multi-Exit Discriminator** (MED) służy do opisania priorytetów równoległych tras prowadzących do tego samego systemu sąsiedniego. Niższe wartości oznaczają wyższe priorytety. Parametr ten jest używany pomiędzy partnerami eBGP.

• Parametry **Communities** są etykietami służącymi do oznaczania wymienianych zbiorów danych aktualizacyjnych i prefiksów (zbiorczych adresów IP). Są to liczby 32-bitowe, które mogą być użyte przez pozostałe bramki w charakterze filtrów. Oprócz standardowych parametrów **Communities** mogą występować także parametry rozszerzone („*extended Communities*“) zapisywane w postaci "12345:12345" lub jako liczba dziesiętna.

• **Local Preference** jest liczbą decydującą o preferencjach dla danej trasy wewnątrz systemu autonomicznego. Większa liczba odpowiada wyższemu priorytetowi.

• **Next Hop** zawiera adres IP następnego pośrednika (na najbliższym odcinku trasy) na drodze do podanego prefiksu (sieci lub ich grupy).

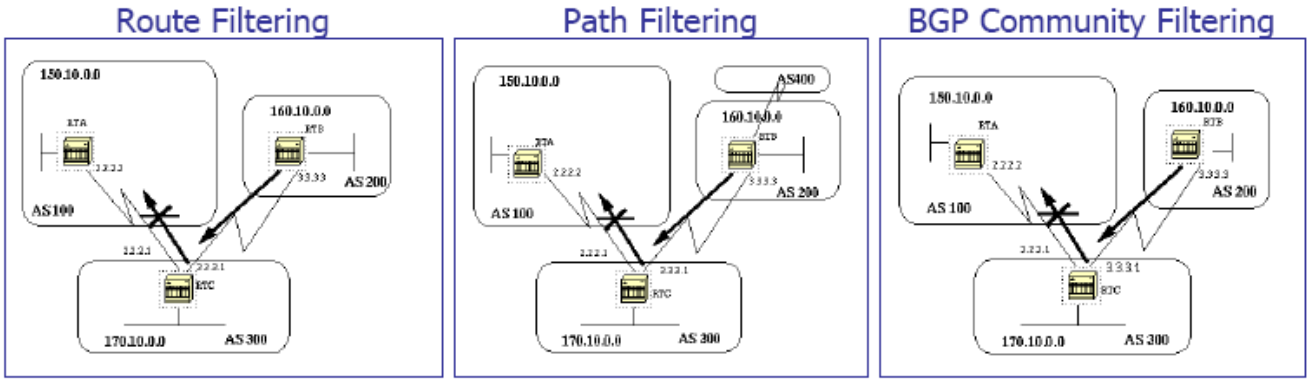
• **Weight** atrybut lokalny (występujący np. w sprzęcie firm Cisco, Mikrotik).

• **Origin** podaje źródło pochodzenia prefiksu: *internal* (wewnętrzne), *external* (zewnętrzne) lub *incomplete* (niepewne).

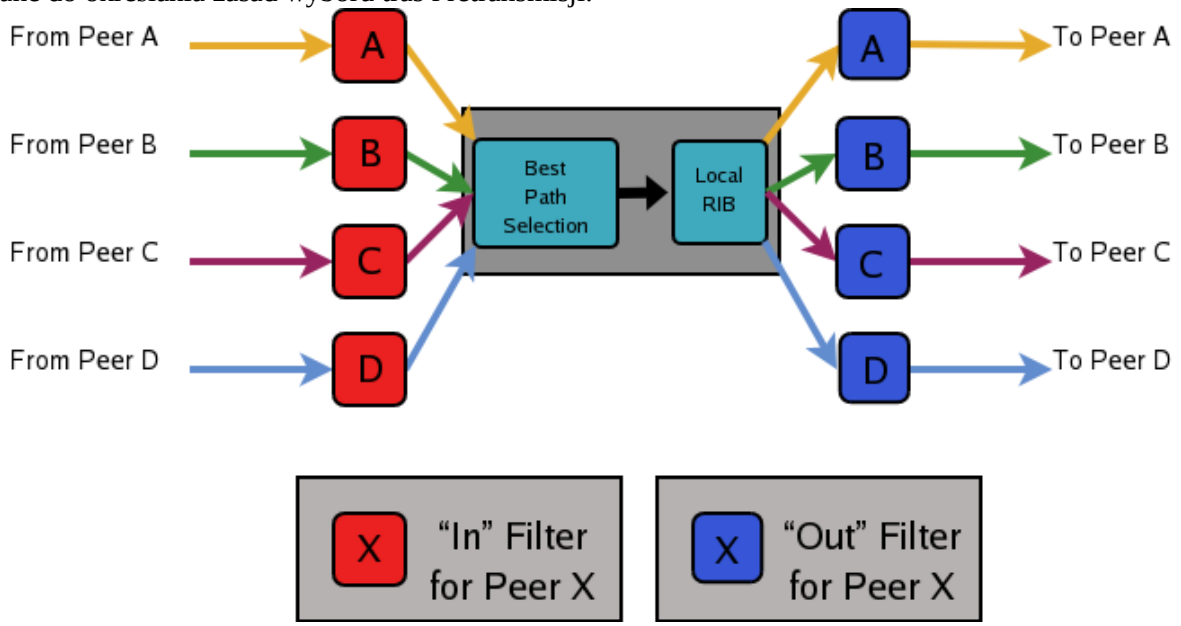
Uwaga: mimo, że BGP jest w stanie w oparciu o atrybut AS_Path uzyskać szeroki wgląd w topologię sieci nie można go jednak zakwalifikować do klasy algorytmów stanu łącza („*Link-state*“) ponieważ rozpowszechniane są jedynie informacje o trasach używanych przez BGP. Jest to zasadniczo cechą charakterystyczną algorytmów opartych na wektorze odległości („***Distance Vector*“)**..

2.14 Zasady wyboru tras i filtry

BGP pozwala na zdefiniowanie przez operatora zasad wyboru tras transmisji danych (ang. „*routing policies*"). Możliwe jest dokładne określenie tras wyjściowych z danego systemu autonomicznego lub też ignorowanie tras związanych z pewnym systemem i pomijanie go w transmisji. Może to znaleźć zastosowanie w sytuacji gdy trasy w sieci Hamnetu nie są optymalne. Można w ten sposób zdecydować również czy własny system autonomiczny będzie pośredniczył w transmisji danych do któregoś innego. Systemy takie nazywane są odpowiednio tranzytowymi („*transit*") lub nie tranzytowymi („*non transit*") – inaczej mówiąc zaporowymi.
Zasada: transmisja i odbiór danych BGP mogą być sterowane ręcznie w trojaki sposób: przez filtrację tras („*route filtering*"), filtrację ścieżek („*path filtering*") i filtrację grup („*community filtering*").



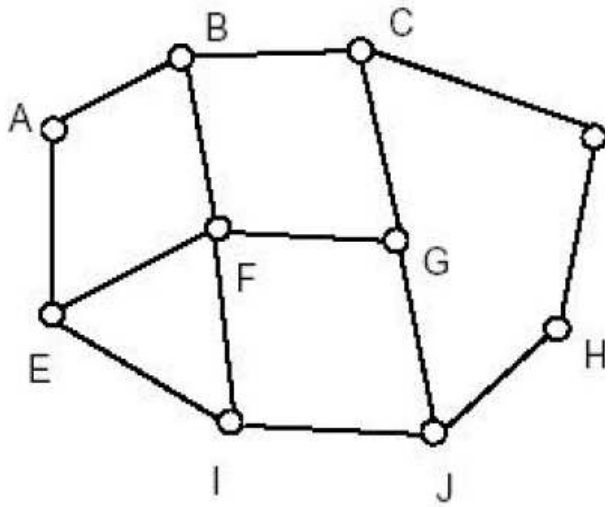
Uwaga: Grupy („*Communities*") są zdefiniowane za pomocą nieobowiązkowego atrybutu służącego do grupowania celów i nie występują obecnie w Hamnecie.
W Hamnecie nie stosuje się też specjalnych zasad wyboru tras i filtrów ponieważ wszystkie systemy autonomiczne powinny być równouprawnione. W szczególnych przypadkach niedociągnięć lub wad topologii sieci mogą one w drodze wyjątku i tymczasowo znaleźć zastosowanie w fazie rozbudowy sieci Hamnetu.
Zasadniczo dane pochodzące z sieci prywatnych nie są retransmitowane w Hamnecie i jest to podstawowa i najważniejsza z obowiązujących zasad. Zasady mogą obowiązywać także w zależności od pewnych wydarzeń i okoliczności. Bramki „Mikrotik" oferują w tym względzie szerokie możliwości.
Każda z sesji BGP może korzystać z filtrów wejściowych i wyjściowych. Mogą one być wykorzystywane do określania zasad wyboru tras i retransmisji.



Filtry wejściowe i wyjściowe sesji BGP – pomiędzy nimi (logicznie) znajduje się tabela tras bramki

2.15 Przykład procesu podejmowania decyzji w BGP

Bramka F otrzymuje od sąsisdów następujące informacje o trasach prowadzących D:
• w ramach sesji BGP z bramką B: „używam trasy BCD.“
• w ramach sesji BGP z bramką G: „używam trasy GCD.“
• w ramach sesji BGP z bramką I: „używam trasy IFGCD.“
• w ramach sesji BGP z bramką E: „używam trasy EFGCD.“



Bramka F znajduje najkorzystniejszą trasę do D w sposób podany poniżej, o ile w grę nie wchodzą żadne filtry ani zasady specjalne (ang. *routing policies*):

- trasy otrzymane od I i E są ignorowane,
- wybór pomiędzy trasami B i G zależy od ich parametrów oceny i ustalonych zasad („kosztów“, priorytetów itp.).

Ustalona w ten sposób trasa jest następnie wykorzystywana do retransmisji pakietów.

2.16 Znaczenie właściwej konfiguracji bramek BGP

Każda zmiana dowolnej z tras odbija się na pracy sieci Hamnetu. Komunikaty aktualizacyjne rozchodzą się wśród wszystkich bramek BGP w ramach własnego systemu (iBGP) i ponad granicami systemów (eBGP) w całej sieci Hamnetu.
Po otrzymaniu danych aktualizacyjnych bramki muszą dopasować swoje tablice tras do nowej sytuacji. I tu właśnie kryją się niebezpieczeństwa protokółu BGP, wymagającego bardzo starannej administracji i znajomości jego działania. Nawet drobne uchybienia w konfiguracji bramki mogą być przycyną poważnych problemów i w najgorszym przypadku przerwać połączenia między znacznymi częściami Hamnetu.
Błędne, zapomniane lub niedostatecznie precyzyjne filtry albo rozpowszechnianie w sieci falszywych informacji mogą spowodować, że inne systemy autonomiczne otrzymają dane tras nie prowadzących do nikąd i będących swego rodzaju „czarnymi dziurami“ dla danych.
Uwaga: błędne dane rozpowszechniane choćby przez jedną jedyną bramke rozchodzą się przez iBGP i eBGP również i w innych systemach autonomicznych a w rezultacie w całej sieci Hamnetu.
Czarna dziura jest jednym z najgorszych zjawisk jakie mogą wystąpić w sieci korzystającej z BGP. Zarówno przyczyny jak i miejsce utraty danych są trudne do zlokalizowania. Oprócz defektu łącza radiowego przyczynami mogą być filtry pakietów lub błędne konfiguracje.

2.17 Wielkość tabeli tras

Tabele tras w BGP mogą też – w zależności od konfiguracji – osiągąć znaczne rozmiary i poważnie obciążać zasoby bramki. Bramki BGP w Internecie mogą zawierać przeciętnie 30000 do 40000 wpisów lub nawet więcej.

3 Praca protokółu i zasady komunikacji

Rozdział ten jest poświęcony konfiguracji nadawcy BGP (niezalażenie od używanego sprzętu) i działaniu protokółu oraz wynikającym z tego zasadom konfiguracji. Praktyczne przykłady konfiguracji sieci w okręgu OE7 (Tyrolu) zawiera rozdział 4.

3.1 Usługa wyboru tras

W każdej bramce będącej nadawcą BGP konieczne jest uruchomienie usługi (niem. *Instanz*) wyboru tras co jest równoznaczne z jej włączeniem. Uruchomienie usługi jest nieskomplikowane i wymaga jedynie niewielu ustawień. W trakcie jej konfiguracji wprowadzane są nastepujące parametry:
• Nazwa usługi (dowolna)
• Numer AS systemu autonomicznego, w którym pracuje bramka
• W razie potrzeby identyfikator bramki – jesli rózni się on od domyślnego
• Parametry dodatkowe określające dane upubliczniane razem z trasami połączeń (przykładowo parametry: „*Redistribute Static*”, „*Redistribute Connected*”, „*Redistribute OSPF-learned*”, …). Zasadniczo wszystkie wyłączone.
Dodatkowe ustawienia wywierają istotny i niejednokrotnie negatywny wpływ na pracę sieci. Są one opisane wraz z odpowiednimi przykładami konfiguracji „Winboxu” w dalszym ciągu instrukcji.
Domyślnie (w przypadku nie wprowadzenia innej nazwy – identyfikatora bramki) jako identyfikator bramki występuje jej adres IP.
Po skonfigurowaniu usługi można przystąpić do konfiguracji sesji BGP.
Zasada: w bramceBGP w sieci Hamnetu konieczne jest skonfigurowanie i uruchomienie tylko jednej kopii usługi. Obsługuje ona wszystkie sesje BGP.

3.2 Podstawowa konfiguracja sesji BGP

Sesja BGP musi zostać odpowiednio skonfigurowana u obu partnerów. Nawiązuje ona połączenia TCP w kanale logicznym 179 między stacjami należącymi do segmentu sieci szkieletowej w oparciu o ich adresy IP. W większości modeli bramek konfiguracja sieci BGP jest dostępna w punkcie „*Peers*” („Partnerzy”) lub podobnie brzmiacym.

Przykład eBGP:

Ustawienia OE7ABC:
W bramce OE7ABC dodawany jest partner (ang. “*peer*“) o następujących parametrach:
Remote-Adresse (adres korespondenta): 44.143.244.254
Remote-AS-Nummer (numer AS korespondenta): 64520
Routing-Instanz: nazwa wykorzystywanej usługi (np.: „default“ albo „OE7ABC“)
Interface: *pole puste – ustawienie domyślne*

Ustawienia OE2XYZ:
W bramce OE2XYZ dodawany jest partner (“*peer*“) o następujących parametrach:
Remote-Adresse (adres korespondenta): 44.143.244.100
Remote-AS-Nummer (numer AS korespondenta): 64570
Routing-Instanz: nazwa wykorzystywanej usługi (np.: „default“ albo „OE2XYZ“)

Interface: *pole puste – ustawienie domyslne*

Zasada: partenerzy muszą być osiągalni w kanale TCP 179. Sesja jest nawiązywana pod warunkiem, że partnerzy „widzą się" wzajemnie. Po krótkim czasie koniecznym na jej nawiązanie („*connect*") pojawia się komunikat ***„Established"*** („połączenie nawiązane") np. w spisie „*Winbox BGP-Peer*".

Uwaga: automatycznie nawiązywana jest sesja eBGP ponieważ numery AS obu partnerów są różne.

Przykład iBGP:

Ustawienia OE7ABC:
W bramce OE7ABC dodawany jest partner ("*peer*") o następujących parametrach:
Remote-Adresse (adres korespondenta): 44.143.244.240
Remote-AS-Nummer (numer AS korespondenta): 64570
Routing-Instanz: nazwa wykorzystywanej usługi (np.: „default" albo „OE7ABC")

Ustawienia OE7DEF:
W bramce OE7DEF dodawany jest partner ("*peer*") o następujących parametrach:
Remote-Adresse (adres korespondenta): 44.143.243.254
Remote-AS-Nummer (numer AS korespondenta): 64570
Routing-Instanz: nazwa wykorzystywanej usługi (np.: „default" albo „OE2XYZ")

Zasada: partenerzy muszą być osiągalni w kanale TCP 179. Sesja jest nawiązywana pod warunkiem, że partnerzy „widzą się" wzajemnie. Po krótkim czasie koniecznym na jej nawiązanie („*connect*") pojawia się komunikat ***„Established"*** („połączenie nawiązane") np. w spisie „*Winbox BGP-Peer*".

Uwaga: Automatycznie nawiązywana jest sesja iBGP ponieważ numery AS obu partnerów są identyczne. W ramach danego systemu autonomicznego (regionu, okręgu) musi być nawiązany pełny komplet sesji – czyli po jednej z każdą z pozostałych bramek (sesja całościowa).

3.3 Podstawowe informacje o upublicznianiu sieci

Po skonfigurowaniu usługi i sesji BGP oraz po nawiązaniu sesji łączności patrnerzy mogą przekazać sobie informacje o znanych sieciach.

Przykład:

Osiągnięta / kanał dla:
44.143.160.254/24 (User)
44.143.169.254/25 (Services)

Osiągnięta / kanał dla:
44.143.161.254/24 (User)
44.143.172.254/25 (Services)

Stacje OE7AAA i OE7BBB są wyposażone w kanały dostępne dla użytkowników DHCP i kanały do celów serwisowych. Mają one też w sieciach swoje adresy jako bramki. Mogą więc rozpowszechniać – udostępniać sąsiadom – informacje o znanych prefiksach (zbiorczych adresach IP o określonej długości podanej w bitach) w celu wpisania ich do tabel tras. Informacje te są publikowane w ramach sesji BGP. Najprostszym sposobem jest wpisanie sieci przeznaczonych do upublicznienia na listę sieci – „*Networks*" (w programie „Winbox"), w niektórych modelach noszącej nazwę „*BGP-Networks*".

Ustawienia w liście „*Networks*" OE7AAA:
Dodanie sieci
Prefix: 44.143.160.0/24
Synchronize: No (nie)
Dodanie następnej sieci
Prefix: 44.143.169.128/25
Synchronize: No (nie)
Sieci wpisane na listę powinny pojawić się w tabeli tras w OE7BBB i być tam oznaczone jako aktywne. Wpisane muszą być także stacje sieci szkieletowej.
Dodanie kolejnej sieci
Prefix: 44.143.243.0/24
Synchronize: No (nie)

Ustawienia w liście „*Networks*" OE7BBB:
Dodanie sieci
Prefix: 44.143.161.0/24
Synchronize: No (nie)
Dodanie następnej sieci
Prefix: 44.143.172.128/25
Synchronize: No (nie)

Sieci wpisane na listę powinny pojawić się w tabeli tras w OE7BBB i być tam oznaczone jako aktywne. Wpisane muszą być także stacje sieci szkieletowej.
Dodanie kolejnej sieci
Prefix: 44.143.243.0/24
Synchronize: No (Nein)
Wpisane muszą być także wszystkie ewentualne pozostałe sieci połączone z bramką, np. sieci pakietowe, sieci OLSR itp.

Zasada 1: Sieci mogą być wpisane w bramkach BGP niezależnie od tego czy są one dla danej bramki osiągalne, a nawet czy wogóle istnieją. Można w ten sposób stworzyć błędne wrażenie dostępności sieci XY i doprowadzić do powstania w Hamnecie „czarnej dziury". Funkcja ta może być jednak przydatna w okresie prób i badania treści komunikatów.

Zasada 2: Wpisanie sieci w bramkach BGP nie powoduje umieszczenia ich we własnej tabeli tras ale poprzez sesje BGP trafiają one do wszystkich (logicznych) sąsiadów, o ile nie staną temu na przeszkodzie zdefiniowane gdzieś filtry.

Zasada 3: Informacje o sieciach lub prefiksach są rozpowszechniane w Hamnecie jedynie w oparciu o zapisy na listach sieci. Zasada ta jest prosta i łatwa do zrozumienia, a o szczegółach komunikatów decydują dodatkowe parametry takie jak: „*Redistribute Static Routes*", „*Connected Interfaces*", OSPF, „*Other BGP*" wybrane w konfiguracji usługi. Domyślnie są one wyłączone ponieważ mogą łatwo doprowadzić do wystąpienia błędów w pracy.

Zasada 4: Dane z listy sieci są rozpowszechniane w ramach wszystkich sesji skonfigurowanych i aktywnych na danej bramce. Nie muszą być podawane oddzielnie dla każdej z sesji.

Zasada 5: Informacje otrzymane od sąsiednich bramek („*User*“, „*Services*“, itp. …) mogą być rozpowszechniane tylko wtedy gdy nie jest to bramka BGP i gdy prowadzi do niej trasa statyczna.

3.4 Dalsze informacje o upublicznianiu sieci

3.4.1 Funkcja synchronizacji sieci – „*Networks-Synchronize*“

Omówiona w poprzednim rozdziale funkcja sieciowa pozwala na rozpowszechnianie wśród partnerów (sąsiadów) i w całej sieci BGP informacji o sieciach docelowych.
Posiada ona niewiele parametrów wpływających na jej działanie ale jedną z dodatkowych możliwości jest funkcja synchronizacji („*Synchronisation*“).
Włączenie synchronizacji powoduje porównanie listy sieci z własną tabelą tras. Tylko w przypadku znalezienia w tabeli trasy zgodnej z zawartą na liście – dane tej ostatniej są publikowane.

Przykładowy wpis:
Prefix: 44.143.161.0/24
Synchronize: No (nie)
• Informacje o prefiksie są zawsze upubliczniane

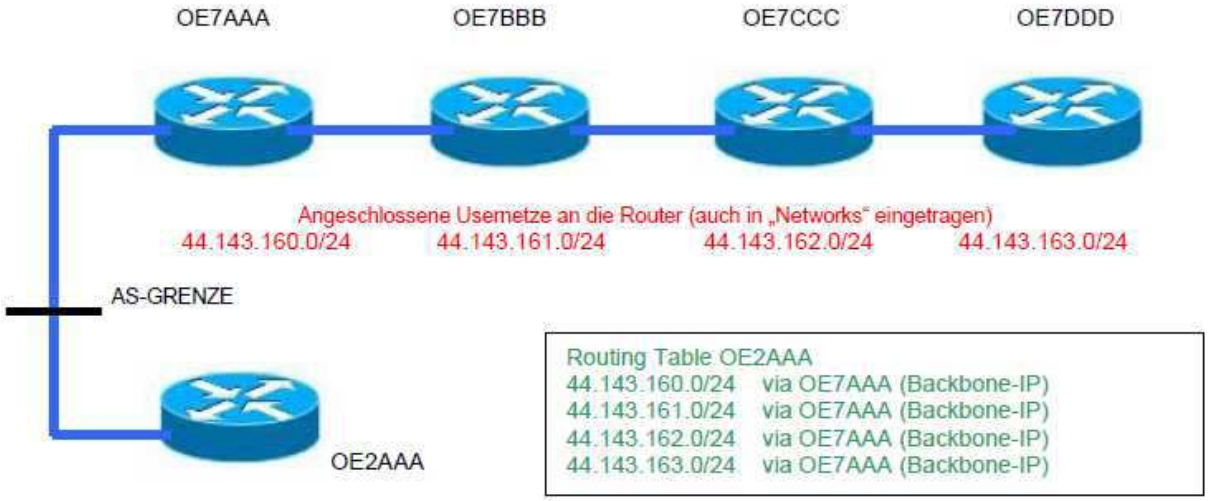
Przykładowy wpis:
Prefix: 44.143.161.0/24
Synchronize: **Yes (tak)**
• Informacje o prefiksie są upubliczniane tylko wówczas gdy w tabeli tras znajduje się pasująca trasa np. funkcjonujące złącze fizyczne (kanał) zapewniające dostęp do tej sieci – czyli pasujący wpis DaC.

Zastosowanie:
Funkcja zapewnia rozpowszechnianie wyłącznie celów naprawdę osiągalnych z danej bramki. Funkcjonuje ona tylko dla sieci dostepnych przez kanały bezpośrednie (mostki między sieciami są zawsze osiągalne).

Zastosowanie w Hamnecie:
Zasadniczo nie przewidziane jest stosowanie synchronizacji w sieci Hamnetu ponieważ dla kanałów dostępu do sieci docelowych instalowane są mostki (ang. *bridge*). Nie informują one o defekcie kanału i nie wyłączają się samoczynnie.
Nie powoduje to problemów ponieważ nie funkcjonujące bramki lub kanały sieci przerywają sesję BGP i trasy te nie trafiają do tabel u sąsiadów i w pozostałych bramkach Hamnetu.

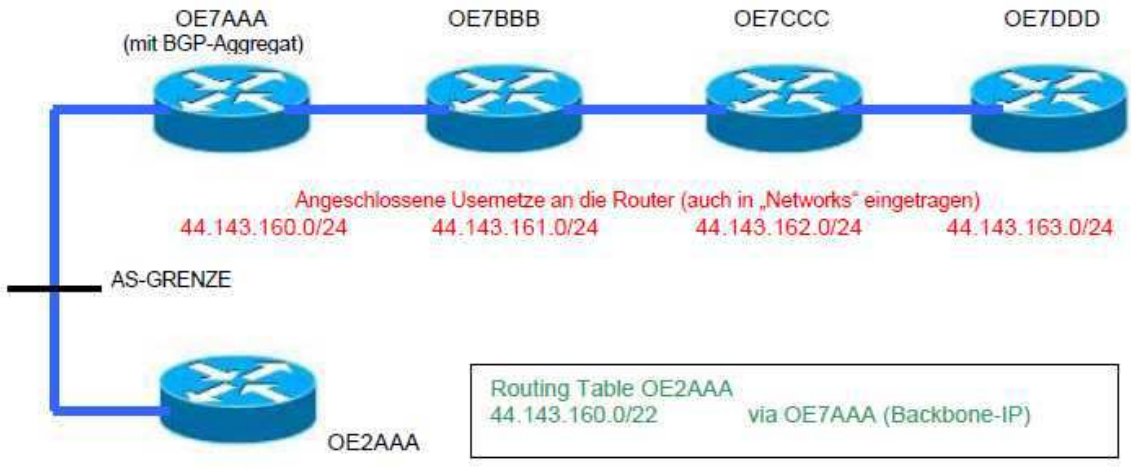
3.4.2 Grupowanie sieci

Bramki mogą na czas transmisji grupować sieci docelowe i przesyłać ich dane we wspólnym meldunku (niem. *Aggregat*).
Przykład:
We wspólnej gałęzi łączy (fizycznych łączy radiowych) znajduje się większa liczba bramek OE7. Na rysunku nie uwzględniono całościowej wymiany komunikatów iBGP w sieci OE7.
Objaśnienia do rysunku: pod symbolami bramek podano adresy sieci użytkowych, wymienionych również w liście sieci („*Network*“). Granica systemów autonomicznych leży między OE2AAA i OE7AAA.
W ramce podano tabelę tras dla bramki OE2AAA.



Bez grupowania:
Zgodnie z zasadą pracy protokółu BGP wymiana informacji przebiega następująco:
• Ponieważ OE7AAA, OE7BBB, OE7CCC, OE7DDD przeprowadzają pełny komplet sesji iBGP, w każdej z bramek OE7 wpisane są po trzy pozostałe sieci użytkowe – jako pojedyńcze trasy w tabeli.
• Znajdująca się na granicy systemów autonomicznych bramka OE7AAA przeprowadza ze stacją OE2AAA również sesję eBGP, w ramach której przekazuje do OE2AAA informacje o wszystkich czterech sieciach.
• OE2AAA wpisuje te 4 sieci pojedyńczo do swojej tabeli tras: 44.143.160.0/24, 44.143.161.0/24, 44.143.162.0/24, 44.143.163.0/24.
W przedstawionej na rysunku topologii przerwanie połączenia miedzy OE2 i OE7 uniemożliwia dostęp ze strony OE2 do następujących sieci (ponieważ były one od strony OE2 osiągalne jedynie przez łącze OE2AAA – OE7AAA):
44.143.160.0/24
44.143.161.0/24
44.143.162.0/24
44.143.163.0/24.
Bramki BGP mogą tworzyć grupy sieci dzięki czemu przekazują do stacji sąsiednich (np. w innym systemie autonomicznym) mniej szczegółowe informacje, co zmniejsza liczbę wpisów w tabeli tras sąsiada i wszystkich dalej położonych systemów.

Z grupowaniem:



Wszystkie cztery sieci zostają w OE7AAA zgrupowane pod wspólnym adresem (prefiksem) 44.143.160.0/22 – o 22 bitach znaczących zamiast 24 jak dla pojedyńczych sieci.

Objaśnienie do rysunku – dla tej samej topologii i tych samych sieci użytkowych OE2AAA zawiera tylko jeden wpis w tabeli tras zamiast czterech jak w poprzednim przykładzie.

Przebieg wymiany informacji
• W ramach kompletu sesji iBGP stacja OE7AAA otrzymuje od partnerów wszyskie onformacje o sieciach OE7.
• Po złożeniu ich w jedną grupę (niem. *Aggregat*) 44.143.160.0/22 OE7AAA przekazuje do OE2AAA (przez eBGP) tylko ta jedną zbiorczą informację.
• OE2AAA wpisuje tylko ta jedną trasę do swojej tabeli tras, a mianowicie otrzymaną od OE7AAA grupę 44.143.160.0/22.
• Połączenie pomiędzy OE2 i OE7 funkcjonuje identycznie jak w poprzednim przykładzie ale tabela tras w OE2 jest krótsza.

Tworzenie grup w celu przekazania ich sąsiedniemu AS ma sens, gdy wchodzące w jej sklad bramki są połączone w szereg w jednej gałęzi. Dla osiągnięcia sieci znajdujących się w tej gałęzi sąsiedniemu systemowi wystarczy informacja zgrupowana.

Grupa ta będzie upubliczniana w ramach sesji iBGP także wśród bramek OE7 o ile nie zapobiegną temu odpowiednie filtry u partnerów. W całościowej wymianie danych (ang. *full-mesh*) w sieci OE7 obecność grupy wcale nie szkodzi, występuje ona wprawdzie w tabelach tras ale w transmisji pokietów wykorzystywane będą trasy opisane dokładniej – w praktyce grupa ta mimo obecności w tabelach nie jest aktywna i nie wymaga odfiltrowania.

Uwaga: Konfiguracja grup nie oznacza zmian w przydziale adresów elementów sieci ale jest tylko dopasowaniem konfiguracji na poziomie BGP.

3.4.3 Upublicznianie grupy

Informacja grupowa może być przekazywana do sąsiada w dwojaki sposób.
44.143.160.0/24
44.143.161.0/24
44.143.162.0/24
44.143.163.0/24 ----------→ grupa
44.143.160.0/21
44.143.164.0/24
44.143.165.0/24
44.143.166.0/24
44.143.167.0/24

Wariant a): W zwykły sposób przy wykorzystaniu funkcji sieciowej używanej do rozpowszechniania informacji o sieciach (patrz: podstawowe informacje o upublicznianiu sieci).
Realizacja:
W bramce znajdującej się na granicy systemów wystarczy wpisać grupowy adres o większym zasięgu (mniejszej liczbie bitów znaczących) aby został on opublikowany. W przypadku wpisania go na listę sieci („*Networks*“) należy zwrócić uwagę aby nie publikować pojedyńczych sieci wchodzących w jego skład, ponieważ jednoczesne publikowanie grupy i jej elementów nie ma sensu. Zapewniają to używane w ramach sesji filtry.
Synchronizacja („*Synchronize*“):
Włączenie synchronizacji powoduje, że informacja o grupie jest publikowana tylko wówczas gdy w tabeli tras znajduje się co najmniej jeden pasujący wpis (ang. *matching entry*) np. wpis jednej z sieci należących do grupy albo wpis własnego złącza fizycznego (kanału) o pasującym adresie IP.

Wariant b) Funkcja grupująca (niem. *Aggregate-Funktion*) – np.: w oprogramuwaniu „Winbox"

Adres grupowy (prefiks) należy wpisać na listę grup (niem. *Aggregate-Liste*). Informacja o grupie jest rozpowszechniana tylko wówczas, gdy tabela tras zawiera co najmniej jeden pasujący wpis otrzymany przez BGP, np. dotyczący jednej z sieci wchodzących w skład grupy.
Funkcja grupowania dodaje automatycznie do prefiksy poszczególnych sieci do zapisanej sieci grupowej.
Funkcja streszczania („*Summarize*"): Po jej włączeniu informacje o sieciach wchodzących w skład grupy są automatycznie pomijane w sesjach. Oznacza to, że w odróżnieniu od wariantu a zbędne są dodatkowe filtry dla sesji.
Grupy posiadają dodatkowe (dobrowolne) ustawienia.

3.4.4 Pętle i prawidłowo wybrane konfiguracje tras

Konfiguracja 1: BŁĘDNA
W poniższym przykładzie przedstawiono błędne konfiguracje grup dopuszczające do publikacji dłuższych tras w pętlach.

Przykład:
W sieci na granicy OE2 – OE7 występuje widoczna na ilustracji pętla. Zakładamy, że bramki OE7AAA i OE7FFF są skonfigurowane tak aby publikowały grupę (niem. *Aggregat*) 44.143.160.0/21 występującą w sieci OE7. Grupy te są odbierane przez ich sąsiadów OE2AAA i OE2BBB w systemie OE2 (granice systemów – niem. *AS-Grenze* – leżą między OE2AAA i OE7AAA oraz OE2BBB i OE7FFF).

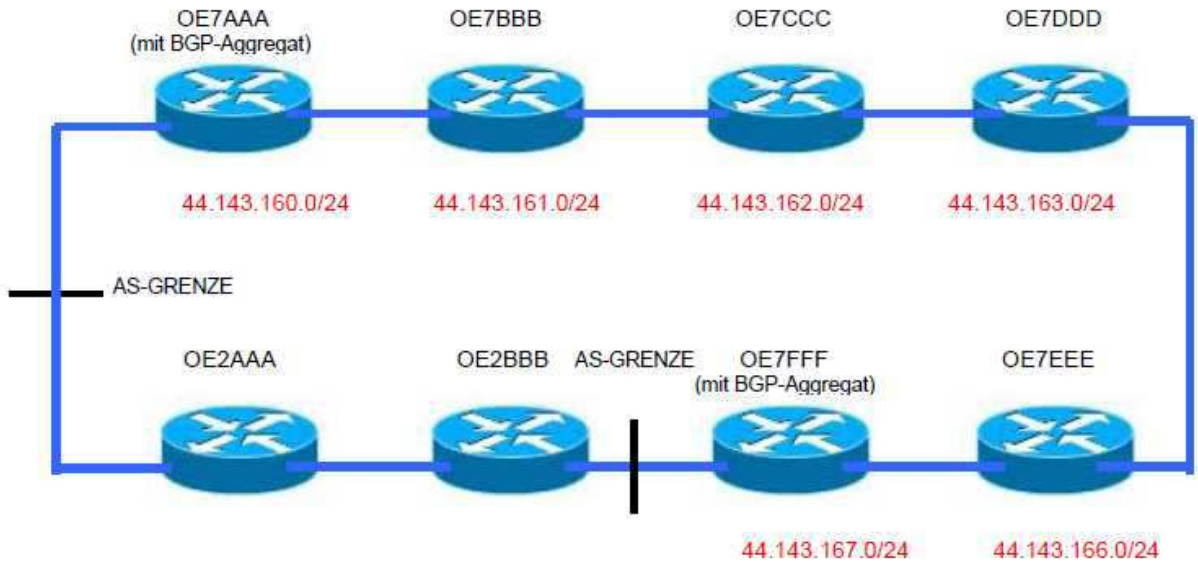


Tabela tras OE2AAA
44.143.160.0/21 via OE7AAA (Backbone-IP) aktive Route – czynna, używana,
44.143.160.0/21 via OE2BBB (Backbone-IP) – nieczynna

Tabela tras OE2BBB
44.143.160.0/21 via OE7FFF (Backbone-IP) aktive Route – czynna
44.143.160.0/21 via OE2AAA (Backbone-IP) inaktive Route – nieczynna

Problem 1: w przypadku gdy OE2AAA retransmituje pakiety do użytkownika sieci połączonej z OE7FFF (44.143.167.x), są one przekazywane do OE7AAA i przed dotarciem do celu przechodzą przez znaczną część pętli OE7.

Problem 2: w przypadku gdy OE2BBB retransmituje pakiety do użytkownika sieci połączonej z OE7AAA (44.143.160.x), są one przekazywane do OE7FFF i przed dotarciem do celu przechodzą przez znaczną część pętli OE7.

Wnioski :
• grupowanie stacji wchodzących w skład dużych pełnych pętli zamykających się przez sąsiedni system jest nieekonomiczne i powoduje znaczne przedłużenie tras retransmisji danych.
• grupowanie jest korzystne dla gałęzi nie tworzących (jeszcze) pierścieni.
Prędzej czy później w sieci Hamnetu zaczną występować mniejsze lub większe pętle zamykające się także poprzez sąsiadujące kraje.

<u>Konfiguracja 2: PRAWIDŁOWA</u>
Grupowanie pętli nie jest jenak zgóry wykluczone!
Pętle zawierające wewnątrz struktury gwiaździste (tworzące w ostatecznym wyniku struktury mieszane) mogą podlegać grupowaniu i być w ten sposób publikowane w sąsiednich systemach.

Przykład:
Pętla z dodatkowym łączem radiowym pomiędzy dwoma jej stacjami. Rysunek odpowiada ilustracji z przykładu poprzedniego z dodatkowym łączem między bramkami granicznymi OE7AAA i OE7FFF, które podobnie jak w przykładzie poprzednim grupują trasy przed przekazaniem informacji do OE2.

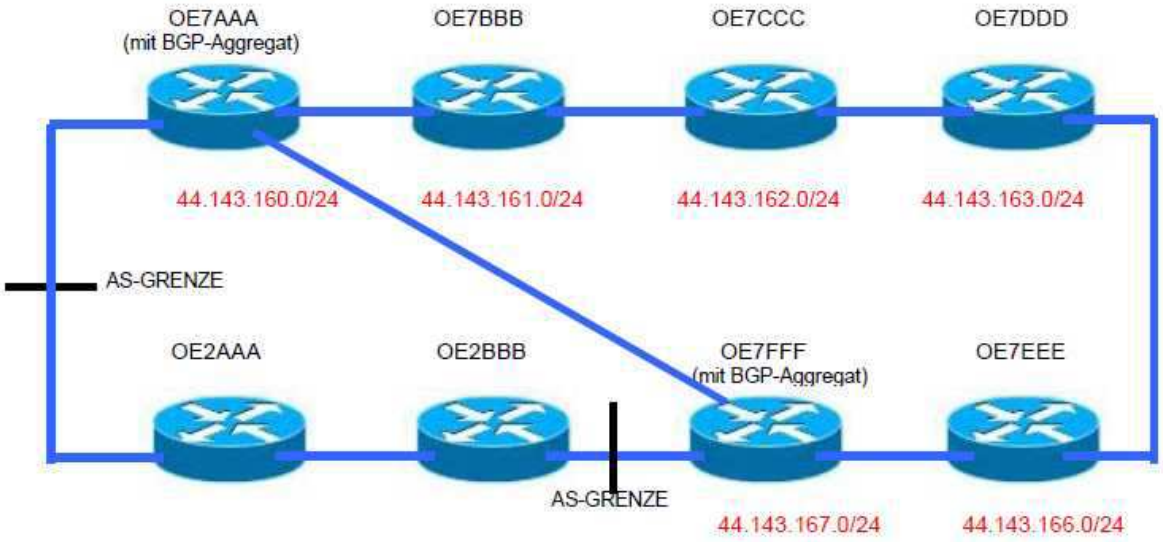


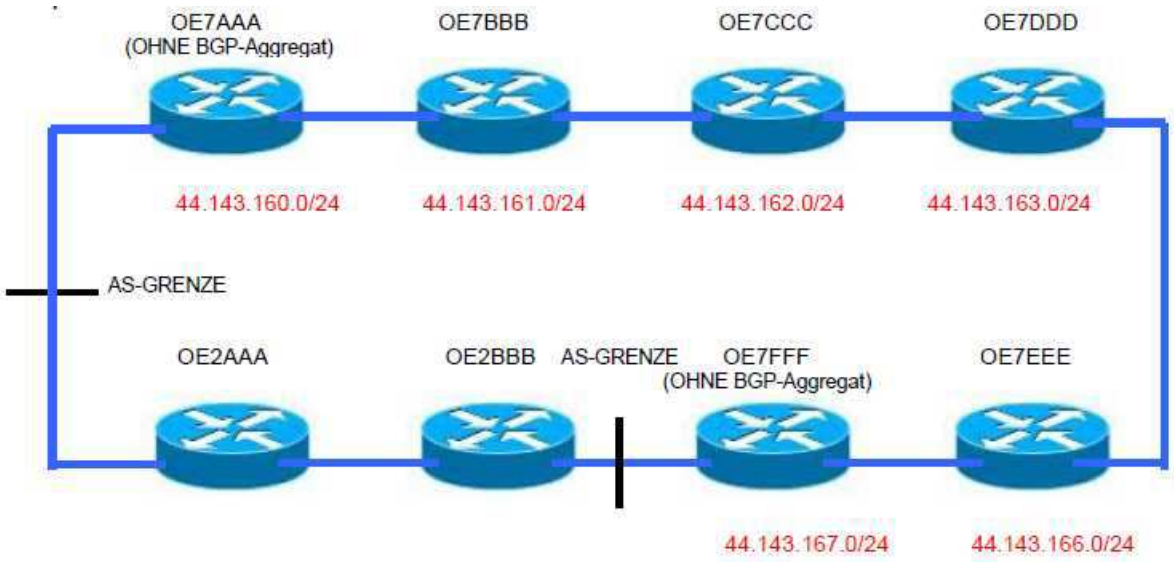
Tabela tras OE2AAA
44.143.160.0/21 via OE7AAA (Backbone-IP) aktive Route – czynna, używana
44.143.160.0/21 via OE2BBB (Backbone-IP) inaktive Route – nieczynna

Tabela tras OE2BBB
44.143.160.0/21 via OE7FFF (Backbone-IP) aktive Route – używana
44.143.160.0/21 via OE2AAA (Backbone-IP) inaktive Route – nieczynna
Tabele tras w bramkach OE2 są identyczne jak w przykładzie poprzednim. Pakiety z OE2AAA do OE7FFF są też tak samo przekazywane do OE7AAA ale dzięki dodatkowemu połączeniu docierają do celu krótszą trasą. Protokół iBGP w systemie OE7 korzysta od razu z połączenia OE7AAA -> OE7FFF. Warunkiem prawidłowego działania jest w miarę stabilna praca łączy radiowych i ich zbliżona jakość.

Wniosek :
Grupowanie może przyczynić się do srócenia tabel tras, ale nie ma uniwersalnego rozwiązania dla niego w topologiach mieszanych. Konieczne jest zawsze indywidualne rozpatrzenie lokalnej topologii. W początkowym stadium rozbudowy i uruchamiania sieci nie należy korzystać z grupowania.

Konfiguracja 3: PEWNA I PRAWIDŁOWA

W tym przykładzie rozpatrujemy identyczną pętlę jak w przykładzie 1 ale na granicach systemów (w stacjach OE7AAA i OE7FFF) nie korzysta się grupowania. Obie stacje przekazują sąsiadom w OE2 pełne i szczegółowe informacje o wszystkich sieciach.



Tabele tras OE2AAA i OE2BBB zawierają więc kompletne dane wszystkich sieci. Dane te występują w każdej ze stacji podwójnie, ponieważ otrzymują je one z dwóch stron. Wybór tras czynnych i ignorowanych (nieczynnych) przez każdą stację zależy od wyboru dokonanego przez algorytm BGP („*BGP Path Selection Process*“). Na wybór ten można wpływać przez ustalenie odpowiednich zasad i zdefiniowanie filtrów w bramkach.
Niezależnie od tego proces wyboru przebiega zawsze w następujący sposób:

1. Preferowane są trasy **o największych wartościach parametru "*Weight*" (wadze)**. Jego wartość może być także zmieniana lokalnie przez filtry, tak aby operator mógł dopasować preferencje dla pewnych tras ze względów topologicznych lub innych.

2. Dla tras o tej samej wadze – wartości parametru "*weight*" o wyborze decyduje wartość lokalnego priorytetu – parametru **"local preference"** (preferowane są trasy o jego większej wartości). *Local Preference* jest parametrem (wagą) pochodzącym z sesji iBGP, służącym do wyboru najkorzystniejszego wyjścia z własnego systemu (AS) w kierunku danego celu. Oprócz tego możliwe jest wprowadzenie wagi (oceny) trasy przez operatora – parametr ten jest wykorzystywany analogicznie jak „*weight*“. Atrybut ten jest rozpowszechniany tylko w ramach sesji iBGP.

3. Jeżeli i wartości parametru "*local preference*" są sobie równe wybierana jest trasa utworzona w bramce przez BGP.

4. Jeżeli brak jest takiej trasy wybierana jest trasa **o najkrótszym atrybucie AS_PATH**.

5. Dla tras o tej samej długości AS_PATH wybierana jest tras o najkorzystniejszym pochodzeniu – najmniejszym atrybucie **Origin Typ**. Atrybut ten informuje o jej pochodzeniu np. od partnera iBGP albo eBGP. Atrybut ma dla iBGP wartość niższą niż dla eBGP a dla nieznanych („*incomplete*“) wartość najwyższą.

6. Dla tras o tym samym pochodzeniu („*Origin Typ*“) decyduje **najniższa wartość atrybutu MED** („*Multi-Exit-Discriminator*“). Jest to parametr wagowy BGP dla wyboru najkorzystniejszej z równoległych tras prowadzących do tego samego celu w sąsiednim systemie – tzw. punkt wejściowy do systemu

sąsiedniego. Atrybut ten jest rozpowszechniany wyłącznie w sesjach eBGP jako propozycja ze strony sąsiada.

7. Spośród tras o tym samym atrybucie MED **preferowane są trasy zewnętrzne przed wewnętrznymi**.

8. W przypadku równości wszystkich poprzednio wymienionych atrybutów preferowana jest trasa do **najbliższego sąsiada BGP**.

9. W ostateczności wybierana jest trasa o najniższym adresie IP spośród partnerów BGP (sesji) w porównaniu do własnego identyfikatora.

Tabele tras OE2AAA i OE2BBB wyglądają więc jak następuje:
Tabela tras OE2AAA
44.143.160.0/24 via OE7AAA(Backbone-IP) aktive Route – czynna
44.143.160.0/24 via OE2BBB(Backbone-IP) inaktive Route – nieczynna
44.143.161.0/24 via OE7AAA(Backbone-IP) aktive Route
44.143.161.0/24 via OE2BBB(Backbone-IP) inaktive Route
44.143.162.0/24 via OE7AAA(Backbone-IP) aktive Route,
44.143.162.0/24 via OE2BBB(Backbone-IP) inaktive Route
44.143.163.0/24 via OE7AAA(Backbone-IP) aktive Route
44.143.163.0/24 via OE2BBB(Backbone-IP) inaktive Route
44.143.166.0/24 via OE2BBB(Backbone-IP) aktive Route
44.143.166.0/24 via OE7AAA(Backbone-IP) inaktive Route
44.143.167.0/24 via OE2BBB(Backbone-IP) aktive Route
44.143.167.0/24 via OE7AAA(Backbone-IP) inaktive Route

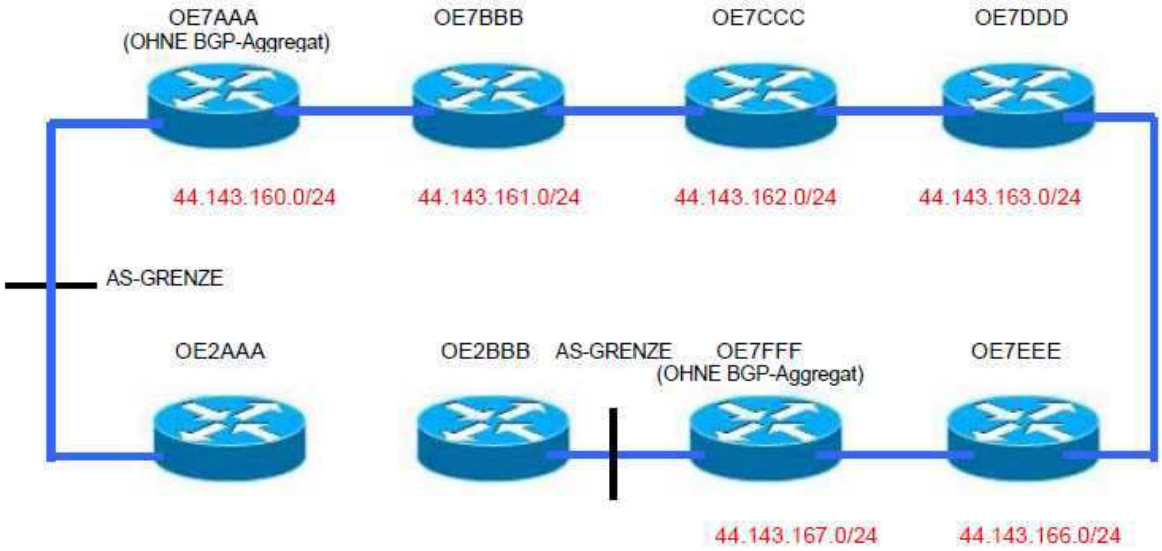
Tabela tras OE2BBB
44.143.160.0/24 via OE2AAA(Backbone-IP) aktive Route
44.143.160.0/24 via OE7FFF(Backbone-IP) inaktive Route
44.143.161.0/24 via OE2AAA(Backbone-IP) aktive Route
44.143.161.0/24 via OE7FFF(Backbone-IP) inaktive Route
44.143.162.0/24 via OE2AAA(Backbone-IP) aktive Route,
44.143.162.0/24 via OE7FFF(Backbone-IP) inaktive Route
44.143.163.0/24 via OE2AAA(Backbone-IP) aktive Route
44.143.163.0/24 via OE2AAA(Backbone-IP) inaktive Route
44.143.166.0/24 via OE7FFF(Backbone-IP) aktive Route
44.143.166.0/24 via OE2AAA(Backbone-IP) inaktive Route
44.143.167.0/24 via OE7FFF(Backbone-IP) aktive Route
44.143.167.0/24 via OE2AAA(Backbone-IP) inaktive Route

Uwaga: przedstawione tabele zawierają oczywiście również wpisy dla sieci szkieletowej, ponieważ również i one muszą być publikowane. Dla ułatwienia orientacji w powyższym przykładzie przedstawiono jedynie wpisy tras użytkowych. Trasy oznaczone jako nieczynne („*inactive*“) są znane bramce ale obecnie nie używane.

3.4.5 Pętla przerwana

W punkcie tym omawiamy pętlę przerwaną powstałą w wyniku przerwania jednego z łączy radiowych.

Uwaga: Pętla przerwana w rozumieniu BGP powstaje już wówczas gdy z jakich kolwiek powodów przerwaniu ulegnie lub zostanie w niej wyłączona jedna z sesji BPG (np. wskutek wyłączenia jednego z partnerów w „Winboxie”).
Przerwanie łącza radiowego pomiędzy OE2AAA i OE2BBB:



Po aktualizacji tabele tras OE2AAA i OE2BBB wyglądają jak następuje:

Tabela tras OE2AAA
44.143.160.0/24 via OE7AAA(Backbone-IP) aktive Route – trasa czynna
44.143.161.0/24 via OE7AAA(Backbone-IP) aktive Route
44.143.162.0/24 via OE7AAA(Backbone-IP) aktive Route,
44.143.163.0/24 via OE7AAA(Backbone-IP) aktive Route
44.143.166.0/24 via OE7AAA(Backbone-IP) aktive Route
44.143.167.0/24 via OE7AAA(Backbone-IP) aktive Route

Tabela tras OE2BBB
44.143.160.0/24 via OE7FFF(Backbone-IP) aktive Route
44.143.161.0/24 via OE7FFF(Backbone-IP) aktive Route
44.143.162.0/24 via OE7FFF(Backbone-IP) aktive Route,
44.143.163.0/24 via OE7FFF(Backbone-IP) aktive Route
44.143.166.0/24 via OE7FFF(Backbone-IP) aktive Route
44.143.167.0/24 via OE7FFF(Backbone-IP) aktive Route

Występują w nich tylko trasy czynne (aktywne) ponieważ z drugiej strony nie napływają żadne meldunki.
OE2AAA i OE2BBB komunikuja się ze sobą przez sieć OE7. Również i tutaj pominięto wpisy dla sieci szkieletowej.

3.4.6 Parametry „Redistribute Static“, „Connected“, „OSPF“, „Other BGP“

W trakcie uruchamiania i konfiguracji usługi BGP operator może ustawić dodatkowe parametry decydujące o jej pracy (w Hamnecie i wielu innych przypadkach wystarczy tylko pojedyńcze wywołanie usługi w bramce (jedna czynna kopia), patrz p. 3.1).
Jej argumenty zarówno w bramkach Mikrotik jak i Cisco oraz innym sprzęcie mają przeważnie identyczne ustawienia.
Oprócz podstawowych parametrów takich jak własny numer AS, dowolna nazwa usługi i ewentualna zmiana identyfikatora bramki opraetor może korzystać z następujących parametrów:
• **redistribute-connected** (yes | no; domyślne: **no**) – po włączeniu bramka publikuje w sesjach z sąsiadami informacje o bezpośrednio połączonych („*connected*“) sieciach. Są to przykładowo sieci podłączone bezpośrednio do własnych złączy lub mostków i zaznaczone w tabeli jako połączone (DaC), Nadanie tej informacji nie wymaga wpisania wymienionych sieci na listę („*Networks*“).
• **redistribute-ospf** (yes | no; domyślnie: **no**) – po włączeniu bramka publikuje w BGP także trasy otrzymane przez OSPF.

• **redistribute-other-bgp** (yes | no; domyślnie: **no**) – określa, czy publikowane są także trasy otrzymane z innej kopii usługi (np. w bramce obsługującej równolegle dwa różne systemy AS.
• **redistribute-rip** (yes | no; domyślnie: **no**) – po włączeniu w BGP publikowane są też wszystkie trasy otrzymane przez RIP.
• **redistribute-static** (yes | no; domyślnie: **no**) – po włączeniu publikowane w sesjach BGP są także wszystkie trasy statyczne zawarte we własnej tabeli.

W HAMNECIE obowiązuje zwykle:
wyłączenie wszystkich parametrów grupy „Redistribute“ (NO).

Włączenie parametrów (i związanych z nimi funkcji) „*redistribute connected*“ i „*redistribute static*” może spowodować powstanie w sieci czarnych dziur, błędnych tras domyślnych, upublicznienie lokalnie zdefiniowanych tras statycznych, próbnych kanałów i złączy albo innych tras nie przeznaczonych do szerszego użytku!
Mogą to być przykładowo połączenia kablowe z DLC7, bramkami Linsys dla packet-radio itp. Pulikacją informacji powinny w sieci Hamnetu sterować tylko wpisy sieci i grup jak to omówiono powyżej. należy pamiętać, że błędne informacje o trasach rozprzestrzeniają się w sieci bardzo szybko. Funkcje „*redistribute*“ mogą być przydatne tylko w nielicznych wyjątkowych przypadkach, ale przed ich użyciem nalezy dokładnie przejrzeć i przeanalizować lokalną sytuację i ustawienia bramki.

3.4.7 Odległość administracyjna w tabelach tras

Odległość administracyjna podawana w tabelach bywa często źle rozumiana. Informuje ona o wiarygodności trasy lub informacji o niej. Nie jest ona w żadnym wypadku miarą fizycznej długości trasy albo liczby odcinków, z których się składa (długości logicznej), czy też kosztów itp.
Standardowymi wartościami parametru w BGP są 20 (dla tras otrzymanych przez eBGP) i 200 (dla tras otrzymanych przez iBGP). Wartości domyślne przyjmuje się następująco:

Connected interface (DaC)	0 – połączenie bezpośrednie
Static route (AS)	1 – trasa statyczna
External BGP (DaB)	20 – trasa otrzymana przez eBGP
OSPF	110 – trasa otrzymana przez OSPF
IS-IS	115 – trasa otrzymana przez IS-IS
RIP	120 – trasa otrzymana przez RIP
Internal BGP (DaB)	200 – trasa otrzymana przez iBGP
Unknown	255 – nieznane źródło pochodzenia lub charakter trasy

Podstawowa zasada: dla identycznych sieci połączenie typu „DaC” ma pierwszeństwo przed wpisami „AS-„ i „DaB”. Oznacza to, że bezpośrednie połączenie bramki z celem ma pierwszeństwo przed trasami statycznymi i otrzymanymi w ramach sesji BGP. Pierwszeństwo to wynika jedynie z wiarygodności trasy – czyli tzw. odległości administracyjnej. Na odległość tą można wpływać za pomocą ustalonych zasad (ang. „*routing policies*“) i filtrów.

3.5 Filtry, zasady wyboru tras

Zasada podstawowa: Ustawienia filtrów i zapory przeciwwłamaniowej (ang. „*firewall*“) to dwie różne pary kaloszy!
Filtry pozwalają na praktyczne wprowadzenie zasad wyboru tras (ang. “*routing policies*“). Dotyczy to zarowno ignorowania prywatnych obszarów adresowych jak i wpływu na priorytety wyboru tras. Jedną z możliwości może być rozmyślne preferowanie trasy dłuższej w stosunku do krótszej i szybszej jeżeli jest ona pewniejsza (pracuje stabilniej). Czasami stosowane bywa także sztuczne przedłużanie trasy AS (AS_PATH) dla zmniejszenia jej atrakcyjności. Filtry pozwalają w miarę potrzeby na eliminację niektórych informacji z sesji np. sieci składających się na publikowaną już grupę.
Zasadniczo wszystkie prywatne sieci powinny być ignorowane przez Hamnet. Ignorowanie adresów IP związanych z sieciami prywatnymi nie jest tożsame z funkcjonowaniem zapory przeciwwłamaniowej.
Przykłady konfiguracji „Winboxu” i definiowania prostych filtrów podano w rozdziale 4.

4 HAMNET Przykładowe konfiguracje WINBOX

W punkcie 4.1 opisane są menu programu „Winbox" i związane z nimi funkcje. Opisana jest tylko wizualna konfiguracja „Winboxu" w oknach. Dopuszczalna jest wprawdzie także konfiguracja w konsoli (oknie wiersza poleceń), ale nie została ona tutaj opisana.

W punktach 4.2 do 4.4 przedstawiono przykładowe konfiguracje wraz z ujęciami ekranowymi dla przykładowych lokalizacji – ze wszystkimi niezbędnymi parametrami.

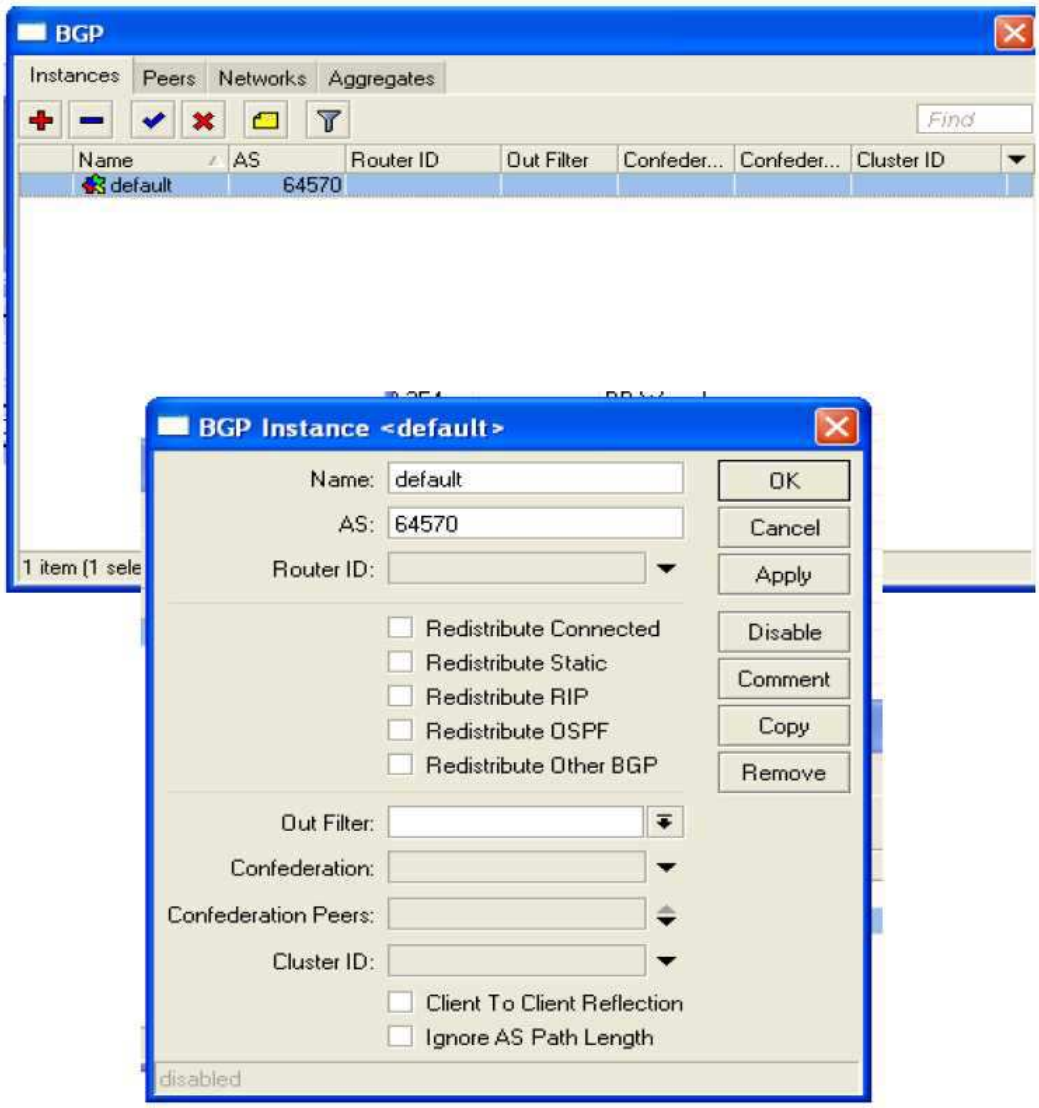
Punkty 4.2 do 4.4 dają w miarę możliwości przepis na podstawową konfigurację Hamnetu!

4.1 Opis menu

W tym punkcie opisane są menu programu „Winbox" i ich parametry.

4.1.1 „*Instances*" (usługa BGP)

Po wybraniu w zakładce „*Instances*" („Usługi") czynnej usługi lub dodaniu nowej w celu jej uruchomienia na ekranie wyświetlane jest następujące okno:

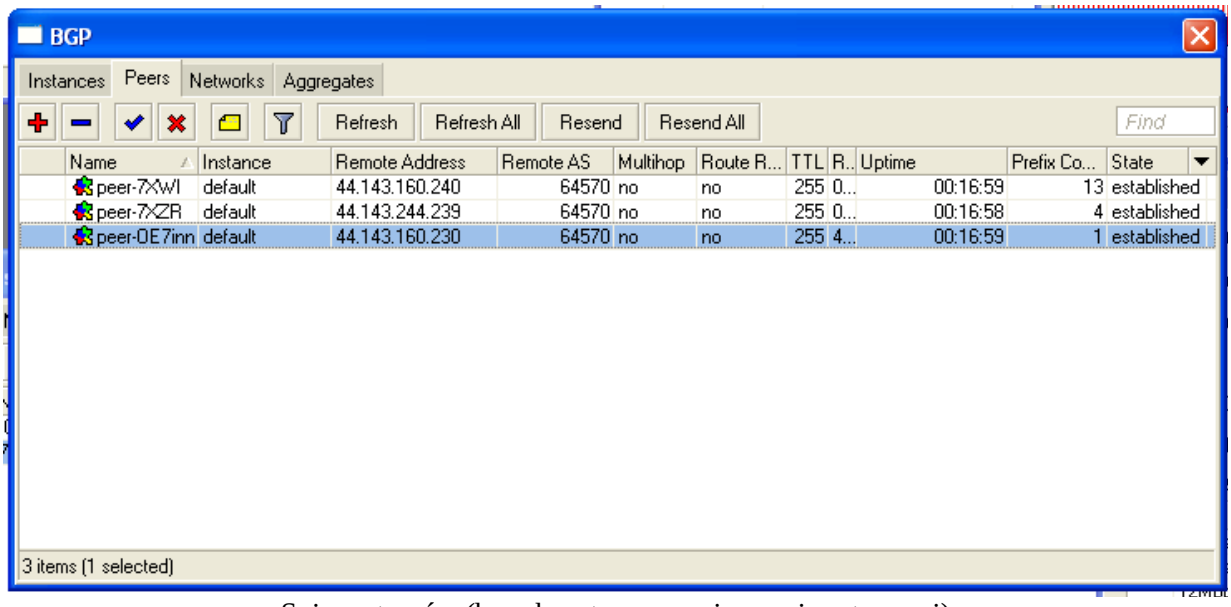


Okno to zawiera następujące pola:

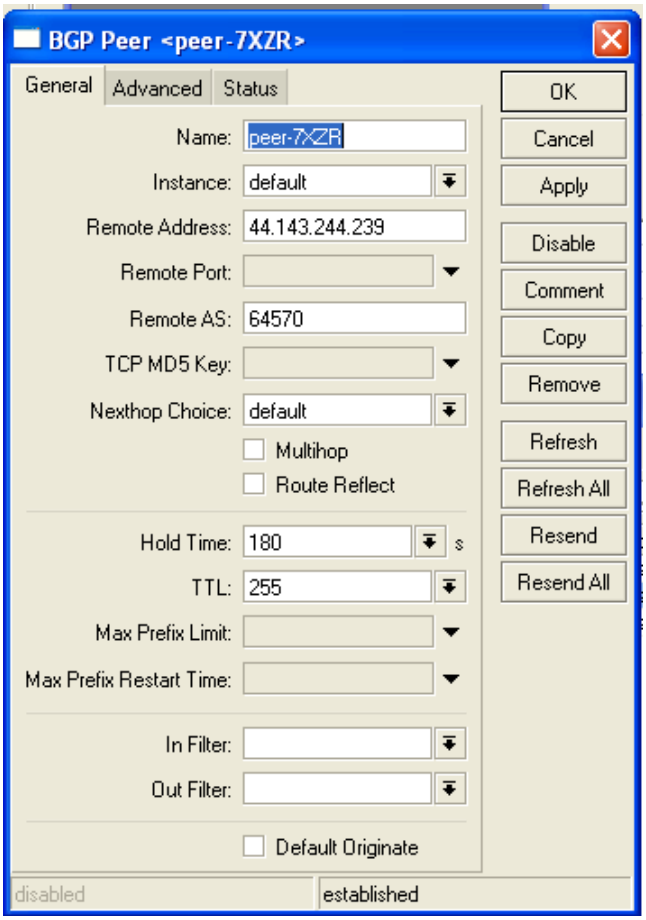
as (*liczba całkowita*: 0..65535) – numer systemu AS, w którym pracuje dana bramka (usługa), przykładowo: 64560 dla OE6).
Domyślne ustawienie dla Hamnetu: **Numer AS kraju związkowego [w Austrii, gdzie indziej regionu lub okręgu – przyp. tłum.], w którym zlokalizowana jest bramka**.
name (*nazwa*; domyślnie: "") – nazwa usługi, np.: „default“ albo „OE6XKR“
out-filter (*nazwa*; domyślnie: "") – wybór ogólnego filtru wyjściowego czynnego dla wszystkich sesji BGP tej usługi.
redistribute-connected (yes | no; domyślnie: **no**) – po włączeniu bramka rozpowszechnia w ramach sesji BGP informacje o wszystkich bezpośrednio z nim połączonych sieciach („*connected*”) korzystających z fizycznych złączy bramki lub mostków i zapisanych jako połączone w tabeli tras („DaC”). Rozpowszechnianie tych informacji nie wymaga umieszczenia ich na liście sieci („*Networks*”). Ta i pozostałe możliwości nie są wykorzystywane w Hamnecie.
Domyślne ustawienie dla Hamnetu: **no**
redistribute-ospf (yes | no; domyślnie: **no**) – po włączeniu bramka rozpowszechnia w ramach sesji BGP informacje otrzymane przez OSPF.
Domyslne ustawienie dla Hamnetu: **no**
redistribute-other-bgp (yes | no; domyślnie: **no**) – decyduje o rozpowszechnianiu informacji o trasach otrzymanych z innej czynnej kopii usługi (np. jeśli bramka obsługuje jednocześnie sieci dwóch systemów).
Domyślne ustawienie dla Hamnetu: **no**
redistribute-rip (yes | no; domyślnie: **no**) – decyduje o rozpowszechnianiu przez BGP tras otrzymanych przez RIP.
Domyślne ustawienie dla Hamnetu: **no**
redistribute-static (yes | no; domyślnie: **no**) – decyduje o rozpowszechnianiu przez BGP tras statycznych znajdujących się we własnej tabeli.
Default-Einstellung für HAMNET: **no**
router-id (*adres IP*; domyślnie: 0.0.0.0) – identyfikator bramki w postaci adresu IP. W przypadku braku identyfikatora system ustala go automatycznie w oparciu o otrzymywane trasy.

4.1.2 „Peers“ (partnerzy)

Po dodaniu nowej sesji BGP w zakładce „*Peers*“ (partenerzy; sąsiedzi) lub wybraniu jednej z czynnych wyświetlane jest następujące okno:



Spis partnerów (bramka z trzema wpisanymi partnerami)



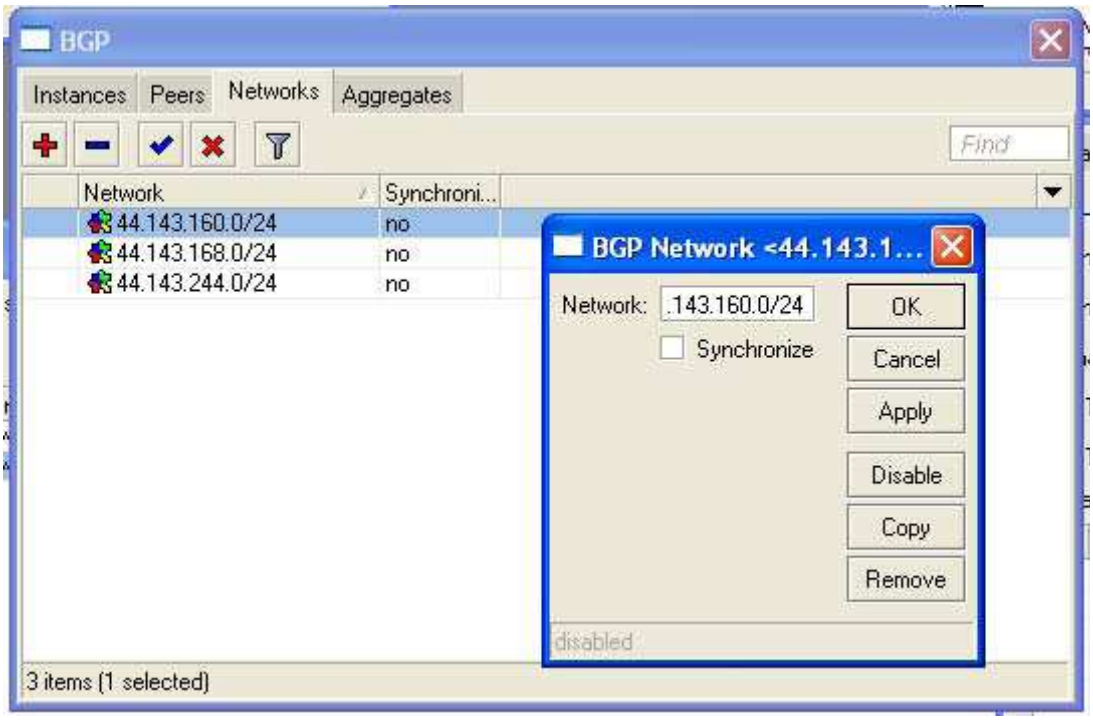
Okno partnerów zawiera następujące pola:
Name (*tekst)* – zawiera nazwę sesji BGP. Ustawienie dla Hamnetu: **peer-0XXX (ostanie 4 pozycje znaku wywoławczego partnera).**
Instance (*tekst)* – nazwa usługi. Ustawienie dla Hamnetu: **default.**
remote-address (*adres IP*; domyślnie: **0.0.0.0**) – adres IP partnera (dla tej sesji BGP).
Ustawienie dla Hamnetu: **adres partnera w sieci szkieletowej des Partners, oparty na koncepcie IP.**
remote-as (*liczba całkowita*; domyślnie: **0**) – numer AS systemu partnera (dla tej sesji BGP).
Ustawienia dla Hamnetu: **w Austrii numer AS kraju związkowego OE1–OE9, gdzie indziej – rejonu lub okręgu.**
hold-time (*czas*) – czas oczekiwania na aktywność w trakcie sesji BGP (czas braku aktuwności). Dla jej podtrzymania przed upływem zadanego czasu powinny do bramki dotrzeć od partnera komunikaty użytkowe dowolnego rodzaju albo komunikaty podtrzymujące połączenie. Po jego upływie bez żadnej aktywności połączenie zostaje przerwane.
Domyślne ustawienie dla Hamnetu: **180**
keepalive-time (*czas*) – odstęp czasu między transmisjami komunikatów podtrzymujących do partnerów połączenie („*Keepalive*“). Po nawiązaniu sesji łączności (otrzymaniu komunikatu „*Established*“) czas ten jest komunikowany partnerom.
Domyślnie dla Hamnetu: **255**
multihop (yes | no; domyślnie: **no**) – po włączeniu pozwala na nawiązywanie sesji w kanałach kilkuodcinkowych („*multihop*“), a więc z partnerami niedostępnymi bezpośrednio. Połączenia takie nie są nawiązywane jeśli trasa prowadząca do sąsiada jest trasa domyślną (0.0.0.0/0).
Domyślnie dla Hamnetu: **no**
in-filter (*nazwa*; domyślnie: "") – nazwa filtru wejściowego oddziaływującego na informacje napływające w trakcie sesji BGP (z danym partnerem), np. filtr dla adresów prywatnych.
out-filter (*nazwa*; domyślnie: "") – nazwa filtru wyjściowego oddziaływującego na informacje nadawane w trakcie sesji BGP (z danym partnerem), np. filtr dla adresów prywatnych.

4.1.3 „Advertisments“ (publikacje) – dane tylko do odczytu

W menu „***Advertisments***“ (publikacje) wyświetlana jest informacja o aktualnie wychodzących komunikatach rozpowszechniających trasy.
TYLKO W KONSOLI
prefix (*prefiks IP*) – właśnie nadawany prefiks NLRI,
nexthop (*adres IP*) – aktualnie nadawany atrybut NEXT_HOP,
as-path (*tekst*) – aktualnie nadawany atrybut AS_PATH,
origin (igp | egp | incomplete) – bieżący atrybut ORIGIN, pochodzenie danych z własnego systemu, z obcego lub nieznane,
local-pref (*liczba całkowita*) – bieżąco nadawany atrybut LOCAL_PREF,
med (*liczba całkowita*) – aktualnie nadawany atrybut MULTI_EXIT_DISC,
atomic-aggregate (yes | no) – aktualnie nadawany atrybut ATOMIC_AGGREGATE (informuje o tym czy prefiks oznacza grupę kilku AS) *),
aggregator (*adres IP*) – właśnie nadawany dodatkowy atrybut AGGREGATOR (adres IP, w przypadku grupy informacja o grupującym *),
originator-id (*adres IP*) – aktualnie nadawany atrybut ORIGINATOR_ID,
cluster-list (*tekst*) – aktualnie nadawany atrybut CLUSTER_LIST,
peer (*tekst*) – partner.
*) Szczegóły w dokumencie RFC4271, w rozdziale 5.1.6 ATOMIC_AGGREGATE (grupowanie kilku AS) – w ausrtiackim Hamnecie na razie bez znaczenia.

4.1.4 „*Networks*“ (sieci)

W menu „*Networks*“ (spisie sieci) dodawane są informacje o sieciach przeznaczonych do pulikacji. Wpisy te nie powodują zapisania trasy we własnej tabeli tras.
Przy prawidłowej konfiguracji BGP w Hamnecie **dane ze spisu jednej z bramek rozchodzą się w szybkim tempie w całej sieci za pomocą sesji iBGP i eBGP**.



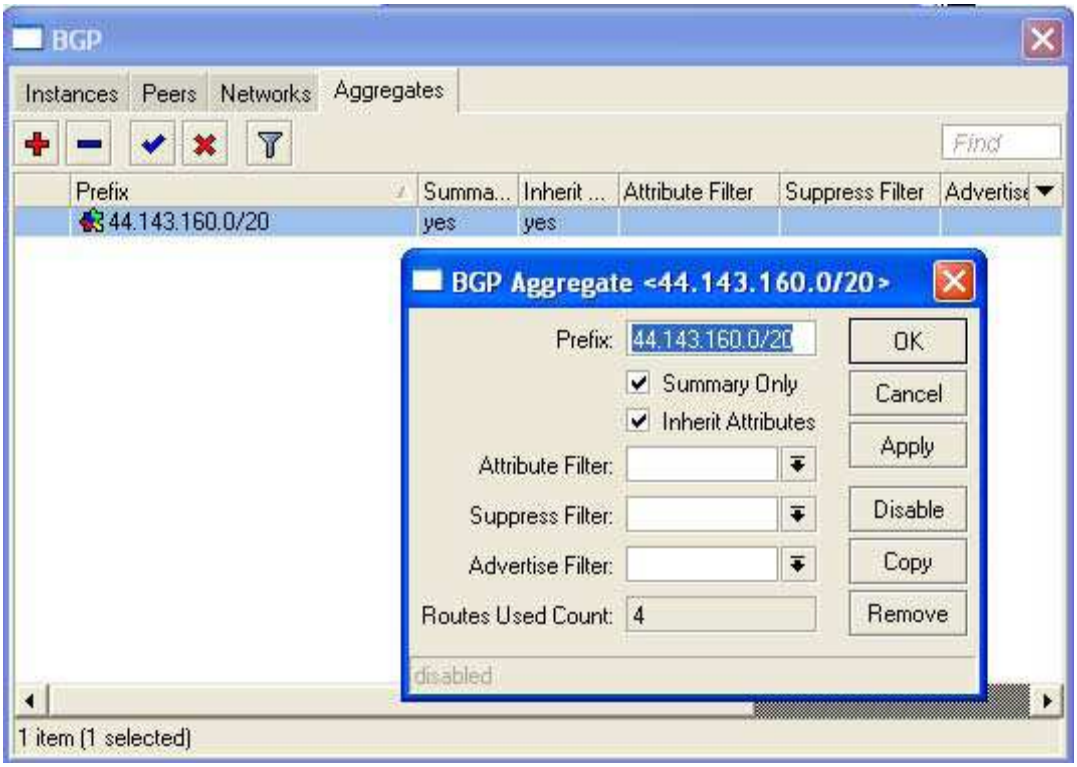
Okno sieci z okienkiem wprowadzania danych do listy

Okno zawiera następujące kolumny:
network (*prefiks IP*; domyślnie pusty) – prefiks przeznaczony do rozpowszechnienia, możliwe podanie grupy.

Domyślne ustawienie dla Hamnetu:
Wpisy wszystkich sieci podłączonych bezpośrednio do bramki (sieć szkieletowa, sieci użytkowe, usługowe i inne np. OLSP, PR) przeznaczone do rozpowszechniania w sieci Hamnetu. Możliwe jest wprowadzanie grup jako alternatywy – z sumowaniem prefiksów i utajnianiem ich składników.
synchronize (yes | no; domyślnie: **no**) – włączenie powoduje publikowanie wyłącznie informacji o trasach, dla których w tabeli tras znajdują się pasujące dane (ang. *„Matching-Route“*).
Domyślne ustawienie dla Hamnetu: **no**, poza sytuacjami szczególnych topologii lub grup.

4.1.5 *„Route Aggregates“* (grupowanie tras)

BGP pozwala na grupowanie poszczególnych wybranych tras w jedną wspólną. Menu to ('/routing bgp aggregate') służy do podania grupowanych tras i atrybutów grupy. Pozwala na bardziej wyczerpujące zdefiniowanie grupy aniżeli za pomocą listy sieci.



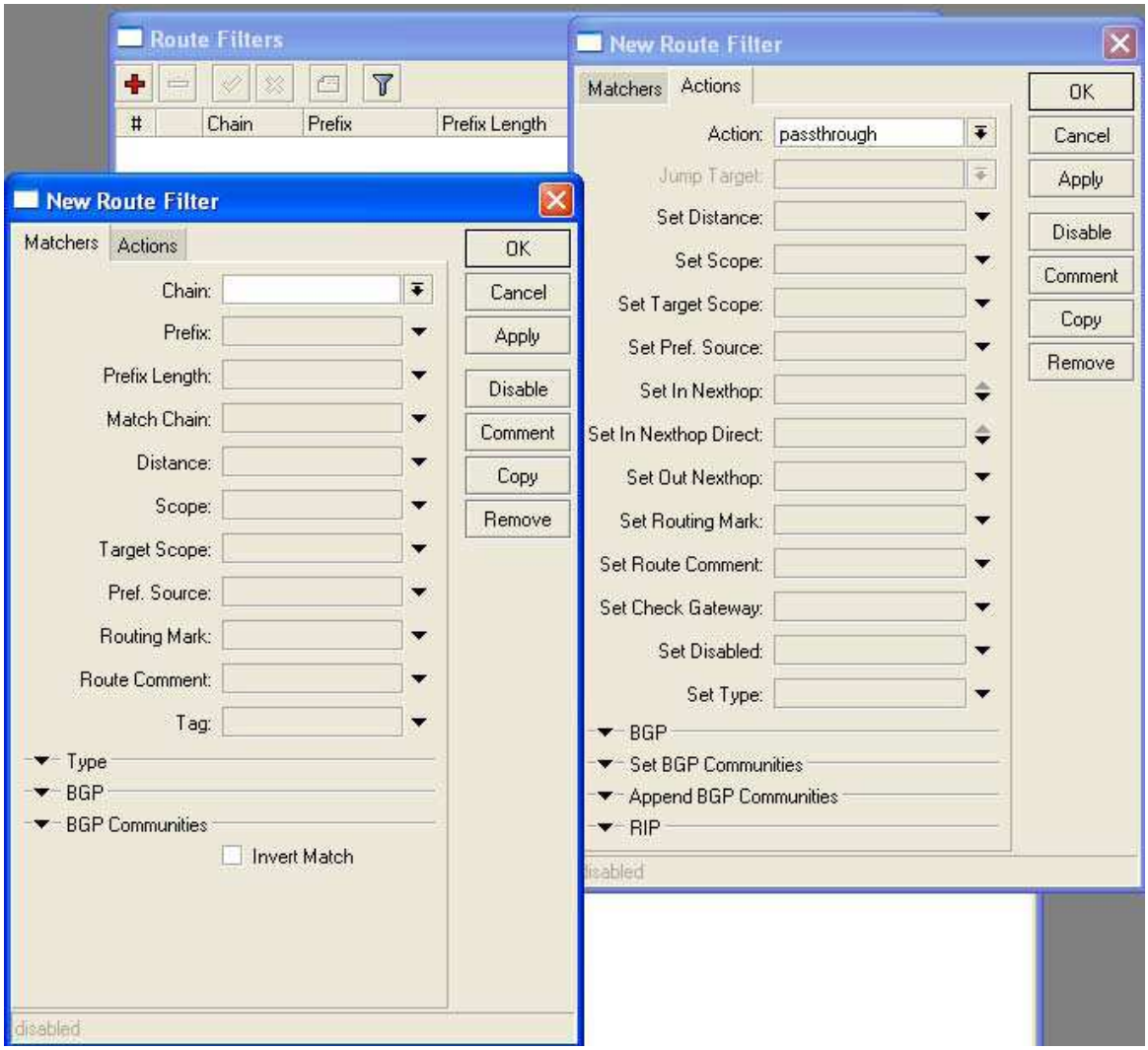
Grupowanie tras

Okno zawiera następujące pola:
advertise-filter (*tekst*; domyślnie: "") – nazwa istniejącego (wcześniej zdefiniowanej) sekwencji filtrów (*„Verkettung“ / „Chain“*) służącej do wyboru atrybutów tras przekazywanych grupie (dziedziczonych przez nią).
attribute-filter (*tekst*; domyślnie: "") – nazwa istniejącej sekwencji (ciągu) filtrów nadających grupie atrybuty.
inherit-attributes (yes | no; domyślnie: yes) – decyduje o tym, czy atrybuty grupy mogą być dziedziczone.
instance (*tekst*; domyślnie pusty) – usługa związana z daną siecią.
prefix (prefiks IP; domyślnie pusty) – prefiks grupy (adres IP z odpowiednią liczbą bitów znaczących)
summary-only (yes | no; domyślnie: yes) – decyduje o tym, czy pojedyńcze sieci wchodzące w skład grupy są utajniane czy też dalej publikowane.
Uwaga: Utajniane są wszystkie pasujące sieci z tabeli tras, ale nie dane zawarte w tabeli sieci nawet jeżeli należą do tego samego zakresu adresów co grupa.
suppress-filter (*tekst*; domyślnie: "") – nazwa istniejącej sekwencji filtrów służących do wyboru utajnianych tras.

4.1.6 Wyświetlana informacja o grupowaniu tras

TYLKO W KONSOLI
routes-used (*liczba całkowita*) – statystyka grupy tras.
in console – spis używanych identyfikatorów konsoli, liczba używanych tras (tylko dla „Winboxu“).
aggregated routes – wszystkie trasy wchodzące w skład zakresu grupy. Naj[prawdopodobniej są one wszystkie utajnione i nie są publikowane pojedyńczo, o ile nie są dopuszczone do publikacji przez specjalny filtr utajniający (ang. „*suppress-Filter*“).
aggregate route – trasa utworzona w wyniku grupowania.
Uwaga:
Grupowane są tylko trasy otrzymane od partnerów w ramach sesji BGP i tylko przez tą samą kopię usługi. W Hamnecie i tak usługa BGP jest uruchamiana tylko raz na danej bramce.
Porady:
• Filtry utajniające (ang. „*Suppress-Filter*“) przynoszą efekty tylko wtedy gdy parametr '**summary-only=no**'
• Filtry upubliczniania (ang. „*Advertise-filter*“) przynoszą efekty tylko wtedy gdy parametr '**inherit-attributes=yes**'
• W przypadku gdy filtry atrybutów (ang. „*Attribute-Filter*“) zareagują na polecenia '*reject*' albo '*discard*' dane grupy nie są publikowane.

4.1.7 Filtry



Menu filtrów

System operacyjny bramki zawiera obszerne funkcje filtrowania, co pozwala na definiowanie zasad rozpowszechniania tras (ang. „*Routing-Policies*“) niezależnie od ustawień zapory przeciwwłamaniowej (ang. „*firewall”*). Powiązane ze sobą filtry lub ich grupy pracują sekwencyjne – kolejno jeden po drugim. Pominąwszy zasadę ignorowania sieci prywatnych i jednolitych ustaleń odnośnie publikowanych danych, w sieci Hamnetu nie obowiązują żadne inne zasady ogólne. Poszczególne bramki mogą jednak wymagać sformułowania lokalnych zasad.

Do dyspozycji są następujące polecenia:
action (accept | discard | jump | none | reject | return; default: **none**) – akcja przeprowadzana na danych trasy lub jej atrybutach dla przefiksów NLRI spełniających kryteria filtracji.
accept – akceptowanie informacji o trasach dla danego prefiksu NLRI.
discard – całkowite wykluczenie danego prefiksu z przetwarzania przez BGP. Trasa jest całkowicie usuwana z otrzymanego komunikatu. W komunikatach wychodzących funkcja **discard** jest identyczna z **reject jump** – przekazaniem przetwarzania innej sekwencji filtrów. Sekwencja ta musi być zdefiniowana jako cel skoku – „**jump-target“**.
none – brak jakiej kolwiek akcji i przejście do następnego punktu.
reject – usunięcie informacji o trasie spełniającej kryteria filtracji. Prefiks ten występujący w otrzymywanym komunikacie jest zaznaczony za pomocą **R** („*rejected*“) w polu RT po wywołaniu spisu w konsoli za pomocą polecenia **ip route print.** Prefiks ten nie jest rozpowszechniany w komunikatach wychodzących.
return – powrót do poprzedniej sekwencji, w której wystąpił skok (**jump)**.
as-path (*tekst***)** – kryterium poszukiwania w atrybucie AS_PATH. Dodatkowy argument ^ przed kryterium powoduje poszukiwanie tekstu na początku AS_PATH, a $ – na jego końcu.
as-path-length (*liczby całkowite*) – długość atrybutu AS_PATH oznaczająca liczbę zawartych w nim przebytych systemów autonomicznych. Uwaga: wielokrotne AS_SET są traktowane jako jeden system AS.
atomic-aggregate (absent | present) – sprawdzenie czy atrybut ATOMIC_AGGREGATE ma wartość „yes“.
chain (*tekst*) – nazwa modyfikowanej sekwencji. W przypadku gdy sekwencja o danej nazwie nie istnieje jest on zakładany jako nowy.
distance (*liczby całkowite*; domyślnie: **nic**) – odległość administracyjna niezależna od protokółu służąca do porównania tras otrzymanych z innych źródeł (parametr wiarygodności tras).
jump-target (*nazwa*) – nazwa sekwencji stanowiącej cel skoku gdy **action=jump**.
local-pref (*liczby całkowite*) – poszukiwanie podanej wartości w atrybucie LOCAL_PREF.
match-chain (*nazwa*) – nazwa grupy filtrów lub ich sekwencji używanej do filtracji określonej grupy tras. Jeżeli trasa została przyjęta przez filtry jest to sygnalizowane w celu „wyciągnięcia“ trasy z komunikatu.
med (*liczby całkowite*) – poszukiwanie podanej wartości w atrybucie MULTI_EXIT_DISC.
origin (igp | egp | incomplete) – poszukiwanie podanego typu w atrybucie ORIGIN.
prefix (*adres IP address*/*maska sieci* | *adres IP-adres IP*) – poszukiwanie podanego prefiksu NLRI.
prefix-length (*liczby całkowite*) – poszukiwanie podanej długości prefiksu NLRI.
prefsrc (*adres IP address*/*maska sieci* | *adres IP – adres IP*) – poszukiwanie podanego adresu IP źródła danej trasy.
route-comment (*tekst*) – poszukiwanie podanego komentarza w trasie (operatorzy mogą dodawać dowolne komentarze dla wyróżnienia określonych tras lub podania szczególnych informacji o nich).
routing-mark (*tekst*) – poszukiwanie wpisu zaznaczającego trasę jako wymagającą szczególnego przetworzenia („*Routing mark*“). Jest to chętnie stosowane przez operatorów różnych systemów autonomicznych. W Hamnecie stosowane w zależności od potrzeb – brak specjalnych zaleceń.
scope (*liczby całkowite*: 0..255-0..255) - **scope** i **target-scope** sa stosowane do rekursywnego poszukiwania adresu następnego odcinka (“*Next hop*“). Trasy używane w poszukiwaniu adresu odcinka określonej trasy powinny mieć wartość parametru **scope** mniejszą lub równą wartości **target-scope** tej trasy.
set-check-gateway (ping | arp) – określa czy bramka BGP musi wypróbować dostęp do danej trasy za pomocą „ping“ lub „arp“ przed opublikowaniem jej danych. Pozwala to na stwierdzenie czy bramka wejściowa trasy (ang. *gateway*) jest rzeczywiście czynna.

set-disabled – powoduje wyłączenie trasy. Trasy wyłączone nie są brane pod uwagę przez algorytm BGP poszukujący najlepszych tras.
set-distance (*liczba całkowita*: 0..255) – służy do wprowadzenia niestandardowej odległości administracyjnej (różnej od: eBGP 20, iBGP 200). Odległość ta nie jest związana z protokołem i jest wykorzystywana do porównania między sobą tras prowadzących do tego samego celu otrzymanych z różnych źródeł. Określa ona stopień wiarygodności tras i jest wyświetlana w tabeli tras w „Winboxie".
set-localpref (*liczba całkowita*: 0..4294967295) – wartość atrybutu LOCAL_PREF dla danej trasy.
set-med (*liczba całkowita*: 0..4294967295) – wartość atrybutu MULTI_EXIT_DISC.
set-nexthop (*adres IP*) – docelowy adres IP następnego odcinka danej trasy.
set-prefsrc (*adres IP*) – adres preferowanego źródła danej trasy (ang. "*preffered source address*").
set-prepend (liczba całkowita: 0..16) – określa dopuszczalną liczbę kolejnych zapisów własnego AS w atrybucie AS_PATH. Dodawanie systemów do trasy jest stosowane w celu obniżenia jej atrakcyjności dla partnerów (z różnorodnych przyczyn). Jest to jeden z wielu sposobów obniżenia atrakcyjności trasy.
set-route-comment (*tekst*) – dodanie komentarza do danej trasy np. przez operatorów lub administratorów.
set-routing-mark (*tekst*) – dodanie znacznika „*routing mark*" (patrz wyżej) ułatwiającego rozpoznanie trasy przez którąś z innych bramek i np. zastosowanie wobec niej szczególnych zasad. Funkcja chętnie używana przez operatorów rozmaitych systemów autonomicznych.
set-scope (*liczba całkowita*: 0..255) – wartość parametru **scope** dla danej trasy. Parametry **scope** i **target-scope** są używane w rekursywnym poszukiwaniu adresu następnego odcinka danej trasy. Trasy uwzględniane w poszukiwaniu muszą mieć parametr **scope** równy lub mniejszy od parametru **target-scope** danej trasy.
set-target-scope (*liczba całkowita*: 0..255) – wartość parametru **target-scope** danej trasy, patrz **scope**
set-weight (*liczba całkowita*: -2147483648..2147483647) – wartość „wagi" danej trasy. Jest ona uwzględniana trasy na samym początku przez algorytm BGP poszukujący najkorzystniejszej.
target-scope (*liczba całkowita*: 0..255-0..255) – parametry **scope** i **target-scope** w rekursywnym poszukiwaniu adrsu następnego odcinka trasy. Patrz: **scope**.
type (absent | present) – poszukiwanie podanej wartości atrybutu ATOMIC_AGGREGATE.
unset (*wybór z podanych możliwości:* prefsrc | routing-mark | check-gateway | disabled) – kasuje wymieniony parametr danej trasy (np.: usunięcie znacznika „*Routing Mark*" przed rozpowszechnieniem trasy).
weight (liczba całkowita: -2147483648..2147483647) – poszukiwanie wymienionej wagi trasy.

4.1.8 Tabela tras

Tabela tras zawiera znane sieci docelowe i trasy prowadzące do nich. Sieci mogą być osiągalne przez partnerów lub podłączone bezpośrednio (fizycznie).

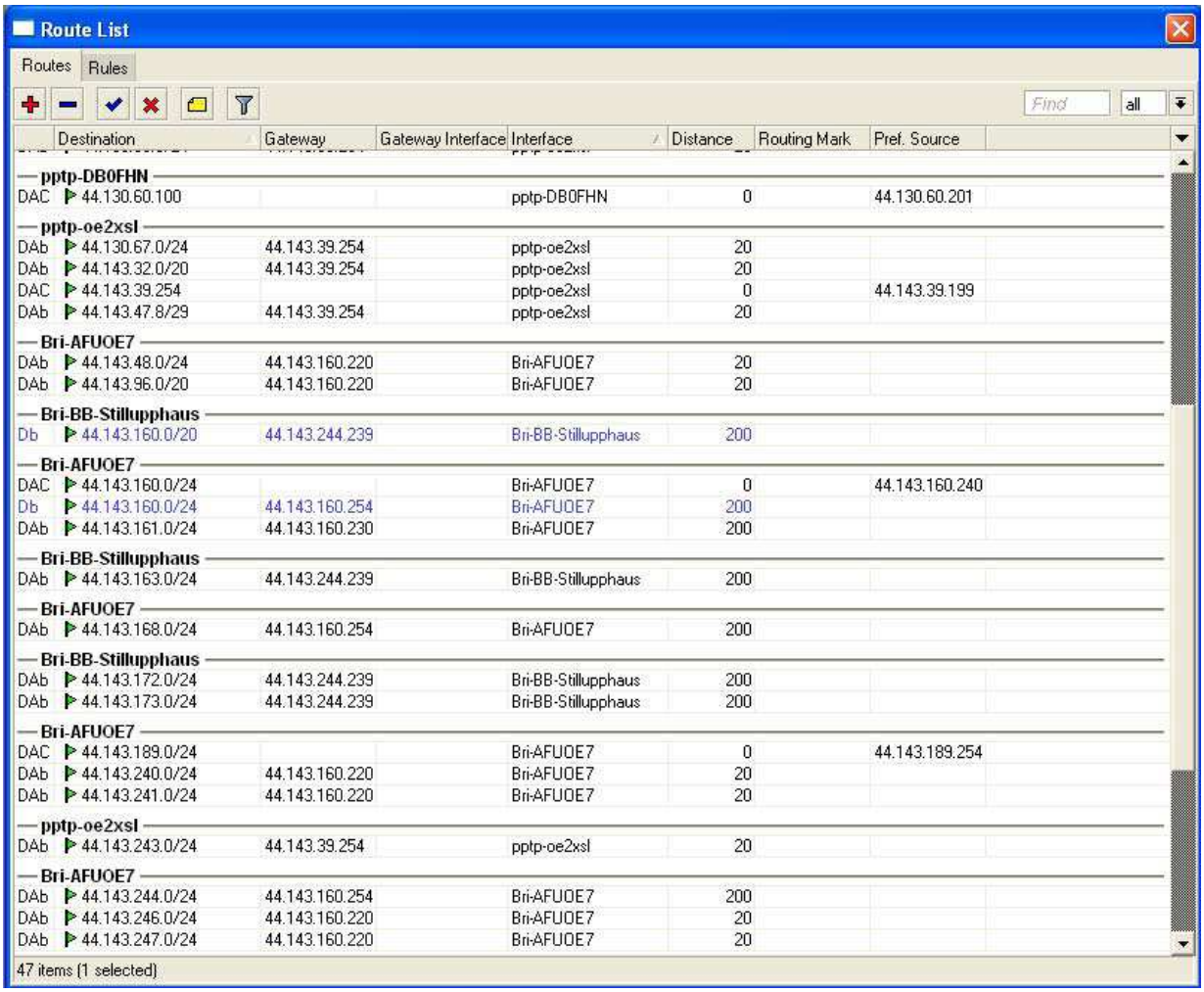


Tabela tras programu „Winbox“ w postaci kolumnowej („*show columns*“)

AS: czynne trasy statyczne.
DAC – trasy prowadzące przez mostki lub własne złącza – „*Dynamisch Aktiv Connected*“ (dynamiczne, połączone, czynne).
DAb – trasy otrzymane w trakcie sesji BGP – „*Dynamisch Aktiv BGP*“ (dynamiczne, czynne trasy BGP).
Db – trasy otrzymane w trakcie sesji BGP ale nie czynne – „*Dynamisch BGP*“ (dynamiczne BGP).

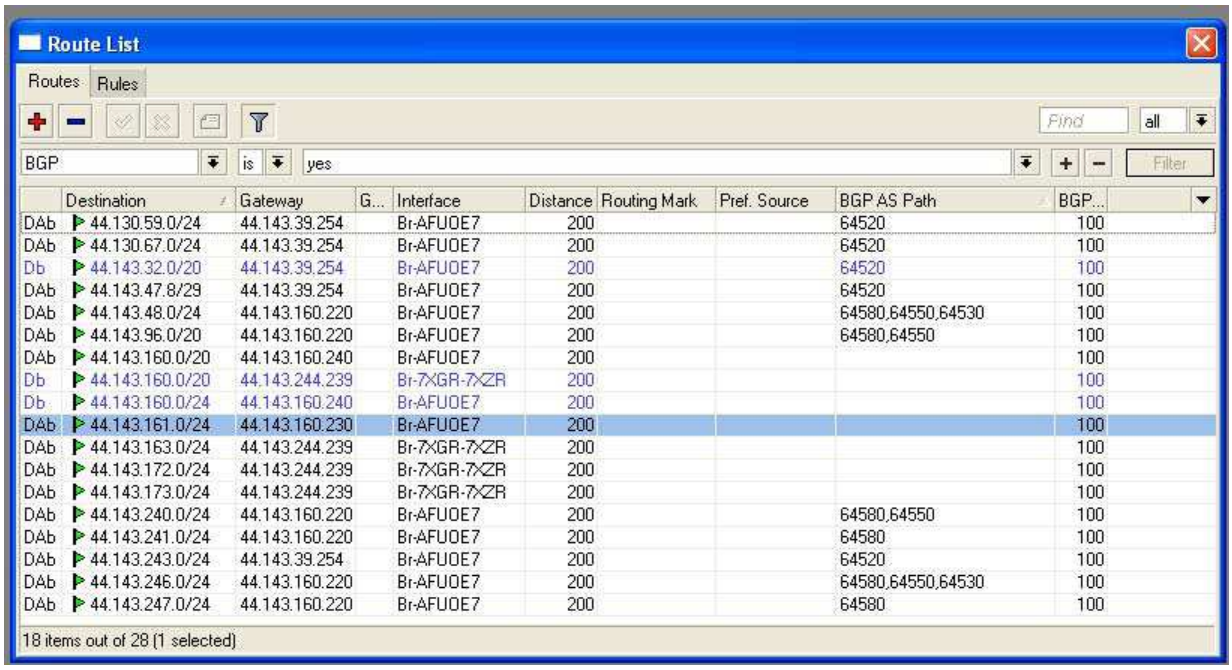
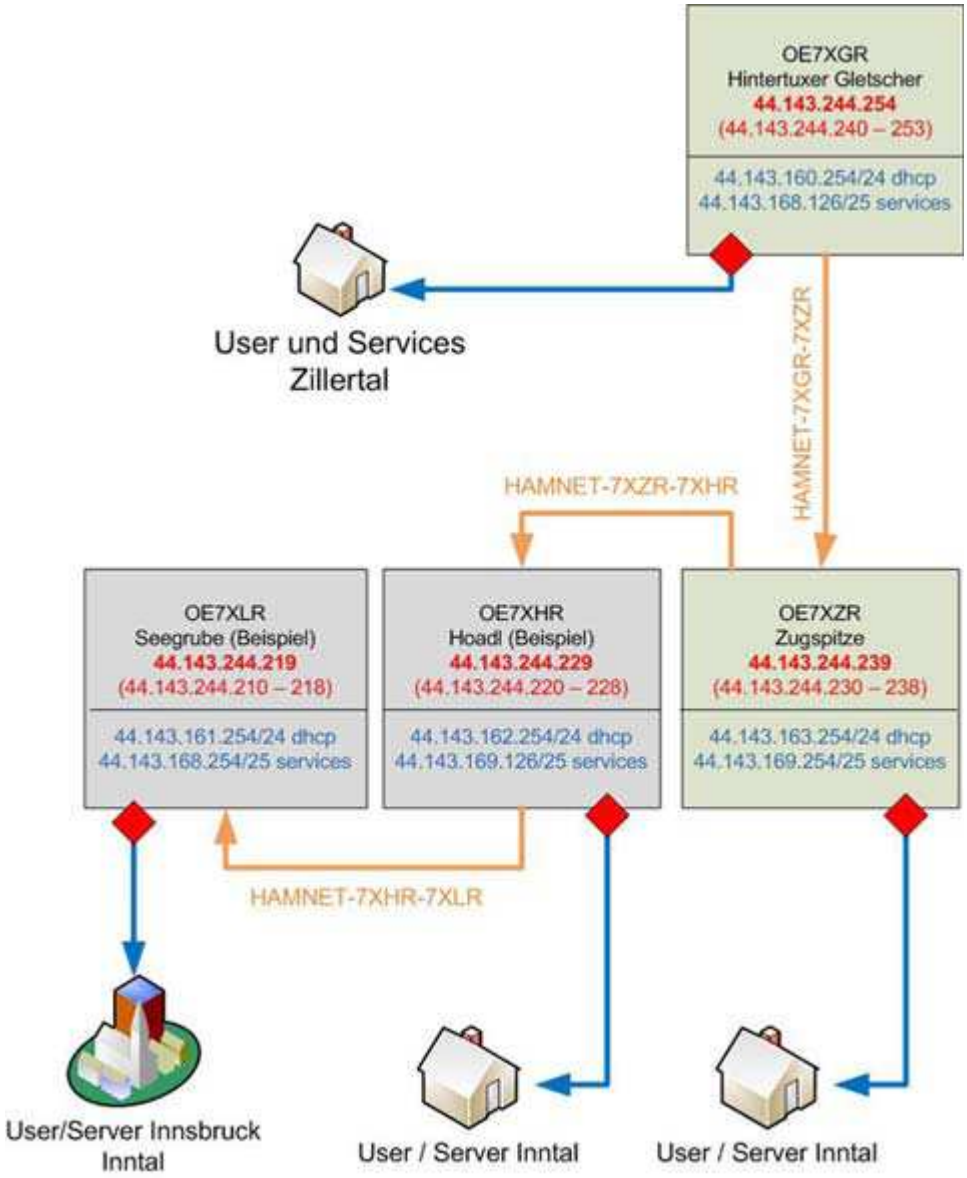


Tabela tras w „Winboxie“ w postaci standardowej, m.in. z wyświetlaną kolumną BGP PATH.

4.2 Przykladowa konfiguracja jako węzła lub bramki iBGP

Przykładowa, omawiana dalej konfiguracja BGP węzła **OE7XGR** opiera się na podanej na ilustracji fikcyjnej topologii systemu autonomicznego w Tyrolu (AS = 64570). W każdej z kratek symbolizujących węzły podane są:znak wywoławczy węzła, jego lokalizacja (QTH), jego adres IP z zakresu adresów IP jego podsieci, adresy IP dla DHCP i do celów służbowych sieci. Każdy z nich posiada wejścia dla użytkowników w swojej okolicy.

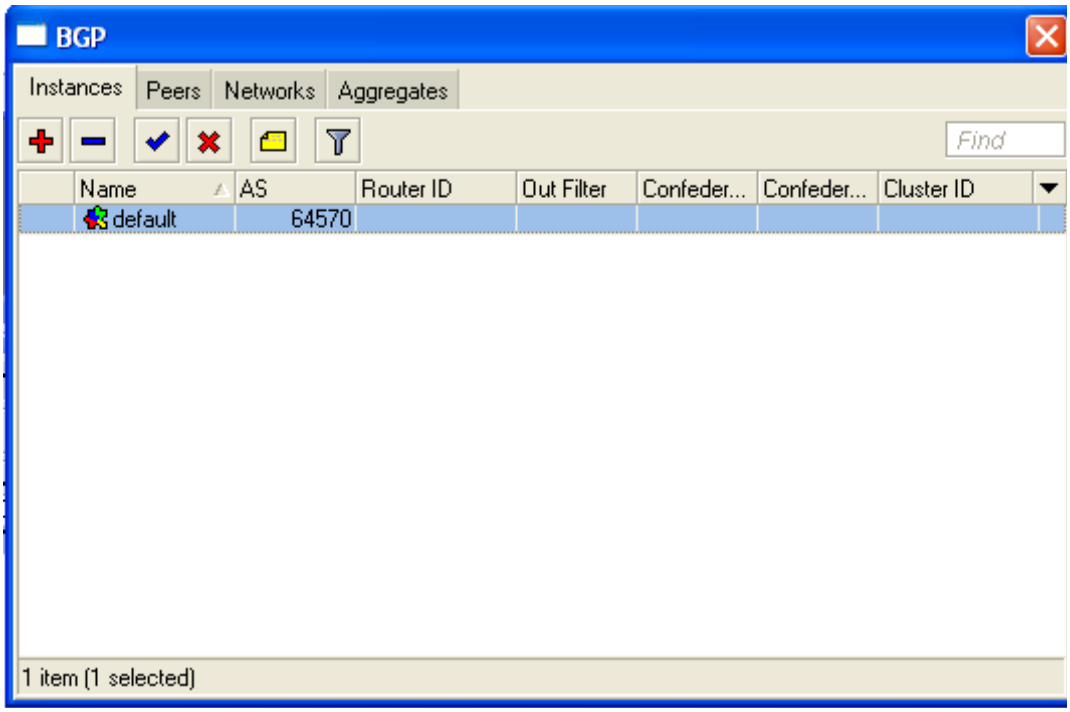


Na początek przyjmujemy, że ta fikcyjna sieć OE7 nie posiada połączeń z innymi regionami kraju i za granicą. Na czas konfiguracji BGP w rejonie Tyrolu sieć ta jest rozpatrywana w oderwaniu od reszty Hamnetu. Informacje o trasach są w niej rozpowszechniane za pomocą sesji iBGP.

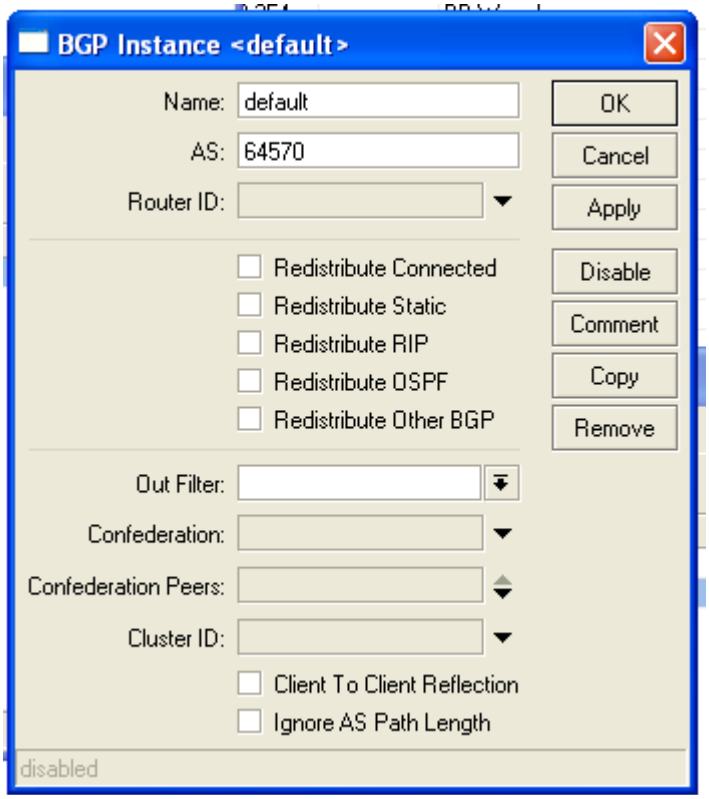
4.2.1 Krok 1: konfiguracja usługi wyboru tras na OE7XGR

Zakładamy, że usługa BGP na OE7XGR nie jest jeszcze skonfigurowana ale podstawowe konfiguracje dostępu dla użytkowników, usług, złączy i mostków są już wykonane prawidłowo. Przyjmujemy, że widoczne na ilustracji węzły są już uruchomione i osiągalne przez sieć szkieletową. W celu dotarcia do omawianych i pokazanych na ilustracjach okien podawana jest kolejność wywoływanych punktów menu, wybieranych zakładek itp.

Winbox -> ROUTING->BGP->INSTANCES
Wyświetlane jest okno usług („*instances*“), które może ewentualnie zawierać już wpis domyślny.



Za pomocą przycisku „plusa” wprowadzane są w poniższym oknie konfiguracji dane nowej usługi, a przez podwójne naciśnięcie myszą istniejącego wpisu (domyślnego – o nazwie „default“ jak na ilustracji) otwierane jest to samo okno z danymi dla ich modyfikacji.



• Pole „Name“: wpisać lub pozostawić nazwę „default“

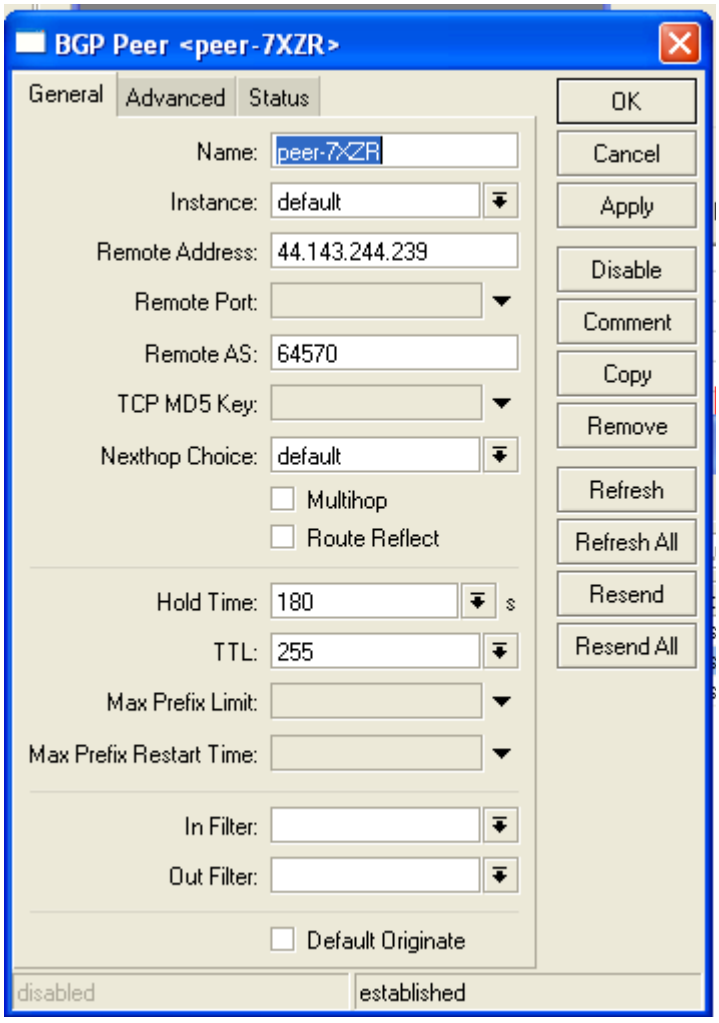
• Pole „AS”: podać numer AS, dla OE7 jest to 64570
• w pozostałych polach nie należy niczego włączać ani wybierać
• potwierdzić przyciskiem „ OK“
• Gotowe

Uwaga: Na bramce Hamnetu usługa BGP jest uruchamiana zasadaniczo tylko raz. Należy upewnić się, że w oknie usług wymieniona jest tylko jedna z nich – ta pożądana i właśnie skonfigurowana.

4.2.2 Krok 2: Konfiguracja sesji BGP

Każda z sesji jest przypisana do jednego z partnerów (ang. *peer*) bramki BGP. W skład przykładowej sieci OE7 wchodzą cztery bramki. Zgodnie z zasadą przeprowadzania pełnego kompletu sesji – sesji całościowej – (ang. *full-mesh*) w ramach danego systemu konieczne jest skonfigurowanie trzech sesji dla trzech pozostałych bramek sieci – trzech partnerów.

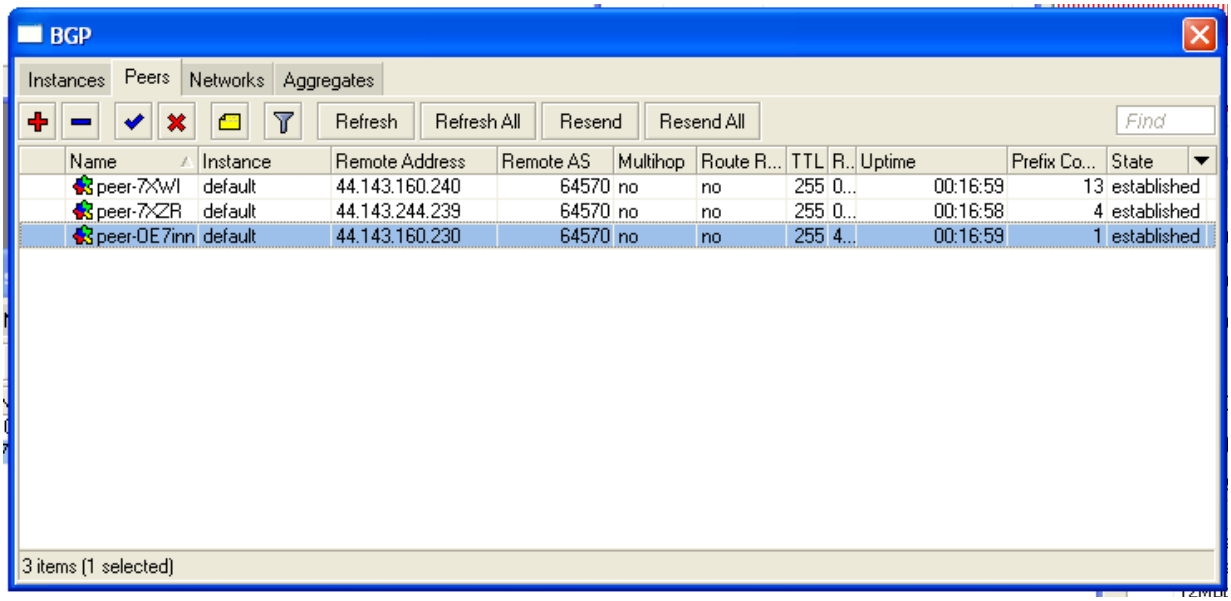
Winbox -> ROUTING->BGP->Peers
Otwierane jest okno zawierające spis partnerów („*Peers*“), które początkowo jest puste. W celu dodania partnera należy posłużyć się przyciskiem z symbolem plusa, który powoduje otwarcie pokazanego poniżej okna dialogowego. Przykład na ilustracji zawiera dane dla partnera OE7XZR:



• Pole „Name“: peer-7XZR (nazwa może być dowolna, jest to tylko praktyczny przykład!)
• Pole „Instance“: „default“ – nazwa poprzednio skonfigurowanej usługi.
• Pole „Remote-Adress“: 44.143.XXX.XXX (adres IP partnera)
• Pole „Remote Port“: puste = logiczny kanał domyślny (kanał TCP 179)

• Pole „Remote AS“: 645xx (numer AS systemu zgodnie z przydziałem dla regionu)
• Pozostałe pola: jak na ilustracji
• Potwierdzić przyciskiem „OK“
• Gotowe

Ilustracja przedstawia konfigurację sesji BGP z OE7XZR. W identyczny sposób należy skonfigurować sesje połączeń z OE7XLR i OE7XHR, tak że w ostatecznym wyniku skonfigurowane zostają trzy niezbędne sesje. Oczywiście do prowadzenia sesji potrzebne są odpowiednie konfiguracje u partnerów (kroki 1 i 2 należy więc odpowiednio powtórzyć w bramkach OE7XZR, OE7XHR i OE7XLR.
Po zakończniu tych wszystkich konfiguracji bramki powinny rozpocząć między sobą sesje iBGP i powinny się one pojawić w spisach z atrybutem nawiązanych („*Establshed*“).

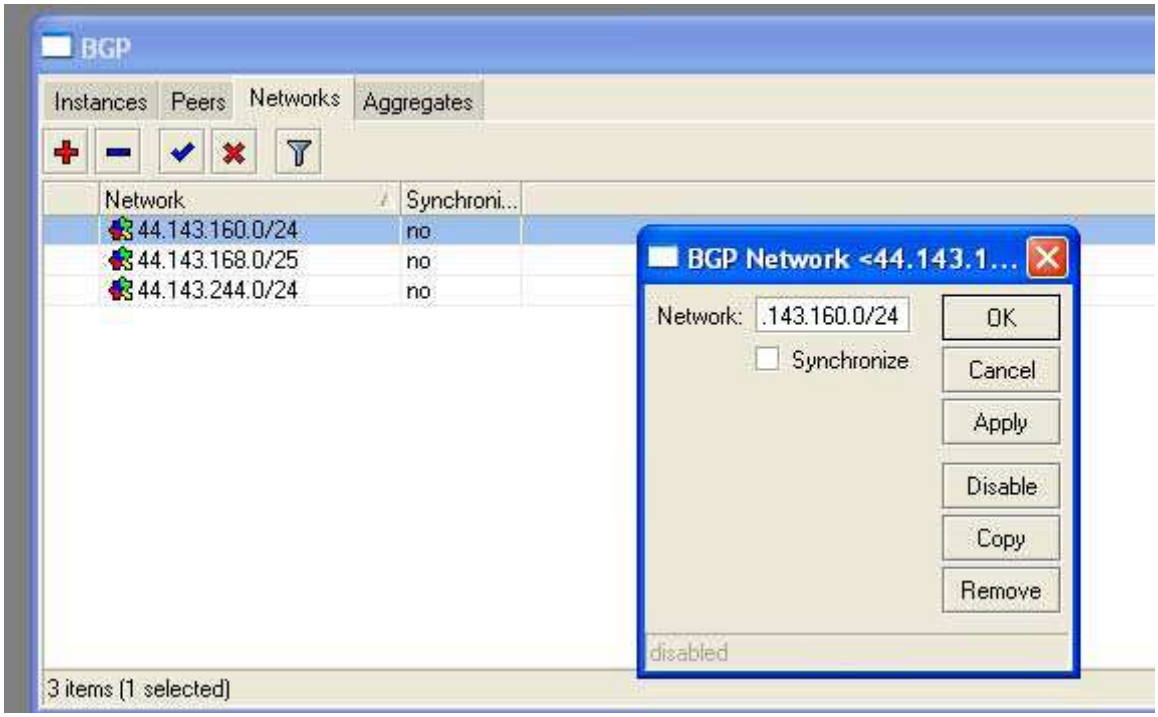


Przykład – spis sesji iBGP z trzema partnerami („*Peers*“)

Uwaga: W spisie podane są adresy („*Remote-Adress*“), numery AS („*Remote-AS-Nummer*“), liczba wymienionych informacji o trasach i dalsze dane dla każdego z partnerów.

4.2.3 Krok 3: Publikacja celów i własnych sieci

W Hamnecie obowiązuje zasada, że bramki muszą udostępniać partnerom informacje o wszystkich sieciach połączonych z nią fizycznie i bezpośrednio za pomocą złączy lub mostków.
Dlatego też w OE7XGR należy (pojedyńczo, kolejno) wprowadzić następujące wpisy:



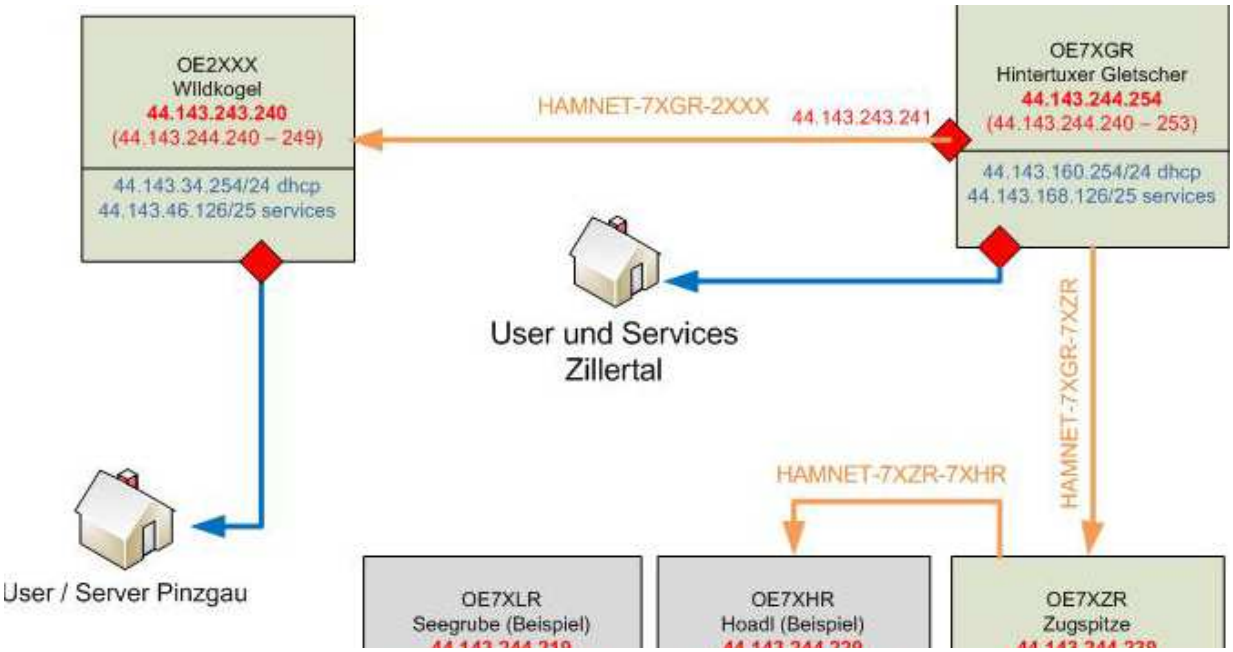
OE7XGR posiada złącza
• do sieci szkieletowej OE7 (44.143.244.0/24)
• dla użytkowników – pula DHCP (44.143.160.0/24)
• w obszarze serwisowym (służbowym) (44.143.168.0/25)
Te trzy prefiksy muszą być wpisane więc do listy sieci („*Networks*“) i opublikowane (zwykle bez synchronizacji,patrz rozdział 3).
 Podstawowa konfiguracja jest już gotowa. W tabelach tras partnerów pojawiają się sieci docelowe.

4.2.4 Krok 4: dodatkowy – dalsze sieci przeznaczone do publikacji

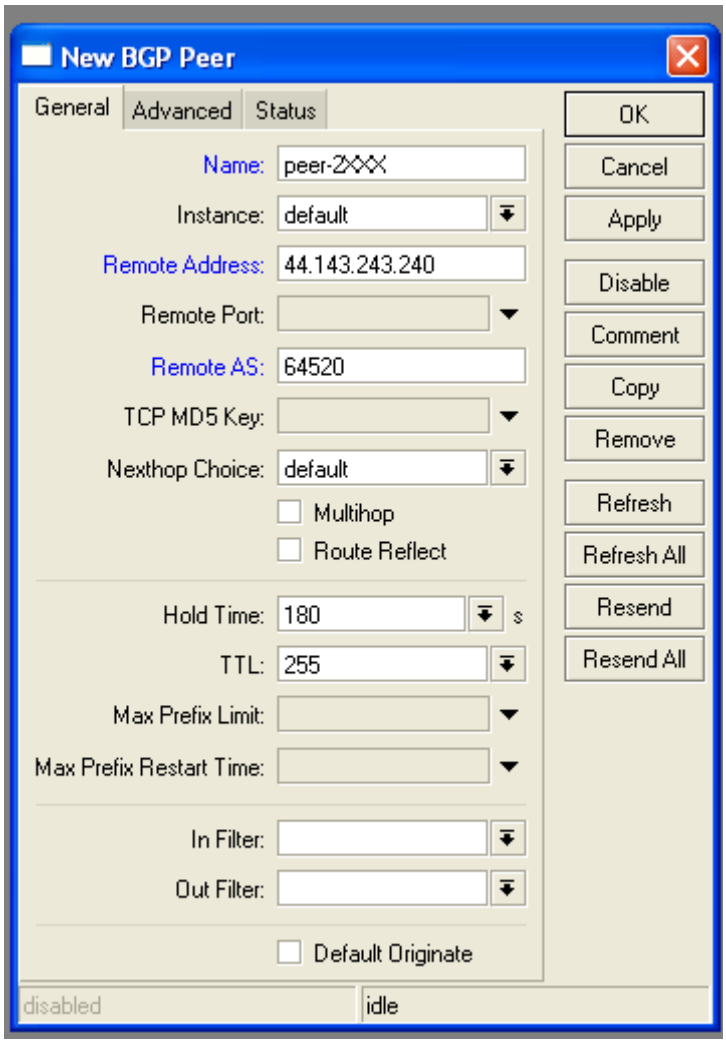
Przykład:
Bramka posiada jeszcze dalszych partnerów nie będących nadawcami BGP. Trasy prowadzące do nich należy wpisać jako statyczne. Przykłady partnerów tego rodzaju:
o Bramki nie wyposażone w protokół BGP,
o Połączenia ze stacjami zagranicznymi nie stosującymi protokołu BGP lub innych protokołów wyboru tras.
 W tej sytuacji należy wpisać trasy jako statyczne w spisie sieci („*Networks*“) najbliższej bramki BGP.

4.3 Przykładowa konfiguracja na granicy systemów autonomicznych

Dalsza konfiguracja **OE7XGR** uwzględniająca połączenie z regionem OE2 oparta jest na przykładzie z poniższej ilustracji. Zgodnie z przedstawioną tam topologią i z zasadmi konfiguracji opisanymi w rozdziale 3 konieczne jest jedynie uzupełnienie konfiguracji u partnerów granicznych OE7XGR i OE2XXX. Nie dotyczy to więc pozostałych stacji: OE7XLR, OE7XHR i OE7XZR.
Sposób uzupełnienia konfiguracji OE7XGR przedstawiono poniżej.



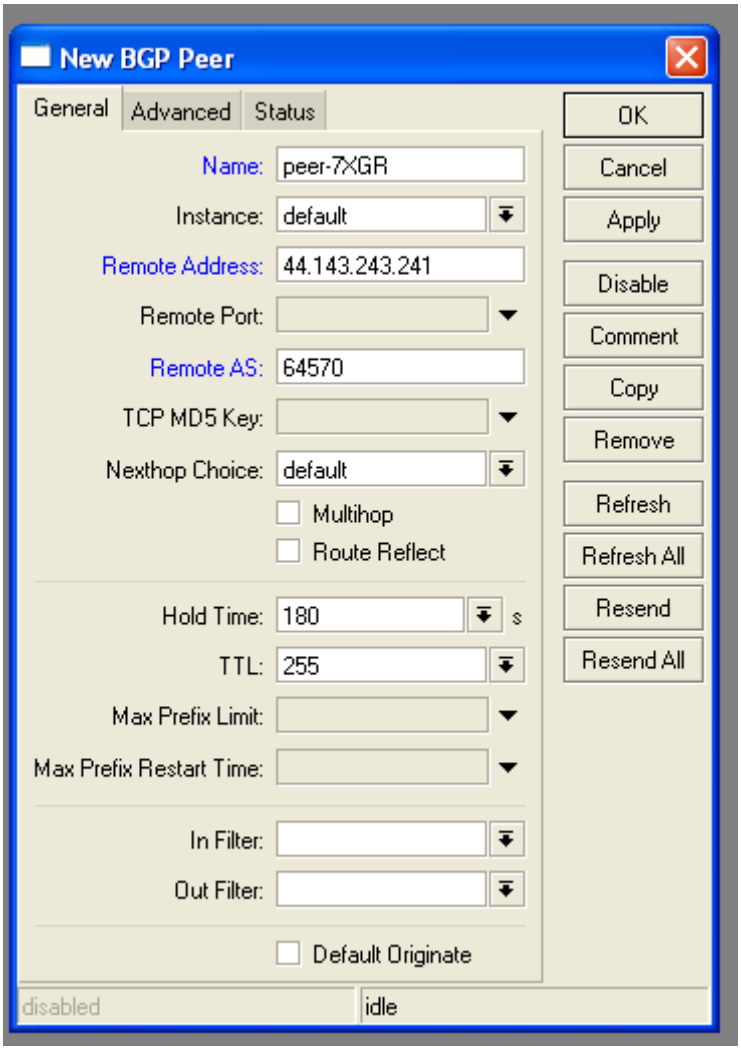
Konieczne jest skonfigurowanie sesji do nowego partnera: OE2XXX jak to przedstawiono w poniższym oknie. Numer AS wynika z przydziału dla poszczególnych regionów (okręgów).



Ustawienia w OE7XGR

• Pole „Name“: peer-2XXX (nazwa dowolna, to tylko praktyczny przykład!)
• Pole „Instance“: „default“ (nazwa czynnej usługi)
• Pole „Remote-Adresse“: 44.143.XXX.XXX (adres IP partnera)
• Pole „Remote Port“: puste = domyślny kanał logiczny (kanał TCP 179)
• Pole „Remote AS“: 645xx (numer AS partnera odpowiadający jego regionowi)
• Pozostałe pola: jak na ilustracji
• Potwierdzić przyciskiem „OK“
• Gotowe

Konieczna jest oczywiście odpowiednia konfiguracja sesji u partnera (OE2XXX).



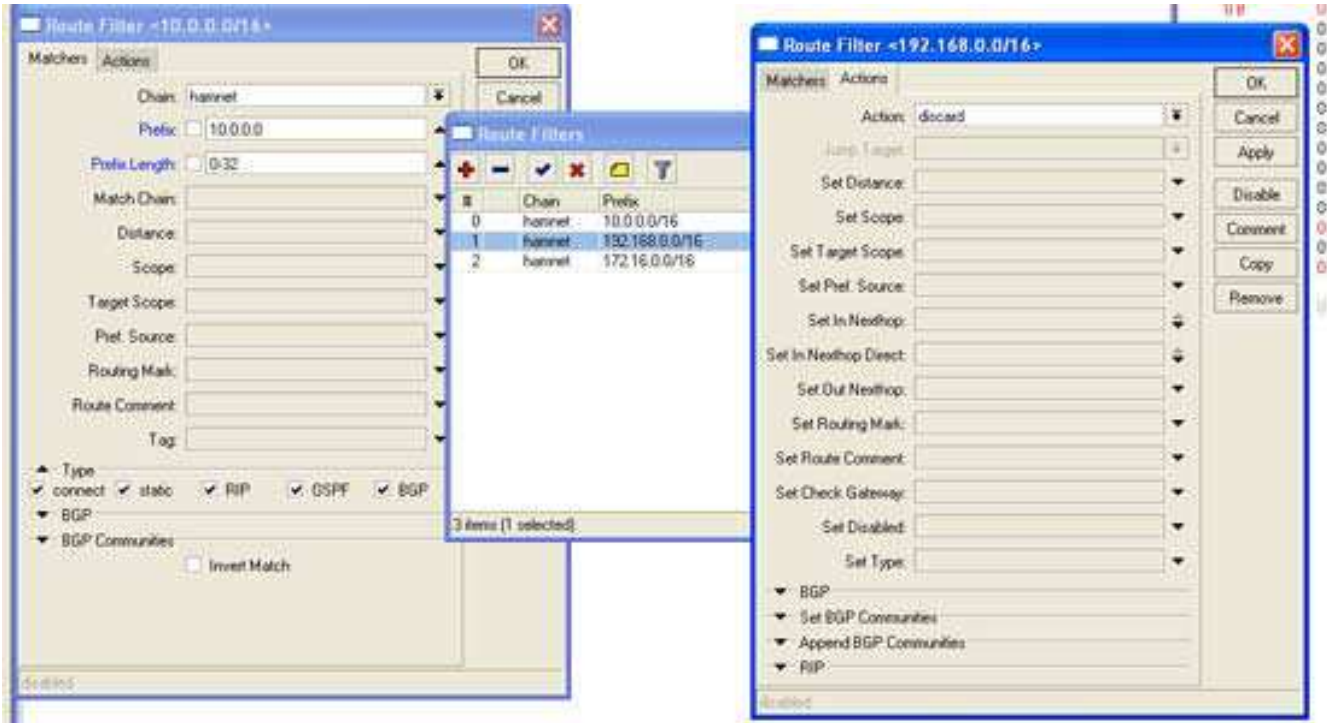
Pasujące ustawienia w OE2XXX

• Pole „Name“: peer-7XGR (nazwa dowolna, to tylko praktyczny przykład!)
• Pole „Instance“: „default“ (nazwa czynnej usługi)
• Pole „Remote-Adress“: 44.143.XXX.XXX (adres IP partnera)
• Pole „Remote Port“: puste = domyślny kanał logiczny (kanał TCP 179)
• Pole „Remote AS“: 645xx (zgodnie z przydziałem numerów dla poszczególnych regionów)
• Pozostałe pola: jak na ilustracji
• Potwierdzić przyciskiem“ OK“
• Gotowe

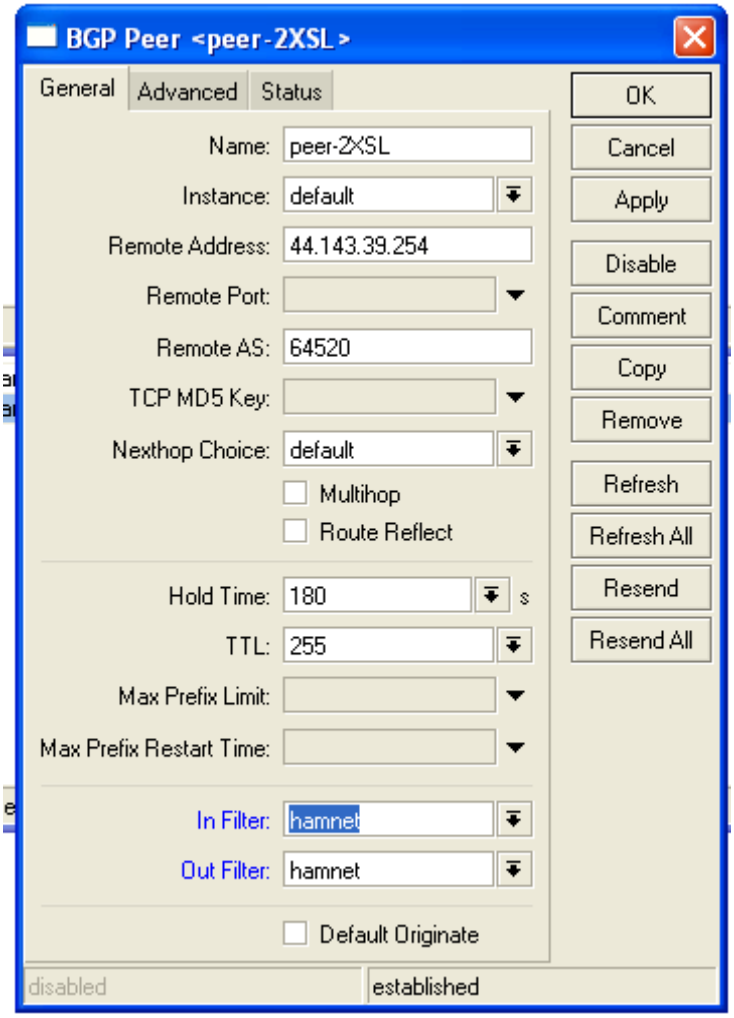
 Podstawowa konfiguracja jest już zakończona. W tabelach tras partnerów pojawiają się wpisy sieci. OE7 otrzymuje także informacje z OE2 i dalej położonych sieci i odwrotnie zgodnie z za-wartością list sieci.
Uwaga: Grupowanie zostało omówione wcześniej w rozdziałach 3 i 4 i dlatego pominięto je tutaj.
Konfiguracja przez: **Winbox -> ROUTING->BGP->AGGREGATES**

4.4 Filtry / sekwencje

Możliwości oferowane przez filtry są bardzo szerokie (patrz: punkt 4.1) i pozwalają m.in. na ustalenie zasad publikacji tras i zmianę ich priorytetów. Poniżej przedstawiono przykład filtrów eliminujących informacje dotyczące prywatnych sieci (prywatnych obszarów adresowych).



Sekwencje muszą zostać wpisane do konfiguracji sesji, w których mają być czynne. Mogą być używane do filtrowania danych przychodzących („*in-Processing*“) albo wychodzących („*out-Processing*“).


BGP Peer <peer-2XSL>
General
Advanced
Status
Name: peer-2XSL
Instance: default
Remote Address: 44.143.39.254
Remote Port:
Remote AS: 64520
TCP MD5 Key:
Nexthop Choice: default
Multihop
Route Reflect
Hold Time: 180 s
TTL: 255
Max Prefix Limit:
Max Prefix Restart Time:
In Filter: hamnet
Out Filter: hamnet
Default Originate
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Refresh
Refresh All
Resend
Resend All
disabled
established

5 Encyklopedia terminów

Rozdział ten jest poświęcony wyjaśnieniu znaczenia terminów i skrótów używanych w niniejszym dokumencie. Mają one charakter encyklopedyczny.

5.1 AMPR, sieć 44.

Zarówno w Hamnecie jak i w transmisji radiowej TCP/IP w sieci AX.25 (packet radio) – AMPR – używana jest grupa adresów klasy C: 44.x.x.x przyznana w skali światowej wyłącznie do użytku krótkofalowców. Początki sieci AMPR sięgają lat 1980-tych i jest ona zarządzana przez lokalnych administratorów. W zakresie 44.143.x.x przyznanym krótkofalowcom OE zarządzaniem zajmuje się Krzysztof OE1KDA. Dla potrzeb Hamnetu przyznane zostały nowe podzakresy adresowe zgodnie z nowoopracowanym konceptem.

5.2 Cyfrowa sieć szkieletowa („*BACKBONE*”)

Siecią szkieletową (ang. *backbone*) nazywana jest podstawowa część sieci Hamnetu złożona z łączy radiowych o bardzo dużej przepustowości gwarantującej skuteczną transmisje wszystkich strumieni danych użytkowych (packet radio, ATV, obsługa stacji zdalnych, transmisja głosu VoIP, APRS, http itd.). Oprócz tego konieczne jest posiadanie rezerw i połączeń redundantnych zapewniających jej działanie w przypadku awarii niektórych połączeń. Trasy transmisji danych są w niej wybierane oczywiście automatycznie w zależności od sytuacji.
Szybkie łącza i skutecznie działający wybór tras są niezbędne dla właściwego działania Hamnetu. Do sieci szkieletowej w Austrii zaliczane są szybkie łącza radiowe (częściowo oparte na technologii WLAN) ale nie zalicza się do niej radiowych wejść użytkowych, części klasycznej sieci packet radio i świadczonych usług.

5.3 Algorytm wyboru tras BGP

Zasadniczo na wybór tras wpływają zarówno ustalone zasady jak i zdefiniowane filtry. Niezależnie od tego BGP korzysta z algorytmu wyboru tras opisanego w punkcie 3.4.4 w konfiguracji 3.

5.4 CIDR

Algorytm „*Classless Inter-Domain Routing*“ (CIDR) jest metodą skuteczniejszego wykorzystania istniejącego 32-bitowego obszaru adresowego IP (IPv4). Został on wprowadzony w 1993 r. w celu zmniejszenia objętości tabel tras i lepszego wykorzystania zasobów adresowych. W CIDR nie występuje stałe przyporządkowanie adresów do klas i podział na sieci ani grupowanie sieci należących do tej samej klasy. Występuje tu jedynie maska sieci dzieląca adres na dwie części: sieciową i indywidualną. Wprowadzono w nim nowy sposób zapisu tzw. sufiksy. Sufiks podaje liczbę bitów znaczących w masce sieci. Zapis ten (np. 172.17.0.0/17) jest znacznie krótszy niż klasyczny zapis dziesiętny (np. 172.17.0.0/255.255.128.0) i jednakowo jednoznaczny.
Zapis w IPv6 jest identyczny jak w CIDR dla IPv4 i składa się z adresu IPv6 oraz długości prefiksu (np. 2001:0DB8:0:CD30::1/60).

5.5 Bramka, bramka domyślna (ang. *Gateway, Default-Gateway*)

Bramka (ang. *gateway*) służy do połączenia sieci opartych na różnych protokołach. W mowie potocznej nazwa ta jest używana wymiennie z bramką (lub punktem dostępowym do internetu; ang. *router*) pomimo, że te ostanie pracują tylko na poziomie 3 wartstwy modelu ISO natomiast bramka międzysieciowa – na poziomach warstw 4 – 7.
Bramka domyślna jest adresem, pod który przekazywane są dane dla adresatów znajdujących się poza własną siecią gdy brakuje innych dokładnieszych danych dostępowych.

5.6 Adres IP

Najważniejszym elementem protokółu IP są adresy IP jednoznacznie identyfikujace wszystkie stacje sieci. Każde ze złączy fizycznych (kontrolerów sieciowych) otrzymuje własny adres IP. W wyjątkowych przypadkach urządzenia mają przypisane kilka adresów IP albo też kilka z nich jest osiągalnych pod wspólnym adresem. Adres IP można w przybliżeniu przyrównać do adresu pocztowego w życiu codziennym. Adresy IP w postaci cyfrowej mają długość 32 bitów i są w zależności od potrzeb zapisywane w postaci dziesiętnej lub szesnastkowej.

Przykłady zapisu adresów w różnych systemach liczbowych

Dwójkowy	0111 1111	0000 0000	0000 0000	0000 0001
Szesnastkowy	7F	00	00	01
Dziesiętny	127	0	0	1

Dla zwiększenia czytelności kod 32-bitowy jest zapisywany w postaci czterech liczb 8-bitowych (bajtów) oddzielonych kropkami. Każdy z bajtów może przyjmować wartości w zakresie 0 – 255 a więc jedną z 256 możliwych wartości.

5.7 Adresy IP – podstawowe zasady

• Adres IP 127.0.0.1 z powyższych przykładów jest lokalnym adresem IP każdej stacji – i jest przypisany do wirtualnego złącza niezależnego od wyposażenia sprzętowego. Jego nazwą symboliczną jest „localhost”. Pakiet skierowany pod adres 127.0.0.1 jest w praktyce kierowany do nadawcy. Mamy więc do czynienia z echem lub inaczej mówiąc z zamkniętą pętlą wewnętrzną. Adres ten jest używany do różnego rodzaju prób (sprawdzania prawidłowości instalacji i konfiguracji) lub łączności wewnętrznej TCP/IP między różnymi programami pracującymi na tym samym komputerze. Dotyczy to nie tylko tego pojedyńczego adresu ale wszystkich adresów z zakresu 127.0.0.0 – 127.255.255.255.
• Adres IP zakończony zerem np. 127.0.0.0 nie jest ważnym adresem indywidualnym a adresem całej lokalnej sieci.
• Adres IP zakończony numerem 255 np. 127.0.0.255 nie jest również ważnym adresem indywidualnym a adresem ogólnym sieci 127.0.0.0 służącym do rozgłaszania informacji do wszystkich członków sieci (wszystkich połączonych z nią stacji lub komputerów).
• Zakres wartości 0 – 255 oznacza występowanie 256 adresów w sieci x.x.x.0 z maską 255.255.255.0 ale uwzględniając powyższe uwagi w jej skład mogą wchodzić najwyżej 254 stacje o własnych adresach.
• Dla sieci prywatnych prewidziane są specjalne obszary adresowe, których nie można wykorzystywać do adresowania w internecie.

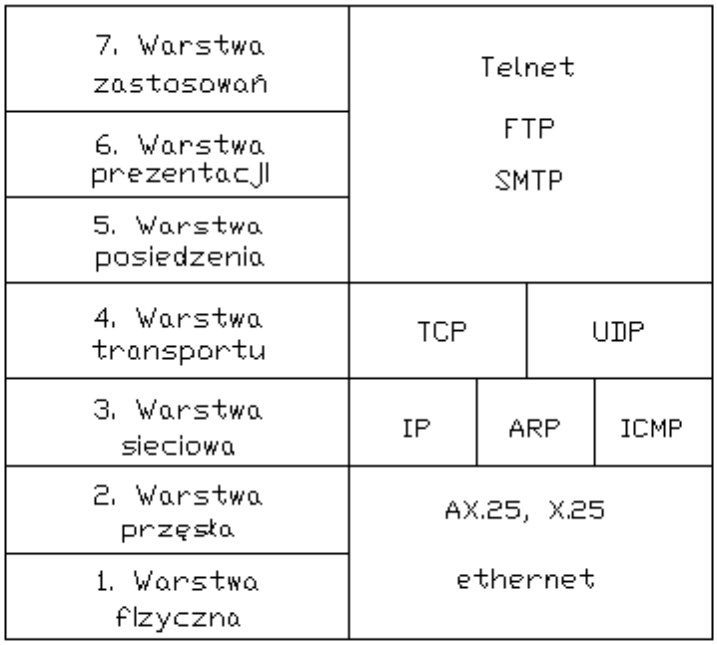
Prywatne obszary adresowe IP:

Klasa	**Od**	**Do**	**Maska sieci**
Sieci klasy A	10.0.0.0	10.255.255.255	255.0.0.0
Sieci klasy B	172.16.0.0	172.31.255.255	255.255.0.0
Sieci klasy C	192.168.0.0	192.168.255.255	255.255.255.0

Adresy z zakresów prywatnych nie są upubliczniane w Hamnecie i są blokowane za pomocą filtrów i dodatkowo ustawień w zaporach przeciwwłamaniowych.

5.8 Protokół IP – *„Internet-Protocol”*

Protokół IP (*Internet Protocol*) jest szeroko rozpowszechnionym w sieciach komputerowych protokółem sieciowym. Stanowi on podstawę zarówno internetu jak i Hamnetu i jest implementacją warstwy sieciowej modelu TCP/IP odpowiadającej warstwie 3 modelu ISO. Warstwa ta jest najniższą warstwą niezależną od fizycznej strony łącza. Adresy IP i maski sieci (ang. *subnet mask*) dla IPv4 i prefiksy IPv6 pozwalają na przyporządkowanie komputerów w sieci do mniejszych jednostek logicznych – lokalnych sieci (ang. *subnet*). Ułatwia to adresowanie (logiczne) komputerów w sieci i wybór tras do nich prowadzących.



Rys. 1 Układ warstw TCP/IP

5.9 Pętla zamknięta

Pętla zamknięta jest kanałem transmisji o jednym końcu co oznacza, że nadawca i odbiorca danych są tożsami. Przykładem takiej pętli jest pętla wewnętrzna – lokalna – o adresie 127.0.0.1.

5.10 Złącze pętli

Złącze pętli pozwala na korzystanie z protokółu sieciowego przez usługi lokalne a więc w ramach danego urządzenia np. bramki lub komputera.

5.11 Pętla sieciowa

W protokóle IP zdefiniowana jest również pętla sieciowa. Przewidziany jest dla niej w IPv4 obszar adresowy 127.0.0.1 do 127.255.255.254, przy czym najczęściej używanym adresem jest 127.0.0.1, a w Ipv6 – ::1. W większości implementacji protokółu IP można korzystać z pętli, przy czym pakiety danych skierowane do niej są adresowane do własnego komputera. Standardową nazwą pętli jest „localhost”.

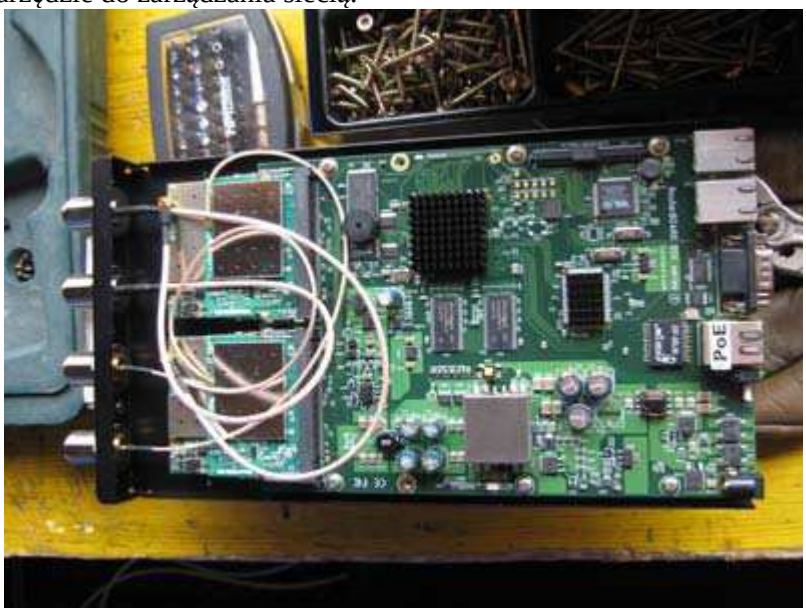
5.12 Adres MAC

Adres MAC (*Media-Access-Control*, także występujący pod nazwą *Ethernet-ID*) jest adresem sprzętowym każdego urządzenia sieciowego, służącym do jego jednoznacznej identyfikacji w sieci.
Adres MAC jest przypisany warstwie przęsła (warstwie 2) modelu ISO. Urządzenia sieciowe muszą posiadać adresy MAC jeżeli mają być adresowane na poziomie warstwy 2 w celu udostępnienia swoich usług warstwom wyższym.

5.13 Mikrotik

Miktrotik jest producentem bramek i urządzeń radiowych stosowanych w sieci szkieletowej Hamnetu:
• MikroTik RouterOS (system operacyjny konfigurowany za pomocą programu „Winbox”).
• MikroTik RouterBOARD (różne modele modułów).
• Kompletne systemy oparte o MikroTik.

• „The Dude” – narzędzie do zarządzania siecią.



Moduł „Miktrotik Routerboard 600“ użyty w OE7XGR

5.14 Klasy sieci

Sieci a co za tym idzie i adresy IP są podzielone na 5 klas. Różnią się one podziałem adresu na część sieciową i część indywidualną adresującą komputery sieci.

- Do klasy A zaliczane są sieci składające się z dużej liczby stacji lub sieci lokalnych. Teoretyczny obszar adresowy rozciaga się od 0.0.0.0 do 127.255.255.255 a rzeczywisty – od 1.0.0.1 do 127.255.255.254. W sumie możliwe jest istnienie 126 sieci klasy A o maksymalnej liczbie 16.774.214 komputerów w każdej z nich.
- Sieci klasy B zawierają średnią liczbę komputerów lub sieci lokalnych. Pierwsze dwa bity mają zawsze wartość 10. Teoretyczny obszar adresowy rozciąga się od 128.0.0.0 do 191.255.255.255 a rzeczywisty od 128.0.0.1 do 191.255.255.254. W sumie możliwe jest istnienie 16384 sieci klasy B o maksymalnej liczebności 65.534 w każdej z nich.
- Sieci klasy C zawierają małą liczbę komputerów w każdej z nich – każda z sieci klasy C jest jednocześnie siecią lokalną (ang. *subnet*). Pierwsze trzy bity adresu mają zawsze wartość 110. Teoretyczny obszar adresowy rozciąga się od 192.0.0.0 bis 223.255.255.255 a rzeczywisty – od 192.0.0.1 do 223.255.255.254. W sumie możliwe jest więc istnienie 2.097.152 sieci klasy C o maksymalnej liczbie członków (komputerów) 254 w każdej z nich.

CIDR likwiduje sztywne przyporządkowanie masek sieci do klas. W miejsce ustalonych masek dla każdej z klas używane są maski o dowolnych długościach.

Zapis masek	**Zapis długości**
192.168.1.0/255.255.255.0	192.168.1.0/24
172.16.4.0/255.255.252.0	172.16.4.0/22
195.16.85.80/255.255.255.248	195.16.85.80/29

Klasa A (0.0.0.0 do 127.255.255.255)
0 człon sieci (7 bitów) człon indywidualny (24 bity)
Klasa B (128.0.0.0 do 191.255.255.255)
1 0 człon sieci (14 bitów) człon indywidualny (16 bitów)
Klasa C (192.0.0.0 do 223.255.255.255)
1 1 0 człon sieci (21 bitów) człon indywidualny (8 bitów)
Klasa D (224.0.0.0 do 239.255.255.255)
1 1 1 0 adresy grup wielokrotnych (28 bitów)
Klasa E (240.0.0.0 do 255.255.255.255)
1 1 1 1 0 zarezerwowane do przyszłych zastosowań (27) bitów

5.15 Informacje NLRI – („Network Layer Reachability Information“)

Protokół BGP wysyła informacje aktualizujące stan tras w postaci NLRI. Format NLRI składa się z prefiksu i długości maski. Długość zapisana jest w formacie CIDR (np. /25) i oznacza liczbę bitów należących do adresu sieci. Prefiks jest adresem danej sieci.
Przykład:
NLRI: 44.143.160.0/24
Prefiks: 44.143.160.0
Długość: /24

5.16 Model ISO

Model ISO, zwany również modelem warstwowym ISO opracowany przez Międzynarodową Organizację Standardów stanowi podstawę dla opracowań protokółów komunikacyjnych. Zadania występujące w komunikacji sieciowej podzielone są na 7 warstw (patrz rys. w p. 5.8). Dla każdej z warstw opracowane są dokładne specyfikacje opisujące stawiane im wymagania. Wymagania te muszą być spełnione przez protokóły należące do danej warstwy. Specyfikacje nie ustalają jednak sposobu ich realizacji pozostawiając wolną rękę projektantom i realizatorom. Dla każdej z warstw opracowano do chwili obecnej wiele różnych protokółów. Z protokółów nie wymienionych na ilustracji na poziomie warstw 4–7 znajdują się takie protokóły jak HTTP, HTTPS, LDAP, NCP itd.

5.17 Packet Radio

Nowoczesne rozwiązania węzłów packet radio takie jak DLC korzystają z protokółu IP i pozwalają na transmisję datagramów IP w sieci AX.25 („*AX over IP*“). Na ilustracji węzeł XNET w próbnym połączeniu z Hamnetem.

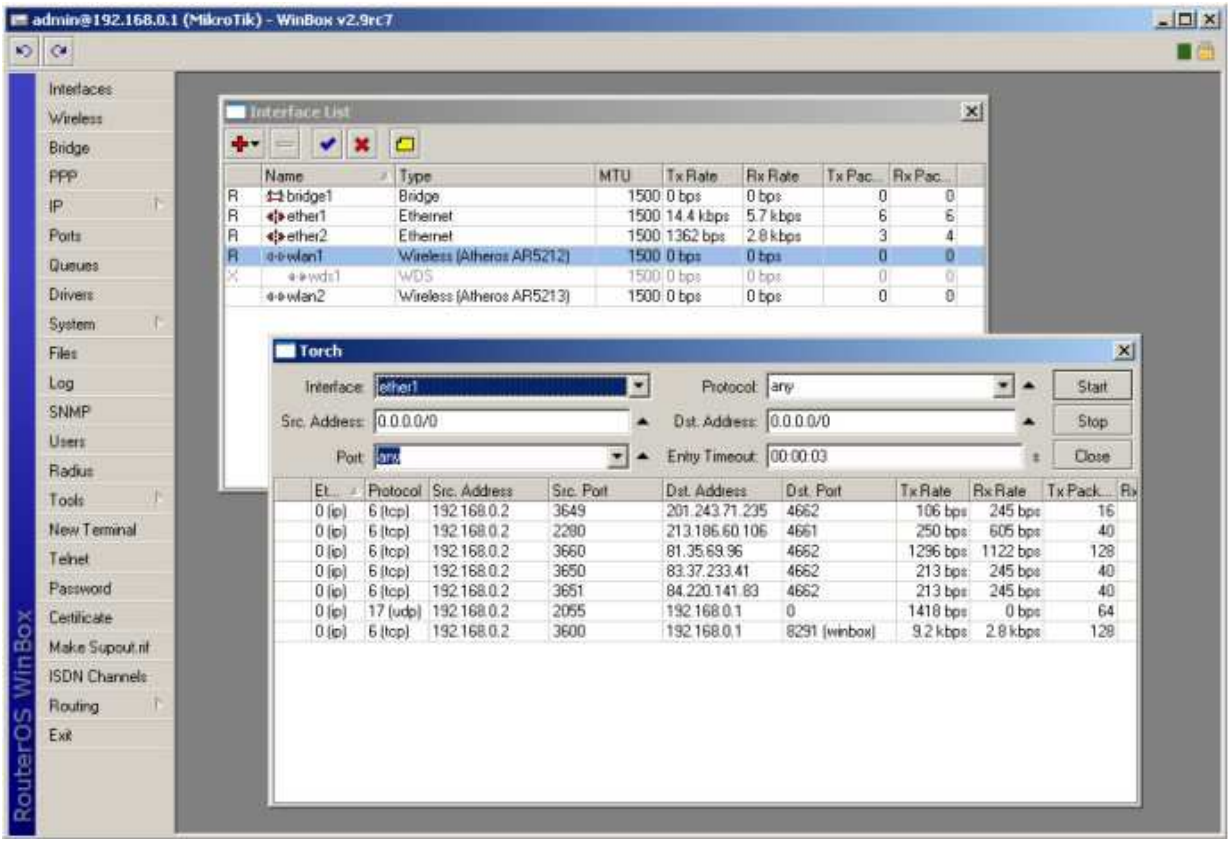
Packet radio jest systemem transmisji danych opracowanym przez krótkofalowców dla potrzeb krótkofalarstwa. Dane dzielone są na pakiety AX.25 o maksymalnej długości 255 bajtów, transmitowane w tej postaci a po stronie odbiorczej po sprawdzeniu ich bezbłędności składane ponownie w pierwotny strumień.
Sieć packet radio składająca się z przekaźników cyfrowych (warstwa 2) i węzłów (warstwa 3) pozwala, dzięki mechanizmom wyboru tras, na prowadzenie łączności między stacjami odległymi o jej wiele odcinków.
W oparciu o model ISO możliwy jest transport pakietów AX.25 za pośrednictwem datagramów AXUDP lub „AX przez IP“ („*AX over IP*“) w sieci Hamnetu. Szybkość transmisji w sieci przewyższa wielokrotnie szybkości 9600 bit/s lub 19200 bit/s stosowane w dotychczasowych łączach. Pakiety AX.25 przekazywane są do sieci Hamnetu za pomocą kanałów łączących je z przekaźnikami cyfrowymi (np. w standardzie KISS) albo bezpośrednio z nowszych ich rozwiązań (np. DLC7 z oprogramowaniem XNET). Łącza radiowe Hamnetu mogą więc służyć jako łącza między przekaźnikami cyfrowymi packet radio. Użytkownicy mogą też łączyć się z przekaźnikami AX.25 przez Hamnet.
Dotychczas używany był także odwrotny wariant transportu: datagramy TCP/IP były przed nadaniem pakowane do pakietów AX.25 i przesyłane w sieci packet radio. Pozwalało to na dostęp do witryn http i innych usług IP ale z ograniczoną szybkością. Stacje przekaźnikowe musiały być w tym celu wyposażone w odpowiednie oprogramowanie j.np. Flexnet, AGW, WAMPES lub Linuks (z dodatkiem AX.25). W obu przypadkach używane są adresy IP.

5.18 Protokóły

W informatyce i telekomunikacji protokół oznacza ustalenia dotyczące połączeń, przebiegu komunikacji i przebiegu transmisji danych między korespondentami. Jest on więc czymś w rodzaju kodeksu drogowego dla danych – przyp. tłum. Protokoły wypełniają rozmaite zadania począwszy od nawiązania połączenia i sterowania przepływem danych aż do przekazywania ich warstwom wyższym do warstwy zastosowań włącznie.
Do najważniejszych z nich należą protokół IP (*Internet Protocol*) i TCP (*Transmission Control Protocol*). TCP/IP jest oznaczeniem zbiorczym podkreślającym ich znaczenie w internecie i innych opartych o nie sieciach i oznaczającym cały zbiór powiązanych z nimi i powszechnie stosowanych protokołów.
W sieciach packet radio stosowany jest protokół AX.25 oparty na X.25 stosowanym w sieciach kablowych („Ethernet“).

5.19 System operacyjny bramki Mikrotik

System operacyjny bramki „*RouterOS*“ jest systemem stosowanym w sprzęcie firmy Mikrotik. Umożliwia on wszechstronną konfigurację bramki a dla jej ułatwienia opracowany został program „Winbox” dla PC. Do najważniejszych konfigurowalnych funkcji należą zapora przeciwwłamaniowa, dostęp bezprzewodowy, wybór tras i VPN. Konfigurację można przeprowadzić także przy użyciu wiersza poleceń np. w ramach sesji telnetu.



Konfiguracja systemu „RouterOS“ w oknach „Winboxu“

5.20 Maski sieci

Adresy IP można w przybliżeniu porównać z adresami zamieszkania. W odróżnieniu od nich są one podawane w postaci cyfrowej – czterech bajtów czyli 32 bitów. Mogą też być, dla ułatwienia odczytu przez ludzi, zapisywane dziesiętnie lub szesnastkowo.

Zapis dwójkowy	0111 1111	0000 0000	0000 0000	0000 0001
Zapis szesnastkowy	7F	00	00	01
Zapis dziesiętny	127	0	0	1

W powyższym przykładzie przedstawiono sposoby zapisu adresu 127.0.0.1 ale ta sama zasada dotyczy wszystkich adresów IP. Adresy te można podzielić na dwie części (człony). Część początkowa jest adresem sieci, do której należy dana stacja a pozostała – adresem indywidualnym stacji lub komputera. Sposób podziału podany jest za pomocą maski sieci (niem. *Subnetzmaske*; ang. *subnetmask*). Maska składa się z 32 bitów, z których pewna liczba bitów początkowych ma wartość 1 (i ona właśnie odpowiada członowi adresu sieci) a pozostałe mają wartość 0 i odpowiadają członowi indywidualnemu. Przykład: 11111111 11111111 11111111 00000000. W zapisie dziesiętnym odpowiada to 255.255.255.0. Kombinacja logiczna maski sieci z adresem IP daje następujący (przykładowy) wynik podziału na człony:

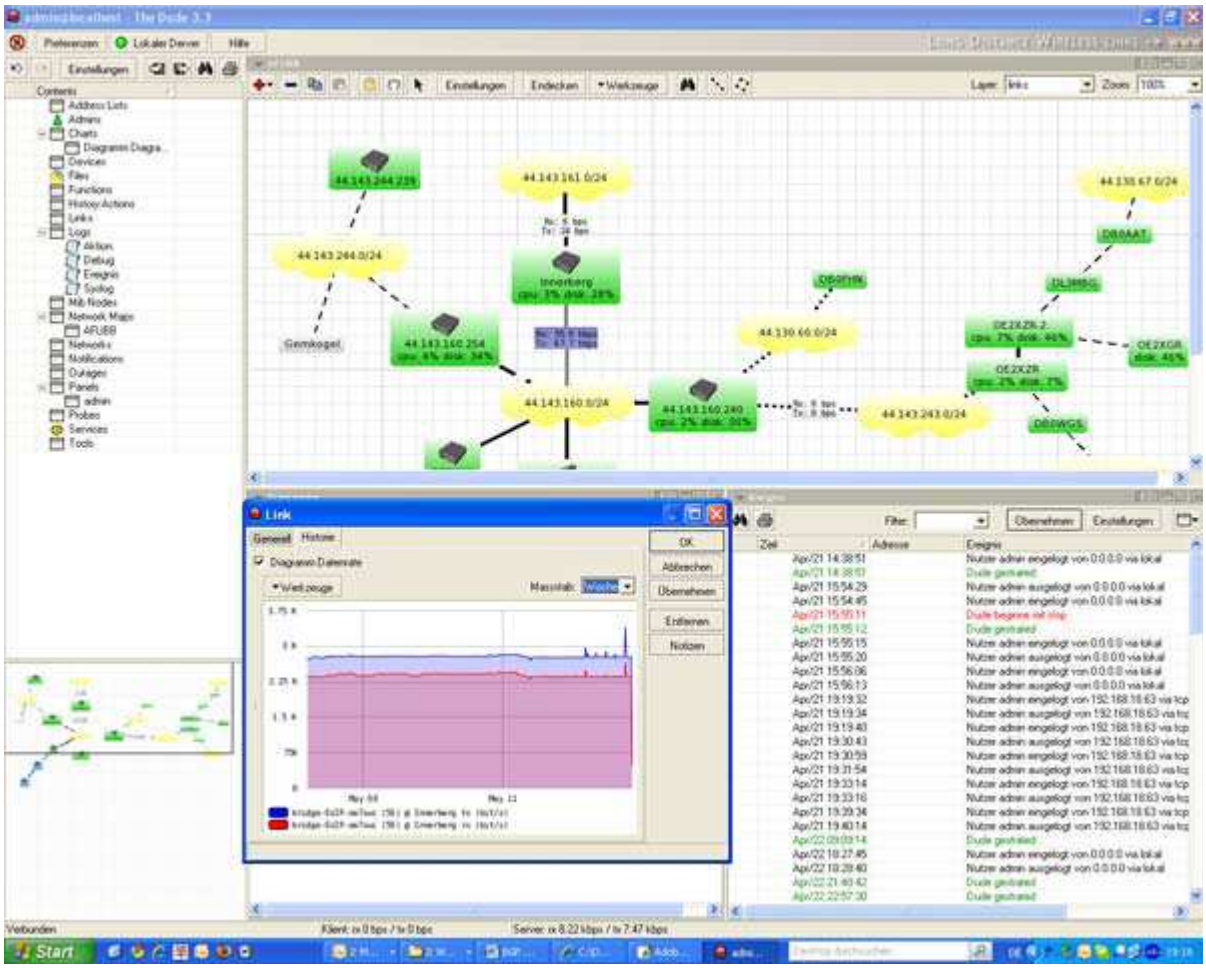
Adres IP	127.	0.	0.	1
Maska sieci	255.	255.	255.	0
Człon sieci	127.	0.	0.	0
Adres stacji				1

Pierwsza część adresu (adres sieci) wynosi 127.0.0.0 a druga (indywidualny adres stacji) – 1.

Przykłady prawidłowych masek sieci
255.255.255. 0
255.255. 0. 0
255. 0. 0. 0
255.255.255.252
255.255.255.128

Przykłady nieprawidłowych masek sieci (w części początkowej nie mogą występować bity zerowe, a w drugiej – jedynki)
250.255.255. 0
255.255. 0.255
255. 0.255.255
255. 0. 0.255
255.255.255.200

5.21 „The Dude“



Okno monitora stanu sieci – programu „Dude“

„Dude“ jest rozbudowanym narzędziem nadzoru sieci. Kontaktuje się ono ze wszystkimi połączonymi z nią urządzeniami, wyświetla ich stan w postaci graficznej w oknie i ułatwia sporządzenie dokumen-

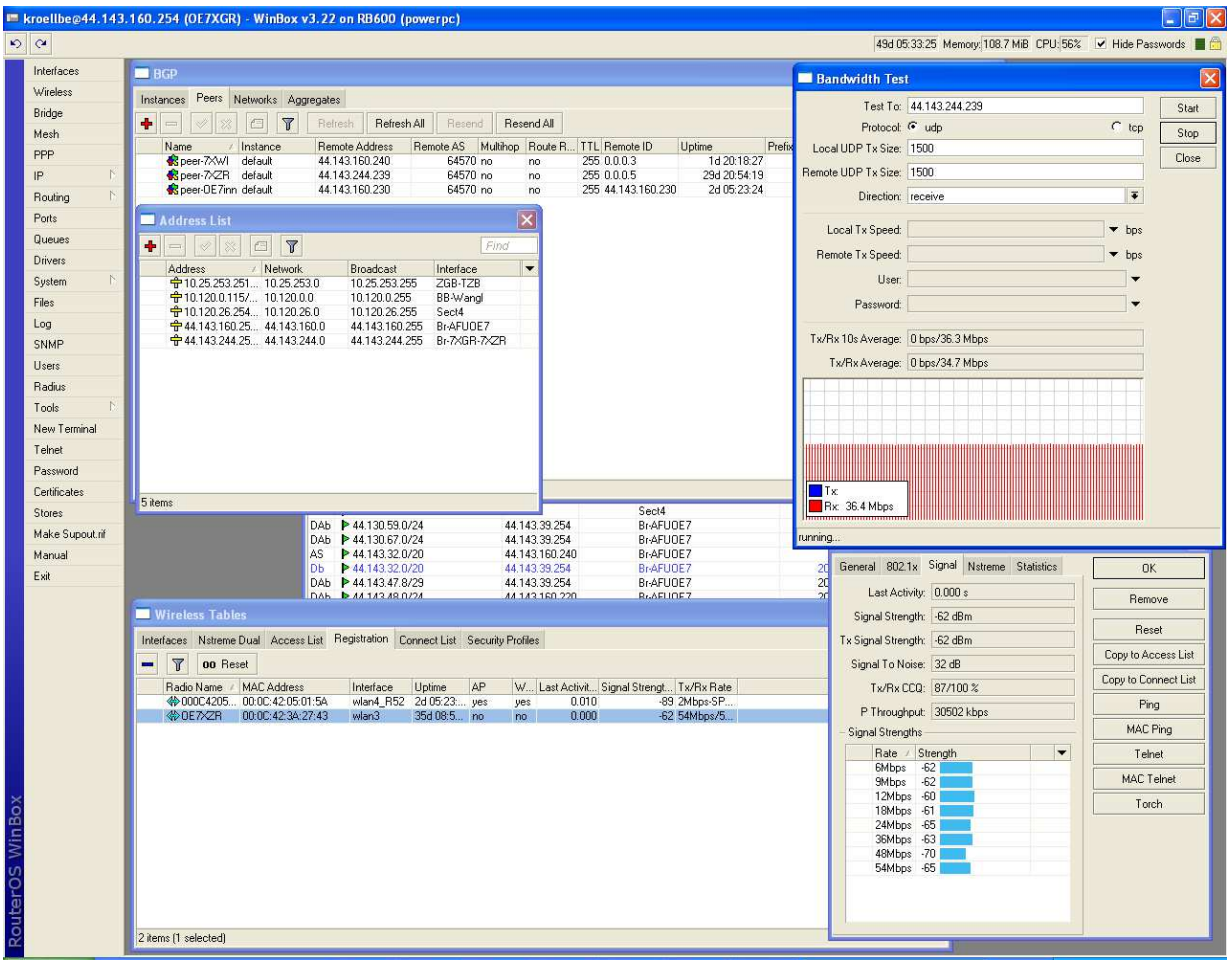
tacji sieci. Informuje on też administratora o stanie urządzeń, połączeń i o występujących problemach. Wśród wyświetlanych danych znajdują się informacje o połączeniach kablowych i radiowych, obciążeniach łączy, trasach i transmisji pakietów.

5.22 TCP

TCP (ang. *Transmission Control Protocol*) jest protokółem warstwy 4 – warstwy transportu. Odpowiada on za sposób wymiany danych między komputerami. Wszystkie obecne systemy operacyjne komputerów posługują się nim w wymianie danych z innymi. Protokół ten dzieki nawiązaniu połączenia z korespondentem udostępnia obu stronom wirtualny kanał transmisji danych. Sesje BGP posługują się właśnie protokołem TCP korzystając z kanału logicznego 179.
Protokół ten jest niezawodnym sposobem transportu pakietów (datagramów) danych w ramach sesji łączności i stanowi element rodziny protokołów internetowych TCP/IP.
Warstwa 4 jest warstwą nadrzędną w stosunku do warstwy sieciowej (trzeciej), w której jest umiejscowiony protokół IP.
Na poziomie warstwy 4 umiejscowiony jest też m.in. protokół UDP (*User Datagram Protocol*) służący do transmisji danych w trybie bezpołączeniowym. Ponieważ tryb ten nie wymaga kwitowania danych i ich powtarzania w razie wystąpienia przekłamań protokół UDP jest stosowany często do transmisji danych w czasie rzeczywistym, np. strumieni danych dźwiękowych albo wizyjnych a także krótkich komunikatów i danych służbowych sieci.

5.23 Winbox

Winbox jest narzędziem graficznym służącym do konfiguracji bramek sieciowych firmy Mikrotik.



Okna programu „Winbox“

5.24 WLAN

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 zawiara 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.

6 RFC 4271 – „A Border Gateway Protocol 4 (BGP-4)”

Protokół BGP jest zdefinowany w oficjalnym dokumencie RFC 4271 dostępnym m.in. w internecie.

Literatura i adresy internetowe do wstępu

[1] „Hamnet – schnelles Amateurfunk-Backbone-Netz”, Stefan Hüpper, DH5FFL, CQ-DL 1/2010, str. 6
[2] „Hamnet. Hohe Netzabdeckung in Österreich”, Robert Kiendl, OE6RKE, Michael Zwingl, OE3MZC i in., CQ-DL 1/2010, str. 8
[3] „Erste Hamnnet Linkstrecken in Oberbayern“, Christian Entsfellner, DL3MBG, CQ-DL 1/2010, str. 10
[4] „In Zukunft schneller Datenverkehr auf 5 GHz“, Dominik Bugmann, HB9CZF, HB-Radio 1/2010, str. 12
[5] wiki.oevsv.at/index.php/Kategorie:Digitaler_Backbone – dokumentacja sieci Hamnet
[6] www.swiss-artg.ch – dokumentacja sieci Hamnet
[7] db0fhn.efi.fh-nuernberg.de/doku.php?id=projects:wlan:hamnet – dokumentacja sieci Hamnet (ang.)
[7a] db0fhn.efi.fh-nuernberg.de/doku.php?id=projects:wlan:proposal – dokumentacja sieci Hamnet
[8] en.wikipedia.org/wiki/High-speed_multimedia_radio
[9] www.mikrotik.com – witryna firmy MikroTikls SIA
[10] www.ubnt.com – witryna firmy Ubiquiti Networks Inc.
[10a] www.interprojekt.pl, anteny24.pl/pl, www.cyberbajt.com, www.technologic.pl – dystrybutorzy produktów Ubiquiti w Polsce
[11] wiki.oevsv.at/index.php/Datei:DocuHAMNETmesh.pdf – „HAMNETmesh. Installation und Konfiguration”, Robert Kiendl, OE6RKE.
[12] wiki.oevsv.at/index.php/Datei:HAMNETmesh.zip – oprogramowanie Hamnet dla WRT54GL
[13] wiki.oevsv.at/images/a/ab/NS2-OE2XZR.pdf – autor Michael Wedl, OE2WAO, konfiguracja modeli Nanostation 2 i Bullet2 u użytkownika indywidualnego
[14] wiki.oevsv.at/images/a/a2/IM-OE2XZR.pdf – instalacja i konfiguracja klienta „Instant Messaging”
[15] wiki.oevsv.at/images/5/5e/Packet-OE2XZR.pdf – dostęp Packet-Radio, konfiguracja Flexnetu i Paxona
[16] www.afthd.tu-darmstadt.de/~flexnet/modules.html – witryna Flexnetu
[17] www.paxon.de/download.html – witryna Paxona
[18] wiki.oevsv.at/images/d/da/BGPtb38.pdf – Zastosowanie protokołu BGP w sieci Hamnetu. Autorzy Bernhard Kröll, OE7BKH i Markus Fankhauser OE7FMI.

W serii „Biblioteka polskiego krótkofalowca” dotychczas ukazały się:

Nr 1 – „Poradnik D-STAR”
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”
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”