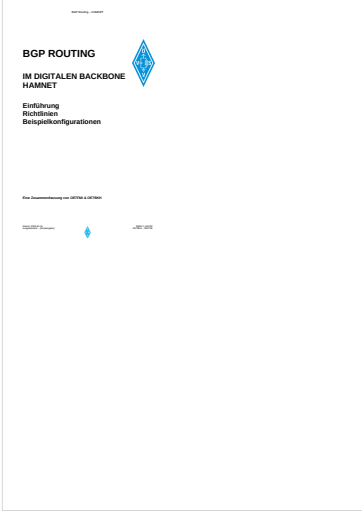
Inhaltsverzeichnis

1. Datei:BGPtb38.pdf 5
2. Benutzer:Oe7xwi 4
3. Dokumentationen 7
4. Routing digitaler Backbone 12

Datei:BGPtb38.pdf

- Datei
- Dateiversionen
- Dateiverwendung
- Metadaten

Gehe zu Seite OK



nächste Seite →

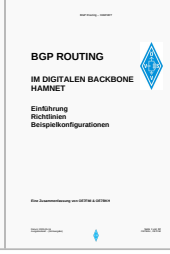
Größe der JPG-Vorschau dieser PDF-Datei: 424 × 600 Pixel. Weitere Auflösung: 170 × 240 Pixel.

Originaldatei (1.240 × 1.754 Pixel, Dateigröße: 2,61 MB, MIME-Typ: application/pdf, 186 Seiten)

BGP-ROuting im HAMNET / Difgitaler Backbone Austria

Dateiversionen

Klicken Sie auf einen Zeitpunkt, um diese Version zu laden.

	Version vom	Vorschaubild	Maße	Benutzer	Kommentar
aktuell	20:44, 19. Mai 2009		1.240 × 1.754, 186 Seiten (2,61 MB)	Oe7xwi (Diskussion | Beiträge)	BGP-ROuting im HAMNET / Digitaler Backbone Austria

Sie können diese Datei nicht überschreiben.

Dateiverwendung

Die folgenden 2 Seiten verwenden diese Datei:

- Dokumentationen
- Routing digitaler Backbone

Metadaten

Diese Datei enthält weitere Informationen, die in der Regel von der Digitalkamera oder dem verwendeten Scanner stammen. Durch nachträgliche Bearbeitung der Originaldatei können einige Details verändert worden sein.

Fotograf	fm
Kurztitel	Die Wichtigkeit der richtigen spezifischen Konfiguration an den Routern
Software	Adobe Acrobat 8.1 Combine Files
Umwandlungsprogramm	Adobe Acrobat 8,1
Verschlüsselt	no
Papierformat	• 595,22 x 842 pts (A4) • 612 x 792 pts (letter)
Version des PDF-Formats	1,6

OE7XWI

Name OE7XWI

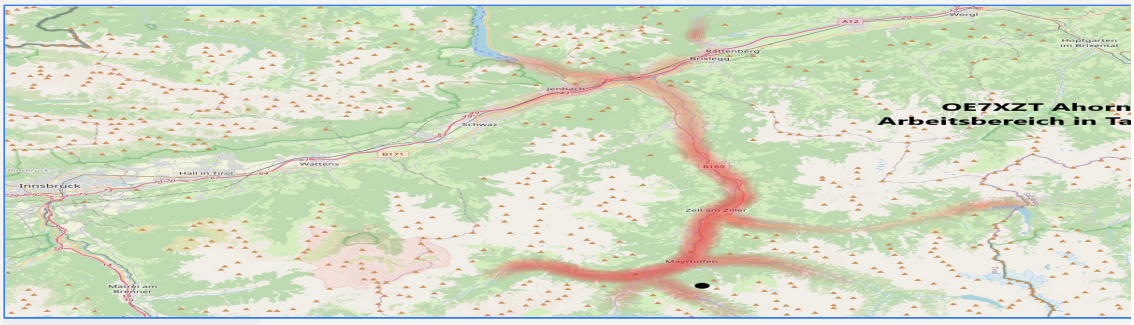
OE7XWI

Name OE7XWI

70cm Relais OE7XZT

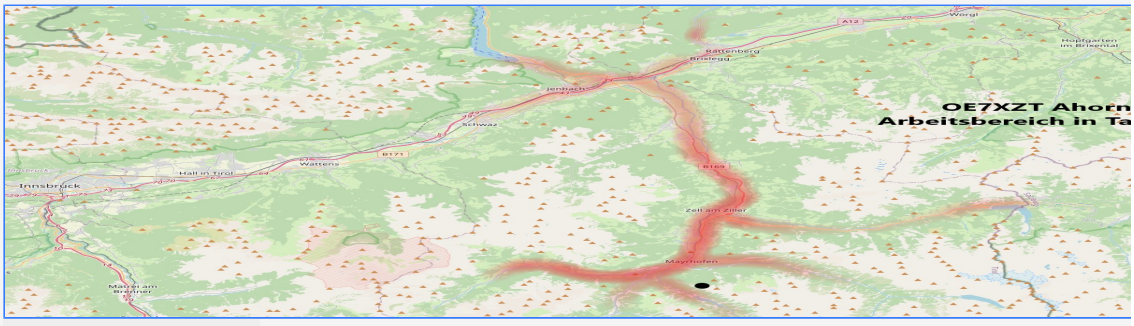
Hauptseite

OE7XWI hinterlegte



OE7XZT-Arbeitsbereich in Tallage.jpg

OE7XWI hinterlegte

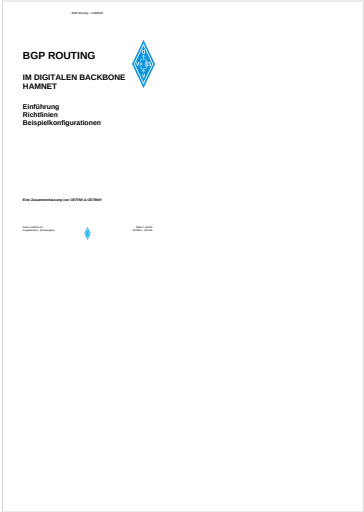


OE7XZT-Arbeitsbereich in Tallage.jpg

Datei:BGPtb38.pdf

- Datei
- Dateiversionen
- Dateiverwendung
- Metadaten

Gehe zu Seite OK



nächste Seite →

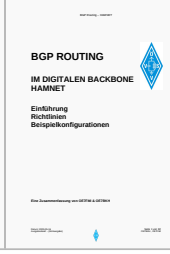
Größe der JPG-Vorschau dieser PDF-Datei: 424 × 600 Pixel. Weitere Auflösung: 170 × 240 Pixel.

Originaldatei (1.240 × 1.754 Pixel, Dateigröße: 2,61 MB, MIME-Typ: application/pdf, 186 Seiten)

BGP-ROuting im HAMNET / Difgitaler Backbone Austria

Dateiversionen

Klicken Sie auf einen Zeitpunkt, um diese Version zu laden.

	Version vom	Vorschaubild	Maße	Benutzer	Kommentar
aktuell	20:44, 19. Mai 2009		1.240 × 1.754, 186 Seiten (2,61 MB)	Oe7xwi (Diskussion | Beiträge)	BGP-ROuting im HAMNET / Digitaler Backbone Austria

Sie können diese Datei nicht überschreiben.

Dateiverwendung

Die folgenden 2 Seiten verwenden diese Datei:

- Dokumentationen
- Routing digitaler Backbone

Metadaten

Diese Datei enthält weitere Informationen, die in der Regel von der Digitalkamera oder dem verwendeten Scanner stammen. Durch nachträgliche Bearbeitung der Originaldatei können einige Details verändert worden sein.

Fotograf	fm
Kurztitel	Die Wichtigkeit der richtigen spezifischen Konfiguration an den Routern
Software	Adobe Acrobat 8.1 Combine Files
Umwandlungsprogramm	Adobe Acrobat 8,1
Verschlüsselt	no
Papierformat	• 595,22 x 842 pts (A4) • 612 x 792 pts (letter)
Version des PDF-Formats	1,6

Dokumentationen

Hier sind diverse Anleitungen zu den Geräten bzw. Einstellungen zu finden.

Inhaltsverzeichnis

1 Inbetriebnahme eines Mikrotik Routerboard 8
1.1 Zuweisen einer IP Adresse 8
1.2 Schritt für Schritt Anleitung für HAMNET Backbone Equipment 8
2 Routing im digitalen Backbone 8
3 Modifikation eines Mikrotik Routerboard der 400 Serie bei Shutdown Problemen 9
4 Benutzerzugänge (User Accesspoint) 9
5 Dualhomed Heimnetzwerke 9
6 konventioneller PR-Userzugang über HAMNET 10

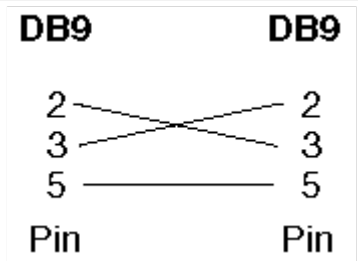
Inbetriebnahme eines Mikrotik Routerboard

Zuweisen einer IP Adresse

Im Auslieferungszustand besitzen Mikrotik Routerboards soweit keine fixen Adresseingaben.

Um auf das webbasierte Interface zu kommen, oder sich per Winbox verbinden zu können, ist es erforderlich, dem Board eine IP Adresse zu zuweisen.

Dies erfolgt mithilfe einer seriellen Verbindung (Null-Modem Kabel) und einem Telnetclient. Das serielle Null-Modem Kabel kann auch selbst angefertigt werden, wobei zwei Stück weibliche 9pol SUB-D Stecker benötigt werden. Hierbei kreuzt man die Pins 2 und 3 aus, Pin 5 verbindet man direkt.



Null-Modem Kabel

Nun lädt man den Client, unter Windows am Besten das freie Programm "Putty" (einach Google bemühen), und startet es im seriellen Modus mit 115200 Baud. Wenn das Routerboard und der PC über das Null-Modem Kabel verbunden sind, kann man am Routerboard die Spannung anlegen.

Es sollte sich das Routerboard nun "melden". Als Login ist bei einem unveränderten Routerboard standartmässig "admin" und kein Passwort eingestellt.

Nach dem Login gibt man "setup" ein, und folgt den Anweisungen um dem Board eine IP Adresse (bspw. 192.168.1.1/24) auf dem ETHER1 Port (erster RJ45 Netzwerkport) zu zuweisen. Mit Beenden des Setup-Programms ist nun die IP Adresse zugewiesen. Da aber DHCP am Board nicht aktiviert ist, muss man nun die IP Adresse am PC im selben Bereich manuell fix auswählen (bspw. 192.168.1.100) um sich bspw. per Webbrowser oder Winbox verbinden zu können.

Das Konfigurationsprogramm "Winbox" kann direkt von der Startseite (erreichbar im Browser unter Eingabe der Board IP) heruntergeladen werden. Eine Installation ist nicht notwendig, das Programm ist direkt startbar.

Schritt für Schritt Anleitung für HAMNET Backbone Equipment

Diese Anleitung erklärt Schritt für Schritt die Konfiguration eines Routerboard mit miniPCI WLAN Karte zum Einsatz im HAMNET Backbone.

Routing im digitalen Backbone

Für das BGP-Routing im HAMNET steht eine umfangreiche Dokumentation zur Verfügung. Siehe auch Routing digitaler Backbone

Diese Dokumentation gibt eine Einführung und Detaillierung der Konfigurationsmöglichkeiten im Backbone. Die Konfigurationsbeispiele und Richtlinien sind Ergebnisse aus nachgebauten Teststellungen und Versuchsaufbauten. (Dokumentation Stand 19.05.2009)

Modifikation eines Mikrotik Routerboard der 400 Serie bei Shutdown Problemen

Häufig kommt es bei der Verwendung von miniPCI WLAN Karten anderer Hersteller bei den Routerboards zum Shutdown, meist sogar ohne Reboot. Die Probleme treten auch häufiger bei höheren Sendeleistungen auf.

Diese Modifikation erklärt wie man Abhilfe schaffen kann.

Benutzerzugänge (User Accesspoint)

Für die HF-Zugänge zum HAMNET werden überwiegend bandbreitenmodifizierte (meist auf 5MHz beschränkt) Geräte benötigt. Solche Router bzw. Accesspoints mit entsprechender Software gibt es derzeit von Mikrotik und Ubiquiti (Nanostation, Bullet).
Beschreibungen zu den Benutzerzugängen zum HAMNET finden sie in der Rubrik Teststellungen der jeweiligen Bundesländer.
Weitere Infos zum Equipment sind auch hier zu finden.

Dualhomed Heimnetzwerke

Um das Heimnetzwerk an Internet und Hamnet anzubinden muss am Router oder am PC eine Routingrule eingetragen werden. Da früher das ganze 44.0.0.0/8 Netz uns gehörte, war das relativ einfach. Nun wurde aber das obere Viertel der IP Adressen verkauft. Dazu muss man diese Routingrule wie folgt ändern.

```
Adresse/Netz    oder mit Netzmaske
44.0.0.0/9      255.128.0.0      zum HAMNET Interface routen
44.128.0.0/10   255.192.0.0      zum HAMNET Interface routen
```

```
Address:   44.0.0.0              00101100.0 0000000.00000000.00000000
Netmask:   255.128.0.0 = 9       11111111.1 0000000.00000000.00000000
Wildcard:  0.127.255.255         00000000.0 1111111.11111111.11111111
=>
Network:   44.0.0.0/9            00101100.0 0000000.00000000.00000000
Broadcast: 44.127.255.255        00101100.0 1111111.11111111.11111111
HostMin:   44.0.0.1              00101100.0 0000000.00000000.00000001
HostMax:   44.127.255.254        00101100.0 1111111.11111111.11111110
Hosts/Net: 8388606
```

```
Address:   44.128.0.0            00101100.10 000000.00000000.00000000
Netmask:   255.192.0.0 = 10      11111111.11 000000.00000000.00000000
Wildcard:  0.63.255.255          00000000.00 111111.11111111.11111111
=>
Network:   44.128.0.0/10         00101100.10 000000.00000000.00000000
Broadcast: 44.191.255.255        00101100.10 111111.11111111.11111111
HostMin:   44.128.0.1            00101100.10 000000.00000000.00000001
HostMax:   44.191.255.254        00101100.10 111111.11111111.11111110
Hosts/Net: 4194302
```

konventioneller PR-Userzugang über HAMNET

Folgende Anleitung beschreibt die Einrichtung von AXUDP (PC/Flexnet32) und Paxon für einen 'konentionellen' Zugang zum PR-Netz über das HAMNET zu OE5XBL.

HAMNET AXUDP PR Installation für OE5XBL

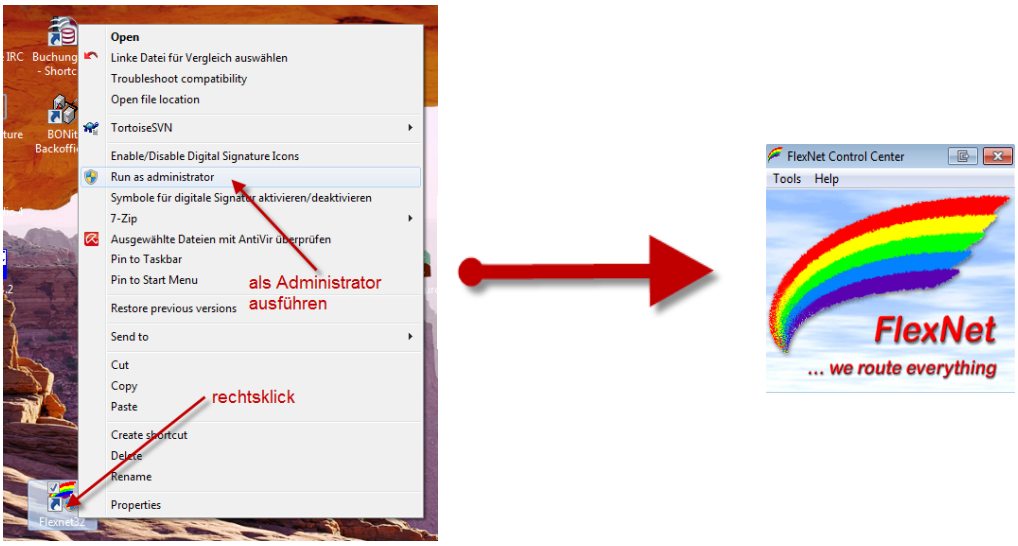
Diese Anleitung beschreibt den Zugang zum PR-Digi OE5XBL über das HAMNET unter Windows 7, bis auf wenige Kleinigkeiten sollte diese Anleitung auch für Windows XP verwendet werden können.

Mit der HAMNET Anbindung an OE5XBL bzw. an jeden anderen Knoten steht auch ein High-Speed PR-Zugang im herkömmlichen Sinn zur Verfügung.
Es werden lediglich 2 Softwarepakete dazu benötigt:

- PC/Flexnet32 als „L2-Treiber"
  http://web.oe5xbl.ampr.at/download/packet/flexnet32.zip
  http://www.afthd.tu-darmstadt.de/~flexnet/archive/flexnet32.zip
- Paxon als Terminalprogramm
  http://web.oe5xbl.ampr.at/download/packet/SetupPaxon1114.exe
  http://www.paxon.de/download/SetupPaxon1114.exe

Installation / Konfiguration PC/Flexnet32
flexnet32.zip kann an einen beliebigen Ort entpackt werden, ich empfehle C:\Program Files (x86) oder C:\Programme (x86) oder C:\Programme
Danach legt man sich optional für den leichteren Zugriff eine Verknüpfung auf dem Desktop zu „flexctl.exe" an.

1) **PC/Flexnet starten:**



Rechtsklick auf die erstellte Verknüpfung oder flexctl.exe ---> Als Administrator ausführen.
Damit Flexnet ordentlich auf die Hardware zugreifen kann muss dieses als Administrator laufen, alternativ kann man auch die „Benutzerkontensteuerung" unter Windows 7 ganz nach unten drehen.

Flexnet sollte wie dargestellt starten.

Routing digitaler Backbone

Inhaltsverzeichnis

1 Erläuterung 13
2 Dokumentation 13
3 Betriebliche Notizen für Sysops 13
3.1 Force Self im iBGP-Peer beachten 13
3.2 Peer auf ein Interface beschränken 14
3.3 iBGP Peers nicht über verschiedene Netze ziehen 15
3.4 Handling von Aggregates 15
4 BGP Mikrotik Beschreibung 16

Erläuterung

Ähnlich wie im Packet-Radio-System müssen auch im HAMNET (respektive im dahinterliegenden Backbone dafür) die Datenpakete ihre Ziele finden. Es ist im HAMNET unvermeidbar, das komplexe Mischtopologien (Stern, Ring) entstehen, welche bei der Linkstreckenplanung durch Österreich einem Routing - ähnlich dem Packet-Radio - bedürfen.

Die Pakete müssen oft mehrere „Hops“ überwinden. Pakete-Sender und Empfänger wechseln einander ständig ab. Daher müssen die Pakete duplex ihren Weg durch das Netz finden, damit eine Anwendung schlussendlich funktioniert.

Da händische Routeneintragungen in einem derart großem Netzwerk nicht mehr administrierbar sind, müssen Automatismen angewendet werden, welche das System möglichst rasch über die vorhandenen Zielnetze informieren. Dies beinhaltet die automatische Wegefindung von Alternativrouten, z.B.: bei Ausfall eines HF-Links oder bei einer Störung. Im bekannten Packet-Radio System bedient man sich etwa dem Flexnet-Routing.

Aufgrund verschiedener Untersuchungen wurde BGP „Border Gateway Protocol“ als das ideale Routing-Protokoll für den digitalen Backbone definiert.

Zielgruppe dieser Informationen: Sysops, Knotenbetreiber

Dokumentation

Diese Dokumentation gibt eine Einführung und Detaillierung der Konfigurationsmöglichkeiten im Backbone. Die Konfigurationsbeispiele und Richtlinien sind Ergebnisse aus den durch OE7BKH und OE7FMI nachgebauten Teststellungen und Versuchsaufbauten. (Dokumentation Stand 19.05.2009)

Betriebliche Notizen für Sysops

Folgende beitriebliche Notizen, zusätzlich zum Dokument ergaben sich aus dem bisher laufenden Betrieb.

Force Self im iBGP-Peer beachten

Bei allen Peers des iBGP (internal BGP) – also Peers zu Routern innerhalb der selben AS-Nummer (meist der Backbone im Bundesland, full mesh peers) muss bei der Funktion **Nexthop Choice** die Einstellung **force self** getätigt werden. Diese Einstellung muss auf allen Routern an den iBGP-Peers eingestellt werden.

Dadurch substituiert der Router sich selbst als next hop (Gateway) dem nächsten iBGP Partner, und meldet nicht die IP-Adresse eines dahinterliegenden Routers aus dem eBGP als Gateway. Letzteres produziert beim Empfängerrouter Routen in das falsche Interface (meist ins Default Gateway), da der Router nicht weiß, wo das um einen Hop weiter entfernte Gateway liegt.

Bei den eBGP Peers scheint die Funktion „force self“ aus dem bisherigen Betrieb nicht erforderlich, und kann auf default belassen werden.

Beschreibung der Funktion (englisch):

Affects the outgoing NEXT_HOP attribute selection.

default - select the nexthop as described in RFC 4271

force-self - always use a local address of the interface that used to connect to the peer as the nexthop;

propagate - try to propagate further the nexthop received; i.e. if the route has BGP NEXT_HOP attribute, then use it as the nexthop, otherwise fall back to the default case

Peer auf ein Interface beschränken

Peers lassen sich auf ein bestimmtes Interface und eine Update-Source-Interface einschränken, auf dem sie laufen dürfen. Dies ist in den Einstellungen zu jedem Peer unter "Advanced" möglich.

Versuche in OE7 haben gezeigt, dass die Einstellung bisher gut funkioniert.

Aus OE2 wurde berichtet, dass nach dieser Einstellung an einem Board das Peer nicht mehr zustande kam, obwohl das Peer mit dieser Einstellung genauer definiert wurde.

Bisher wurde noch nirgendwo beobachtet, dass sich ein Peer tatsächlich und unerwünschterweise um eine ausgefallene Linkstrecke herum über ein anderes AS (bei Vorhandensein eines Rings) aufbaut. Es wurde jedoch der Versuch des Routers bemerkt und getraced. Der Aufbau kam aber nicht zustande.

Empfohlene Einstellung in allen Peers (Reiter Advanced):

Interface: Das Interface für das Peering angeben *If specified, then outgoing connection will be made using only this interface;*

Update Source (optional)Selbes Interface oder die Routeradresse des eigenen Routers angeben. *If address is specified, this address is used as the source address of the outgoing TCP connection. If interface name is specified, an address belonging to the interface is used as described.*

Danach übrprüfen, ob das Peering wieder established wird. (ggf. ein zwei Versuche mit disable / enable) durchführen. Sollte es keine Beeinträchtigung geben, kann die EInstellung belassen werden.

Erläuterung wozu diese Funktion oft gerne benutzt wird:

internal BGP-Peers werden oft gerne mit Loop-Back-Interfaces geführt.

Peers über Loopback interfaces erlauben es, interne BGP-connections (iBGP Peers) unabhängig davon "am Leben" zu halten, egal welches Interface dazu benutzt werden muss, um den Nachbarn zu erreichen. Hintergrund ist, um nicht wegen einem defekten Interfaces (zb..: kaputtes eth oder Anschlusskabel an einem Router) das Peer zu verlieren - obwohl der Partner an einem anderen Interface sehr wohl zu erreichen wäre. Unter anderem wird bei diesem Vorhaben die Update Source dann auf ein (generiertes) loopback Interface gestellt und die Neighbour Update Source-Funktion aktiviert. Das Peering im iBGP (via Loopback) anstatt über das direkt zum Nachbarn "schauende" Interface ist speziell bei für ausfallsicheren Kabelnetzwerke der Standard.

iBGP Peers nicht über verschiedene Netze ziehen

Gemäß IP-Konzept des HAMNETS OE kommt dies nicht vor.(iBGP Peers bleiben innerhalb des Backbone Netzes /24 pro Bundesland).

Bei der Sondersituation OE7XWI, in dem am Userrouter im Tal DB0FHN angebunden ist und ein Routing benötigt, konnte das full mesh-Peering nicht störungsfrei aus dem Usernetz in das Backbonenetz hochgezogen werden. (Trotz unterschiedlich versuchter Einstellungen und statisch geroutetem Unterbau für die Peers). Dem Userrouter wurde daher eine eigene AS-Nummer aus dem OE7-Freiraum gegeben. Zudem gibt es eine nicht unerwünschte PATH Verlängerung und AS-Path Bekanntgabe des speziellen Routers.

Das Problem ist eine Sondersituation und kommt im üblichen Backbone-Netz (Verlinkte Relaisstandorte mit ihren Routern) nicht vor. Dort verlaufen die iBGP-Peers innerhalb des selben /24 Netz.

Handling von Aggregates

Das Announcen von Aggregaten ist aus mehrern Gründen derzeit nicht vorgesehen. Detailrouten für detailliertere Netze erlauben auch mehr Übersicht und helfen bei der Fehlersuche.

Unabhängig vom derzeitigen oder zukünftigen Handling: Werden Aggregate announced, so müssen diese an allen AS-Grenzen (also wo eBGP Peers vorhanden sind) ident announced und summarized werden.

Sonst kann es dazu kommen, dass Datenpakete zu einem entfernten Punkt hinwärts über einen anderen Link verlaufen, als rückwärts. Wird dies nicht berücksichtigt kommt es dann dazu, dass einem externen Router (aufgrund eines Ringes) über einen anderen HF-Weg trotz Aggregat noch immer die detaillierten Routen gemeldet werden. Dies führt dazu, dass die Retourpakete an das Gateway der detaillierten Route zurückgesendet werden. Dabei wird dann ein anderer Weg beschritten, die Verbindung hakt oder kommt nicht zustande.

Daher müssen allfällige Aggregate an allen AS-Grenzen ident announced werden.

Derzeit sind Aggregate nicht vorgesehen und sollen auch nicht announced werden.

BGP Mikrotik Beschreibung

Die aktuelle Beschreibung der Funktionen im BGP-Menü (Winbox) sind unter http://wiki.mikrotik.com/wiki/BGP beschrieben.