Routing digitaler Backbone

Versionsgeschichte interaktiv durchsuchen
VisuellWikitext

Version vom 1. November 2009, 17:38 Uhr (Quelltext anzeigen)	**Version vom 1. November 2009, 17:38 Uhr (Quelltext anzeigen)**
Oe7xwi (Diskussion | Beiträge)	Oe7xwi (Diskussion | Beiträge)
K (→Force Self im iBGP-Peer beachten)	K (→Force Self im iBGP-Peer beachten)
← Zum vorherigen Versionsunterschied	Zum nächsten Versionsunterschied →

Zeile 35: **Zeile 35:**

	Bei den eBGP Peers scheint die Funktion „force self“ aus dem bisherigen Betrieb nicht erforderlich, und kann auf default belassen werden. Sollte sich aufgrund eines Firmwareupgrades an den Miktrotik-Boards hier etwas am Default-Wert ändern, wird eine Information hier eingebracht.		Bei den eBGP Peers scheint die Funktion „force self“ aus dem bisherigen Betrieb nicht erforderlich, und kann auf default belassen werden. Sollte sich aufgrund eines Firmwareupgrades an den Miktrotik-Boards hier etwas am Default-Wert ändern, wird eine Information hier eingebracht.
−	Beschreibung der Funktion (englisch):	+	
		+	'''Beschreibung der Funktion (englisch):'''
	''Affects the outgoing NEXT_HOP attribute selection.		''Affects the outgoing NEXT_HOP attribute selection.

Version vom 1. November 2009, 17:38 Uhr

Inhaltsverzeichnis

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

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 getätigt 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. Die Default-Einstellung ist offensichtlich "propogate" (Fortpflanzen) was nicht zum IP-Konzept passt bzw. ein darunterliegendes Routingprotokoll oder statische "Pflasterl" zusätzlich verlangen würde.

Bei den eBGP Peers scheint die Funktion „force self“ aus dem bisherigen Betrieb nicht erforderlich, und kann auf default belassen werden. Sollte sich aufgrund eines Firmwareupgrades an den Miktrotik-Boards hier etwas am Default-Wert ändern, wird eine Information hier eingebracht.

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

Update Source optional, selbes Interface oder die Routeradresse des eigenen Routers *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 des direkt zum Nachbarn "schauende" Interface ist insbesondere für Ausfallsichere 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.