IP-ADRESSKOORDINATION IN DL

Egbert Zimmermann, DD9QP
Thomas Osterried, DL9SAU

I N H A L T S V E R Z E I C H N I S

A. VORWORT

1. AUSGANGSLAGE
1.1 Aktivitätsinseln und Schwächen im Netz
1.2 Entwicklung und Aufbau der DL-IP-Koordination
1.2.1 auf internationaler Ebene
1.2.2 auf nationaler Ebene
1.2.3 auf regionaler Ebene
1.3 Reorganisation der DL-IP-Koordination
1.3.1 aus 1 mach 3
1.3.2 Bewährtes beibehalten: Regionalzonenkonzept

2. DAS NEUE DNS-KONZEPT
2.1 Digis, Aktivitätszentren, Subnetze
2.2 Die DNS-Hubs
2.2.1 Anzahl, technische Anforderungen an einen Hub
2.2.2 Einzugsgebiete und Vernetzung der Hubs
2.2.3 Anbindung von Digis, Informationsfluss BottomUp/TopDown
2.3 DL und der Rest der Welt
2.3.1 Sammeln und Prüfen aller DL-Daten
2.3.2 automatisches Update bei ucsd.edu, Fehler, Redundanz
2.3.3 Laufzeiten

3. TECHNIK
3.1 Aufsetzen und Betrieb von Nameservern
3.1.1 Welche DNS-Version ?
3.1.2 Der Betrieb der DNS an den Hubs
3.1.2.1 Welche Zonen gibt es? -> "zones-hub-de.txt"
3.1.2.2 Bereitstellen von Scripten und Zonendaten
3.1.2.3 einheitliche Ordnerstruktur auf allen Hubs
3.1.2.4 Zugriff und Download auf vielen Wegen
3.1.3 Aufsetzen eines DNS an einem Digipeater
3.1.3.1 allgemeine Anforderungen
3.1.3.2 Grundkonfiguration
3.1.3.3 automatisches Erzeugen der Konfiguration
3.1.3.4 automatische Aktualisierung der Zonendateien
3.1.3.5 Verwaltung der eigenen Region
3.1.4 Die weltweite Bereitstellung der DL-Daten auf ucsd.edu
3.1.4.1 redundantes, automatisiertes Update
3.1.4.2 Problematik der Umsetzung in die ampr.org Zone

4. PRAXIS
4.1 Stand der Realisierung auf Hubebene
4.2 Stand der Realisierung auf Regionalebene
4.3 Beliebte Fehler im Zonefile

5. DISKUSSION, ANREGUNGEN, HINWEISE

B. Anhang

I. Beispiel eines Zonefiles
II. "named.conf" am Beispiel von Hub Sued
III. "zones-hub-de.txt"

IP-ADRESSKOORDINATION IN DL

- Neue Koordinatoren
- Das DNS Subzonen Projekt
  - ❖ Konzept,
  - ❖ Status,
  - ❖ Ausblick
  - ❖ Konfiguration

A. VORWORT

In der Zeit vom 15.10.2003 bis 31.10.2003 wurden 3 IP-Koordinatoren für DL gewählt. Die drei neu gewählten Koordinatoren

- Egbert Zimmermann <dd9qp>,
- Thomas Osterried <dl9sau>,
- Thomas Maisl <dl3sbb>
  haben die Wahl angenommen.

Bei dieser Gelegenheit nochmals unseren Dank an unseren Wahlleiter Jens Schoon <dh6bb> für seine Mühe, und an Fred Baumgarten <dc6iq> für seine langjährige Tätigkeit als IP-Koordinator für DL.

Vorausgegangen war eine Diskussion in der Amateurfunk-Newsgroup ampr.de.config, die im April 2003 begann und einige Wochen andauerte. An dieser Diskussion und Meinungsbildung waren zahlreiche Aktive aus ganz DL beteiligt. Besprochen wurden insbesondere die Punkte

- Status Quo des bisherigen DNS Subzonenprojektes,
- Schwachstellen und Lösungsmöglichkeiten,
- die Notwendigkeit von mehreren DL-Koordinatoren
  (Arbeitsteilung, Ausfallsicherheit usw.).

Im Folgenden möchten wir das Konzept und den Stand der Realisierung des DNS-Subzonen-projektes und seine Bedeutung für den nationalen Betrieb sowie die technische Realisierung der internationalen Einbindung in die weltweite IP-Nummernverwaltung des Amateurfunkdienstes vorstellen. Dabei wollen wir aufzeigen, wie durch die Einführung neuartiger Strukturierungselemente und durch automatisierte Koordinierungsverfahren die Arbeit der Koordinatoren und Sysops vor Ort vereinfacht und die Konsistenz und das Zusammenführen der Teilnetze in ein deutschlandweit funktionierendes, nationales Amateurfunk-IP-Netz zusammengeführt werden kann.

Angesprochen sind die regionalen IP-Koordinatoren, alle Sysops von TCP/IP-gestützten, automatischen Stationen in DL und alle technisch interessierten.

Für das DL-Koordinatoren-Team - Thomas Osterried <dl9sau>

1. AUSGANGSLAGE

1.1 Aktivitätsinseln und Schwächen im Netz

Bereits Ende der achtziger, Anfang der neunziger Jahre setzte in einigen Regionen in DL das Interesse für TCP-basierte Übertragungen im digitalen Amateurfunknetz ein. Der von Phil Karn KA9Q entwickelte IP-Protokollstack und die weltweit einsetzende Verbreitung von PCs auf 8086-Basis ermöglichten es, mit verhältnismäßig geringem Aufwand TCPIP-basierte Dienste auf DOS-Maschinen abzuwickeln.

Parallel zu dieser Entwicklung wurde von den Funkamateuren in DL unter dem Namen "Packet Radio" ein digitales Funkübertragungssystem aufgebaut, welches ihnen auf der Grundlage des AX.25 Protokolls, einer auf die Belange eines relativ langsamen Funkübertragungsnetzes für Funkamateure spezialisierten Abwandlung des X.25 Protokolls, eine drahtlose Kommunikation über eine solche Funkstelle, auch Digipeater genannt, ermöglichte. Mit der Einrichtung von Richtfunkstrecken (Interlinks) wurden dann solche Digipeater miteinander verbunden. Aus Aktivitätsinselchen wurden Aktivitätsinseln. Zur Vermeidung bzw. Optimierung typischer Probleme, die in solchen Funknetzen auftreten können, wurden Protokollvarianten wie NET/ROM, später auch FlexNet entwickelt. Bis heute sind weitere hinzugekommen.

Diese in allen technisierten Ländern der Welt verlaufene Entwicklung war die Geburt einer kompletten, von Funkamateuren erbauten und betriebenen Netzwerkinfrastruktur, aus meiner Sicht eine der großartigsten Leistungen des weltweiten Amateurfunkdienstes der Nachkriegszeit. Natürlich gibt es auch noch weitere, wie etwa der Satellitenfunkdienst und andere. Dies war aber auch die Grundlage für sinnvolle Anwendungen auf TCP/IP-Basis. Schon sehr frühzeitig testeten TCP/IP-interessierte Funkamateure Anwendungen wie Email, Newsgroups oder FTP. Das Internet spielte damals im Amateurfunk keine Rolle. Man wollte lediglich die TCP/IP basierten Anwendungen auch im Amateurfunk testen und nutzen. Zum Einsatz kamen mit Ausnahme von FTP fast ausschließlich textbasierte Anwendungen, weil diese das geringste Datenvolumen verursachten.

Sehr schnell wurde eine der größten Schwächen des Packet-Funknetzes offenbar, nämlich die damals sehr geringe Bandbreite. Sowohl Interlinks als auch Benutzerzugänge liefen mit einer Bandbreite von 1,2kBit/s, aus heutiger Sicht einer Art "schnelles RTTY", die sich zudem noch zahlreiche Funkamateure teilen mussten. Schon eine einzige FTP-Verbindung war in der Lage, den Betrieb weiterer Verbindungen über einen Interlink oder Benutzereinstieg erheblich zu behindern bzw. einen Neuaufbau von Verbindungen zu verhindern.

So nimmt es nicht Wunder, dass Verbreitung und Akzeptanz von TCP/IP-gestützten Anwendungen im Amateurfunkdienst nicht konfliktfrei verliefen.

Alsbald erfreuten den geneigten User im Connecttext einiger weniger Digipeater Informationen wie "TCPIP ist hier unerwünscht" oder andere Dinge, die das Herz des TCP/IP-freudigen OMs bewegten. Mit der Zeit wurden die Connect-Texte dann durch eine "++noWire++" Aktion und heute, fast 15 Jahre später, hin und wieder durch Sätze wie "Internetverbindungen sind hier unerwünscht" ersetzt.

Oft waren gerade solche Netzknoten beteiligt, die für überregionale Verbindungen eine gewisse Bedeutung hatten und/oder deren Betreibergruppen erheblichen Einfluss auf die Entwicklung des Packet-Netzes in DL insgesamt nehmen konnten, und die natürlich die volle Wucht des Nachteils der viel zu langsamen Interlinktechnik traf, noch bevor sie den letzten ihrer mit viel Geld, Arbeit und unendlicher Mühe aufgebauten Interlinks aktiviert hatten.

Dies hatte auf die regionale Ausformung der Aktivitätszentren, ihren unterschiedlichen Grad von Aktivität und deren Kommunikationsmöglichkeiten untereinander erheblichen Einfluss und muss bei der Entwicklung eines neuen DNS-Konzeptes berücksichtigt werden.

Mögen solche Reaktionen auch menschlich verständlich sein, so waren sie über die Jahre hinweg gleichermaßen ungeeignet, die Ausbreitung TCP/IP-basierter Anwendungen im Amateurfunkdienst zu verhindern.

Heute ist unser Netz zwar schneller, aber leider nicht durchgehend und, wie bei anderen Netzwerken auch, natürlich nie schnell genug. Immer mehr Anwendungen sind TCP/IP-basiert (Convers, DX-Cluster etc.) und schon lange nicht mehr rein textorientiert. Der Webbrowser mit seinen multimedialen Möglichkeiten hat auch im Amateurfunk seinen Einzug gehalten (HTML-Schnittstellen zu traditionellen Anwendungen wie Mailboxen, Newsserver und andere, Bildübertragungen und diverse weitere PlugIn-Spielereien).

Neuere Entwicklungen zielen ganz klar auf den Einsatz von Streamingtechnologien im Amateurfunk (z.B. VoIP, Echolink, ATV-Bildübertragungen per Realplayer und viele mehr). Darüber hinaus werden vereinzelt auch Ansätze wie bedarfsgesteuerte IP-Nummernzuteilung oder der Aufbau von VPN-Netzen für den autorisierten Zugriff aufs Amateurfunknetz aus Hf-mässig nicht versorgten Gebieten getestet.

Dies hat zur Folge, dass nicht nur der Bedarf an IP-Adressen für Individualnutzer steigen wird, sondern auch eine nicht unerhebliche Zahl von IP-Adressen für Anwendungs- und Serverdienste bereitgehalten und koordiniert werden muss. Von daher muss eine zeitgemäße IP-Koordination in DL die historisch gewachsenen Gegebenheiten unseres Packetnetzes genauso berücksichtigen, wie sie Antworten auf Anforderungen künftiger Anwendungen oder Aktivitäten aus Regionen, die heute vielleicht noch ein weißer Fleck in der Landkarte der deutschen TCP/IP-Regionalnetze sind, bereithalten muss.

1.2 Entwicklung und Aufbau der DL-IP-Koordination

1.2.1 auf internationaler Ebene

Dem Amateurfunkdienst ist weltweit ein 44/8 Netz zugewiesen. Es ist in maximal 256 44.xxx/16 Netze aufgeteilt, wovon ein oder mehrere dieser Netze den jeweiligen Nationen zugewiesen wurden. Das weltweite 44/8 Netz wird unter der einheitlichen Domain "ampr.org" (ampr steht für "AMateurPacketRadio" und org für eine "non-profit ORGanization") über 5 im Internet eingebundene Nameserver verwaltet.

Für Deutschland steht derzeit das 44.130/16 Netz zur Verfügung. Jede Nation darf über ihre nationalen IP-Koordinatoren die IP-Adresszuteilung innerhalb des zugeteilten Adressraumes eigenverantwortlich verwalten.

Jegliche Änderungen in der nationalen Adresszuteilung müssen von den nationalen IP-Koordinatoren an den zentralen ampr.org-Nameserver bei "ucsd.edu" gemeldet werden. Sie werden dort automatisch eingetragen und weltweit über die vier anderen DNS-Mirrors verteilt. Bisher wurde dies von einem deutschen IP-Koordinator in der Regel "von Hand" zu Zeitpunkten seiner Wahl an ucsd.edu übermittelt.

Nur was bei "ucsd.edu" eingetragen ist, hat international Gültigkeit. Der Nameserver bei "ucsd.edu" hat somit die höchste Autorität für alle Zuteilungen im weltweiten Amateurfunkdienst. Das DNS-System im ampr.org Netz ist genau wie jedes andere DNS-System streng hierarchisch aufgebaut. Daran lässt sich strukturell nichts ändern.

1.2.2 auf nationaler Ebene

Die nationalen IP-Koordinatoren sammeln alle Adressvergaben und Namenszuteilungen ihres Landes und müssen sie auf Konsistenz (Doppelvergaben, syntaktische Fehler, Neuzuweisungen, Löschungen etc) prüfen, bevor sie Aktualisierungen international verfügbar machen können. Dazu benötigen sie sämtliche Daten aus dem ganzen Land, die ihnen auf geeignete Art und Weise zur Verfügung gestellt werden müssen.
Die Aktualität der Daten auf ucsd.edu hängt wesentlich von der Aktualität der Daten ab, die den nationalen Koordinatoren zur Verfügung stehen. Wie sie an diese Daten kommen können, war bisher nie verbindlich festgelegt worden.

1.2.3 auf regionaler Ebene

Wegen der ausgeprägten "Inselstruktur" mit schlechten bis gar nicht vorhandenen Kommunikationsmöglichkeiten (auf TCP/IP-Ebene) zwischen diesen Inseln wurde in Deutschland das Regionalkoordinatorensystem eingeführt. Regionalkoordinatoren mit stark variierenden Fachkenntnissen und Motivationen waren für die Vergabe von IP-Adressen in ihrer Region verantwortlich.

Diese konnten aus einem ihnen zugeteilten IP-Adresskontingent (meist ein bis zwei 44.130.xx/16 Netze) selbst die IP-Adressvergabe für ihre Region durchführen. Die von den Regionalkoordinatoren in der Region gepflegten Datenbestände lagen in unterschiedlichen Formaten vor (flache, traditionelle "HOSTS" Datei, Domaindateien für die diversen NOS-Programmvarianten, Zonendateien für BIND-Nameserver, eigene Konstrukte).

Teilweise wurden diese Dateien der Allgemeinheit und den nationalen IP-Koordinatoren über verschiedene Transportwege zugänglich gemacht. Dazu gehörten zum Beispiel die Verbreitung über die Mailboxen (Rubrik TCPIP). Auch die nicht überall in Deutschland verfügbaren Newssysteme wurden verwendet und in Einzelfällen zeitweise auch drahtgebundene Transportmechanismen.

Die Vielfalt der verwendeten Dateiformate bedingte von der Region bis hinauf zur weltweiten Verfügbarkeit oft mehrfaches Umwandeln von einem Format ins andere. Dies geschah nicht in einem standardisierten Verfahren, sondern eher willkürlich, je nach Geschmack des gerade zuständigen Koordinators. Es geht das Gerücht, das manche sogar alles von Hand editiert haben sollen.

Dem Einschleichen von Fehlern und dem Verlust von Informationen waren Tür und Tor geöffnet.

Mit dem zunehmenden Einsatz von Linux in Amateurfunknetzen war man später in der Lage, in vielen Regionen "echte" BIND-Nameserver zu betreiben, auf denen man zumindest die IP-Adressen der eigenen und evtl. einiger benachbarter Regionen autoritativ und maschinennutzbar vorhalten konnte.

Da ein DNS aber nur für eine begrenzte Teilmenge an Adressen, nämlich die seiner lokalen Region, autoritativ sein kann, wurde in Deutschland das Regionalzonenkonzept eingeführt. Die flache Domainstruktur ampr.org wurde innerhalb Deutschlands in Subdomains aufgegliedert und um sich von künftigen Regionalisierungen im Ausland unterscheiden zu können, wurden sie national eindeutig gekennzeichnet. Es entstanden Konstrukte wie

rr.de.ampr.org für die Region Rhein-Ruhr
dd.de.ampr.org für die Region um Dresden

und viele andere. Mit der Verbesserung der Netzwerkstruktur begann nun die Zeit des großen Sammelns.

Jeder Sysop, der etwas auf sich hielt, wollte möglichst alle Domains auf seinem TCP/IP-Server verfügbar haben, um das TCP/IP-Netz scheinbar zusammenhalten zu können. Jeder Digi mit eigenem DNS versuchte bei jeweils allen anderen in regelmäßigen Zeitabständen die dort autoritativ vorgehaltenen Zonendaten zu bekommen. Ungünstig gewählte Zeitintervalle sorgten zusätzlich dafür, dass ein und dieselbe Zonendatei auf den großen überregionalen Interlink-strecken zigfach am Tag hin und her transportiert wurde. Jeder einzelne Digi benötigte rund 120 dieser Zonendateien.

Trotz dieser Nachteile funktionierte der technische Zonentransfer per DNS jahrelang erstaunlich stabil. Allerdings fehlte irgendwo immer etwas. Server wurden umgebaut, IP- und ARP-Adressen geändert, TCP/IP-fähige Digis kamen hinzu, andere fielen weg. Jeder Sysop musste ständig die Parameter für alle Systeme in DL kennen und in seiner Konfiguration aktuell halten, obwohl diese Parameter nie regelmäßig oder gar zentral veröffentlicht wurden.

Die Aktualität und Authentizität der Daten konnte trotz größtem Eifer und Einsatz mancher Sysops nicht gewährleistet werden. Die Datenbestände drifteten regional auseinander und enthielten mehr und mehr Fehler. Schließlich waren sie praktisch nicht mehr bei ucsd.edu einpflegbar.

Bei vielen Koordinatoren aller Ebenen machten sich Enttäuschung und Frustration breit. Andere verloren aus anderen Gründen das Interesse oder hatten einfach keine Zeit mehr. In einigen Regionen entstand eine Art "Wildwuchs" ("wild.de.ampr.org"), ohne Synchronisation auf ucsd.edu, andernorts brach der TCP/IP Betrieb fast vollständig zusammen oder er beschränkte sich in seiner Funktionalität auf die berühmten "Inseln" der Anfangszeit. Man war froh, wenn es mit dem direkten Nachbarn klappte.

Für moderne TCP/IP-gestützte Anwendungen ist ein funktionierendes DNS-System von essentieller Bedeutung und daher auch für den Amateurfunkdienst in DL dringend geboten. Eng damit verknüpft ist die Koordination der IP-Adressen, deren Organisation sich an der hierarch-ischen Grundstruktur des DNS-Systems orientieren muss, wenn sie effektiv sein soll.

1.3 Reorganisation der IP-Koordination in DL

1.3.1 Aus 1 mach 3

Die Erfahrungen der vergangenen Jahre zeigen, dass Arbeitsaufwand und Zeiteinsatz von einem einzelnen, ehrenamtlich tätigen, nationalen IP-Koordinator langfristig nicht geleistet werden können.

Als organisatorische Neuerung ist deshalb in DL seit Ende 2003 in einem nationalen Wahlver-fahren eine Gruppe von 3 nationalen IP-Koordinatoren eingerichtet worden, die sich die Arbeit teilen und sich gegenseitig vertreten können. Dies gewährleistet Kontinuität nach oben bei der Aktualisierung der DL-Daten auf ucsd.edu und intensivere Kontakte und Unterstützung der Koordinatoren in den einzelnen Regionen bis hin zur Betreuung von einzelnen Usern aus Regionen, in denen es noch keine größeren TCP/IP Aktivitäten gibt. Die Zahl drei soll bei Entscheidungen eine Pattsituation verhindern helfen und das Team dadurch arbeitsfähig halten.

Diese Konstruktion hat sich bereits gleich zu Beginn unserer Tätigkeit bei einem kurzfristigen Ausfall eines Teammitgliedes als richtig erwiesen. Die Arbeit wurde nicht unterbrochen.

1.3.2 Bewährtes beibehalten: Regionalzonenkonzept

Das Regionalzonenkonzept und die Arbeit von Regionalkoordinatoren haben sich vom Grundsatz her in jahrelangem Betrieb bewährt.

Regionalzonenprinzip und hierarchische Struktur sind Grundvoraussetzung für das Zusammenschalten zahlreicher Nameserver, die immer nur für einen kleinen Teil des Namensraumes autoritativ sind, aber den ganzen Namensraum für die User bereitstellen müssen. Das Zusammenschrumpfen auf eine kleine Anzahl von Nameservern ist wegen der im Vergleich zu Drahtnetzen um Größenordnungen schlechteren Antwortzeiten in unserem Funknetz nicht praktikabel und würde von den Usern kaum akzeptiert.

Der DNS-Betrieb mit Zonentransfers über Interlinks innerhalb eines Gebietes von mehreren benachbarten Regionalzonen arbeitet stabil und sicher genug. Bei Aufrechterhaltung des Status Quo im Netz oder aber bei weiterem Netzausbau ist normalerweise nicht mit einer Verschlechterung dieser Situation zu rechnen.

Regionalkoordinatoren kennen die spezifischen Besonderheiten und Bedürfnisse innerhalb ihrer Region viel besser, als die in der Regel weiter entfernt sitzenden, nationalen Koordinatoren.

In der Fläche stehen interessierten Usern dadurch viel mehr Ansprechpartner zur Verfügung. Teilweise sind diese Ansprechpartner in ihrer Region ohnehin bekannt (Sysop oder andere Funktion).

Der insgesamt anfallende Koordinationsaufwand wird auf viele Schultern verteilt, der Zeit- und Arbeitsaufwand für den einzelnen Koordinator kann deutlich verringert werden.

2. DAS NEUE DNS-KONZEPT

In den ersten drei Monaten unseres Wirkens wurde von uns ein neues Konzept zur IP-Adresskoordination in DL erarbeitet und getestet.
Vorausgegangen waren intensive Diskussionen mit allen Interessenten in einschlägigen Newsgruppen wie ampr.de.config.

Wir haben uns nicht zuletzt aus Kompatibilitätsgründen entschieden, das auch in anderen Netzen bewährte Nameserverprinzip, seine Datenstruktur und die Zonentransfers moderner Bind-Versionen zu integrieren. Die Übertragung hat sich als außerordentlich robust und sicher erwiesen und es können alle von uns benötigten Informationen in der Datenstruktur untergebracht werden.

Das Konzept setzt auf dem beschriebenen Status Quo auf und implementiert Bewährtes. Gleichzeitig werden neuartige automatisierte Verfahren eingeführt, die die Fehleranfälligkeit minimieren sollen und den Arbeitsaufwand für Sysops und Regionalkoordinatoren vor Ort deutlich reduzieren helfen können.

Auch technisch weniger versierte Sysops sollen in die Lage versetzt werden, mit einfachen Hilfsmitteln ein zuverlässig funktionierendes und sich weitgehend automatisch updatendes DNS-System aufzusetzen, das nur sehr wenig Wartungsaufwand erfordert.

Außerdem ermöglicht dieses Konzept in seinem Endausbau erstmals einen zuverlässigen überregionalen Austausch wirklich aller Zonen in ganz DL mit voller Synchronisation auf ucsd.edu. Die technischen Aspekte dieses Konzeptes werden nun näher beschrieben.

2.1 Digis, Aktivitätszentren, Subnetze

Das Regionalzonenkonzept wird beibehalten. Die Zuweisung der Subnetze und Zonen auf einen oder mehrere Digipeater, die TCP/IP-Dienste anbieten und einen DNS betreiben, soll erhalten bleiben.

Was wir derzeit vorfinden ist Folgendes:

a) kleinere Aktivitätsinseln (mehrere User, 1 Digi, ein Subnetz)

TCP/IP Aktivitäten finden sich in der Regel um einen Digipeater herum. Die Abwicklung von lokalen TCP/IP-Diensten ist normalerweise problemlos und je nach Benutzerzugang auch mehr oder weniger schnell, solange sie sich auf lokale Dienste beschränkt. Die Linksituation spielt dabei keine große Rolle. Bandbreitenkritische Anwendungen sind möglich und fast nur von der Geschwindigkeit des Userzuganges abhängig. Solche "Inseln" bilden die kleinste Einheit im deutschen Packetnetz und sind darin überall verstreut aufzufinden. Traditionell wurde diesen Aktivitätsinseln ein 44.130.xx/16 Netz zugewiesen und auf Wunsch eine Regionalzone zugeteilt. An den meisten der beteiligten Digipeater wird ein Host auf Linux-Basis betrieben, der einen autoritativen Nameserver für die Zone hat und für die User weitere Dienste anbietet. Ein Regional-zonenkoordinator ist mehr oder weniger aktiv.

b) Aktivitätszentren (mehrere User, mehrere Digis, ein Subnetz)

Oftmals wuchsen innerhalb einer solchen Zone die Userzahlen und ihre Aktivitäten über den Einzugsbereich eines einzelnen Digipeaters hinaus. Es entstanden Aktivitätszentren, wo mehrere unmittelbar benachbarte Digipeater mit ihren Usern innerhalb einer Zone TCP/IP Betrieb ermöglichen. Die Linksituation bezogen auf die Übertragungssicherheit zwischen benachbarten Digipeatern ist in der Regel sehr gut bis gut, besonders dann, wenn die Geschwindigkeit auf den Interlinks ein Mehrfaches der Geschwindigkeit der Userzugänge betragen kann. Solche Aktivitätszentren haben ebenfalls meist einen für die ganze Zone autoritativen Nameserver an einem der beteiligten Digipeater. Es sind ein oder (meist wegen der hohen Userzahl) zwei 44.130.xx/16 Netze innerhalb einer Zone zugewiesen. In einigen Fällen werden auch mehrere Nameserver betrieben, die gleichberechtigt für die ganze Zone autoritativ sind (mehrere "Primaries" bzw. "hidden Primaries"). Ein Regionalzonenverwalter und ein bis zwei DNS-Administratoren sind mehr oder weniger aktiv.

c) Regionen mit TCP/IP Aktivität

Abhängig von der Struktur des Packet Netzwerkes lassen sich Regionen ausmachen, in denen benachbarte Aktivitätszentren über die zwischen ihnen vorhandenen Interlinks TCP/IP-Betrieb abwickeln. Innerhalb dieser Gebiete funktioniert in der Regel das IP-Routing zwischen den Zonen gut und stabil. Die Situation auf Seite der Interlinkvernetzung ermöglicht dauerhaften, sicheren und meist auch redundanten TCP/IP Betrieb für schmalbandige Anwendungen wie Email, News, Convers, DX-Cluster usw. Der automatische Austausch von Zonendateien zwischen Nameservern stellt ebenfalls eine schmalbandige Anwendung dar und funktioniert meist problemlos. Multimediales WWW oder FTP ist bereits nur eingeschränkt möglich. Man behilft sich mit Caching-Proxies und relativ hohen Haltezeiten, die allerdings im Amateurfunk noch tolerierbar sind.
Anwendungen, die Echtzeitcharakter haben, z.B. Streamingverfahren, sind wegen der Bandbreite auf den Interlinks kritisch und noch keinesfalls Standard. Die Ausdehnung solcher Regionen kann sehr unterschiedlich sein und durchaus die Größenordnung eines Bundeslandes erreichen. Sie ist in erster Linie von der in der Region vorherrschenden Linksituation und Useraktivität abhängig und lässt sich nicht an politischen oder verwaltungsrechtlichen oder geografischen Grenzen festmachen.

Charakteristisch für das TCP/IP-Amateurfunknetz in DL sind solche meist historisch gewachsenen Regionen, innerhalb derer das TCP/IP Routing und der Nameserverbetrieb recht stabil funktionieren. Sie verteilen sich über die ganze Fläche der Republik und sind durch mehr oder weniger große Gebiete unterbrochen, in denen es (noch) keine bemerkenswerten TCP/IP Aktivitäten gibt. Diese Regionen mit TCP/IP Aktivität sind aber oft zu weit voneinander entfernt und die Netzverbindungen zwischen ihnen zu schlecht, als dass zwischen diesen Regionen direkt sinnvoller TCP/IP Betrieb stabil möglich wäre.
Insbesondere ist ein automatischer Zonentransfer von Nameservern zwischen diesen Regionen äußerst problematisch und wegen des kritischen Timeoutverhaltens neuerer DNS-Software (lässt sich nicht patchen) teilweise sogar unmöglich. Als geradezu klassischer Dauerbrenner sei die seit vielen Jahren fast nie funktionierende Verbindung zwischen der NORD-Region (TNN-Land) und anderen Regionen in DL erwähnt.

Beispiele für einige traditionelle Regionen sind:

NORD-DL : Großraum Hamburg, SW, Friesland, Nord-DNS
SUED-DL : Großraum Stuttgart oder Nürnberg (Bayern + BW)
OST-DL : Großraum Berlin bis Dresden, Leipzig (MVP?)
WEST-DL : Großraum NRW, Teile RP,Saarland
MITTE : Großraum Hessen (Hannover, Goettingen, Frankfurt)

Fakt ist, dass der Einsatz von immer bandbreitenintensiveren TCP/IP-Anwendungen in den Regionen bereits jetzt stattfindet und zunehmen wird und die unerlässliche, zentrale IP-Koordination nicht darauf warten kann, bis sich die Linksituation zwischen den Regionen entscheidend verbessert hat. Es muss jetzt etwas geschehen!

2.2 Die DNS-Hubs

Zwischen ucsd.edu und seinen Mirrors als höchste Instanz für das weltweite ampr.org Netz und den zahlreichen lokalen Nameservern in den oben beschriebenen Regionen wird eine neue Ebene von wenigen Nameservern gezogen, die untereinander sehr gut verbunden sind und in der Hierarchie zwischen dem lokalen DNS und dem Rest der Welt eine nicht zu umgehende Instanzebene bilden. Diese Nameserver bilden für das deutsche Regionalzonen- und DNS-System die Klammer zwischen den einzelnen Regionen. DNS-Traffic (Austausch von Zonendateien) zwischen den Regionen soll über diese Nameserverebene laufen. Ein lokaler DNS muss nicht mehr _ALLE_ anderen lokalen DNS in DL kennen und ein funktionierendes Routing zu ihnen haben, um an alle Zoneninformationen zu kommen und somit über eine aktuelle, konsistente Datenbank von ganz DL und darüber hinaus zu verfügen. Für diese neuen Nameserver verwenden wir den Begriff DNS-Hub oder Großregions-Hub.

2.2.1 Anzahl, technische Anforderungen an einen Hub

In jeder der existierenden, oben näher beschriebenen (Groß-)Regionen wird ein solcher DNS-Hub installiert. Damit ist sichergestellt, dass alle in einer Region aktiven, lokalen Nameserver diesen für sie zuständigen DNS-Hub im Netz erreichen können und ein automatischer Zonentransfer stattfinden kann.

Zwei der DNS-Hubs können alternativ und ausfallsicher das automatische Updaten der deutschen Daten auf ucsd.edu übernehmen. Von daher ist ohnehin eine Internetanbindung für einen DNS-Hub in der Regel Voraussetzung.

Die DNS-Hubs müssen gut gewartet und jederzeitiger Zugang des Betriebspersonals gewährleistet sein. Das Ausfallrisiko ist möglichst gering zu halten.

Alle DNS-Hubs kennen alle Zonen und halten diese und weitere Informationen für User jederzeit bereit. Die Hubs synchronisieren ihre Informationen permanent.

DNS-Hubs, die über Internetzugang verfügen, können ihre Informationen sowohl über das Funknetz als auch über das Internet anbieten.

Informationen und Daten sind auf allen Hubs unter den gleichen Adressen (z.B. URLs und Ordnerstrukturen) zu erhalten. Nur die IP-Adresse ist jeweils entsprechend unterschiedlich. Dazu später mehr.

Unter Berücksichtigung der Regionsstrukturen, der Linksituation im Packet-Netz, der Internetzugriffsmöglichkeiten, der Verfügbarkeit und Erfahrung der betreffenden Sysops sowie der Zugriffs- und Wartungsmöglichkeiten auf die Hardware der DNS-Hubs haben wir nach längeren Untersuchungen und Gesprächen mit interessierten OMs folgende DNS-Hubs vorgesehen:

Hub-NORD : 44.130.0.100 db0hht.ampr.org
Hub-SUED : 44.130.60.100 db0fhn.ampr.org
Hub-WEST : 44.130.146.101 db0res-svr.ampr.org
Hub-OST : 44.130.90.100 db0tud.ampr.org
Hub-MITTE: 44.130.14.100 db0smg.ampr.org

2.2.2 Einzugsgebiete und Vernetzung der Hubs

Jeder der DNS-Hubs ist für die in seiner Region angesiedelten Regionalzonen zuständig (zu ergänzen mit .de.ampr.org):

NORD :	hh, hhn, hhs, ros, hhm, wen, lg
SUED :	stgt, swb, brsg, rnk, enz, hrh, lake, mue, doi, ostbay, nbg, westmfra, ofr, ufra, bawue, ual, in
WEST :	owl, dssd, ac, ms, rmn, ka, nww, pfalz, myk, mosel, wat, bri, rr, si, me, baden
OST :	bln, pgntz, ohvl, oder, havel, dahme, neisse, eeosl, amk, lpz, hot, dd, wsx, hdf, osx
MITTE:	os, bs, goe, ks, ssa, sthur, ndh, erf, esa, shg

Diese Aufteilung bezieht sich auf das Anliefern der Zonen von den autoritativen, lokalen Nameservern zu den Hubs. Jeder Hub verfügt wie oben erwähnt selbstverständlich über alle Zonendateien von ganz DL, die er den an ihn angeschlossenen, lokalen Nameservern der Großregion zur Verfügung stellt.

Die DNS-Hubs sind nach Art eines DNS-Backbones möglichst redundant, meist über alternative Transportwege miteinander verbunden. Dies ist in der Regel ein Funkweg und/oder ein schneller Internet-Tunnel. So lassen sich die Lücken und Schwachstellen im Netz zwischen den Regionen sicher überbrücken. Über diese Backbonestruktur gelingt es, die in der ganzen Republik anfallenden Daten zwischen allen Regionen kanalisiert hin und her zu transportieren und einen automatischen Austausch zu ermöglichen.

2.2.3 Anbindung von Digis, Informationsfluss BottomUp/TopDown

Digis und Aktivitätszonen, die einen eigenen Nameserver betreiben, der für eine oder mehrere Regionen autoritativ ist, brauchen diese Zonendateien per Zonentransfer ihres laufenden Nameservers nur noch bei dem für sie zuständigen DNS-Hub abliefern. Dies wird durch entsprechende Einträge in der Konfigurationsdatei für den lokalen Nameserver sichergestellt. Sie brauchen sich nicht mehr um den Austausch und die weitere Verbreitung ihrer Zone in der ganzen Republik zu kümmern. Wir werden später noch zeigen, wie eine passende Konfiguration vom zuständigen Sysop besonders einfach eingerichtet werden kann und stellen hierfür passende

Scriptdateien zur Verfügung. Ein solcher Zonentransfer geschieht automatisch per Notify sofort nach einer Änderung oder nach Ablauf der Gültigkeitsdauer der verfügbaren Daten (TTL gesteuert).

Das Einsammeln der Daten für die DL-weite Verteilung und die Updates auf ucsd.edu geschieht in allen Regionen somit nach dem Bottom-Up Prinzip.
Hört der zuständige DNS-Hub von einem lokalen DNS seiner Region allerdings längere Zeit nichts, fragt er seinerzeit dort nach, ob es etwas Neues gibt. Datentransfer findet nur dann statt, wenn sich in einer Zonendatei wirklich etwas geändert hat.

Durch die feste Zuordnung der lokalen Nameserver einer Region auf einen darin erreichbaren DNS-Hub bleibt der Datenfluss auf die im allgemeinen sicher genug funktionierenden Interlink-strukturen der Region beschränkt. Mehrfachbelastungen der überregionalen Linkstrecken fallen weg.

Das Verteilen der Zonendateien von Zonen außerhalb der eigenen Region geschieht nach dem Top-Down Verfahren. Der hierzu erforderliche Traffic beschränkt sich ebenfalls auf die Interlinkstrukturen in der eigenen Region, da die lokalen Nameserver sich die ihnen fehlenden Zonendateien von dem für sie zuständigen Regions-Hub holen können und nicht mehr kreuz und quer durch die Republik connecten müssen. Auch dies geschieht, wie oben angedeutet, durch die Konfiguration des lokalen Nameservers automatisch.

Da fast alle DNS-Hubs über direkte Internetanbindung verfügen, ist es für jeden, an einen solchen Hub angebundenen lokalen Nameserver möglich, per Caching-Abfrage auch alle anderen, internationalen Abfragen auflösen zu können. Da dies mit Ausnahme von Grenzregionen relativ seltener geschieht, kann hierzu eine bei Erstanfragen etwas längere Wartezeit in Kauf genommen werden. Hier ist zu bedenken, dass das Auflösen beliebiger, aktueller IP-Adressen bisher für die meisten lokalen Digis nicht möglich war.

2.3 DL und der Rest der Welt

2.3.1 Sammeln und Prüfen aller DL-Daten

Das Bottom-Up Prinzip stellt sicher, dass alle in DL vorhandenen Zonendaten meist sehr schnell auf dem zuständigen Hub und dann auch auf den anderen Hubs verfügbar sind. Dies trifft für alle Netze zu, die mit einem Nameserver am Regionalzonenkonzept angeschlossen sind oder ihre Zone mangels eigenem Nameserver direkt auf dem zuständigen Hub hosten wollen.

Zu diesem Zweck werden von uns Zugriffsmöglichkeiten vorbereitet werden, die Regional-koordinatoren, die eine Zone verwalten wollen, aber keinen eigenen Nameserver zur Verfügung haben, auf verschiedene Art und Weise die Pflege ihrer Zonendaten ermöglichen (Emailrobot, WWW-Interface usw.). Es ist derzeit auch ein WWW-Interface in Entwicklung, dass es ermöglicht, eine einfache HOSTS-Datei zu pflegen.
Dies ist für Zonen interessant, die aus verschiedenen Gründen nicht am Regionalzonenkonzept teilnehmen können.

Die Teilnahme am Regionalzonenkonzept mit eigenem, lokalen DNS und die Pflege der Zone auf einem DNS-Hub schließen sich allerdings gegenseitig aus. Um die Konsistenz der Daten sicher zu stellen, kann man nicht beides haben.

2.3.2 automatisches Update auf ucsd.edu, Fehlersicherheit, Redundanz

Durch das neue DNS-Konzept wird weitgehend sichergestellt, dass nahezu alle Zonen-informationen automatisch auf den DNS-Hubs eintreffen. Bei einem der DNS-Hubs findet die Zusammenfassung und Überprüfung aller Daten statt.

Sind einzelne Zonendaten nicht in Ordnung oder aus anderen Gründen nicht bei ucsd.edu updatebar, werden sie ausgesondert und der zuständige Regionalkoordinator verständigt. Er kann dann auf seinem lokalen DNS Korrekturen vornehmen. Der Rücktransport erfolgt dann im Rahmen des Konzeptes wieder wie oben beschrieben im Bottom-Up Verfahren ohne dass der Sysop oder Regionalkoordinator sich weiter darum kümmern muss.

Sind die Daten in Ordnung, werden sie automatisch entsprechend aufbereitet und in regelmäßigen Zeitabständen an ucsd.edu übermittelt. Dort findet alle 24h ein Updatelauf statt, sodass neu eingelieferte Daten bei ucsd.edu spätestens nach einem Tag weltweit verfügbar sind.

In welchen Zeitabständen ein Update der DL-Daten bei ucsd.edu stattfinden soll, ist noch nicht endgültig geklärt. Sicher ist zumindest, dass eine Updatefrequenz von weniger als einem Tag relativ sinnlos wäre.

Neu an diesem Verfahren ist, dass auch der Updateprozeß mit ucsd.edu weitgehend automatisiert ablaufen wird und bei Ausfall eines Koordinators oder des dafür zuständigen Hubs ein anderer jederzeit diese Aufgabe übernehmen kann. Es bleibt also nichts mehr liegen.

2.3.3 Laufzeiten

Das weitgehend durchautomatisierte Verfahren stellt sicher, dass vom Eintrag einer Zuweisung durch einen Regionalkoordinator auf seinem DNS bis zum Erscheinen des Eintrages auf ucsd.edu keine endlos langen Wartezeiten mehr entstehen.

Durch geeignete Einstellung der Timeouts in den Zonendateien muss Rücksicht auf Eigenheiten wie Geschwindigkeit und Belastbarkeit unseres Funknetzes genommen werden.
Durch Verwendung moderner Bind-Versionen sind die Hubs in der Lage, von manchen Regional-koordinatoren möglicherweise ungünstig gewählte TTL-Einstellungen in den Zonendateien zu überschreiben.

Dynamische DNS-Updates mit schneller, weltweiter Verfügbarkeit und Lebensdauern von kleiner 5 Minuten nach dem Muster von DynDNS.Org sind im Amateurfunk nach unserer Einschätzung nicht notwendig. Nach dem derzeitigen Stand können wir sagen, dass im ungünstigsten Fall, wenn alle TTL-Timereinstellungen maximal greifen und alle Notifies verloren gehen würden, ein Zeitraum von maximal einer Woche vergehen kann, bis ein Neueintrag in einer Region bei ucsd.edu eingetragen ist. Dies gilt unter der Voraussetzung, dass das DNS-Konzept vollständig umgesetzt ist und alle Systeme (inkl.ucsd.edu) laufen. Wir halten dies für die Belange im Amateurfunk für vertretbar.

In 98 Prozent der Fälle wird das deutlich schneller gehen und ist auch davon abhängig, auf welcher Ebene eine Verzögerung eintreten sollte.

Lokal vor Ort ist eine Änderung oder ein Neueintrag in einem DNS praktisch sofort verfügbar. Ein neu eingetragener TCP/IP-User kann praktisch sofort arbeiten. Alle lokalen Anwendungen, die einen DNS-Eintrag erfordern, funktionieren ebenfalls sofort. Funktioniert der Notify vom lokalen DNS zum Hub, ist die aktualisierte Zonendatei innerhalb weniger Minuten am Hub verfügbar und gültig.

Weitere wenige Minuten später ist die Information auf allen Hubs abrufbar. Beispiel: Ein Zonenupdate nach erfolgtem Notify dauert von DB0RES zu DB0FHN oder einem anderen DNS-Hub erfahrungsgemäß keine 10 Sekunden. Danach steht die Information auch für das Updaten bei ucsd.edu bereit.

Etwas länger dauert das Rückverteilen der aktualisierten Zonendaten auf alle Regionalserver in ganz DL. Wenn zwischen Hub und Regionalserver kein Notifying für alle Fremdzonen stattfindet (davon ist aus Gründen der örtlichen Linkbelastung abzuraten), wird die Datei erst dann lokal geupdated, wenn der jeweilige lokale DNS für die Zone das Timeout erreicht und bei seinem Hub nachfragt, ob sich für die Zone XY etwas geändert hat. Je nach gewählter TTL sollte dies nach 1-2 Tagen auf allen Nameservern in ganz DL geschehen sein.

Damit alles optimal funktioniert, sind auf allen beteiligten Nameservern bestimmte technische Voraussetzungen zu erfüllen und Anpassungen an der Konfiguration der Nameserver vorzunehmen. Diese können nach unserer Einschätzung von der überwiegenden Mehrheit der in Betrieb befindlichen regionalen Nameserver eingehalten werden.

Weil gerade der Nameservice sehr empfindlich auf Fehler in der Konfiguration reagiert und zu netzweiten Störungen führen kann, werden von uns jedem interessierten Sysop geeignete Scripte und Konfigurationshilfen zur Verfügung gestellt, die auch einem technisch weniger erfahrenen Sysop ermöglichen, sein Nameserversystem umzustellen und alles Weitere automatisch aktualisieren zu lassen, vorausgesetzt, der Rest des Serversystems funktioniert soweit einwandfrei. Ist das System einmal richtig installiert und einige wenige Cronjobs aktiviert, hält es sich ohne weiteres Zutun quasi von selbst auf dem laufenden Stand. Dies ist eine große Arbeitserleichterung für jeden betroffenen Sysop.

Was hierbei zu tun ist, wird nun näher beschrieben.

3. TECHNIK

3.1. Aufsetzen und Betrieb von Nameservern

3.1.1 Welche DNS-Version ?

Aktuell ist der named "bind" in seiner Version 9. Allerdings haben wir Probleme mit bind9 gegenüber bind8 festgestellt: "Notifications" an die anderen sekundären Nameserver (Hubs, zweite NS, etc..) werden hier grundsätzlich per UDP gemacht. Dabei ist ein "timeout" für das Warten auf Antworten von wenigen Sekunden(!) fest einprogrammiert. Der Wert ist nicht konfigurierbar. Dies scheint ein Fehler zu sein.

Hinzu kommt, dass UDP-Pakete von einigen IP-Stacks / Routern als AX25 Mode-DG (UI-Frames) statt auf einer (bestehenden oder neu aufzubauenden) Mode-VC (I-Frames) Verbindung auf den Weg geschickt werden. Auch haben wir beobachtet, dass Bind9 versucht, alle im SOA Header als NS eingetragene Rechner, also auch als "Hidden Primary" konfigurierte, direkt zu erreichen. Er scheint sich also über die eigene Konfiguration der Zonen-Konfiguration (masters-Teil) hinwegzusetzen.

Bind9 bietet insbesondere auf den Hubs bessere Konfigurations-Möglichkeiten. Beispielsweise lassen sich einige Timeouts parametrisieren. Der partielle Zonetransfer (IXFR), das ist eine Art "diff", ist überarbeitet worden. Ein weiterer Vorteil ist, dass sich Bind9 administrativ über unpassende SOA Werte hinwegsetzen.

Bind4 kennt keinen IXFR. Dies führt zu Kompatibilitätsproblemen, wenn die anfragende Seite zunächst einen IXFR versucht. Die Konfiguration von Bind4 ist deutlich anders. Deshalb raten wir von der Benutzung dieser Uralt-Version ab.

3.1.2 Der Betrieb der DNS an den Hubs

3.1.2.1 Welche Zonen gibt es?

Maximal wären unter 44.130.0.0/16 maximal 255 Sub-Zonen in Form von <region>.de.ampr.org denkbar.

Derzeit sind 67 Zonen koordiniert:
ac amk baden bawue bln bri brsg bs dahme dd doi dssd eeosl enz erf esa
goe havel hdf hh hhm hhn hhs hot hrh in ka ks lake lg lpz mainz me mosel
ms mue myk nbg ndh neisse nww oder ofr ohvl os ostbay osx owl pfalz
pgntz rmn rnk ros rr rsk shg si ssa stgt sthur swb ual ufra wat wen
westmfra wsx

Aktuell sind 102 44.130.x.x/24 Netze vergeben, welche durch die entsprechenden Regional-Koordinatoren gepflegt werden. Damit nehmen relativ mehr Zonen am Subdomain-Projekt teil. Nicht berücksichtigt ist bei dieser Zählung, ob die Daten veraltet sind.

Die Netze und ihre Koordinatoren wurden ursprünglich in der Datei "koord.html" von do2ksm zusammengetragen. Diese Datenbestände haben wir aktualisiert. Thomas <dl3sbb> pflegt jetzt diese Liste.

Aus dieser Liste erzeugt haben wir eine Datei "zones-hub-de.txt". S.a. Anhang III. Sie ordnet den regionalen Zonen ihren Hubs zu und sie verweist auf die jeweiligen autoritativen Nameserver.

Damit lässt sich der Prozess automatisieren.

Jeder Nameserver, der nicht nur die eigenen Subzonen kennen möchte (z.B. um darüber Mail- oder Proxy-Routing zu realisieren) oder über Zonetransfer die aktuellen Zuweisungen erhalten möchte, muss auch beim hier vorgestellten Konzept die Regionen namentlich kennen, d.h. sie explizit konfigurieren, damit diese dann vom nahe gelegenen Hub geholt werden können.

Auf Grundlage der Daten in "zones-hub-de.txt" lassen sich script-gesteuert die Einträge für den DNS generieren. Diese Datei wird "gespiegelt" (also automatisiert kopiert) und ist so auf allen Hubs in ihrer aktuellen Version verfügbar. Damit werden auch insbesondere neue Einträge leicht und ohne großen administrativen Aufwand auf einem Regions-Server verfügbar.

Alternativ kann ein Regions-Server alle Anfragen für nicht-lokale Zonen "cachen" (also zwischenspeichern), indem er den Hub als "forwarder" konfiguriert. Damit profitiert die Region, bei minimalem DNS-Verkehrsaufkommen, über aktuelle IP-Adress-Zuweisungen in DL. Allerdings ginge bei dieser Konfiguration die Information über Regionsnamen verloren.

3.1.2.2 Bereitstellen von Scripten und Zonendaten

Die Liste der Regional-Koordinatoren und -Netze, die Datei "zones-hub-de.txt" für den DNS, Dokumentationen und Beispiel-Scripte, aktuelle Zonendaten, ampr.org von ucsd.edu, ein täglich erstelltes "hosts.txt" und zonefile für DL, uvm. wird auf den 5 Hubs zu finden sein und zum Download per http, ftp, rsync zur Verfügung stehen. Wie wir weiter unten sehen werden, ist damit der Betrieb eines Regions-DNS Servers auch ohne tief greifende Kenntnisse des DNS-Systems und mit minimalst nötigen Wartungsaufwand möglich.

3.1.2.3 einheitliche Ordnerstruktur auf allen Hubs

Dies ist noch ein in Entwicklung befindlicher Prozess.
Ein erster Entwurf sieht wie folgt aus:

```
$ find /srv/ampr-dns/
/srv/ampr-dns/
/srv/ampr-dns/lib
/srv/ampr-dns/lib/zones-hub-de.txt
/srv/ampr-dns/lib/koord-neu.html
/srv/ampr-dns/lib/koord.html
/srv/ampr-dns/doc
/srv/ampr-dns/scripts
/srv/ampr-dns/scripts/zone2conf.sh
/srv/ampr-dns/files
/srv/ampr-dns/files/de-44.ampr.org.rev
/srv/ampr-dns/files/de.ampr.org
/srv/ampr-dns/files/hosts_44_130.txt
/srv/ampr-dns/files/hosts.txt
/srv/ampr-dns/README
$
```

3.1.3.4 Zugriff und Download auf vielen Wegen

Z.B.: shell login auf Hub Ost db0tud:

```
$ cd /srv/ampr-dns/
$ cat README
$ bget de.ampr.org
```

Um die Sache noch etwas dynamischer zu machen, haben wir uns erlaubt, die folgenden Aliase zu setzen:

```
dl-mitte      IN     CNAME   db0smg
dl-nord IN     CNAME   db0hht
dl-ost  IN     CNAME   db0tud
dl-sued IN     CNAME   db0fhn
dl-west IN     CNAME   db0res-svr
```

Damit beeinträchtigt selbst der längerfristigem Ausfall oder Wechsel eines Hubs (z.B. wegen Totalausfall) die Scripte nicht.

URLs, um über TCP/IP basierte Dienste die Daten einzusehen:

```
rsync dl-ost.ampr.org::ampr-dns/
http://dl-ost.ampr.org/ampr-dns/
ftp://dl-ost.ampr.org/pub/ampr-dns/
```

3.1.3 Aufsetzen eines DNS an einem Digipeater

3.1.3.1 allgemeine Anforderungen

Vorausgesetzt seien

- ein Unix-Rechner
- konfigurierter IP-Stack
- root Rechte ;)
- ein installierter bind8 oder bind9 als DNS-Server

3.1.3.2 Grundkonfiguration

Die Bind-Konfigurations-Datei stehe unter "/etc/bind/named.conf" [von System zu System unterschiedlich]. In ihr befinden sich Konfigurations-Parameter wie

- standalone, forwarders, Access-Listen, etc..
- Timing-Parameter
- Logging
- Zonen (master, slave, Filename, Pfade dorthin)
- etc..

Im Anhang II die aktuelle "/etc/bind/named.conf" von Hub Sued, db0fhn.

Wenn in der Region eine eigene Zone verwaltet werden soll, werden die Daten in den entsprechenden Dateien der Vorwärts- und Rückwärts-Auflösungen für <region>.de.ampr.org bzw. xxx.130.44.in-addr.arpa gepflegt gespeichert.

Den Aufbau dieser Datei skizziert Anhang I.

3.1.3.3 automatisches Erzeugen der Konfiguration

Im Folgenden möchte ich ein erstes Script, "zones2conf.sh", vorstellen zur Erzeugung der Subzonen-Konfiguration für den bind.

I. Editieren und Anpassen

```
# --- CONFIGURE ME
# Am I Hub?
# NO?
#I_AM_HUB=0
I_AM_HUB=1

MY_HUB=sued
# IP of my DNS serer
MY_DNS_IP=44.130.60.100

# Hubs which are too far away to reach directly
HUBS_TOO_FAR="nord"


FILEPATH=/var/named/maps

HUB_NORD="44.130.0.100;   // db0hht (GrossRegion-NORD)"
HUB_SUED="44.130.60.100;  // db0fhn (GrossRegion-SUED)"
HUB_WEST="44.130.146.101; // db0res-svr (GrossRegion-WEST)"
HUB_OST="44.130.90.100;  // db0tud (GrossRegion-OST)"
HUB_MITTE="44.130.14.100;  // db0smg (GrossRegion-MITTE)"

[...]
```

II. Script starten:

```
# /etc/bind/bin/zone2conf.sh < /etc/bind/etc/zones-hub-de.txt > /etc/bind/zones-region-de-ampr-org.conf
```

In der damit erzeugten Datei "zones-region-de-ampr-org.conf" befinden sich dann Einträge in folgender Form:

```
zone "stgt.de.ampr.org" {
      type slave;
      file "/var/named/maps/stgt.de";
      masters {
            44.130.48.23;
            44.130.146.101; // db0res-svr (GrossRegion-WEST)
            44.130.90.100;  // db0tud (GrossRegion-OST)
            44.130.14.100;  // db0smg (GrossRegion-MITTE)
      };
      also-notify {
            44.130.146.101; // db0res-svr (GrossRegion-WEST)
            44.130.90.100;  // db0tud (GrossRegion-OST)
            44.130.14.100;  // db0smg (GrossRegion-MITTE)
      };
      allow-notify {
            44.130.48.23;
            44.130.0.100;   // db0hht (GrossRegion-NORD)
            44.130.146.101; // db0res-svr (GrossRegion-WEST)
            44.130.90.100;  // db0tud (GrossRegion-OST)
            44.130.14.100;  // db0smg (GrossRegion-MITTE)
      };
};
```

Dieses Verfahren erspart, wie man sieht, eine Menge Tipp-Arbeit und vermeidet Fehler (einen der vielen ";" vergisst man gerne..). Bei 138 Einträgen ein nicht zu verachtender Vorteil ;)

Die Datei "zones-hub-de.txt" wird auf einem der Hubs gepflegt und auf die anderen Hubs verteilt. Von "ihrem" nahe gelegenen Hub können ihrerseits die Regions-Server diese Datei (regelmäßig, auch automatisierbar) beziehen.

Das Script kann, wie man an den Einstellungen sieht, für einen Hub oder für einen Regions-Server vorkonfiguriert werden. Damit lässt sich der komplette Prozess der Konfiguration und Wartung (also das Aktuell halten der bekannten Zonen und Regions-NS) des DNS automatisieren, auf den Hubs wie auch auf Servern in den Regionen.

Bind9 erlaubt es, die Konfiguration in mehrere Dateien zu fächern. So lassen sich die mit obigem Script erzeugten und in einer separaten Datei abgelegten Zonen-Definitionen durch den folgenden Eintrag in der "named.conf" von den ggf. lokal nötigen Konfigurations-Parametern abspalten:

```
include "/etc/bind/zones-region-de-ampr-org.conf";
```

Ein Beispiel für die "named.conf": s. Anhang II.

3.1.3.4 automatische Aktualisierung der Zonendateien

/etc/crontab:
```
 15      03      * * * root /usr/local/etc/update-ampr-dns.sh
```

Hier ein Beispiel-Shell-Script "update-ampr-dns.sh":

```
 #!/bin/sh

 old_sum=$(md5sum /etc/named/etc/zones-hub-de.txt | awk '{print $1}')
 # update zone definitions
 /usr/bin/rsync -qaz --timeout=600 --partial rsync://dl-ost.ampr.org/ampr-dns/lib/zones-hub-de.txt
/etc/named/etc/
 # host unreachable?
 if [ $? -gt 0 ]; then exit 1; fi
 new_sum=$(md5sum /etc/named/etc/zones-hub-de.txt | awk '{print $1}')
 # no change? - done
 if [ "$old_sum" != "$new_sum" ]
 then

   # generate new zone definitions
   /etc/bind/bin/zone2conf.sh < /etc/bind/etc/zones-hub-de.txt > /etc/bind/zones-region-de-ampr-
org.conf
   # make named learn the changes
   /etc/init.d/bind reload
 fi
 # done
```

Danach
```
 $ chmod 755 /usr/local/etc/update-ampr-dns.sh
```
nicht vergessen.

3.1.3.5 Verwaltung der eigenen Region

Im Beispiel von Hub Sued ist db0fhn "master" für die Region nbg.de.ampr.org und die PTR (Rückwärtsauflösungen) für 44.130.60.x (60.130.44.in-addr.arpa).

Damit das in 3.1.3.2 vorgestellte Script, welches die Regionen und Dateien definiert, nicht angepasst werden muss, lässt sich für die eigene Region unter unix elegant mit "symbolischen Links" arbeiten:

/var/named/maps:
```
 lrwxrwxrwx   1 root    root         23 Feb 22 23:13 nbg-60.de.rev -> /etc/bind/nbg-60.de.rev
 lrwxrwxrwx   1 root    root         16 Feb 22 23:12 nbg.de -> /etc/bind/nbg.de
```

cave: Dies wird jedoch nicht funktionieren, wenn der named in einer "chroot-Umgebung" (wie er bei manchen linux-Distributionen vorkonfiguriert ist) läuft.

Die eigentlichen Dateien in /etc/bind/nbg*:
```
 -rw-rw-r--   1 dl9nec   dnsadm       5436 Dec  2 15:54 nbg-60.de.rev
 -rw-rw-r--   1 dl9nec   dnsadm      12135 Dec  2 15:54 nbg.de
```

In unserem Beispiel ist der Nutzer dl9nec (Regional-Koordinator nbg) in der Unix-Gruppe dnsadm. Er und andere Mitglieder dieser Gruppe können diese Dateien dann ändern.

"rndc" ist ein Werkzeug welches mit dem laufenden named kommuniziert.
Dieses Programm liegt der named Installation bei.

Ein Schlüssel regelt die Zugangskontrolle. Er ist in der Datei "/etc/rndc.key" bzw. "/etc/named/rndc.key" (variiert mal wieder) gespeichert. Versieht man die Datei mit 640 Rechten für root.dnsadm, dann kann der Regional-Koordinator seine Änderungen dem Nameserver mitteilen, ohne Administrations-Rechte erlangen und den named neu starten zu müssen:

```
$ rndc reload nbg.de.ampr.org
$ rndc reload 60.130.44.in-addr.arpa
```

Anhang I dokumentiert den Aufbau eines Zonefiles.

3.1.4 Die weltweite Bereitstellung der DL-Daten auf ucsd.edu

Die Daten kommen aus den Regionen zu ihren assoziierten Hubs. Entweder per "notify" angestoßen, oder über den regulärem AXFR.

Wir haben auch erwähnt, dass ein eigener DNS-Server nicht zwingend nötig ist. Er ist eine Erleichterung, mag aber in einer Region mit nur zehn Teilnehmern wie mit Kanonen auf Spatzen geschossen wirken. Deshalb bieten wir auch die Möglichkeit, die Zonen-Daten direkt auf dem Hub zu aktualisieren. Auch wird es einen Email-Bot und ein Web-Interface geben. Diese Dienste werden ebenfalls über das Internet zugänglich sein. Die Daten werden dann auf dem Hub intern ebenfalls in einem Zonefile verwaltet.
Allerdings schließen sich die Verfahren "eigenes Zonefile auf einem Regions-Server" und "zentrale Verwaltung" gegenseitig aus. D.h. Email-Bot und Web-Interface können nur von Regionen genutzt werden,

- deren Zonefile auf einem der Hubs liegt.
- die nicht am DNS-Projekt teilnehmen.

Die Named / des Zonetransfer-Variante ist dennoch die von uns präferierte Methode, weil sie dem Regional-Koordinator vollständige Kontrolle über seine Daten und den Verteilungsprozess gibt.

Die DNS-Daten werden zwischen den Hubs mittels Zonetransfer und aktivem "Notify" abgeglichen. Somit verfügen alle fünf Hubs über die selben Datenbestände.

Einer der Hubs ist so konfiguriert, dass er regelmäßig die Soll-Datenstände (das sind die Zonefile, die über AXFR den Hub erreichten) mit den Ist-Daten (DL-Einträge auf ucsd.edu) vergleicht. Treten keine Konflikte auf (s.a. Kapitel 3.1.4.2 und 4.3) und lassen sich die Daten in Form von [irgendwas.]<call>.<region>.de.ampr.org auf das flachere [irgendwas.]<call>.ampr.org abbilden, dann steht deren weltweiter Veröffentlichung nichts mehr im Wege.

Im Umkehrschluss ziehen sich die Hubs regelmäßig die Daten für die komplette Zone ampr.org / 44.0.0.0/8. Dabei wird die Datei mit den Vorwärtsauflösungen ("ampr.org"), bevor sie in den named geladen wird, über ein Script angepasst:
existiert ein Eintrag in der ampr.org-Datei und ein korrespondierender in der Datei einer Region, dann wird der in der ampr.org-Datei der "IN A" Eintrag ersetzt durch "IN CNAME <call>.<region>".

Beispiel:

```
db0res-svr.ampr.org.        432000  IN   CNAME  db0res-svr.rr.de.ampr.org.
db0res-svr.rr.de.ampr.org.  864000  IN   A      44.130.146.101
```

Diese Information kann nützlich sein für

- domain-basiertes Mail-Routing.
- effizientes Weiterleiten von Anfragen in einem http-Proxy-Verbund.
- beim Generieren von IP-Routing Einträgen.

Die an die hiesigen Bedingungen angepasste ampr.org kann ebenfalls per Zonetransfer aus den Regionen von den Hubs bezogen werden.

3.1.4.1 redundantes, automatisiertes Update

Da jeder der 5 Hubs über das selbe Datenmaterial verfügt, kann bei Ausfall jenes Hubs welcher die Updates für ucsd.edu generiert, diese Aufgabe von einem Hub übernommen werden.

Ein Script welches die Befehle für den Aktualisierungs-Auftrag auf ucsd.edu generiert existiert bereits. Bevor es jedoch autonom laufen kann, müssen noch einige Randbedingungen abgefangen werden:
beispielsweise hat die Zone hot.de.ampr.org auf Grund eines Konfigurationsfehlers derzeit nur einen SOA Header und keinerlei Daten. So würden alle gültigen Zuweisungen gelöscht.

3.1.4.2 Problematik der Umsetzung in die ampr.org Zone

Die wichtigste Vorbedingung ist: die Einträge auf ucsd.edu sollten der Form
[irgendwas.][irgendwas-]<call>[-irgendwas].ampr.org entsprechen.

dhcp1.beispielregion.de.ampr.org
würde umgewandelt zu
dhcp1.ampr.org
Dieser Eintrag kann also nicht übernommen werden.

Doppel-Einträge:

I) Gleicher Name (z.B. nach Umzug in eine andere Region)

```
da0aaa.region254.ampr.org. IN    A    44.130.254.1
da0aaa.region255.ampr.org. IN    A    44.130.255.1
        würde zu
da0aaa.ampr.org            IN    A    44.130.254.1
da0aaa.ampr.org            IN    A    44.130.255.1
```

Das ist zwar ein, aus DNS Sicht, gültiger Eintrag. Jedoch wird es schwierig, diesen Host zu erreichen. DNS wird beim Versuch, da0aaa.ampr.org aufzulösen, mal die eine, und mal die andere IP-Adresse liefern.

II) Gleiche IP-Adresse

```
da1aaa.region255.ampr.org. IN    A    44.130.255.1
dl1bbb.region255.ampr.org. IN    A    44.130.255.1
        würde bei Rückwärtsauflösung zu
1.255.130.44.in-addr.arpa  IN    PTR  da1aaa.region255.ampr.org.
1.255.130.44.in-addr.arpa  IN    PTR  dl1bbb.region255.ampr.org.
```

Die Eindeutigkeit des Rufzeichens ginge dabei verloren.

S.a. Kapitel 4.3: Beliebte Fehler im Zonefile.

4. PRAXIS

4.1 Stand der Realisierung auf Hubebene

Hub Sued und Hub West werden schon unter den neuen Konfigurationen betrieben; auf Hub Sued werden sie getestet.

Hub Nord hat den Testbetrieb aufgenommen. Es gibt genau einen Weg, (der kurzzeitig funktionierte) über db0mar, durch das Netrom Netz, nach HH. Wir hoffen, diese Strecke in einen stabilen Zustand bringen zu können.

Hub Ost ist teils angepasst, läuft in größtenteils aber noch in alter Konfiguration weiter: damit wir weiterhin Daten aus Regionen erhalten, die noch nicht für ihren zugeordneten Hub konfiguriert sind.

4.2 Stand der Realisierung auf Regionalebene

Auf Regionalebene läuft das Projekt in der Region

- West: zwischen DB0RES (Hub West) und DB0GOS (als Regionaldigi).
  Demnächst werden DB0EEO und evtl. DB0DSP hinzukommen.
- Ost: zwischen DB0TUD (Hub Ost) und DB0BLN (als Regionaldigi).

4.3 Beliebte Fehler im Zonefile

Viel Zeit hat es gekostet, die Zonen des -jahrelang nicht mehr gepflegten- DL-DNS-Projektes wieder auf Vordermann zu bringen:

Zonen waren veraltet ("expired") weil

- schlicht das IP-Routing nicht funktionierte, Antworten auf dem Rückweg versackten oder auch nur der AX25-Arp zum Ziel nicht bekannt war.
- der Nameserver nicht gestartet war.
- das Zonefile auf Grund eines Fehlers nicht geladen wurde.
- der Rechner irgendwann neu aufgesetzt wurde.
- in der Region seit mehr als zehn Jahren nichts mehr am DNS gemacht wurde und dieser in Vergessenheit geriet (z.B. weil der Koordinator wegzog oder das Hobby aufgab und der neue (sofern überhaupt ein neuer ernannt wurde) vom DNS Projekt nichts wusste oder ihm niemand half es zu bedienen). So wurden die Daten auf anderem Wege aktualisiert (oder warten noch heute auf verstaubten Zetteln in irgendwelchen Schubladen auf ihre archäologische Entdeckung ;)
- der Digi längst qrt gemacht hat.

Kreisende "Refresh's" von eigentlich expire'ten Zonen (weil "jeder von jedem" Zonen per AXFR wieder belebte) stellten ein zusätzliches Problem dar.

Einige der anderen Probleme werden sich durch das Hub Konzept deutlich reduzieren.

Da oftmals die letzten Veröffentlichungen der "Hosts-Liste" im BBS schon Jahre zurücklagen, standen wir bei verwaisten Regionen manches Mal vor der Frage, was aktueller war: die Einträge auf ucsd.edu (dort gibt es keine Zeitstempel) oder die Serien-Nummer des SOA Headers einer Region.

Deshalb halten wir es für hilfreich, die Serien-Nummer in Form eines Datums zu codieren:
Beispiele:

- Unix-Zeit:
  $ perl -e '{printf("%lu\n", time());}'
  1079986731
  [Trick: Welche Zeit war das noch gleich?
  perl -e '{use Time::localtime; printf("%s\n", ctime(1079986731));}']
- Händisch:
  2004032200
  JahrMMTTxx [MM=Monat, TT=Tag, xx= beliebige zweistellige Zahl]
  cave: schreibt man z.B. mal (am 22.3.2004 12 mal geändert)
  2004032212
  und am nächsten Tag
  200403231
  Dann ist diese Zahl (Serial) kleiner als die zuvor. Die Folge ist, dass der Zonetransfer künftig scheitern wird. Die anderen Nameserver werden die Zone nicht laden. Der "Refresh" scheitert, und in nach Erreichen des "Expire" Wertes (im SOA Header des bisher gültigen Zonefiles) werden die anderen Nameserver keine Antwort mehr geben. Sie werden jedoch auch dann die kleinere Serial nicht akzeptieren!
- Wechsel von 2004032200 nach Unix-Zeit-Format (ähnlich des Problems oben):
  Ein RFC beschreibt, wie es geht. Problem: es klappt nur nicht.
  - Händische Intervention auf allen Nameservern notwendig.
    - Kaum praktikabel. -> Besser so lassen wie es ist.

Weitere Beispiele: Flüchtigkeitsfehler in Zonefiles. Zumeist wurde der Punkt am Ende der Zeile vergessen.

goe.rev:19			PTR	wampes.dl1abc.goe.de.ampr.org
goe.rev:78			PTR	do9ose.goe.de.mapr.org.
goe.rev:82			PTR	dl8oai.goe.de.mapr.org.
goe.rev:83			PTR	dl1odr.goe.de.mapr.org.
rmn24.rev:226			PTR	db0fhd.dk0bp.rmn.de.a.mpr.org.
os.rev:57	5184000	IN	PTR	dh1bm.
os.rev:99	5184000	IN	PTR	dyn4.db0sm.8.130.44.in-addr.arpa.
baden.rev:61	604800	IN	PTR	dh6iaz.baden.de.ampr.org.50.130.44.in-addr.arpa.
rmn.zone:	86400	IN	MX	10 dl5zr.rmn.de.ampr.org.rmn.de.ampr.org.
rmn.zone:	86400	IN	MX	20 db0ais.rmn.de.ampr.org.rmn.de.ampr.org.
wat.rev:148	86400	IN	SOA	wat.de.ampr.org.148.130.44.in-addr.arpa.

Eine weitere Inkonsistenz:
der PTR zeigt direkt auf ampr.org:

```
$ host dl3dbt
dl3dbt.ampr.org is an alias for dl3dbt.si.de.ampr.org.
dl3dbt.si.de.ampr.org has address 44.130.35.1
$ host 44.130.35.1
1.35.130.44.in-addr.arpa domain name pointer dl3dbt.ampr.org.
```

während sonst das Rückwärtsauflösen <region>.de.ampr.org anzeigt:

```
$ host db0bln.ampr.org
db0bln.ampr.org is an alias for db0bln.bln.de.ampr.org.
db0bln.bln.de.ampr.org has address 44.130.36.200
$ host 44.130.36.200
200.36.130.44.in-addr.arpa domain name pointer db0bln.bln.de.ampr.org.
```

Anhang

I. Aufbau eines Zonefiles

```
$TTL 86400      ; 1 day
bln.de.ampr.org         IN SOA  bln.de.ampr.org. dnsadmin.bln.de.ampr.org. (
                        1073237792 ; serial
                        864000     ; refresh (1 week 3 days)
                        86400      ; retry (1 day)
                        6048000    ; expire (10 weeks)
                        86400      ; minimum (1 day)
                        )
$TTL 864000     ; 1 week 3 days
                NS      db0bln.bln.de.ampr.org.
                NS      db0tud.ampr.org.
                TXT     "Region Berlin"
$ORIGIN bln.de.ampr.org.
blntcp          A       44.130.36.0
                TXT     "VFDB Berlin-Brandenburg"
[..]
$ORIGIN db0bln.bln.de.ampr.org.
dns             CNAME   db0bln.bln.de.ampr.org.
```

Die $TTL bestimmt die Lebenszeit des SOA Headers. Nach deren Ablauf muss der Header neu geholt werden. Damit werden Änderungen in Daten werden Serial, Expire, etc.. schnell bekannt, auch vor Erreichen des Refresh-Wertes. Der $TTL Wert vor Beginn des SOA Headers ist seit bind8 Pflicht.
$TTL kann im Zonefile mehrfach vorkommen. -> Dynamische Anpassung der Lifetime mit Werten kleiner als der maximalen, durch die "Refresh"-Variable des SOA Headers angekündigten.

Serial: eindeutige Seriennummer, stets nur aufsteigend. Zahl 0<x<2^31.
Refresh: Nach Ablauf dieser Zeit muss die Serial von einem Secondary DNS erneut geprüft werden.
Retry: Nach Ablauf dieser Zeit wird bei misslungenem Refresh dieser erneut versucht.

Expire: Nach Ablauf dieser Zeit wird bei anhaltend misslungenem Refresh die Zone ungültig. D.h. der Nameserver wird seinerseits keine Antworten mehr für diese Zone liefern (genauer: non-auhoritative, d.h. er kennt sie, darf aber nicht mehr genaueres dazu sagen).
Minimum: minimum negative cache TTL.
Jeder DNS Server der eine eingehende Anfrage delegiert, sei er ein "Secondary NS" für die angefragte Zone, oder ein als "forwarder" konfigurierter, speichert Antworten die er von seinem "Master" erhält. Diese Zeit bestimmt $TTL. Gibt es keinen Eintrag, z.B. für n0call.bln.de.ampr.org, dann führt eine Anfrage für diese Adresse zum Status NXDOMAIN ("gibt es nicht"). Eine "negative" Antwort wie diese kann auch zwischengespeichert werden. Dieser Ansatz vermeidet
unnötigen Traffic. Die Lebenszeit dieser Antwort jedoch bestimmt nicht $TTL (welche für gültige Anfragen / Antworten gilt), sondern der "minimum" Wert des SOA Headers.

Zu:
<TAB>NS<TAB>db0bln.bln.de.ampr.org.
<TAB>NS<TAB>db0tud.ampr.org.

Von diesen Nameservern sind autoritative Antworten für diese Zone zu erwarten. Man gibt hier keine rohe IP-Adresse an, sondern FQDNs.
Dass hier db0tud (Hub Ost) konfiguriert ist hat folgende Vorteile:

- fällt db0bln komplett aus, dann kann die Zone auf db0tud weiter gewartet werden, da jeder NS gelernt hat dass auch db0tud stets gültige Antworten liefern wird. db0tud muss in diesem Fall lediglich von "slave" auf "master" für diese Zone umkonfiguriert werden.
- Eine Änderung auf dem Master db0bln führt auch ohne den "also-notify"-Eintrag in der named.conf für diese Zone automatisch zu einem Notify an unseren Hub Ost.

Für die Notation ohne Subdomain habe ich mich entschieden, damit selbst bei nicht mehr funktionierendem Subdomain-Konzept die IP-Adresse auf Grundlage der Datenbestände auf ucsd.edu stets aufgelöst werden kann. Darüber lässt sich diskutieren ;)

$ORIGIN beschreibt den Beginn der Daten unter der Domain bln.de.ampr.org.
Es folgen die Einträge (A, CNAME, MX, TXT, HINFO, etc..).

PTR's befinden sich in einer anderen Datei. Ähnlicher Header. Notation:
$ORIGIN 36.130.44.in-addr.arpa.
0 PTR blntcp.bln.de.ampr.org.

Man beachte die Punkte am Ende der "Namen" (im SOA Header, bei CNAME, MX oder PTR Daten). Ohne diesen Punkt würde bei Anfragen bzw. bei Zonetransfers die Endung der in der named.conf angegebenen "zone"-Konfiguration angehängt. Daraus resultieren die in 4.3 aufgeführten Fehler.

II. "named.conf" am Beispiel von Hub Sued

```
options {
	directory "/var/cache/bind";
	listen-on { 127.0.0.1; 44.130.60.100; };
	auth-nxdomain no;
	allow-query { any; };
	allow-transfer { any; };
	allow-update-forwarding { any; };
	provide-ixfr yes;
	lame-ttl 1800;
	max-transfer-time-in 28800;
	max-transfer-time-out 28800;
	max-transfer-idle-out 5400;
	max-transfer-idle-in 5400;
	cleaning-interval 4320;
	heartbeat-interval 1440;
	max-ncache-ttl 604800;
	transfers-in 10;
	transfers-out 10;
	transfers-per-ns 1;
	use-ixfr yes;
	request-ixfr yes;
	// overwrite SOA definitions
```

```
        min-refresh-time 86400;         // 1 day
        max-refresh-time 6048000;       // 1 week 3 days
        min-retry-time 3600;            // 1 hour
        max-retry-time 86400;           // 1 day
};
logging {
        channel namedlog {
                file "/var/log/named_log";
                print-time      yes;
        };
        channel xferlog {
                file "/var/log/named_xfer";
                severity info;
                print-time      yes;
        };
};
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};
zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
        type master;
};
include "/etc/bind/zones-region-de-ampr-org.conf";
```

III. "zones-hub-de.txt"

Rein informativ. Beim erstellen habe ich mich selbst oft genug vertippt.
Also bitte nicht abschreiben ;)
Notiert habe ich es der Zuordnung der Regionen zu den Hubs wegen. Und zur Verifikation oder Information, welches der Primary NS ist.

hub	nord	44.130.0.100		
hub	sued	44.130.60.100		
hub	west	44.130.146.101		
hub	ost	44.130.90.100		
hub	mitte	44.130.14.100		
sued	stgt	44.130.48.23	44.130.48.0	
sued	swb	44.130.49.8	44.130.49.0	
sued	brsg	44.130.51.150	44.130.51.0	
sued	rnk	44.130.41.1	44.130.52.0	
sued	enz	44.130.63.100	44.130.53.0	
sued	hrh	44.130.55.50	44.130.54.0	
sued	lake	44.130.55.50	44.130.55.0	
sued	mue	44.130.59.250	44.130.56.0	44.130.67.0
sued	doi	44.130.57.201	44.130.57.0	
sued	ostbay	44.130.59.250	44.130.59.0	
sued	nbg	44.130.60.100	44.130.60.0	
sued	westmfra	44.130.63.100	44.130.61.0	
sued	ofr	44.130.63.100	44.130.62.0	
sued	ufra	44.130.63.100	44.130.63.0	
sued	bawue	44.130.48.23	44.130.176.0	
sued	ual	44.130.57.201	44.130.184.0	
sued	in	44.130.186.100	44.130.186.0	
nord	hh	44.130.0.100	44.130.0.0	
nord	hhn	44.130.0.100	44.130.1.0	
nord	hhs	44.130.0.100	44.130.2.0	
nord	ros	44.130.0.100	44.130.64.0	
nord	hhm	44.130.0.100	44.130.128.0	
nord	wen	44.130.0.100	44.130.150.0	
nord	lg	44.130.130.130	44.130.130.0	
mitte	os	44.130.8.100	44.130.8.0	
mitte	bs	44.130.9.40	44.130.9.0	
mitte	goe	44.130.14.100	44.130.14.0	
mitte	ks	44.130.27.81	44.130.27.0	
mitte	ssa	44.130.81.60	44.130.81.0	
mitte	sthur	44.130.99.11	44.130.96.0	
mitte	ndh	44.130.99.11	44.130.98.0	
mitte	erf	44.130.99.11	44.130.99.0	
mitte	esa	44.130.99.11	44.130.100.0	
mitte	shg	44.130.129.3	44.130.129.0	
west	owl	44.130.144.1	44.130.16.0	44.130.144.0
west	rr	44.130.146.101	44.130.18.0	44.130.146.0
west	dssd	44.130.19.105	44.130.19.0	
west	ac	44.130.20.50	44.130.20.0	
west	rsk	44.130.146.101	44.130.21.0	
west	ms	44.130.22.130	44.130.22.0	
west	rmn	44.130.25.80	44.130.24.0	44.130.25.0

west	ka	44.130.25.80	44.130.29.0
west	me	44.130.146.201	44.130.32.0
west	nww	44.130.34.1	44.130.34.0
west	si	44.130.146.101	44.130.35.0
west	mainz	44.130.146.101	44.130.40.0
west	pfalz	44.130.41.1:44.130.41.64	44.130.41.0
west	myk	44.130.42.3	44.130.42.0
west	mosel	44.130.44.200	44.130.44.0
west	baden	44.130.146.101	44.130.50.0
west	wat	44.130.148.200	44.130.148.0
west	bri	44.130.149.1	44.130.149.0
ost	bln	44.130.36.200:44.130.90.100	44.130.36.0
ost	pgntz	44.130.90.100	44.130.72.0
ost	ohvl	44.130.90.100	44.130.73.0
ost	oder	44.130.90.100	44.130.74.0
ost	havel	44.130.75.100	44.130.75.0
ost	dahme	44.130.90.100	44.130.76.0
ost	neisse	44.130.90.100	44.130.77.0
ost	eeosl	44.130.90.100	44.130.78.0
ost	amk	44.130.84.100	44.130.84.0
ost	lpz	44.130.88.100	44.130.88.0
ost	hot	44.130.89.101	44.130.89.0
ost	dd	44.130.90.100	44.130.90.0
ost	wsx	44.130.91.101	44.130.91.0
ost	hdf	44.130.97.8	44.130.97.0
ost	osx	44.130.90.100	44.130.151.0