Seminarausarbeitung „Routing Design in Operational Networks: A Look from the Inside“

Ralf Stange
(majere@cs.tu-berlin.de)

Betreuer
Amir Mehmood

Seminar „Internet Routing“ ,
Technische Universität Berlin

WS 2007/2008 (Version vom 17. Januar 2008)

Zusammenfassung

Das Routingdesign von großen produktiven Netzwerken wurde bisher nur im geringen Umfang systematisch Untersucht. Wie werden in realen Netzen Routingprotokolle eingesetzt und existiert die Trennung in typische Enterprise- und Backbonearchitekturen nur in „Best Practice“ Empfehlungen oder auch in der Realität von großen Netzen?

Um solche Fragen zu Beantworten benötigt man einfache Methoden um aus realen Netzwerken die notwendigen Informationen zu extrahieren. In ihrer Arbeit „Routing Design in Operational Networks: A Look from the Inside“ [1] beschreiben die Autoren Maltz, Xie, Zhan, Zhang, Hjálmtýsson und Greenberg ein selbst entwickeltes Verfahren zur methodischen Analyse und Auswertung von Netzwerk-Routingdesigns durch Reverse Engineering von Routerkonfigurationen. Diese Ausarbeitung beschreibt die grundlegenden Ideen und Methoden dieses Verfahrens und liefert Fallbeispiele aus den durchgeführten Auswertungen.

1 Einleitung

Was steht hinter dem Begriff *Routingdesign*? Ein Netzwerk besteht aus Routern, ihren Verbindungen und den Routinginformationen die anhand umfangreicher Regelwerke und Protokolle die Netze miteinander verbinden. Hinzu kommen externe Anbindungen, verschiedene organisatorische Einheiten müssen abgebildet werden und das Netzwerk wächst permanent. Das ursprüngliche Ziel – eine simple Erreichbarkeit sicherzustellen – wird ergänzt durch zahlreiche weitere Anforderungen, wie z.B. Stabilität, Ausfallsicherheit und der Notwendigkeit Organisationseinheiten auch auf Netzwerkebene abzubilden. Um diese Ziele zu erreichen müssen sie beim Design des Netzwerkes berücksichtigt werden. Manchmal geschieht dies in Form von sauberer Planung, manchmal nur als Reaktion auf das Wachstum des Netzwerkes.

Bei produktiven Netzwerken stellt sich damit die Frage, *wie* sehen sie Heute aus? Entsprechen Sie noch dem ursprünglichen Designentwurf? Oder *warum* wurden bestimmte Design-Entscheidungen überhaupt getroffen? Hätte man bestimmte Konfigurationen besser gestalten können, bzw. kann man mit geringem Aufwand am bestehenden Netz Optimierungen durchführen?

Um diese Fragen beantworten zu können, benötigen wir die Möglichkeit vorhandene Netzwerke auf ihr Routingdesign hin zu untersuchen. Die Autoren stellen dazu ein Verfahren vor, welches genau jene nachträgliche Analyse von Netzen ermöglicht. Die wichtigsten Kernpunkte des Verfahrens sind:

Reverse Engineering Über Reverse Engineering kann sichergestellt werden, dass aktuelle Informationen für die Auswertung zur Verfügung stehen.
In großen Netzwerken stehen nur sehr selten aktuelle und vollständige Dokumentationen zur Verfügung und selbst dann wären sie auf Grund der nicht standardisierten Form für eine automatisierte Auswertung nicht geeignet.

White-Box Ansatz Es werden die Konfigurationen sämtlicher Router eines untersuchten Netzwerkes gesammelt und anschließend ausgewertet.
Vorteile: Die Untersuchungen können offline erfolgen, die Informationssammlung gestaltet sich leicht und durch den Zugriff auf diese internen Daten (White-Box Ansatz) stehen deutlich mehr Informationen zur Verfügung, als durch einen Black-Box Ansatz verfügbar wären (z.B. Netzwerkscans, DNS, etc.).

Anonymisierung Konfigurationsfiles werden vor ihrer Verwendung anonymisiert.
Nur wenn sichergestellt ist, dass bei der Analyse der Netzwerke keine Firmeninternas herausgegeben werden müssen, werden Netzwerkeigner bereit sein die Konfigurationen der Router zur Verfügung zu stellen.

Automatisierung Es soll möglich sein, eine große Anzahl von Netzwerken automatisiert auszuwerten.
Manuelle Bearbeitung ist selbst bei einem einzelnen Netzwerk mit mehreren hundert Routern und tausenden von Verbindungen untereinander nicht durchführbar.

Für diese Arbeit standen den Autoren schließlich über 20.000 Routerkonfigurationen von Kunden eines großen lokalen Providers zur Verfügung. Aus diesen Daten wurden 31 Netze mit über 8.000 Routern zur näheren Untersuchung der Routingdesigns ausgewählt.

2 Grundlagen

In diesem Kapitel werden die verwendeten Begriffe definiert und die Algorithmen beschrieben mit denen aus den Routerkonfigurationen die strukturellen Informationen extrahiert werden. Für die Konfigurationsbeispiele verwenden wir die Sprache IOS von Cisco [2].

Ein grundsätzliches Verständnis für Routingprotokolle, allgemeines Routingdesign und Netzwerk-Terminologien wird vorausgesetzt [3].

Die wichtigsten Begriffe für das Verständnis dieses Textes fasse ich hier kurz zusammen: Routingprotokolle die innerhalb eines Netzwerkes verwendet werden nennen sich Interior Gateway Protocolls (IGP). Darunter fallen z.B. die Protokolle OSPF, RIP und (E)IGRP. Zwischen getrennten Netzwerken werden die Exterior Gateway Protokolle (EGP) verwendet. Das einzige aktuell eingesetzte EGP ist das Border Gateway Protokoll (BGP). Insbesondere im Zusammenhang mit BGP werden diese einzelnen Netzwerke auch Autonome Systeme (AS) genannt. Verwendet man das BGP Protokoll innerhalb eines Autonomen Systemes, wird zur Unterscheidung von IBGP (internal BGP) und EBGP (external BGP) gesprochen.

Detailkenntnisse zu spezifischen Routingprotokollen wie OSPF oder BGP werden nicht benötigt.

2.1 Link-Level Topologie

In Routerkonfigurationen sind im Allgemeinen für jedes Interface eines Routers eine IP-Adresse und die Subnetzmaske angegeben.

```
interface Ethernet0
   ip address 66.251.75.144 255.255.255.128
!
```

Anhand dieser Daten und der folgenden Regeln können wir bestimmen ob ein Interface zur Kommunikation mit internen oder externen Netzen verwendet wird:

Internes Interface: Es existiert mindestens ein weiteres Interface innerhalb des untersuchten Netzwerkes mit IPs aus dem gleichen Subnetz.

Externes Interface: Es existiert kein weiteres Interface mit IPs aus dem gleichen Subnetz.

2.2 Routing Topologie

Neben der statischen IP-Adresskonfiguration enthalten die Routerkonfigurationen noch Konfigurationsangaben zu den Routingprotokollen. Jeder Router kann mehrere unterschiedliche Routingprotokolle gleichzeitig verwenden, auch können mehrere Instanzen des gleichen Protokolls auf einem Router laufen. Jeder dieser *Routingprozesse* besitzt eine eindeutige Prozess-ID (z.B. mit dem Befehl `router ospf 64`) und ist an mindestens ein Interface (Befehl `network` oder `neighbor`) gebunden.

Zwei Routingprozesse auf getrennten Routern gelten als adjazent, wenn sie direkt Routinginformationen austauschen. Dieses ist der Fall, falls eine der folgenden Bedingungen zutrifft:

BGP Prozesse sind adjazent, wenn sie wechselseitig zum direkten Austausch von Informationen konfiguriert sind (Befehl `neighbor` *`IP`* `remote-as` *`AS`*) und sie sich per TCP/IP erreichen können.

Andere Routingprozesse sind adjazent, wenn ihre beiden Router ein direkt verbundenes gemeinsames Netz besitzen, an das Interface dieser direkten Verbindung gebunden sind (`network` *`IP SUBNET`*) und das gleiche Protokoll verwenden (OSPF, IS-IS, RIP, EIGRP).

Wir definieren eine *Route* als ein IP-Subnetz (z.B. 10.0.0.0/8) zusammen mit einigen zusätzlichen Attributen (Gewicht, AS-Pfad, etc.). Diese Routen sind dem Router entweder direkt verfügbar (statische Routen, direkt verbundene Netze) oder werden dynamisch über die Routingprozesse gelernt.

Für jeden Routingprozess definieren wir eine *Routing Information Base (RIB)*, die Informationen zu gelernten Routen speichert. Für statisch konfigurierte Routen definieren wir eine eigenständige *lokale RIB*. Das ermöglicht die spätere einheitliche Behandlung aller Routinginformationen des betreffenden Routers.

Zusätzlich existiert noch ein zentraler *Router RIB*, diese enthält alle Informationen aus der lokalen RIB und den Prozess-RIBs die zur Weiterleitung von Paketen benötigt werden (route selection und packet forwarding).

Die nächste logische Ebene ist die *Routing Policy*. Sie bestimmt welche Routen zwischen Routingprozessen und Routern ausgetauscht werden und entscheidet damit letztendlich welche Pakete über welche Router weitergeleitet werden. Zur Umsetzung der Routing Policy steht innerhalb eines Router ein Mechanismus zur Verfügung der *Route redistribution* genannt wird. Über ein umfangreiches Regelwerk kann in der Routerkonfiguration festgelegt werden welche RIBs miteinander kommunizieren und welche Informationen dabei weitergegeben werden.

In Abbildung 1 zeigen wir die gerade definierten Begriffe (RIB, Route redistribution) innerhalb eines Routers anhand eines einfachen Beispiels.

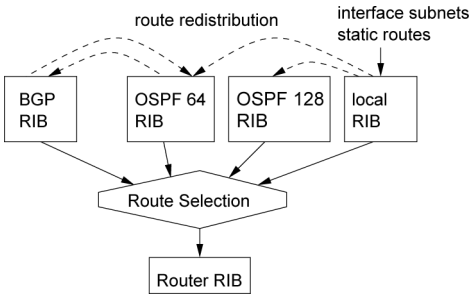

Abbildung 1: Relationen zwischen Routingprozessen und RIBs

Die einzelnen RIBs der dazugehörigen Routingprozesse sind als Kasten dargestellt. Kommunikation zwischen den Prozessen (route redistribution) wird als gestrichelter Pfeil eingetragen. Die lokale RIB ist ein Sonderfall, da sie aus den statischen Konfiguriationen nur Daten an andere RIBs weitergibt und keine erhält (Daten gehen von der lokalen RIB nur weg). Alle lokalen RIBs geben ihre Informationen an die Router-RIB (durchgehende Pfeile), welche anhand dieser Daten die eigentliche Auswahl über das Weiterleiten von Daten trifft (dargestellt als route selection Raute).

2.3 Paketfilter

Zusätzlich gibt es noch ein weiteres getrenntes Regelwerk zur Steuerung der Kommunikation zwischen Routern und Routingprozessen, die *Paketfilter (packet filter)*. Sie klassifizieren ein- oder ausgehenden Netzwerkverkehr nach einfachen Regeln (z.B. Quell-IP) und können Pakete entweder durchlassen (allowed) oder verwerfen (denied). Paketfilter sind jedoch im Gegensatz zu Routinginformationen immer statisch konfiguriert und gelten nur auf dem einzelnen Router.

3 Routingdesigns als Graphen

Gegen eine manuelle Auswertung von Routerkonfigurationen spricht die Größe und Komplexität von realen Netzwerken. Selbst bei einer automatisierten Auswertung wären die vollständigen Informationen zu umfangreich um sie sinnvoll darstellen zu können.

Die Autoren entwickeln 4 verschiedene Modelle zur Darstellung von Routingdesigns/ -informationen die automatisiert aus den Konfigurationsfiles der Router eines Netzwerkes erstellt werden können:

1. Modell der Routingprozesse (Routing Process Graph)
2. Modell der Routinginstanzen (Routing Instance Graph)
3. Modell der Routingpfade (Route Pathway Graph)
4. Modell der Adressraumstruktur (Adress Space Structure)

Die ersten drei Modelle sind aufeinander aufbauende Graphen unterschiedlichen Abstraktionsgrades des dargestellten Netzwerkes und ermöglichen die Betrachtung der Routingdesigns losgelöst von den realen Routern und Konfigurationen.

Das 4. Modell beschreibt den verwendeten Adressraum grafisch indem es Netzadressen geeignet zusammenfasst und dabei einen hierarchischen Baum des Adressraumes aufbaut. Da das 4. Modell unabhängig von den drei anderen Modellen ist und auch in der originalen Ausarbeitung nicht weiter verwendet wird, verzichte ich im Folgenden auf eine weitergehende Beschreibung.

3.1 Modell der Routingprozesse – Routing Process Graph

Der Routing Process Graph soll zu einem existierenden Netzwerk den Fluss der Routing-Informationen abbilden. Dazu definieren wir den Graphen mit den folgenden Eigenschaften:

Knoten Jeder Knoten repräsentiert einen RIB (Prozess-, lokaler, Router-RIB). Diese Informationen sind direkt aus den Konfigurationsfiles extrahierbar.

Kanten Werden zwischen zwei RIBs Routinginformationen ausgetauscht, so ist eine Kante zwischen diesen RIBs in den Graph einzufügen.
Innerhalb eines Routers wird dazu die Konfiguration auf Route Distribution Kommandos untersucht. Zwischen unterschiedlichen Routern wird untersucht ob die Bedingungen für adjazente Routingprozesse gegeben sind (siehe Kapitel 2.2).

Der so generierte Graph lässt einen sehr detaillierten Blick in die Struktur eines Netzwerkes zu. Reduziert auf die RIBs und deren Kommunikationsbeziehungen können zum Beispiel Fragen beantwortet werden, wie externe Routinginformationen in das interne Netz gelangen und wie sie dort weiterverbreitet werden. Auch kann leicht durch Gruppierung der RIBs/Knoten nach Routern die Belastung eines Routers durch Routingprozesse abgeschätzt werden.

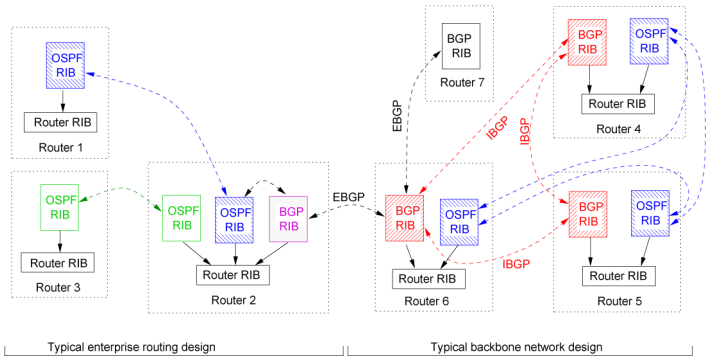

Abbildung 2: Modell der Routingprozesse

In Abbildung 2 wurde der Routing Process Graph für zwei kleine Beispielnetzwerke abgebildet die per EBGP miteinander Routen austauschen (zwischen Router 2 und Router 6).

Im linken Netzwerk mit drei Routern werden sämtliche externen Routingdaten per EBGP am Grenzrouter 2 ausgetauscht. Intern werden Routinginformationen über Interior Gateway Protokolle (IGP) geführt (in diesem Beispiel OSPF zwischen Router 1 und 2 und zwischen 2 und 3). Am Router 2 findet ein Austausch zwischen OSPF und EBGP statt.

Das rechte Netzwerk mit 4 Routern entspricht dem Backbone Routing Design. Externe Routingdaten werden über ein internes BGP Netz (IBGP Mesh) verteilt, davon völlig getrennt werden interne Routen per OSPF verteilt.

3.2 Modell der Routinginstanzen – Routing Instance Graph

Der Routing Process Graph verliert jedoch gerade wegen seiner Detailliertheit schnell seine Übersichtlichkeit sobald die Zahl der Routingprozesse und damit die Komplexität des Routingdesigns steigt.

Um auch für größere Netzwerke ein geeignetes Modell zu erhalten, definieren wir den Routing Instance Graph. Wir gruppieren dazu sämtliche adjazente Routingprozesse des gleichen Routingprotokolls:

1. Ein Routing Process Graph wird generiert.
2. Wir wählen einen freien Knoten und vergeben eine neue eindeutige Instanznummer.
3. Wir lokalisieren alle adjazenten Routingprozesse/Knoten, sie erhalten die gleiche Instanznummer.
4. Von diesen Knoten aus suchen wir weiter nach adjazenten Prozessen (transitive Hülle). Gefundene Prozesse erhalten die gleiche Instanznummer.
5. Finden wir keine weiteren adjazente Knoten, so machen wir weiter mit Punkt 2.
6. Anhand der nun für alle Knoten vergebenen Instanznummern können wir die Gruppierung durchführen.

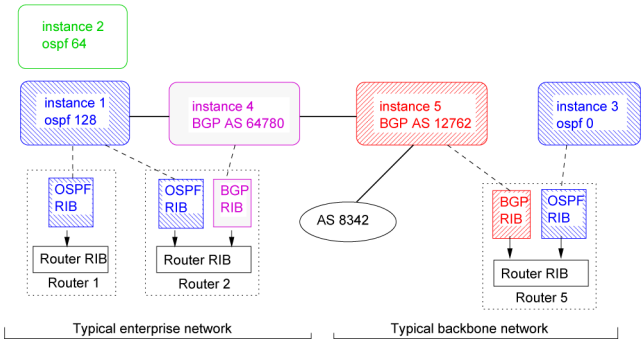

Abbildung 3: Modell der Routinginstanzen zu Abbildung 2

Abbildung 3 bildet das Beispiel aus Abbildung 2 als Routing Instance Graph ab.

Nach dem oben angegebenen Verfahren wurden die OSPF-Prozesse der Router 1 und 2 zur Routinginstanz 1 zusammengefasst. Gleiches gilt für die Instanz 3, die aus den OSPF-Prozessen der Router 5 und den (aus Übersichtlichkeitsgründen nicht dargestellten) Routern 4 und 6 besteht. Die BGP-Prozesse der beiden Netzwerke bilden jeweils die Instanzen 4 und 5. .

Die dick gedruckten Kanten sind Kommunikationsbeziehungen (Routing Redistributions) zwischen unterschiedlichen Routinginstanzen.

3.3 Modell der Routingpfade – Route Pathway Graphs

Basierend auf dem Routing Instance Graph können wir einen *Route Pathway Graph* konstruieren. Dieser zeigt den Weg der Routinginformationen eines bestimmten Routers.

Dazu nehmen wir den Routing Instance Graph und starten bei einem Router (bzw. der dazugehörigen RIB und Routinginstanz). Von dort führen wir eine Breitensuche (breath-first-search) durch.

Ausgehend von dem Netzwerk aus Abbildung 3 konstruieren wir als Beispiel den Route Pathway Graph für die Router R1 und R5 in Abbildung 4:

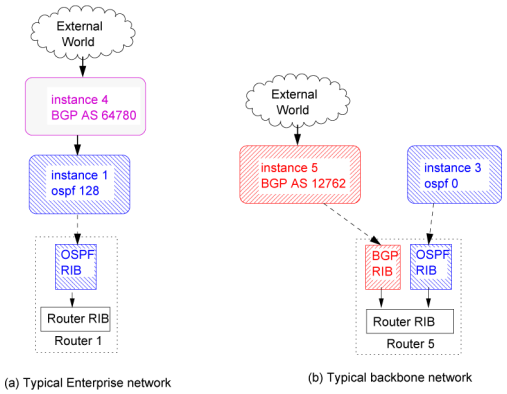

Abbildung 4: Modell der Routingpfade der Router R1 und R5

Der RoutePathway Graph des linken Netzwerkes ist sehr einfach aufgebaut. Über Router 1 als Wurzel erreicht man nur die Routinginstanzen 1 und 4 in direkter Folge, bevor man das Netzwerk verlässt.

Im rechten Netzwerk erreicht man ausgehend von Router 5 direkt die beiden Instanzen 3 und 5. Sie befinden sich damit auf gleicher Höhe und liefern beide Informationen an den Router.

4 Analyse produktiver Netzwerke

Während wir bisher die grundlegenden Analysemethoden vorgestellt haben, beschreiben die folgenden Kapitel die Vorgehensweise und ausgewählte Ergebnisse der Autoren bei der Anwendung ihrer Methoden in echten Netzwerken.

Die Autoren hatten Zugriff auf die Daten von ca. 2.400 Netzwerken der Kunden eines großen Telekommunikationsunternehmens. Zwingende Bedingung für die Herausgabe war unter anderem die garantierte *Anonymisierung* der Konfigurationsdaten.

Nur drei Mitglieder der Arbeitsgruppe hatten Kenntnis von der Identität der untersuchten Netzwerke und besaßen die Kontaktinformationen mit den Netzwerkeignern. Die eigentliche Analyse wurde von den anderen Mitgliedern der Arbeitsgruppe mit anonymisierten Daten ohne Kenntnis der Herkunft durchgeführt. Die Ergebnisse wurden dann wiederum von den ersten drei Mitgliedern zur Verifikation den Netzwerkeignern vorgelegt.

Die verwendeten Methoden zur Anonymisierung werden von den Autoren in [4] beschrieben. Die wichtigsten Arbeitsschritte sind:

- Entfernung aller Kommentare
- Sämtliche nichtnummerische Tokens die nicht zum Sprachstandard gehören werden durch Zufallstrings ersetzt.
- Einfache Integerzahlen werden beibehalten.
- Öffentliche AS Nummern werden ersetzt.
- Sämtliche IP Adressen werden ersetzt (unter Verwendung von `tpcdpriv` [5])
- Anonymisierung aller Dateinamen der Konfigurationsfiles, Zuordnung zu Netzwerken erfolgt über die Verzeichnisstruktur.

Aus den 2.400 Netzwerken wurden schließlich 31 Netzwerke von typischer Größe (von unter 10 bis über 1200 Router) von den Autoren ausgewählt und analysiert.

In den folgenden Kapiteln werden wir auf einige Ergebnisse der durchgeführten Untersuchungen eingehen.

4.1 IGP vs EGP

Die klassische Betrachtungsweise sieht die Routingprotokolle RIP, OSPF, IS-IS und EIGRP als typische Interior Gateway Protocols (IGP) und BGP als (einziges) Exterior Gateway Protocol (EGP). Eine erste Auswertung der 31 Netzwerke zeigt, dass diese Einteilung häufig nicht ausreichend ist.

Um die Häufigkeit einzelner Protokolle in einer bestimmten Rolle (IGP/EGP) zu zählen, haben die Autoren ein weiteres Regelwerk definiert um diese Einstufung ausgehend von einem Routing Instance Graph zu automatisieren. Routinginstanzen die eine adjazente Instanz außerhalb des eigenen Netzwerkes haben werden als EGP behandelt, ansonsten als IGP. Woran erkennt man die Existenz einer benachbarten Routinginstanz die nicht Teil des eigenen Netzwerkes ist?

Werden typische Point-to-Point Transfernetze (/30) verwendet, ist die Einstufung leicht. Es muss einfach überpüft werden, ob die Gegenseite in den untersuchten Konfigurationsfiles vorhanden ist. Falls ja handelt es sich um ein Interface, welches für IGP Instanzen genutzt wird, falls nein wird es für EGP genutzt.

Bei größeren Subnetzen (Multipoint links) ist die Verwendung leider nicht eindeutig. Sie können für interne Netze (z.B. für Clients) verwendet werden, aber auch für Schutzzonen-Netze, die Router in externe Netze unter fremder Kontrolle enthalten. An dieser Stelle werden verfügbare Routinginformationen zur Entscheidung herangezogen. Ein Mulitpoint Link gilt als EGB, falls es Routen zu unbekannten/externen Netzen dorthin gibt, ansonsten gilt er als IGP.

Eine Auswertung für die untersuchten 31 Netzwerke ergab:

	EBGP	IGP			
	Sessions	OSPF	EIGRP	RIP	Total
IGP	1.490	9.624	12.741	156	22.521
EGP	13.830	1.161	1.342	161	2.664

Die Tabelle unterstreicht zwar im Allgemeinen weiterhin die zu erwartende Verwendung von Routingprotokollen, sie zeigt jedoch auch in einem nicht geringen Umfang eine deutliche abweichende Verwendung von Protokollen (z.B. OSPF als EGP in über 10% der Fälle). Diese Abweichung von typischen Routingdesigns wird in Kapitel 4.3 weiter thematisiert.

4.2 Interne Verwendung von Paketfiltern

Eine weiteres überraschendes Ergebnis der Auswertungen war die zahlreiche Verwendung von Paketfiltern bei *internen* Interfaces. Die Verwendung an externen Verbindun-

gen entspricht den bekannten Best Practices, die massive Verwendung an internen Interfaces ist so aber bisher noch nicht dokumentiert worden.

Eine manuelle Untersuchung von internen Paketfiltern hat unterschiedlichste Verwendungen ergeben. Paketfilter scheinen unter anderem zur Zugriffssteuerung auf interne Applikationen auf Netzwerkebene verwendet zu werden. Auch werden sie zur Herausfilterung ungewollter Protokolle oder zur Absicherung gegen mögliche Fehlkonfigurationen verwendet.

4.3 Enterprise- vs. Backbone-Architektur

Die Literatur beschreibt zwei grundsätzlich verschiedene Routingdesigns (Enterprise- und die Backbone-Architekturen). In diesem Kapitel wollen wir die 31 untersuchten Netzwerke darauf überprüfen, ob sie diesen klassischen Designtypen entsprechen.

4 Netzwerke folgen der klassischen Backbone-Architektur: Eine große Zahl von EBGP Sessions zum Peering mit externen Netzwerken, IBGP für die Verteilung der externen Routen zu den internen Routern und eine kleine Anzahl von IGP Instanzen für interne Subnetze. Stammt das Backbone-Netzwerk von einem ISP (Internet Service Provider), so gibt es eine deutliche Abweichung vom Standardroutingdesign: Es werden traditionelle IGP Protokolle (wie OSPF) zur Verteilung von Routinginformationen an Kunden und damit externe Netzwerke verwendet. Scheinbar siegt hier die leichtere Konfigurierbarkeit von IGP Protokollen über die zusätzlichen Features von BGP.

Von den verbleibenden Netzwerken entsprechen 7 dem klassischen Enterprise-Netzwerk: Eine kleine Zahl von Routern spricht EBGP mit den externen Netzen, auf Grenzroutern werden diese Informationen an die IGP-Instanzen weitergeben. Die Mehrheit der eingesetzten Router verwenden IGPs und sind meist in zwei Routinginstanzen getrennt (zur Verbesserung von Skalierbarkeit und Performance).

Die verbleibenden 20 Netzwerke weichen jedoch deutlich von der „Buchform“ der Enterprise-Architektur ab. Das Netz aus Kapitel 4.4 ist ein Beispiel dafür, wie spezielle Designentscheidungen zu völlig neuen Routingdesigns führen können.

4.4 Routingdesign zur Vermeidung von IBGP Meshs?

Das in diesem Beispiel betrachtete Netzwerk (im Folgenden als net5 bezeichnet) besteht aus 881 Routern und 14 internen Autonomen Systemen.

Eine grafische Darstellung mit allen Routern und Kommunikationsbeziehungen ist auf Grund der Größe aussichtslos. Der Routing Instance Graph ermöglicht jedoch eine ausreichende Abstraktion um den Großteil des Netzwerkes übersichtlich darzustellen (in Abbildung 5 wurden 541 von 881 Routern berücksichtigt).

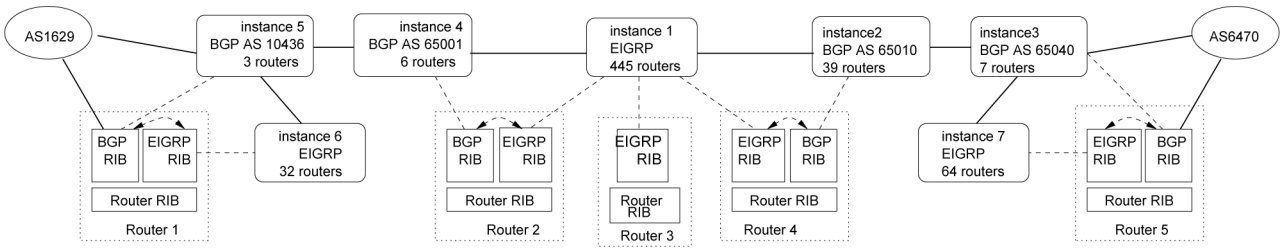

Abbildung 5: Ausschnitt Routing Instance Graph von net5

An den 2 Grenzen zu externen Netzen (Router 1 und Router 5) wird erwartungsgemäß EBGP gesprochen. Normalerweise gäbe es nach dem klassischen Routingdesign zwei verschiedene Möglichkeiten. Beim Enterprise Design werden an den Grenzroutern

die Routinginformationen über *route redistribution* an klassische IGP Protokolle weitergeleitet (wie z.B. EIGRP) und dann im internen Netz verteilt. Oder man folgt dem Backbone Design und leitet diese Informationen per internal BGP (IBGP) an die internen Router weiter. Dabei müssten sämtliche IBGP sprechenden Router des gleichen Autonomen Systems vollständig untereinander vernetzt werden (IBGP full mesh).

Das hier abgebildete net5 geht einen völlig anderen Weg. Statt IBGP wird zwischen Routinginstanzen 4 und 5 und den Instanzen 2 und 3 external BGP (EBGP) zwischen unterschiedlichen Autonomen Systemen gesprochen. Auch können die Instanzen 4 und 2 nicht direkt per BGP miteinander sprechen sondern müssen über die Routinginstanz 1 (die das IGP Protokoll EIGRP verwendet) externe Routen austauschen.

Verdeutlichen kann man das am Route Pathway Graph. Für Abbildung 6 wählen wir als Wurzel einen zentral in Routinginstanz 1 gelegenen Router (Router 3).

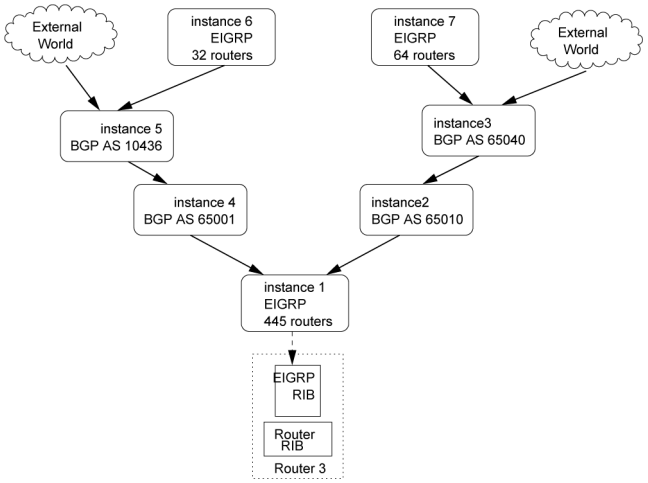

Abbildung 6: Route Pathway Graph von Router 3

Die Abbildung zeigt keine neuen Informationen gegenüber Abbildung 5, die Baumstruktur verdeutlicht aber noch einmal den umfangreichen Weg den in net5 eine externe Routinginformation nehmen muss, bevor sie einer der 445 Router innerhalb der Instanz 1 lernen kann.

Eine weitere Analyse der Konfigurationsdaten lässt vermuten, dass der Netzwerkeigner bewusst diesen Entwurf gewählt hat um die Verwendung von IBGP im internen Netz zu vermeiden. Insbesondere hat er noch eine Reihe weiterer „Tricks“ verwendet, um Eigenschaften innerhalb des EIGRP Protokolls abzubilden, die eigentlich dem mächtigeren BGP Protokoll vorbehalten sind.

Net5 lässt sich keinem der klassischen Routingdesigns zuordnen, zeigt aber sehr schön, wie mit dem Modell der Routinginstanzen auch ungewöhnliche und abweichende Routingdesigns schnell verstanden und untersucht werden können.

5 Ausblick

Bisher haben wir uns direkt mit den Auswertungsmethoden und den daraus resultierenden Ergebnisse beschäftigt. In diesem Kapitel sollen noch kurz Themen angesprochen werden, bei denen die Analyse von Routerkonfiguration wertvolle Unterstützungsarbeit leisten kann, aber auch wo sie an ihre Grenzen stößt.

Die automatisch erstellten Modelle eines Netzes sind sicherlich eine hilfreiche Unterstützung bei der Dokumentation von Netzen und können diese ergänzen oder sogar

verifizieren. Auch unterstützen sie Netzwerkadministratoren bei der Wartung ihres Netzes, sie können leicht zugängliche Informationen bereitstellen über Schwachpunkte im Routingdesign (z.B. Single-Point-of-Failures) oder sogar sicherheitsrelevante Fehlkonfigurationen identifizieren (z.B. Routing Pathways Graphen zur Identifikation von nicht beabsichtigten Routingwegen).

Durch die alleinige Auswertung von Routerkonfigurationen ist man jedoch auch gleichzeitig auf diese Informationen beschränkt. So können unter Umständen zwei interne Netze durchaus miteinander kommunizieren, selbst wenn der Routing Instance Graph das Gegenteil behauptet. Mögliche Kommunikationsbeziehungen über externe Netze bleiben unberücksichtigt.

Weitere Einschränkungen betreffen eher die Interpretation der Analyseergebnisse. Durch die Anonymisierung entfernen wir viele Informationen (DNS-, Router-, Interfacenamen, Kommentare), die zu einem vertieften Verständnis des Routingdesigns verhelfen könnten. Auch fehlen manchmal einfach die Informationen über Entscheidungsgrundlagen (z.B. Leitungsqualitäten, Organsiatorische Zwänge) die das abgebildete Routingdesign verständlich machen könnten.

6 Zusammenfassung

Zum theoretischen Aufbau großer Netzwerke gibt es umfangreiche Literatur. Sollen bestehende Netzwerke analysiert werden, so folgt die Untersuchung üblicherweise dem Black Box Prinzip (z.B. Netzwerkscans) oder auf Basis von statischen (evtl. veralteten) Dokumenten.

Die Autoren verfolgen dagegen einen automatisierbaren White Box Ansatz. Sie entwickeln eine Methode um einen detaillierten Blick in das innere beliebiger Netzwerke zu werfen, unter Verwendung von Offlinedaten – den Routerkonfigurationsdateien:

- Automatisierte Auswertung der Routerkonfigurationen
- Garantierte Anonymisierung der darin enthaltenen Informationen
- Interpretation dieser Daten zu Modellen unterschiedlichen Abstraktionsgrades

  Routing Process Graph – Grafische Darstellung aller Routingprozesse und derer Kommunikationsbeziehungen

  Routing Instance Graph – Zusammenfassung aller zusammenhängenden (adjazenten) Routingprozessen zu Routinginstanzen

  Route Pathway Graph – Grafische Darstellung des Weges von Routinginformationen für Routinginstanzen

  Adress Space Structure – Hierarchische Baumdarstellung der verwendeten Adressräume
- Statistische Auswertungen über mehrere Netzwerke

Dabei standen ihnen dank der Kooperation der Firmen über 20.000 Routerkonfigurationen zur Analyse zur Verfügung. Zur Prüfung ihrer Methoden haben sie schließlich 31 Netzwerke mit über 8.000 Routern näher untersucht.

Die Ergebnisse dieser Analysen brachten einige Überraschungen mit sich. Während ein Teil der Erkenntnisse zum Routingdesign sich mit den Best Practices zum Aufbau von Enterprise- oder Backbone-Netzwerken decken, zeigten doch ein nicht unerheblicher Teil (mehr als 50%) ein Routingdesign, welches kaum den klassischem Designentwürfen entspricht.

Das vorgestellte Verfahren kann damit eine Grundlage für weitere umfassende Untersuchungen produktiver Netze sein um so neue Erkenntnisse im Bereich des Routingdesigns zu erhalten.

Literatur

[1] David A. Maltz, Geoffrey Xie, Jibin Zhan, Hui Zhang, Gisli Hjálmtýsson, Albert Greenberg: *Routing Design in Operational Networks: A Look from the Inside*. Carnegie Mellon University, AT&T Labs-Resarch, Report, 2004.

[2] *Cisco IOS Software*. `http://www.cisco.com/web/psa/products/index.html?c=268438303`, 12.2007

[3] James F. Kurose and Keith W. Ross. *Computer Networking: A Top-Down Approach*. Addison-Wesley, 1st version (online), `http://www.net.t-labs.tu-berlin.de/teaching/computer\_networking/`, 2000

[4] David A. Maltz, Geoffrey Xie, Jibin Zhan, Hui Zhang, Gisli Hjálmtýsson, Albert Greenberg and Jennifer Rexford: *Structure preserving anonymization of router configuration*. Technical Report CMU-CS-04-149, Carnegie Mellon University, 2004.

[5] Greg Ninshall. *tcpdpriv – remove private information from tpcdump -w file*. `htpp://ita.ee.lbl.gov/html/contrib/tpcdpriv.html`, 1997