

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

Ralf Stange

Betreuer
Amir Mehmood

Technische Universität Berlin
WS 2007/2008

Worum geht es?

- Gesucht ist eine Methode zur Analyse des Routingdesigns großer Netzwerke
- Wozu?
 - Vollständiger Überblick / Dokumentation
 - leichteres Netzwerkdesign
 - vereinfachte Fehlersuche
 - Sicherheitsgewinn
 - besseres Verständnis vorhandener Routing-Topologien

Worum geht es?

- Wie?
 - automatisierte Analyse von Routerkonfigurationsfiles
 - Zusammenfassung der Daten in Graphen mit unterschiedlichen Abstraktionsgrad
- Analyse von Routerkonfigurationsfiles?
 - weitgehende Automatisierte Auswertung
 - per Reverse Engineering
 - White-Box Ansatz
 - Anonymisierung der Daten

Routingdesign

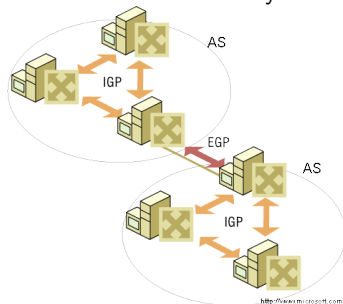
- Aufbau und Struktur von Netzen (Layer 3)
- verwendete Routingprotokolle
- typische Ziele von Routingdesign
 - Erreichbarkeit
 - Ausfallsicherheit
 - Lastverteilung
 - Skalierbarkeit
 - leichte Administrierbarkeit

IGP – EGP

unterschiedlicher Einsatz von Routingprotokollen

IGP Interior Gateway-Protokoll
innerhalb eines Autonomen Systems (AS),
z.B. OSPF, RIP

EGP Exterior Gateway-Protokoll
zwischen Autonomen Systemen, BGP



Typische Routingdesigns

- Enterprise Networks
 - wenige BGP Verbindungen zu fremden Netzen
 - Verteilung der Routinginformationen im internen Netz per IGP
- Backbone Networks
 - viele BGP Verbindungen zu fremden Netzen
 - Weiterverteilung der Routinginformationen per iBGP (internal BGP) im internen Netz

Gliederung

- 1 Einführung
- 2 Verfahren
 - Reverse Engineering
 - RIB und Route redistribution
 - Anonymisierung von Konfigurationsfiles
- 3 Routingmodelle
- 4 A Look from the Inside
- 5 Zum Schluss

Auszug Routerkonfigurationsfile (Cisco IOS)

```
interface Ethernet0
  ip address 66.251.75.144 255.255.255.128
!
router ospf 64
  redistribute connected metric-type 1 subnets
  redistribute bgp 64780 metric 1 subnets
!
router bgp 64780
  redistribute ospf 64 match route-map password
  neighbor 66.253.160.68 remote-as 12762
!
access-list 143 deny 134.161.0.0 0.0.255.255
ip route 10.235.240.71 255.255.0.0 10.234.12.7
```


Informationen aus der Routerkonfiguration

- Link-Level Topologie
 - zu **Internen Interfaces** existiert mindestens ein weiteres Interface mit gleichem Subnetz, ansonsten handelt es sich um ein **Externes Interface**
- Routingprozesse
- Routing Topologie
 - zwei Routingprozesse gelten als **adjazent**, wenn sie direkt Routinginformationen austauschen
- Paketfilter

```
interface Ethernet0  
ip address ...
```

```
router ospf 64  
redistribute connected...  
redistribute bgp 64780...  
router bgp 64780  
redistribute ospf 64...  
neighbor 66.253.160.68
```

```
access-list 143 deny ...
```

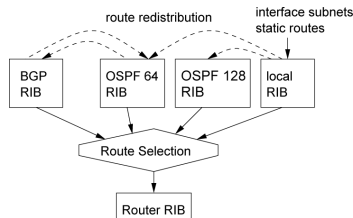
Begriffe RIB und Route redistribution

Routing Information Base (RIB)

- RIBs speichern die Routinginformationen
- jeder Routingprozess besitzt eine eigene *Prozess-RIB*
- jeder Router besitzt eine *lokale RIB* für statisch definierte Routen
- jeder Router besitzt eine zentrale *Router RIB*
- die Router RIB ist zuständig für das eigentliche Paket-Forwarding

Route redistribution

- regelt welche RIBs miteinander kommunizieren
- wird mit der Routerkonfiguration festgelegt



Anonymisierung der Konfigurationsfiles

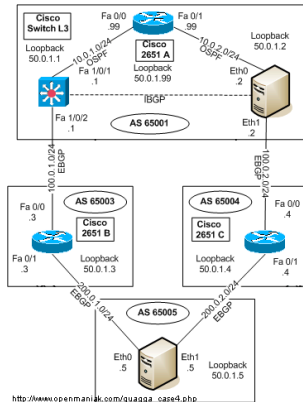
- Entfernung aller Kommentare
- Ersetzung aller Worte die nicht zum Sprachstandard gehören durch Zufallsstrings
- Ersetzung aller IP-Adressen (und AS-Nummern)
- Ersetzung aller Dateinamen der Konfigurationsfiles
- zusätzliche organisatorische Maßnahmen

Gliederung

- 1 Einführung
- 2 Verfahren
- 3 Routingmodelle
 - Warum Routingmodelle?
 - Modell der Routingprozesse - Routing Process Graph
 - Modell der Routinginstanzen - Routing Instance Graph
 - Modell der Routingpfade - Routing Pathway Graph
- 4 A Look from the Inside
- 5 Zum Schluss

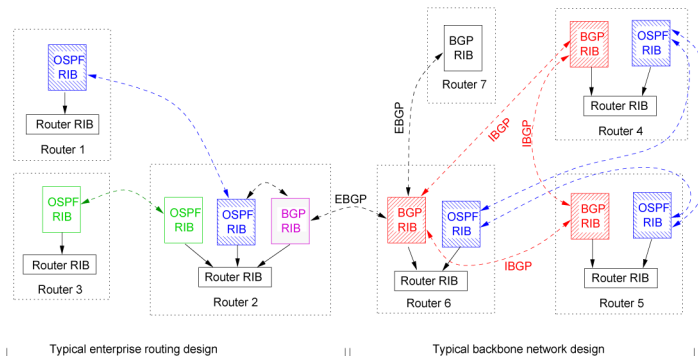
Warum Routingmodelle?

- Darstellung großer Netzwerke unterschiedlichen Abstraktionsgrades
- mögliche Konzentration auf bestimmte Details



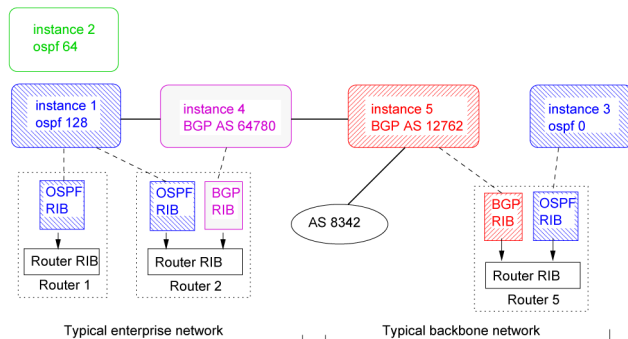
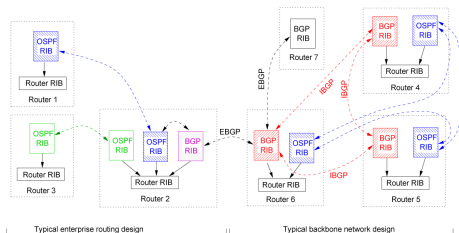
Modell der Routingprozesse - Routing Process Graph

- Knoten entsprechen einem RIB
- Kanten entsprechen route redistribution zwischen RIBs



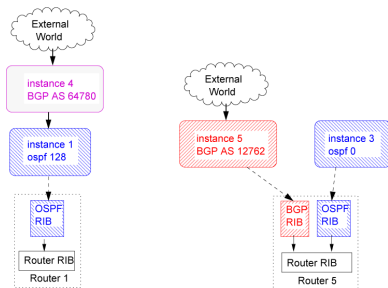
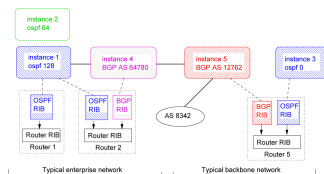
Modell der Routinginstanzen - Routing Instance Graph

- zu einer **Routinginstanz** werden alle adjazenten Routingprozesse eines Protokolls zusammengefasst



Modell der Routingpfade - Routing Pathway Graph

- Baumdarstellung
- einzelner Router als Wurzel
- alle von der Wurzel aus erreichbaren Routinginstanzen



Gliederung

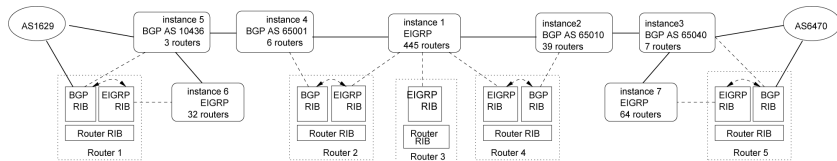
- 1 Einführung
- 2 Verfahren
- 3 Routingmodelle
- 4 A Look from the Inside
 - Was wurde untersucht?
 - Enterprise- vs Backbone-Architektur
 - IGP vs EGP
- 5 Zum Schluss

Was wurde untersucht?

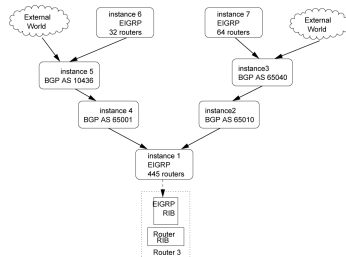
- Zugriff auf ca. 2.400 Kundennetzwerke eines lokalen Telekommunikationsunternehmens
- in Kooperation mit den Kunden
- 31 Netzwerke wurden mit dem vorgestellten Verfahren analysiert
- besonderes Interesse galt dem Vergleich mit klassischen Routingdesigns (Enterprise-, Backbone-Netzwerke)

Routingmodelle am Beispiel eines realen Netzes

Routing Instance Graph zu net5:



Route Pathway Graph von Router 3:



Enterprise- vs Backbone-Architektur

31 untersuchte Netzwerke:

- 4 entsprechen einer klassischen Backbone-Architektur
- 7 entsprechen dem klassischen Enterprise-Netzwerk
- 20 Netzwerke weichen von dem klassischen Design ab

IGP vs EGP

Einteilung der Routingprotokolle in interne (IGP) oder externe Verwendung (EGP):

	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

Über 10% der typischen IGP Protokolle werden als EGP verwendet

Gliederung

- 1 Einführung
- 2 Verfahren
- 3 Routingmodelle
- 4 A Look from the Inside
- 5 Zum Schluss
 - Das vorgestellte Verfahren
 - Ergebnisse

Das vorgestellte Verfahren

- basiert auf automatisierter Auswertung von Routerkonfigurationen bei gleichzeitiger Anonymisierung der Daten
- ermöglicht Interpretation dieser Daten zu Modellen unterschiedlichen Abstraktionsgrades (Process/Instance/Pathway Graph)
- liefert Datenmaterial für statistische Auswertungen
- dokumentiert ein Netzwerk
- unterstützt Administratoren (Fehlersuche, Optimierungen)
- benötigt aber häufig noch menschliche Interpretation
- wurde bisher nur für Cisco Konfigurationsfiles programmiert

Ergebnisse

- das vorgestellte Verfahren wurde bei 31 Netzwerken mit über 8.000 Routern erfolgreich angewendet
- dabei waren bei mehr als 50% der Netzwerke deutliche Abweichungen vom klassischen Routingdesign festzustellen
- weitere Untersuchungen von operativen Netzwerken können neue Erkenntnisse im Routingdesign bringen

Fragen?

Die Originalarbeit:

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.