

# BGP-Alarmssystem

Gunnar Bornemann

Diplomarbeit

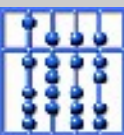
Lehrstuhl für Netzwerkarchitekturen

Technische Universität München

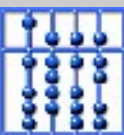
[borneman@net.in.tum.de](mailto:borneman@net.in.tum.de)

31.10.2006

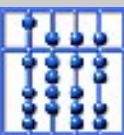
- Motivation
- Background BGP
- Topologie-Übersicht
- Interessantes aus den Daten
- Ziele der Diplomarbeit
- Analyse und Auswertung der BGP-Daten
- Entwurf und Implementierung
- Ablauf der Diplomarbeit



- ***Motivation***
- Background BGP
- Topologie-Übersicht
- Interessantes aus den Daten
- Ziele der Diplomarbeit
- Analyse und Auswertung der BGP-Daten
- Entwurf und Implementierung
- Ablauf der Diplomarbeit

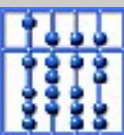


Netzwerk-Administratoren sollten wissen,  
was in ihren Netzwerken passiert!



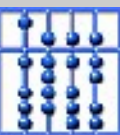
# Motivation

- Netzwerke sind dynamische Systeme
  - Hardware- und Softwarefehler können nicht ausgeschlossen werden
  - Fehlkonfiguration bei Änderungen möglich
- Zu viele Änderungsinformationen für die tägliche Administration

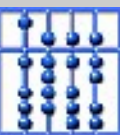


## Daher Unterstützung des Administrators

- Automatisches Filtern und Zusammenfassen von Daten
- Informationen übersichtlich und einfach darstellen
- Auf wichtige bzw. kritische Ereignisse und Systemzustände sofort hinweisen

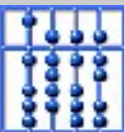


- Motivation
- ***Background BGP***
- Topologie-Übersicht
- Interessantes aus den Daten
- Ziele der Diplomarbeit
- Analyse und Auswertung der BGP-Daten
- Entwurf und Implementierung
- Ablauf der Diplomarbeit

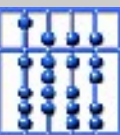


## Border Gateway Protocol (BGP)

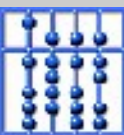
- Router gibt Informationen über Präfixe an benachbarte Router weiter (BGP-Updates)
  - Announcement: Router „sieht“ ein neues Präfix
  - Withdrawal: Router „sieht“ ein Präfix nicht mehr
- „Policy“-basiertes Routing
  - Umsetzung der Richtlinien mittels Attribute



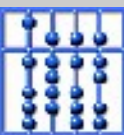
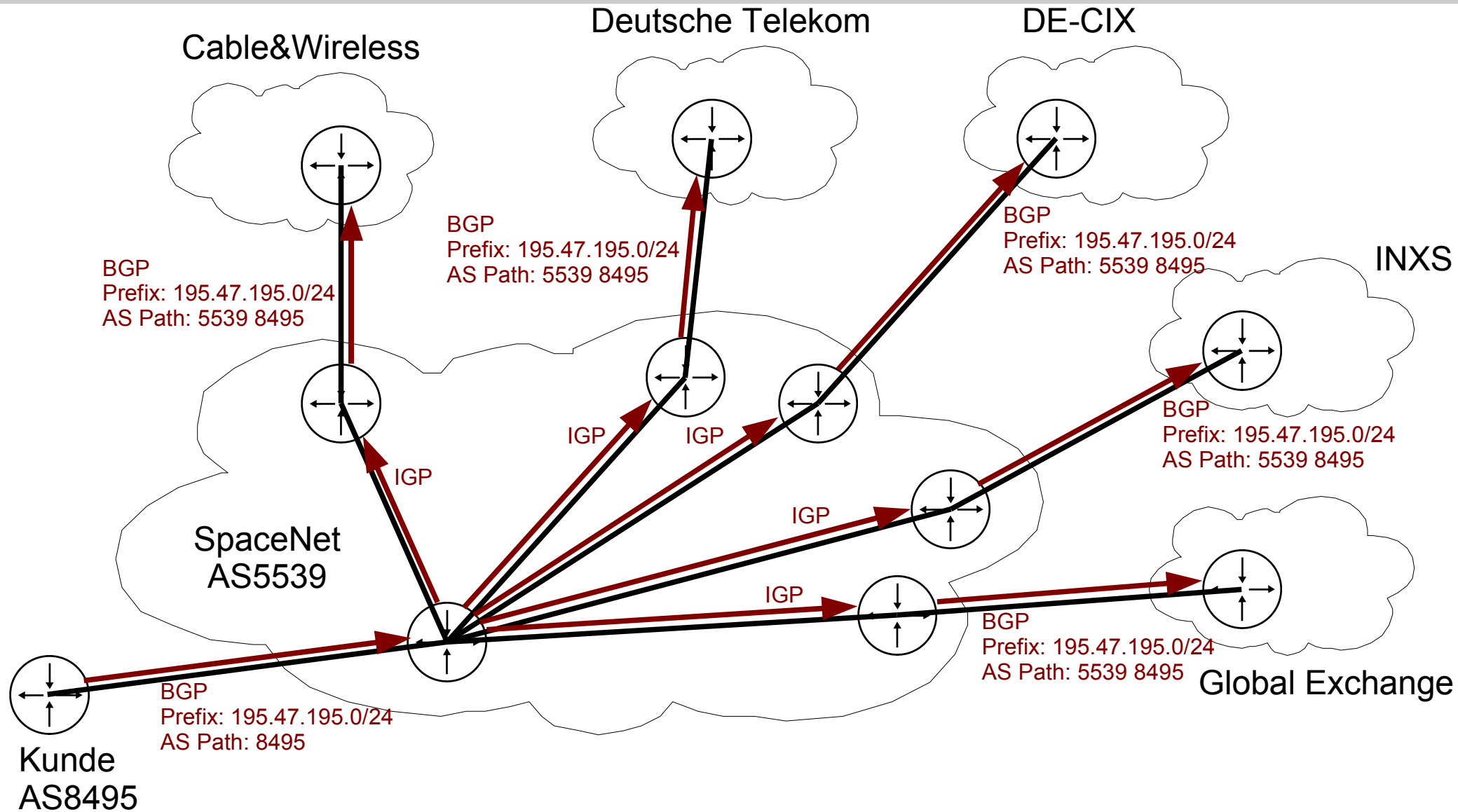
- BGP-Attribut „AS path“
  - Liste von AS-Nummern
  - „Pfad“ zum zuständigen Router/AS des Präfixes
  
- BGP-Attribut „community string“
  - frei definierbares Feld
  - z.B. Beeinflussung der Weitergabe von BGP-Updates
  - z.B. Manipulation des AS-Pfades



- Motivation
- Background BGP
- ***Topologie-Übersicht***
- Interessantes aus den Daten
- Ziele der Diplomarbeit
- Analyse und Auswertung der BGP-Daten
- Entwurf und Implementierung
- Ablauf der Diplomarbeit

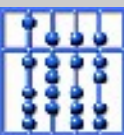


# Topologie-Übersicht

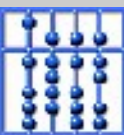
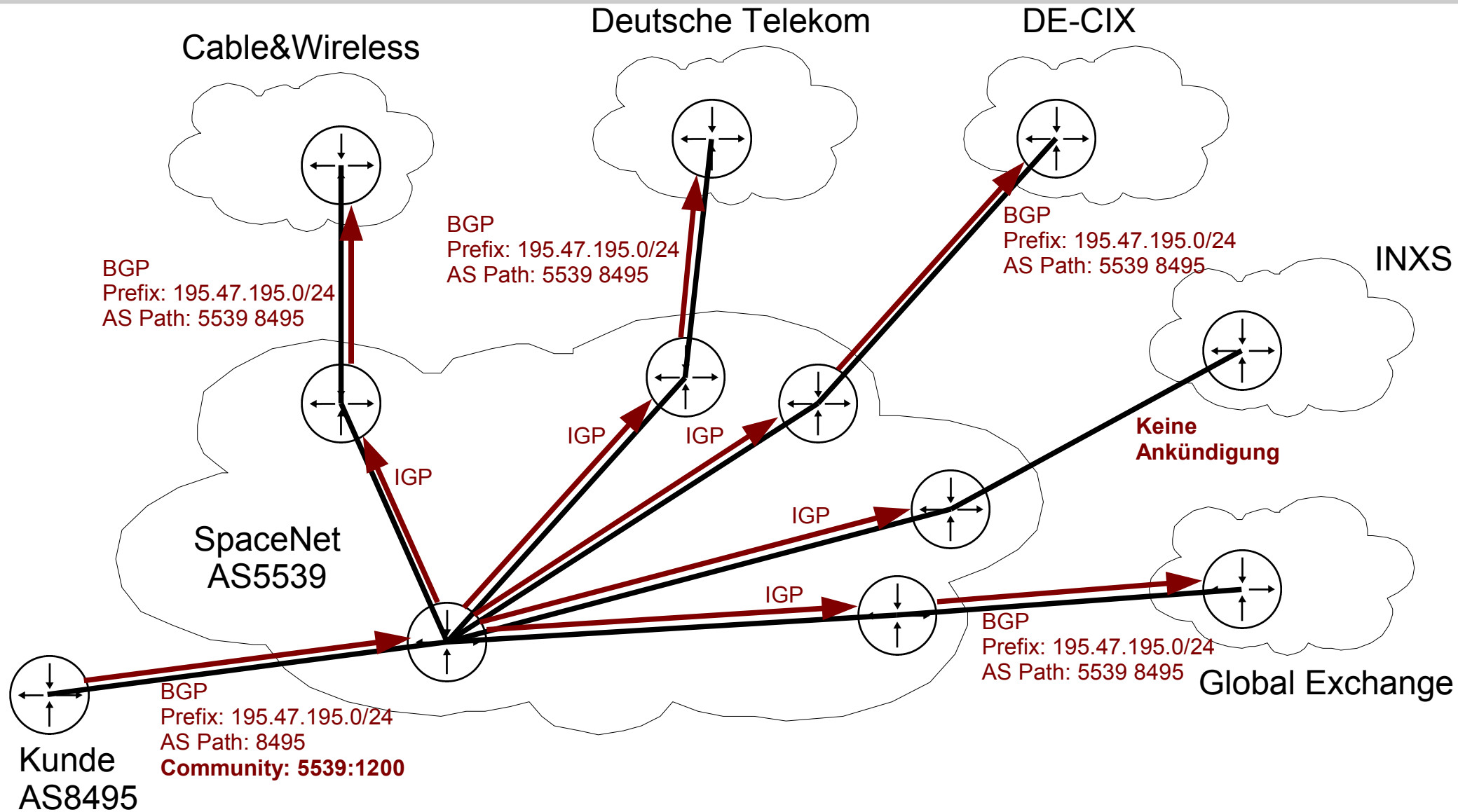


## Community-Einsatz

- Beeinflussung der Weitergabe von BGP-Updates  
Beispiel: Kunde möchte Präfix 195.47.195.0/24 nicht über INXS angekündigt haben  
→ BGP-Update mit „Community 5539:1200“



# Topologie-Übersicht

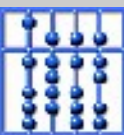


## Community-Einsatz

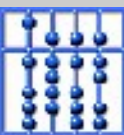
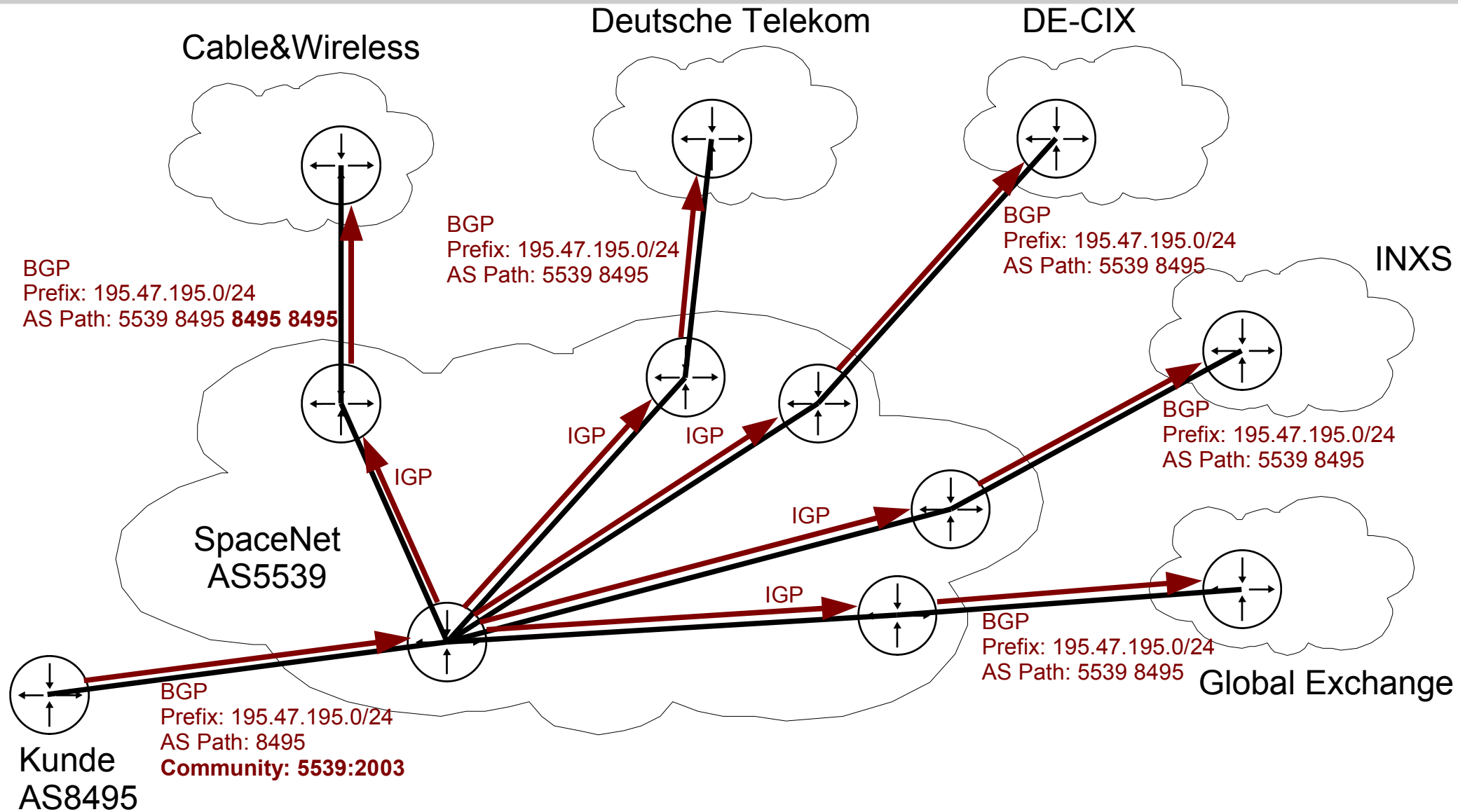
- Manipulation des AS-Pfades

Beispiel: Kunde möchte AS-Pfad für Präfix  
195.47.195.0/24 über Cable&Wireless  
verlängern (AS number prepending)

→ BGP-Update mit „Community 5539:2003“ (3-faches  
prepending)

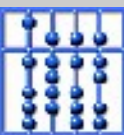


# Topologie-Übersicht

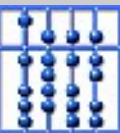
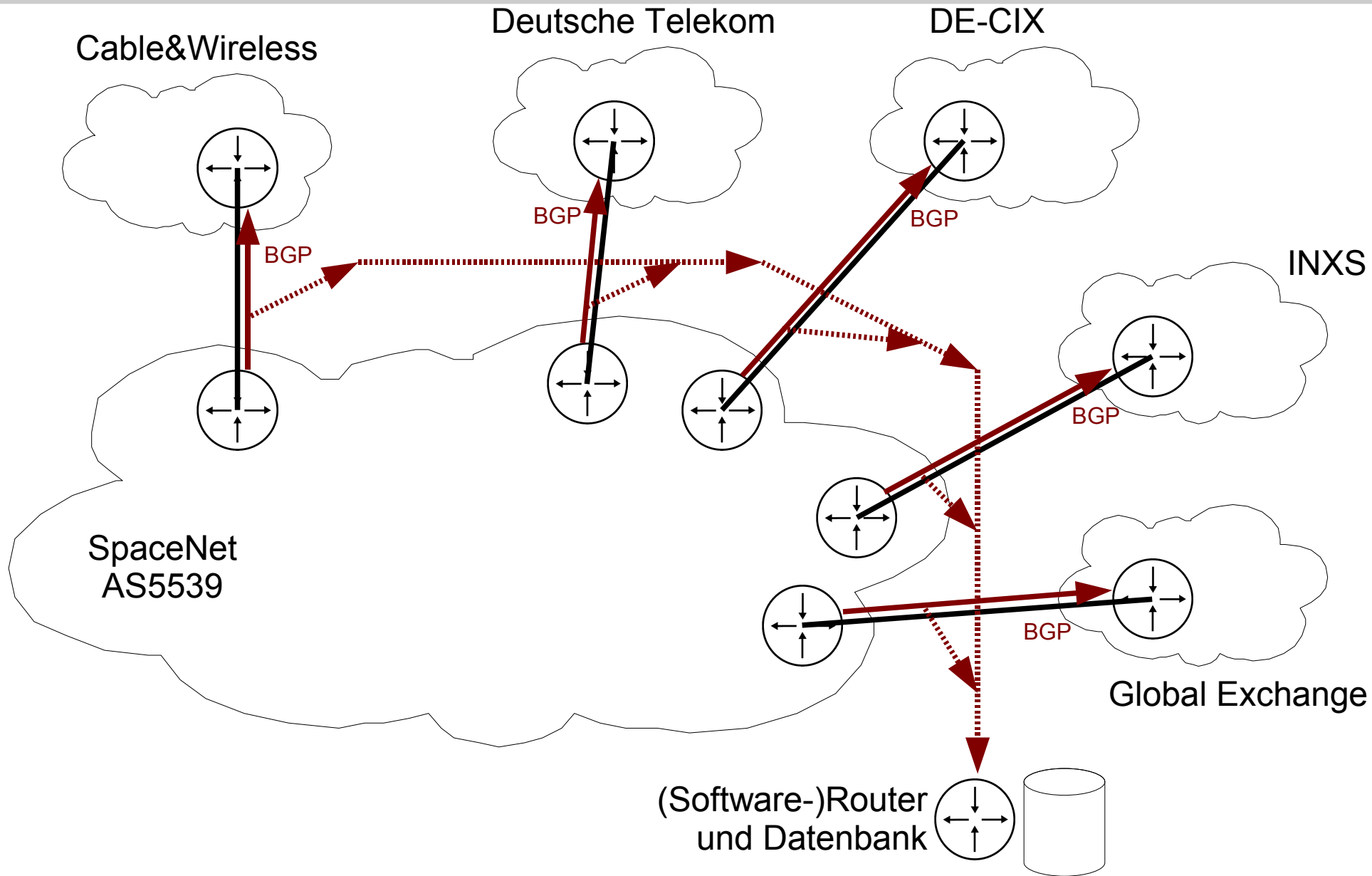


## Setup im Rahmen der Diplomarbeit

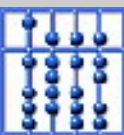
- Interessant: BGP-Daten der Border Router zum Nachbar-AS
- Kopien der BGP-Updates an zentraler Stelle sammeln



# Topologie-Übersicht



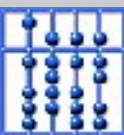
- Motivation
- Background BGP
- Topologie-Übersicht
- ***Interessantes aus den Daten***
- Ziele der Diplomarbeit
- Analyse und Auswertung der BGP-Daten
- Entwurf und Implementierung
- Ablauf der Diplomarbeit



# Interessantes aus den Daten

- Datenbestand: ca. 5 Monate (seit 24.5.2006)
- Insgesamt: 11547 Updates  
ca. 75 Updates pro Tag  
ca. 15 Updates pro Tag und Router
- Präfixe:

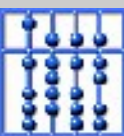
	IPv4	IPv6	Summe
gesehene Präfixe	84	34	118
derzeit angekündigt	44	18	62
derzeit zurückgezogen	40	16	56



- Aktive Präfixe:

- 23 von 44 IPv4 Präfixe über alle 5 Router angekündigt
- alle IPv6 Präfixe über 4 Router angekündigt (kein IPv6 zur Deutschen Telekom)
- verbleibende 21 IPv4 Präfixe nur über einen Router angekündigt (zu Cable & Wireless)

Beobachtung: Mehrheit aller Präfixe wird über alle Router angekündigt



# Interessantes aus den Daten

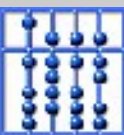
- Beispiel: Präfix 195.47.195.0/24 des AS8495

ID	Timestamp	MsgType	Router	Prefix	AS Path
700	2006-05-28 03:16:50	Announce	193.149.44.46	195.47.195.0/24	5539 8495 8495 8495 8495 8495 8495
706	2006-05-29 16:16:20	Withdraw	193.149.44.46	195.47.195.0/24	
1488	2006-06-10 22:09:05	Announce	193.149.44.46	195.47.195.0/24	5539 8495
1499	2006-06-10 22:10:00	Withdraw	193.149.44.46	195.47.195.0/24	
1506	2006-06-10 22:11:21	Announce	193.149.44.46	195.47.195.0/24	5539 8495 8495 8495 8495 8495 8495

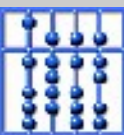
(Analog auf den anderen 4 Routern)

## Beobachtungen:

- Präfix war über 12 Tage nicht angekündigt
- Administrator hat danach zunächst „prepending“ vergessen

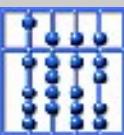


- Motivation
- Background BGP
- Topologie-Übersicht
- Interessantes aus den Daten
- ***Ziele der Diplomarbeit***
- Analyse und Auswertung der BGP-Daten
- Entwurf und Implementierung
- Ablauf der Diplomarbeit

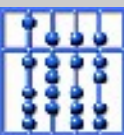


# Ziele der Diplomarbeit

- Analyse und Auswertung von BGP-Daten
  - Woher bekomme ich Daten und wie speichere ich sie?
  - Wie erkenne ich, was passiert ist?
- Entwurf und Implementierung eines BGP-Alarm-systems mit grundlegenden Funktionen
  - Wie reagiere ich auf welche Veränderung?
  - Wie stelle ich welche Informationen übersichtlich dar?



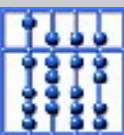
- Motivation
- Background BGP
- Topologie-Übersicht
- Interessantes aus den Daten
- Ziele der Diplomarbeit
- ***Analyse und Auswertung der BGP-Daten***
- Entwurf und Implementierung
- Ablauf der Diplomarbeit



- Suche nach „informativen“ BGP-Datenfeldern

## → Geeignete BGP-Attribute

- ✓ Nachrichtentyp (Announcement, Withdrawal)
- ✓ Zeitstempel der Nachricht
- ✓ Router
- ✓ AS-Pfad
- ✓ „community string“



## → Ungeeignete BGP-Attribute

- x „origin“

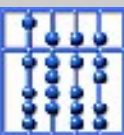
Lernquelle ist immer „IGP“, da sämtliche Präfixe zu SpaceNet bzw. deren Kunden gehören

- x „local preference“

Bietet zu starken Einfluss auf Routing-Entscheidung, daher von SpaceNet nicht erwünscht

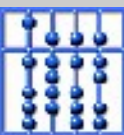
- x „multi-exit discriminator“

In vorhandener Topologie nicht anwendbar, da mehrere Verbindungen zwischen zwei ASen nicht existieren



# Analyse und Auswertung

- Problem: Durch SpaceNet umgesetzte „communities“ werden von Border Routern entfernt
- Lösung: Veränderungen an Attributen (z.B. AS-Pfad) lassen meist Rückschluss auf verwendetes „community“ zu
- Andere Provider betreffende „communities“ bleiben unverändert

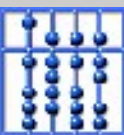


- Problem: Datenkorrelation nötig
  - bezüglich Zeit
  - bezüglich Anzahl der Router

Beispiel: Wegen Konfigurationsänderung wird ein Präfix kurzzeitig zurückgezogen, danach erneut angekündigt

Richtige Reaktion: keine Reaktion nötig

Falsche Reaktion: Meldung „Präfix weg“, danach Meldung „Präfix wieder da“



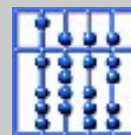
# Analyse und Auswertung

Beispiel: Kunde kündigt Präfix P nur noch über Router R1, nicht mehr aber über R2 und R3 an

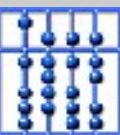
Richtige Reaktion: Meldung „Präfix P nur noch über R1“  
oder Meldung „Präfix P nicht mehr über R2 und R3“

Falsche Reaktion: Meldung „Präfix P nicht mehr über R2“ und Meldung „Präfix P nicht mehr über R3“

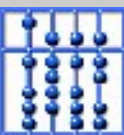
Besonderheit: Gleichzeitige Korrelation bezüglich Zeit und Anzahl der Router auch nötig!



- Idee: Looking Glas Server
  - Daten der Border Router liefern Sicht auf das AS „von Innen“
  - Looking Glas Server (z.B. von RIPE) bieten Sicht „von Außen“
  - Direkter Informationsgewinn?
  - Oder durch Vergleich der Sichten?

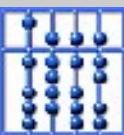


- Motivation
- Background BGP
- Topologie-Übersicht
- Interessantes aus den Daten
- Ziele der Diplomarbeit
- Analyse und Auswertung der BGP-Daten
- ***Entwurf und Implementierung***
- Ablauf der Diplomarbeit

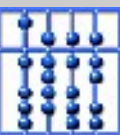


## Abläufe im BGP-Alarmsystem:

- Periodisch (z.B. alle 5 Minuten)
  - Software-Router exportiert Updates
  - Konvertieren und Parsen der Updates und in die Datenbank einfügen
  - Auf kritische Ereignisse und Zustände prüfen und gegeben falls Administrator per E-Mail informieren

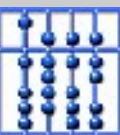


- Täglich
  - Ereignisse der letzten 24 Stunden filtern und zusammenfassen
  - Webseite zur Darstellung der Informationen generieren
- On-demand (mögliche Erweiterung)
  - Webseite mit aktuellen Informationen und Zuständen generieren

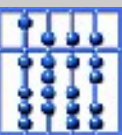


## Verwendete Tools:

- Software-Router „Zebra“
- Datenbank MySQL
- bgpdump (Binäre BGP-Daten konvertieren)
- Skripte in Perl und PHP

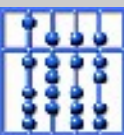


- Motivation
- Background BGP
- Topologie-Übersicht
- Interessantes aus den Daten
- Ziele der Diplomarbeit
- Analyse und Auswertung der BGP-Daten
- Entwurf und Implementierung
- ***Ablauf der Diplomarbeit***

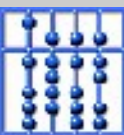


# Ablauf der Diplomarbeit

- Vorarbeiten
  - Installation und Konfiguration eines Software-Routers
  - Erstes „Datensammeln“
  
- Abgeschlossene Arbeiten
  - ✓ Einarbeitung in BGP
  - ✓ BGP-Daten sammeln und analysieren
  - ✓ Grundlegender Entwurf des BGP-Alarmsystems



- Aktuelle Tätigkeiten
  - Detaillierte Auswertung der BGP-Daten
  - Implementierung des BGP-Alarmsystems
  - Ständige Tests (Live-Daten)
  
- Offene Punkte
  - × RIPE-Daten integrieren
  - × Implementierung abschließen
  - × Spezielle Testfälle generieren (z.B. Session Reset)



Vielen Dank für Ihre Aufmerksamkeit!

