

# Erkennung von Routing-Problemen

Lehrstuhl Feldmann

Hauptseminar Internetmeasurement

Richard Hartmann

# Übersicht

- Einleitung
  - Begriffserklärungen
  - Motivation
- Routing Loops
  - Entstehung
  - Folgen
  - End-to-End & Netzknotenüberwachung

# Übersicht

- Replica Streams
  - Erzeugung
  - Verwendete Daten
  - Betrachtungen & Ergebnisse
- Zusammenfassung

# Begriffserklärungen

- Routing Loop
  - temporäre, widersprüchliche Inkonsistenz der Forwarding-Tabellen
- IP Adresspräfix
- Replica Stream
  - ein Paketstrom, in dem jedes Paket eines /24 Präfixes mindestens dreimal vorkommt und die TTL jedes Pakets bei jedem Auftreten abnimmt
- Jitter
- TTL

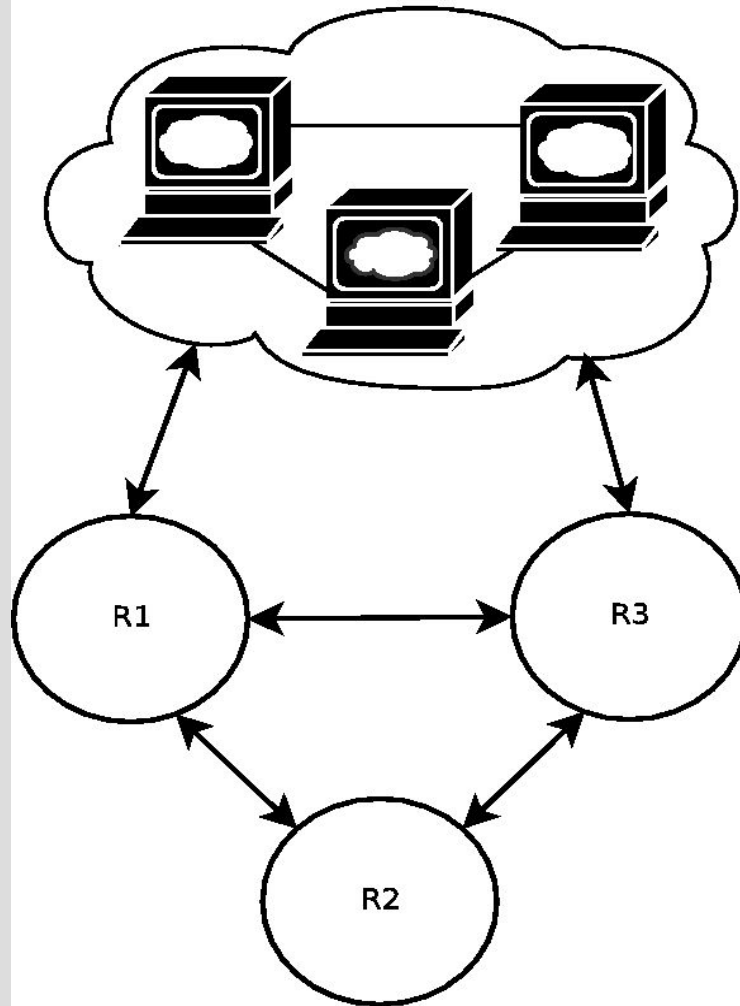
# Motivation

- Pakete können in Routing Loops gefangen werden
- ISPs wollen Informationen über die Qualität ihres Netzes
- Aussagen über die Dauer und Tragweite der Routing Loops

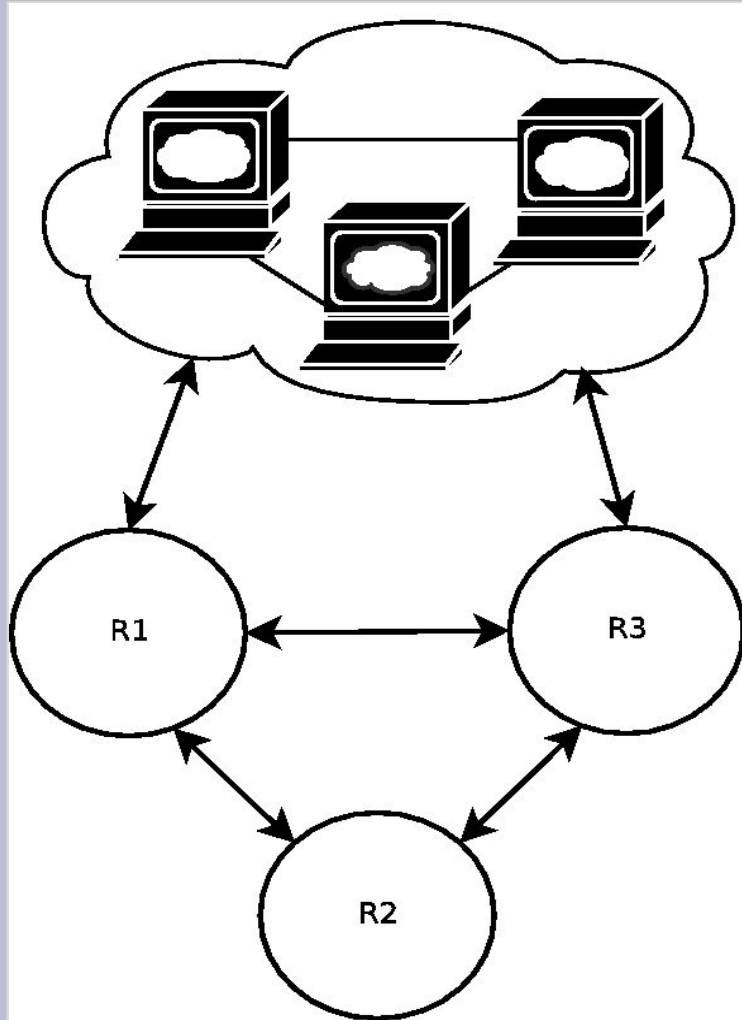
# Entstehung von Routing Loops

- Persistente Routing Loops
  - langfristig
  - meist durch Fehlkonfiguration
  - manuelle Behebung
- Transiente Routing Loops
  - kurzfristig (meist 10 – 25 Sekunden)
  - entstehen im normalen Betrieb
  - lösen sich durch Konvergenz der Forwarding-Tabellen selbst auf

# Entstehung von Routing Loops

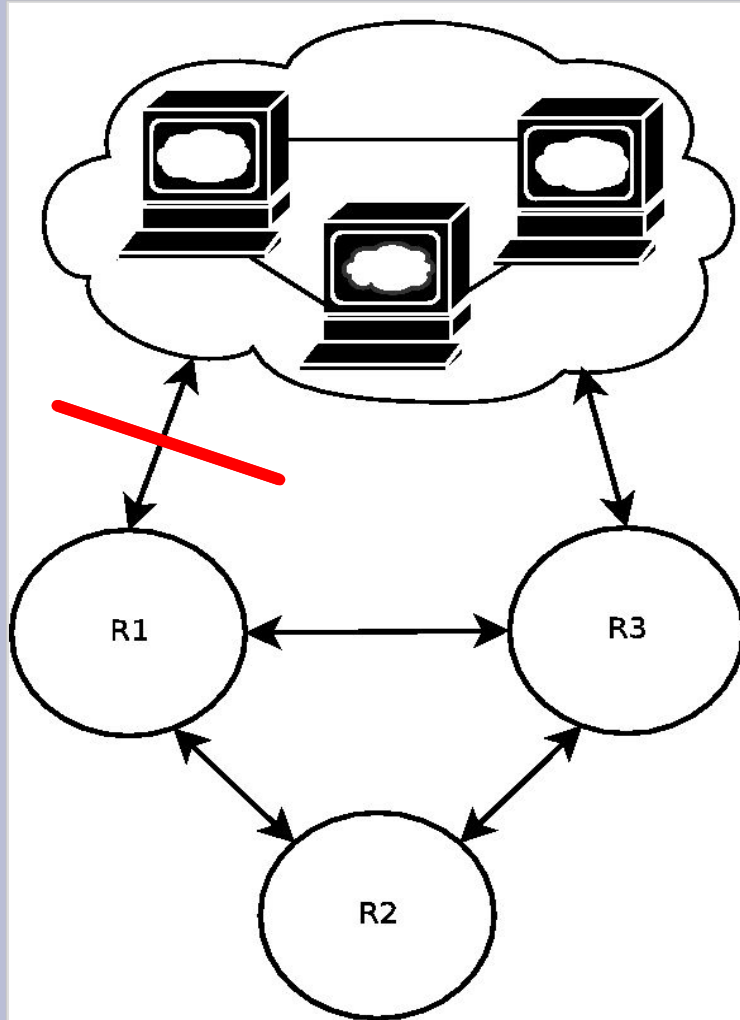


# Entstehung von Routing Loops



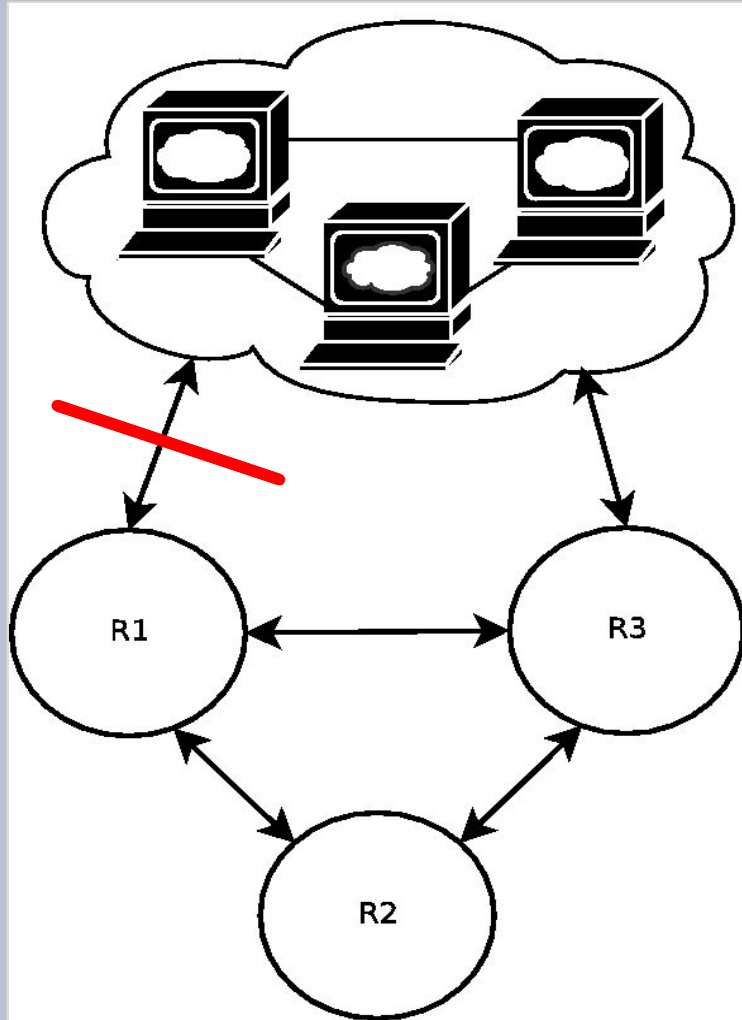
R1	R1
R2	R1
R3	R1

# Entstehung von Routing Loops



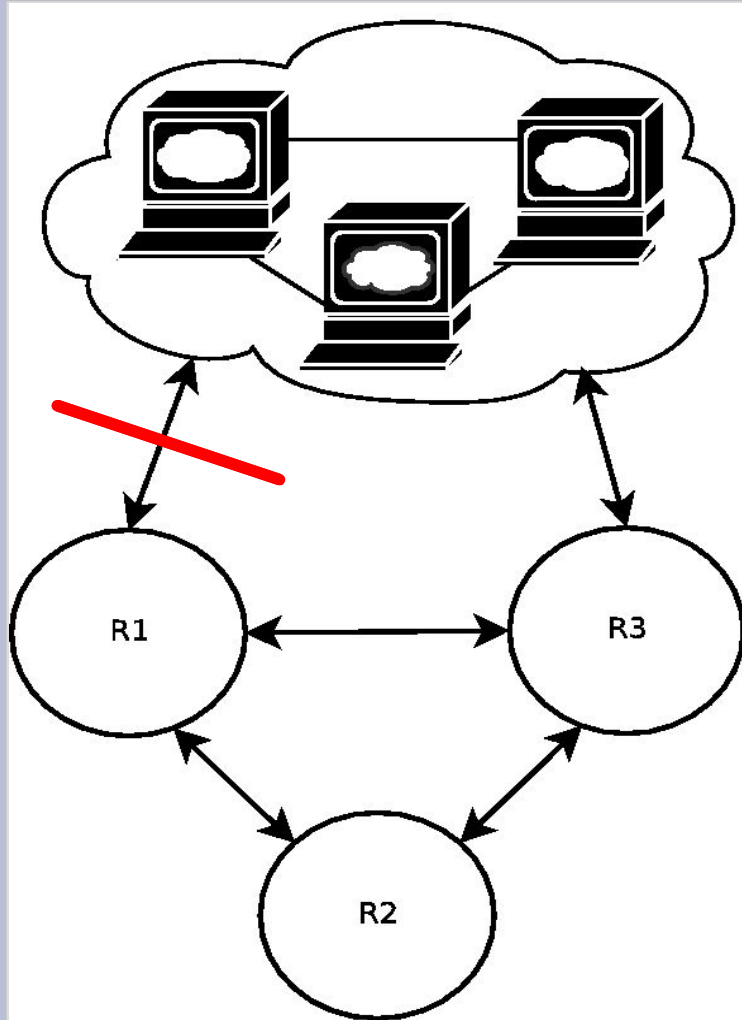
R1	R3
R2	R1
R3	R1

# Entstehung von Routing Loops



R1	R3
R2	R3
R3	R1

# Entstehung von Routing Loops



R1	R3
R2	R3
R3	R3

# Folgen

- Generelle Folgen
  - erhöhte Übertragungszeiten oder Paketverluste
  - Bandbreitenverbrauch steigt
  - Jitter beeinträchtigt Echtzeit- und Out-of-Order-fähige Protokolle
  - für normale Endknoten nicht von anderen Netzwerkfehlern unterscheidbar

# Folgen

- UDP
  - sendet weiter
  - keine Rückmeldung an den Benutzer oder das Programm
  - Routing Loop auf dem Rückkanal hat keine Auswirkung

# Folgen

- TCP
  - Congestion Control reduziert Übertragungsrate
  - kann zu Verbindungsabbruch führen
    - besonders schlimm bei langfristigen Verbindungen wie VPN, SSH, Tunneln, IRC-Servern
  - Routing Loops auf dem “Rückkanal” verhindern Ankunft von ACKs

# End-to-End & Netzknotenüberwachung

- End-to-End-Überwachung
  - für jeden Netzteilnehmer möglich, z.B. per traceroute
  - von möglichst vielen Endknoten
  - Routing Loops nur sichtbar wenn eine der Verbindungen beeinträchtigt ist
  - keine Aussagen über Tragweite der Routing Loops möglich
  - aktiver Eingriff
  - sehr ungenau

# End-to-End & Netzknotenüberwachung

- Netzknotenüberwachung
  - nur schwer möglich, da an zentralen Routern
  - Zugriff auf die Header aller Pakete
  - Router im produktiven Einsatz, die Messung muss sich dem laufenden Betrieb unterordnen
  - politische und private Bedenken
  - lokal vollständiges Bild des Netzzustands
  - passives Beobachten
  - sehr genau

# Erzeugung von Replica Streams

- Ausschluß aller Pakete, die nur einmal vorkommen
- Ausschluß aller Pakete, die exakt zweimal auftreten, auch bei unterschiedlicher TTL (SONET, Token Ring)
- Zusammenfügen aller sich wiederholenden Pakete mit dekrementierender TTL, in deren Adresspräfix sich keine einmalig vorkommenden Pakete befinden (-> Tafel ;)

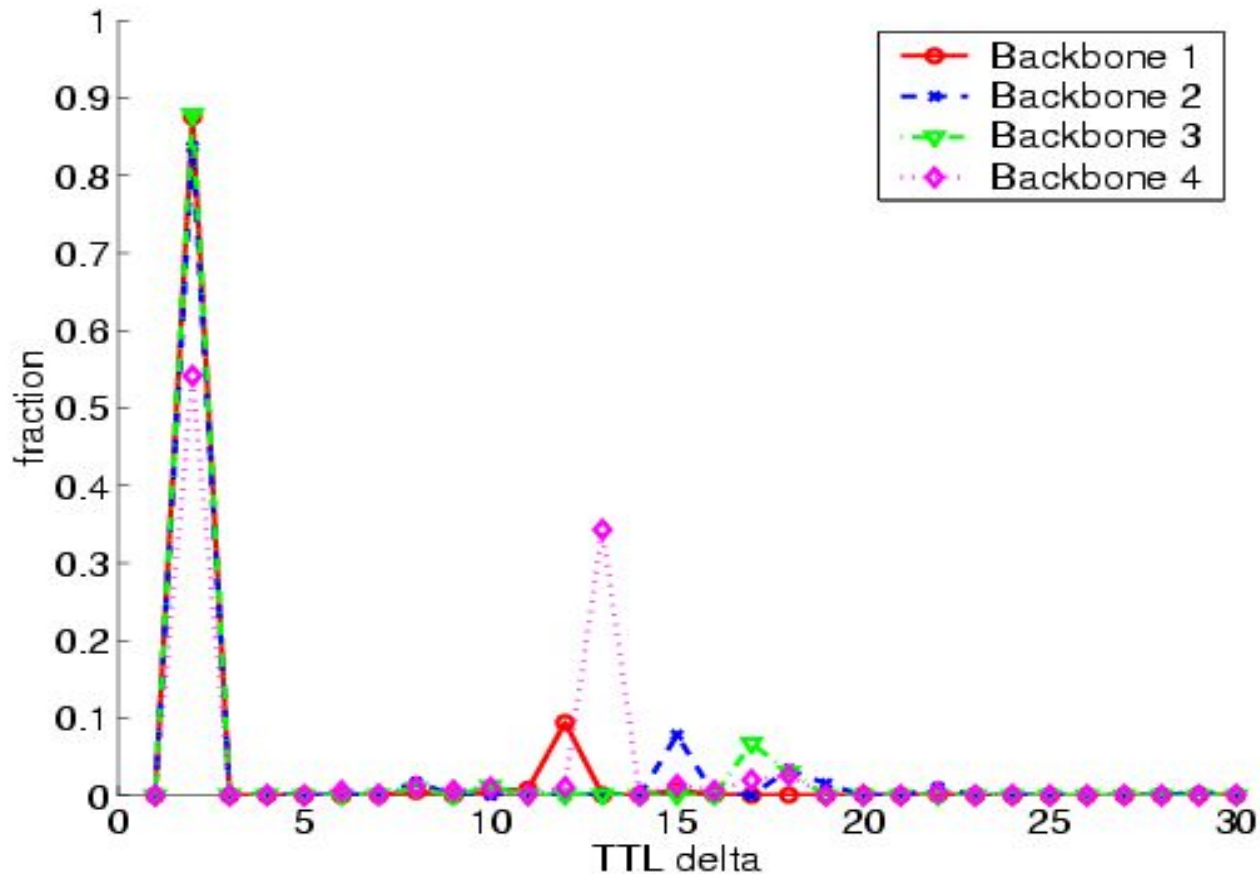
# Verwendete Daten

Trace	Stunden	Mb/s	Millionen Pakete	Paketzahl
Backbone 1	24	1	50	2419792
Backbone 2	1.5	243	1677	1987309
Backbone 3	11	2.2	20	337570
Backbone 4	11	107	1350	364230

# Betrachtung von Replica Streams

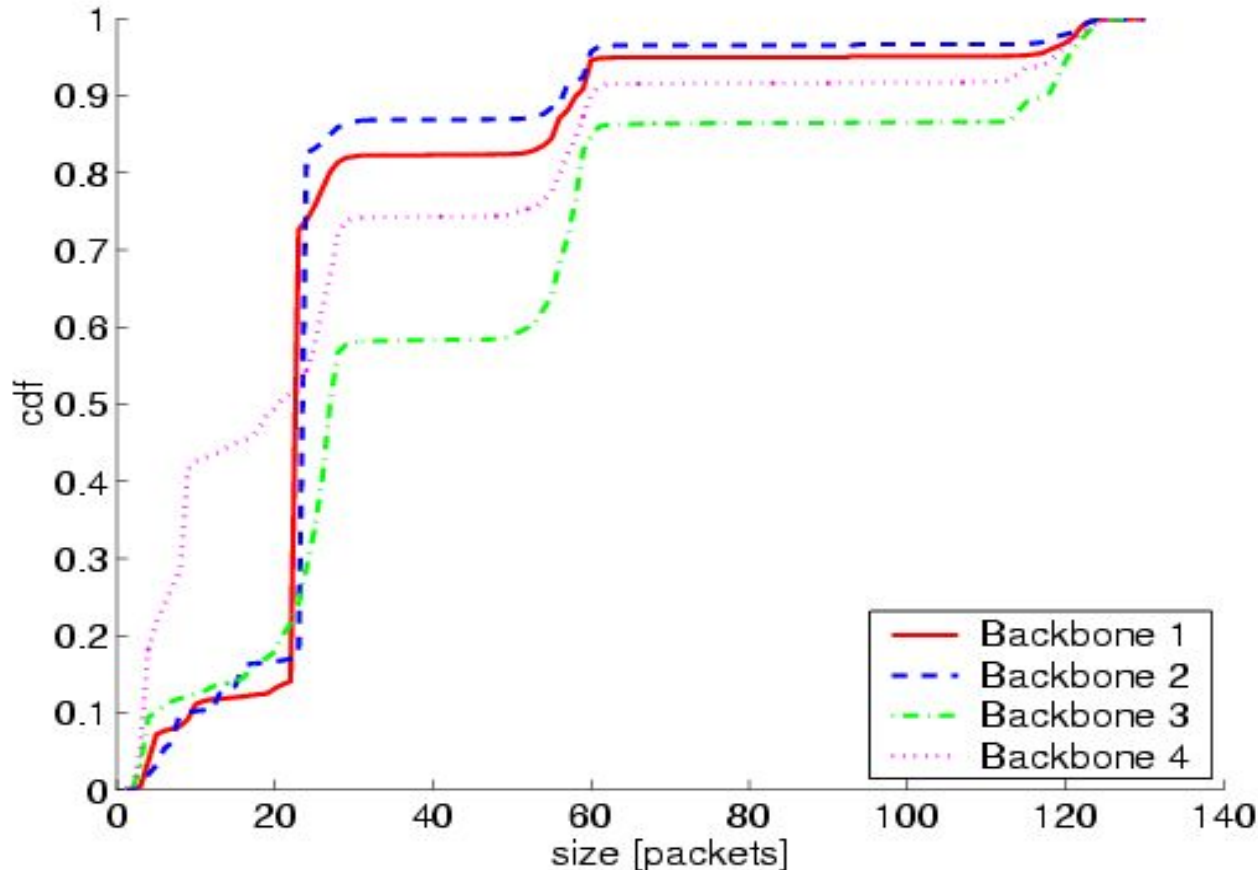
- drei Metriken
  - TTL Delta
  - Anzahl der Replica im Replica Stream
  - Zwischenankunftszeiten der Replica
- sonstige Betrachtungen
  - beeinflusster Verkehr
  - beeinträchtigte Zieladressen
  - Dauer der Routing Loops

# Ergebnisse



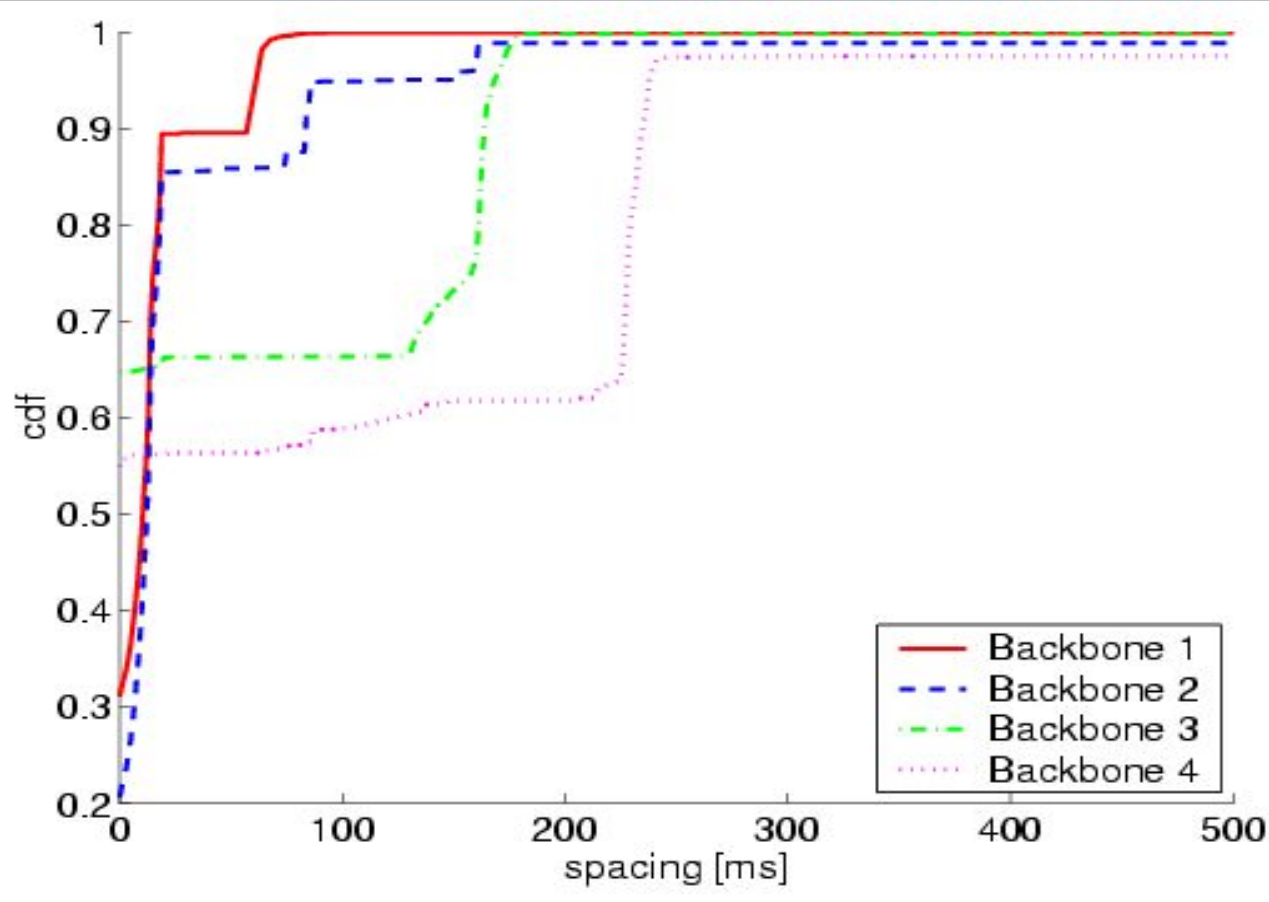
Die meisten Routing Loops haben eine Größe von zwei.

# Ergebnisse



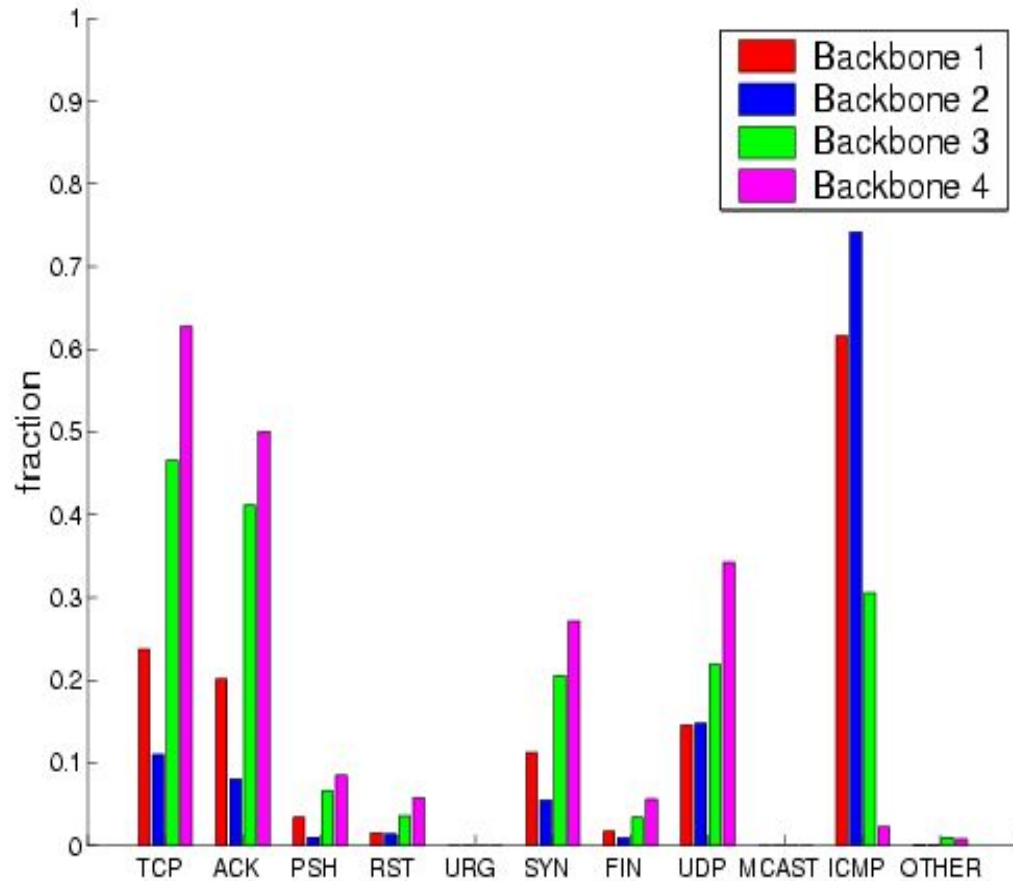
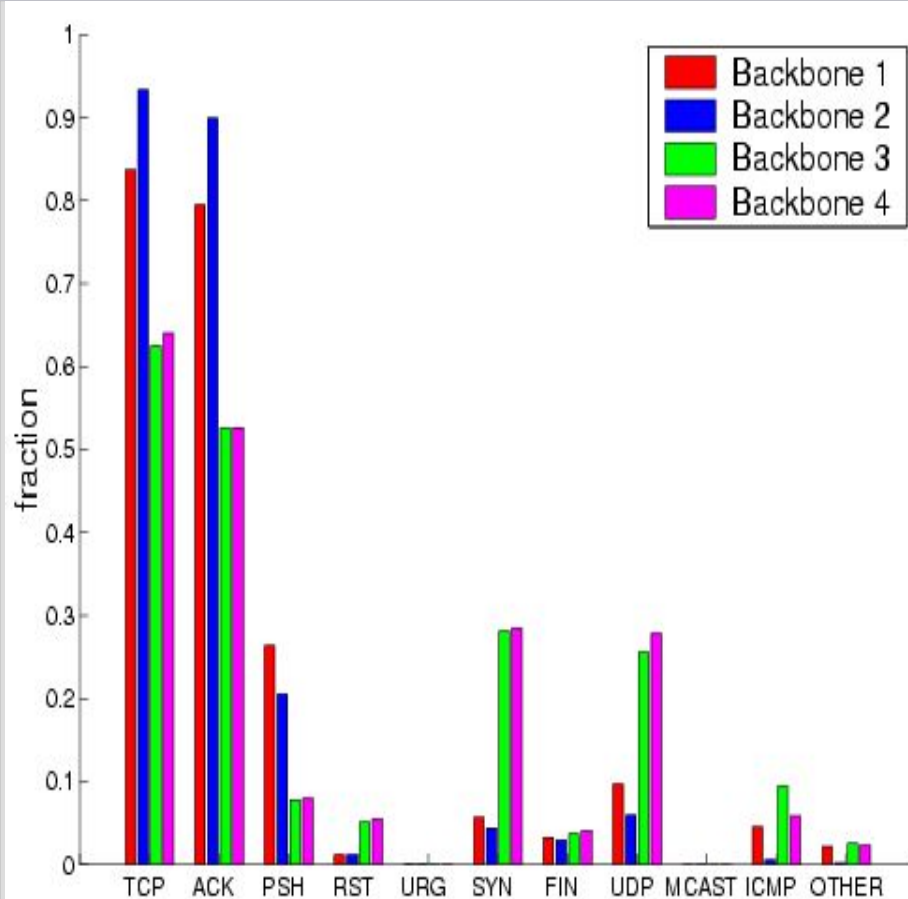
Die Sprünge bei  $\sim 23$  und 60 sind in den Standardwerten für die TTL bei Linux und Windows 2000 und der hauptsächlichsten Routing Loop Länge von 2 HOPs begründet.

# Ergebnisse

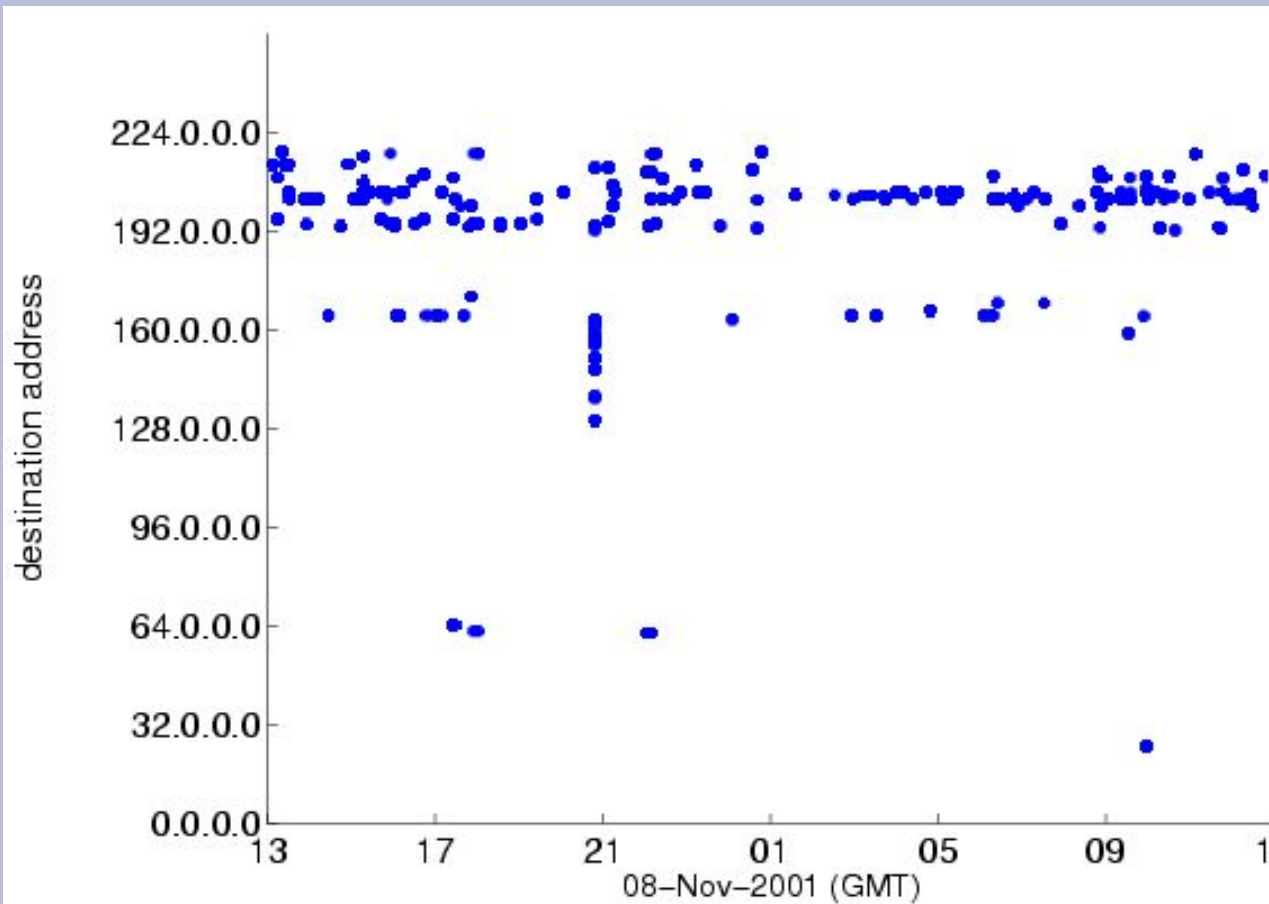


Knapp 90% der Replica aus BB 1 & 2 haben Zwischenan-kunftszeiten unter 20ms. Wieder hängen diese Ergebnisse direkt mit den dominanten TTL Deltas zusammen.

# Ergebnisse

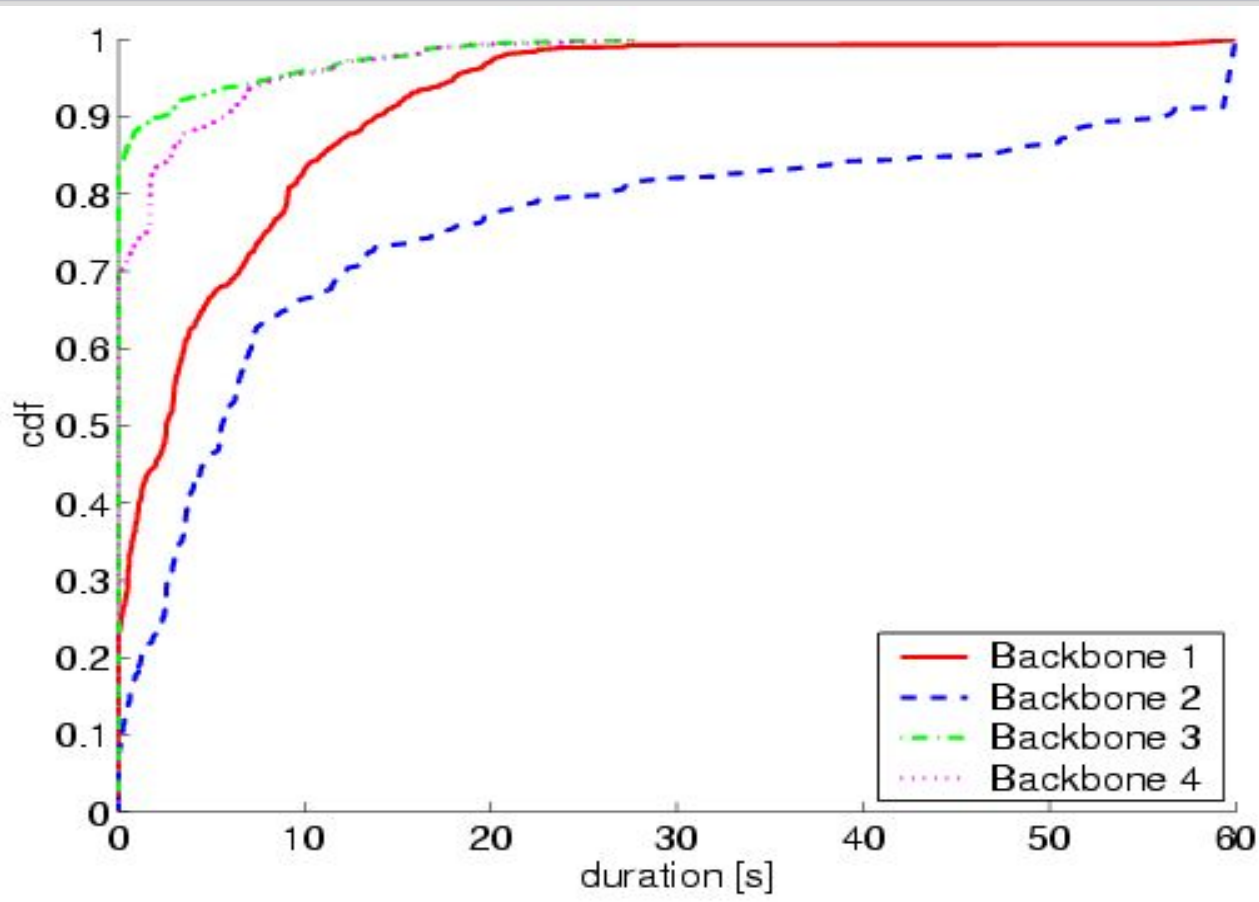


# Ergebnisse



Klasse C Netze  
(192.0.0.0 –  
223.255.255.255)  
unterliegen, bedingt  
durch die starke  
Nutzung und hohe  
Dynamik, den meisten  
Schwankungen.

# Ergebnisse



Der Großteil der Routing Loops endet nach 10-25 Sekunden.

# Zusammenfassung

- Die Erkennung von Routing Loops ist an den Routern besser als an den Knoten
  - exakter, ohne Netz-Overhead
- Auch transiente Routing Loops beeinträchtigen den Verkehr erheblich
- Die meisten Routing Loops sind klein

**Ende**

Fragen?