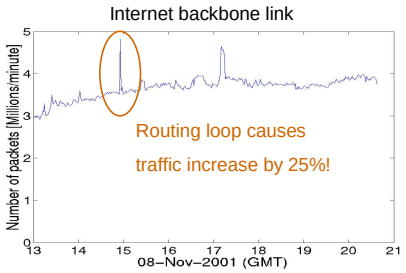
Detection and Analysis of Routing Loops in Packet Traces

IMW 2002

Urs Hengartner, Sue Moon,
Richard Mortier, Christophe Diot

Link Utilization

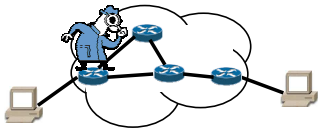


Contributions

- Offline algorithm for detecting routing loops in Internet traffic traces.
- Results of applying algorithm to backbone traffic traces.
  - How often do routing loops occur?
  - How long do they last?
  - How many packets do they affect?
  - Not: Why do they occur?

Loop Detection

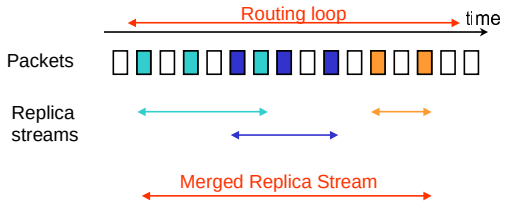
- How can we detect routing loops when looking at packets forwarded by a router?



Look for identical packets with decreasing TTL values!

Replica Stream

Loop Detection



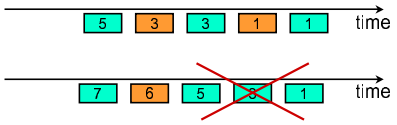
Merged replica stream approximates routing loop!

Detecting Replica Streams

- Replica stream:
  Single looped packet crossing a link multiple times.
- Packets P and Q are part of the same replica stream if
  - P = Q, except TTL and checksum fields
  - $TTL_P - TTL_Q \geq 2$.

Validating Replica Streams

- Goal: Discard streams not caused by routing loops.
- Verify that all packets to the same destination address prefix (/24) create replicas.



Merging Replica Streams

- Goal: Merge replica streams likely to be due to the same routing loop.
- Merging of replica streams with identical destination address prefixes
  - that overlap in time, or
  - that occur less than one minute apart (no not-looped packets to same prefix in-between).

Packet Traces

- Traces collected from links in Sprint's tier-1 Internet backbone.
- Collection dates:
  Nov 8, 2001 and Feb 3, 2002.
- Link capacities:
  OC-12 (622 Mbps) links.
- Each link connects two different ASs.

Packet Traces

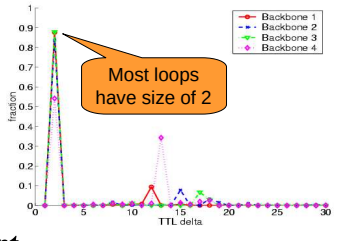
Trace	Length (hours)	Packets Total (10^6)	Looped Packets	Routing Loops
Backbone 1	24			852
Backbone 2				413
Backbone 3				1485
Backbone 4	11	1350	0.026%	1568

…loops occur in bursts and can affect up to 25% of packets!

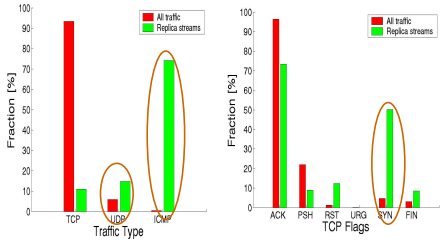
On average, loops do not affect much traffic, but…

Loop Size

Loop size corresponds to TTL delta.



Traffic Types (Backbone 2)

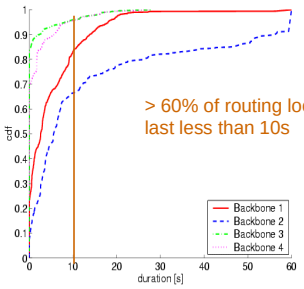


Reasons for Increases

- TCP SYN traffic
  - End point tries to open connection, sends SYN.
  - SYN loops and expires, no other packets are sent.
- UDP traffic
  - UDP is connectionless, no feedback from receiver.
  - Sending application is oblivious of loop.
- ICMP traffic
  - Caused by “traceroute” and “ping”.
  - People are exploring loop.

Observations confirm presence of loops!

Routing Loop Duration



> 60% of routing loops last less than 10s

Conclusions

- Routing loops can be detected and analyzed in packet traces.
- On the average, loops affect few packets.
- Loops are typically 2 hops and persist for <10 seconds.
- More detailed explanations require extending data collection techniques to include “complete” routing messages.