BGP: A Surprisingly Robust Distributed System

David Wetherall, Ratul Mahajan, and Tom Anderson
University of Washington.
Dogma: Good Protocols are Robust

- They tolerate failures well
  - e.g., routing protocols and link/node failures
- They follow design principles
  - e.g., soft-state with refresh
Reality: Most Protocols are Fragile

- Against insider faults
  - Implementation bug, configuration mistake, malicious attack
  - e.g., any ISP can hijack your IP connectivity
- There is a lack of design principles
  - Crypto (authentication), Byzantine consensus not a magic bullet
Our Research Agenda

- Study BGP (Internet routing) measurements to quantify screwups ⇐ this WIP
- Design better routing protocols
- Conquer the world
BGP: What (We Believe) We Found

• Many suspicious route announcements
  – Temporary de-aggregation (flood of routes instead of a trickle)
  – Globally visible typos, e.g., 701 710 701 445 3
  – Private ASNs/addresses (that should not be globally visible)
  – False origins, e.g., ISP A advertises routes from ISP B as its own
  – Customers leaking provider routes (inadvertent transit)

• It’s a mess out there:
  – Screwups add significant routing load
  – Screwups change forwarding paths
Yet BGP is Surprisingly Robust

• Despite screwups there is little loss of connectivity
  – With a few exceptions (actual hijacks)
• Plus, BGP contains a “defense” that mitigates the effects of serious screwups that do occur
  – Route flap damping suppresses regions of instability

• Conclusions?
  – Focus on containing the impact of faults
  – Prevention and detection isn’t enough