How to debug, protect and improve Internet routing?

Z. Morley Mao

Can our routing protocols survive the future?

- Growing number of routing and data plane attacks
- More multi-homed customers
- Increasing edge-based load-balancing
- Overlay networks
- Increasing complexity, e.g., MPLS
- Higher demands for scalability
  - E.g., IPv6

How to debug the routing system?

- Build routing assertions
  - What’s expected? Nothing fails silently
- Cooperation among ISPs
  - Traffic engineering
  - Predictability, debugging
- Public distributed measurement and measurement calibrations
  - Establish guidelines to interpret the measurement data

How to debug the routing system?

- Internet-wide emulation for network configurations
  - Is the network configuration on the verge of instability?
- Understanding routing protocol interactions and implementation variants
  - Tradeoff of increased communication between protocols
- Get application-layer view
  - Impact of packet filters, router filters

How to improve application performance?

- Correlate routing with forwarding plane
- Evaluate using application performance metrics
  - Delay, loss rate, jitter, reordering, etc.
- Stop treating Internet as a black box

How to protect the routing system?

- Understanding vendor implementations
  - Impact of “default” configurations
  - Deviations from specs
- Understanding vulnerability points on the Internet
- Understanding interaction with transport protocols
- Higher priority for routing traffic
- Automated dynamic installation of packet and route filters
  - Coordination across networks
Routing system is inherently NOT end-to-end!

- Destination-based, hop-by-hop, best-effort, multiple autonomous networks
- Consequences:
  - Who is to blame when things go wrong?
    - No accountability, predictability
  - Where is the problem? Edge vs. core
  - What is the problem? Routing vs. data plane vs. application
  - No guaranteed support for real-time applications
    - Online gaming, voice over IP, video conferencing
  - Transient routing problems abundant

How do we deal with it today?

- Routing system is mostly treated as a black box
- Applications do their best to adapt independent of ISPs
  - Application:
    - Time out to infer failures
    - Buffering, error-correction codes
  - Overlay networks
  - Multi-homing, edge-based load-balancing
    - Still limited in number of providers
    - When to choose what provider?

Desirable properties

- Predictability, constancy
- Metrics:
  - Delay, loss rate, jitter, reordering
  - Resilience to traffic variations, routing configuration changes
  - Accountability, visibility when things break!
  - Low convergence delay
    - Not complete picture
    - What about forwarding loops? Dropped packets?

Application is the king

- Need to evaluate routing protocols in the context of applications
- Should there be more control at the end users?
- What is the right interface for users?
- Lack of incentive to provide QoS?
- One idea: auction-based scheme for QoS-sensitive applications
  - Multiple ISPs bid for providing guaranteed service quality, users pick.
  - At TCP connection level
  - Dynamic peering relationships

How content are the packets?

Randy Bush
Christophe Diot
Olaf Maennel
Morley Mao
What is end-to-end routing?
- Internet routing is not end-to-end
  - Destination-based, hop-by-hop, multiple networks
- Our definition
  - How inter- and intra-domain routing protocols affect the data plane
  - End-to-end application performance – happy packets

How to measure happy packets?
- We have well-developed metrics
  - IPPM: IP Performance Metrics Working Group
    - Connectivity
    - One-way delay and loss
    - Round-trip delay and loss
    - Delay variation
    - Loss patterns
    - Packet reordering
    - Bulk transport capacity
    - Link bandwidth capacity

Why are packets unhappy?
- Possible causes:
  - Protocol designs, unexpected protocol interaction, misconfigurations, congestion, worms, attacks
- Areas of study:
  - Protocol issues
  - Vendor implementation
  - Router configuration
  - External events

What to measure to test our conjecture?
- Data plane measurements
  - Continuous monitoring of large interesting sites
  - E.g., RIPE’s Test Traffic measurement, PACTUM
- Device level testing
  - Box level router testing
  - E.g., switch-over time: how long FIB is updated given a routing change

Food for thought...
- What measurement data are ISPs willing to provide?
  - Each ISP monitoring its own network
  - Inter-ISP routing data exchange
  - Where can we place measurement probes?
  - Planetlab as a measurement platform