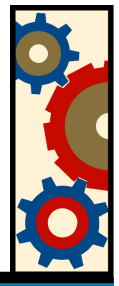
Software and DNS operations at ISC What's new?

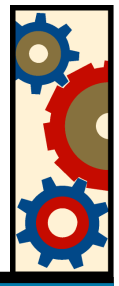
João Damas
ISC

Outline



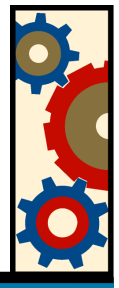
- BIND
- Operations
  - earthquake
  - DDoS

Current BIND versions



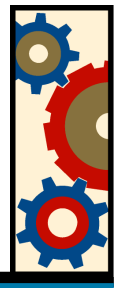
- Current versions of BIND are:
  - Releases: 9.4.0, 9.3.4, 8.4.7
  - Testing: 9.5.0a1

BIND 9.4



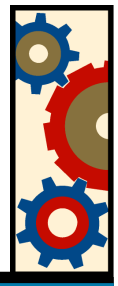
- BIND 9.4 includes a few radical new features and needs exhaustive testing
  - Its performance is much better than that of previews BIND 9 releases.
    - Additional cache
    - Architecture dependant lock relief using atomic operation support

Ongoing work



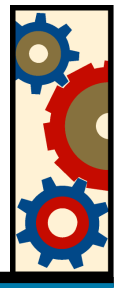
- Things we are working on
  - GSS-TSIG
  - NSEC3
  - New hash support (SHA-256)
  - New resolver library
  - Better, more complete stats and new way of fetching them

GSS-TSIG



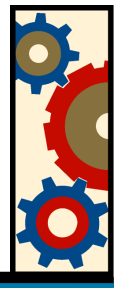
- Work started 2 years ago but stumbled on implementation incompatibilities and fuzzy standard interpretation
- Currently finalising details for running on Windows, though it already interoperates with MS Active directory. Just run it on Unix-like OSes.

NSEC3



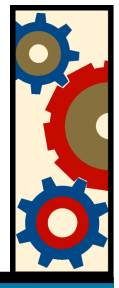
- This is an example of the work ISC does to implement early standards work into BIND to enable analysis of the work in progress
- Work is being sponsored by Verisign and Nominet

SHA-256



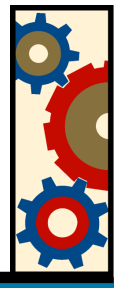
- With the current call on IETF to initiate migration to stronger (than SHA-1) hashes, ISC has implemented SHA-256 in BIND

New resolver library



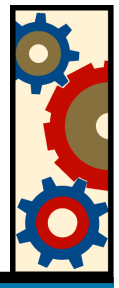
- Work initially undertaken by Jinmei Tatuya of Toshiba, working at ISC
- Will be used first in conjunction with ISC DHCP
- Current work on integration is ongoing

Other stuff



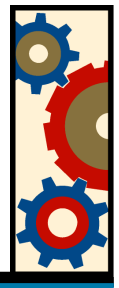
- ISC support: BIND & DHCP
- ISC BIND training
  - First in USA, then Europe,...
  - Based on Johan Ihren's training material

DNS operations



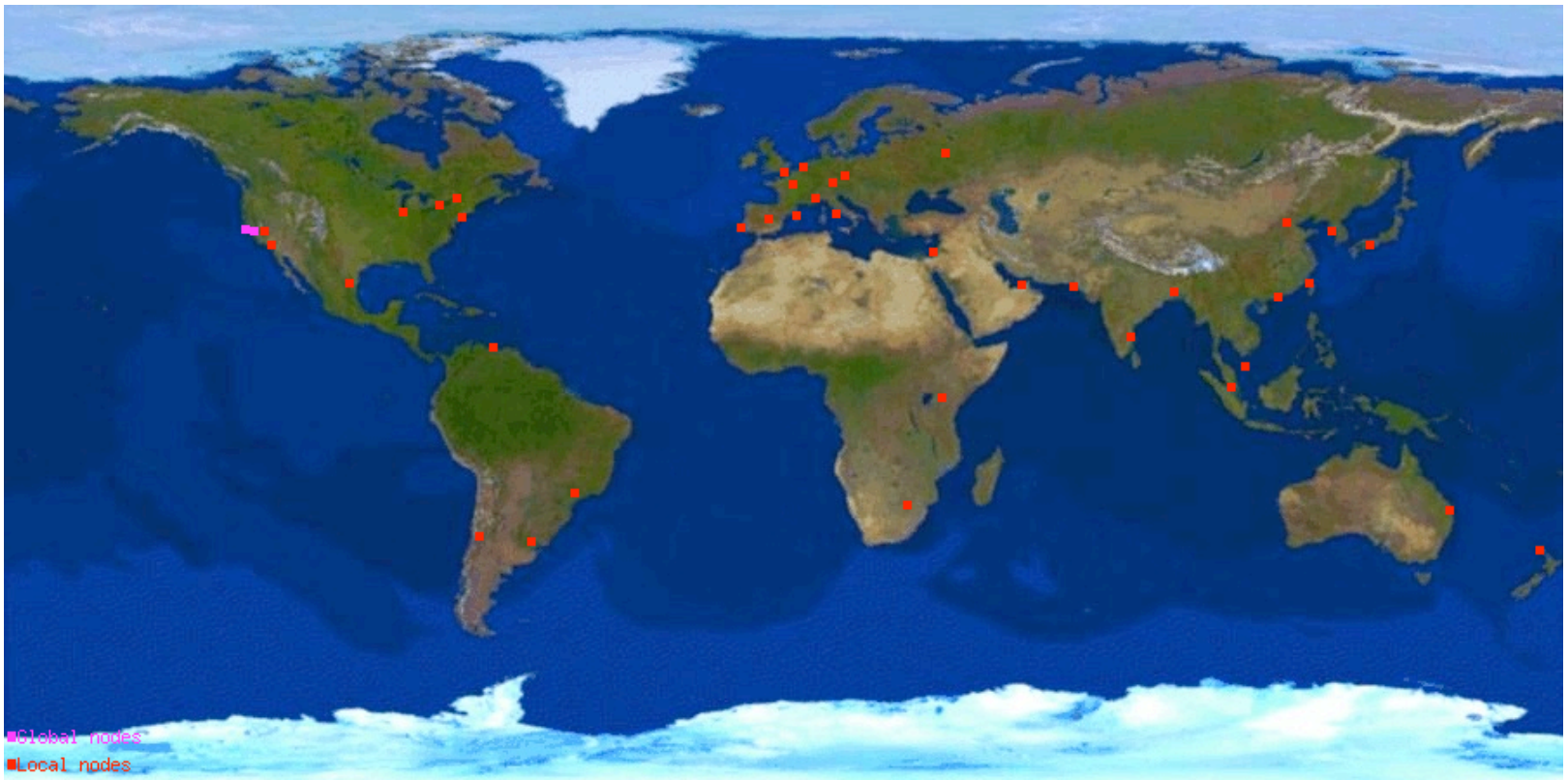
- ns-ext/ns-any
  - ns-ext.isc.org == ns-ext.vix.com
- Secondary service for TLDs or public interest SLDs
  - Free on best effort basis
  - Fee based if SLA required
- Now going to anycast.
  - Each zone operator can tell us if they wish to use the anycast or unicast service.

DNS Operations - F root

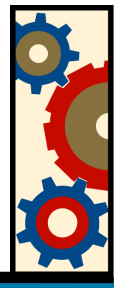


- More, better, faster :)
- Recent anycast nodes added
  - Caracas
- Looking to install in Fiji very soon
- Agreement with Neustar to install on their DNS Shield product

Nice picture

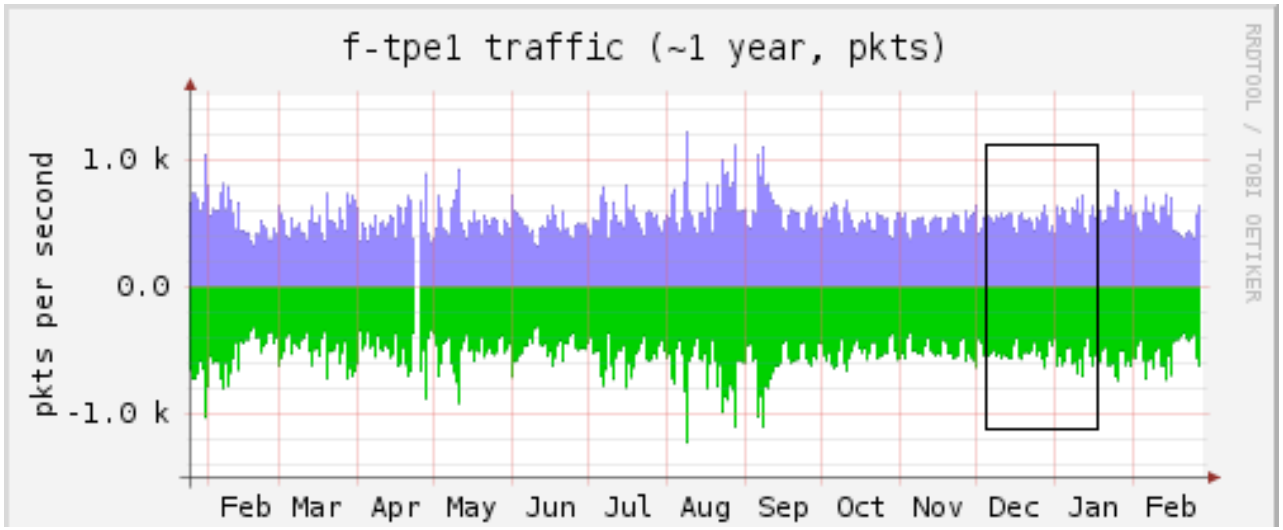


What is this good for?

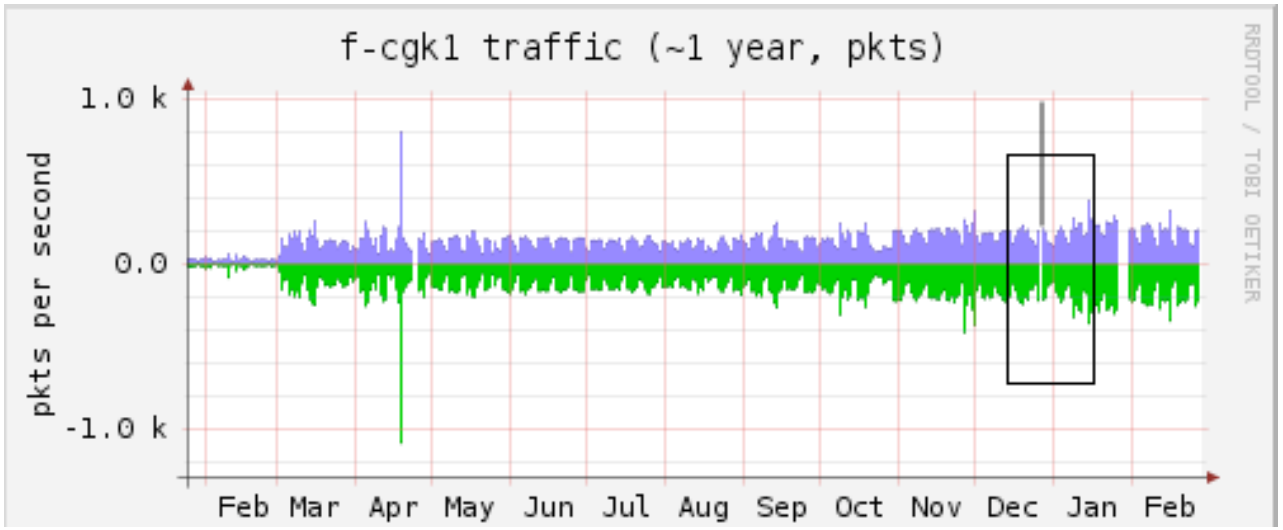


- Examples:
  - Taiwan earthquake
  - DDoS 6 February 2007

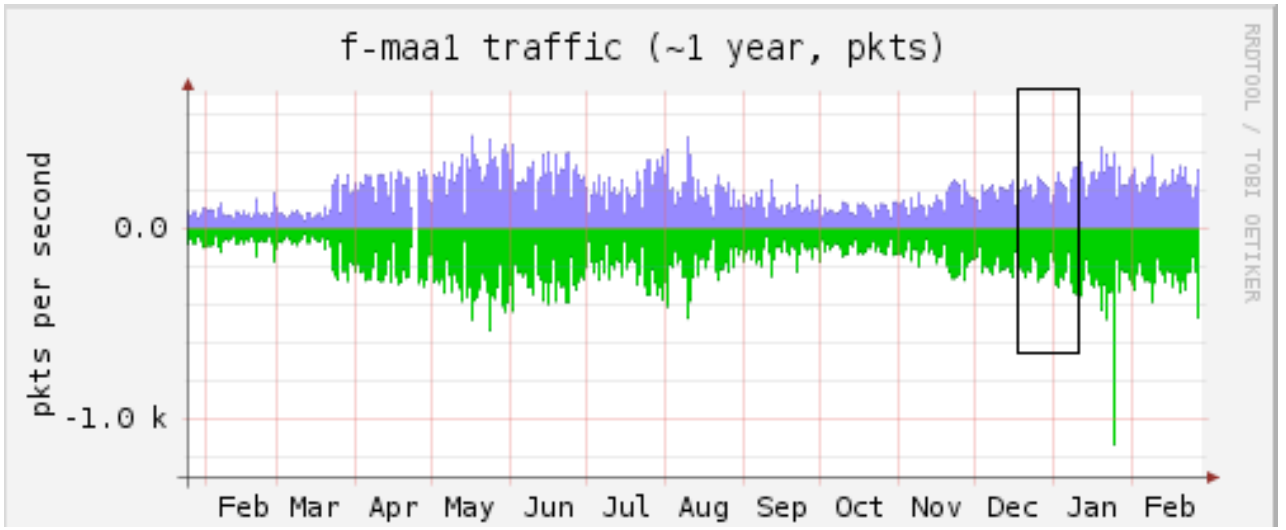
Taiwan earthquake



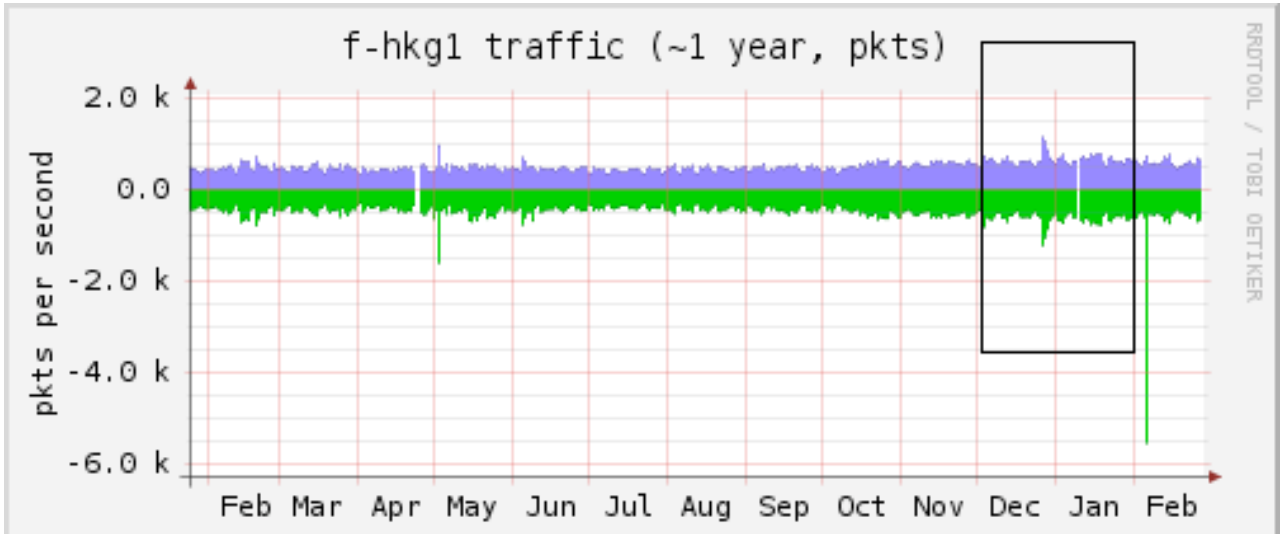
Taiwan earthquake



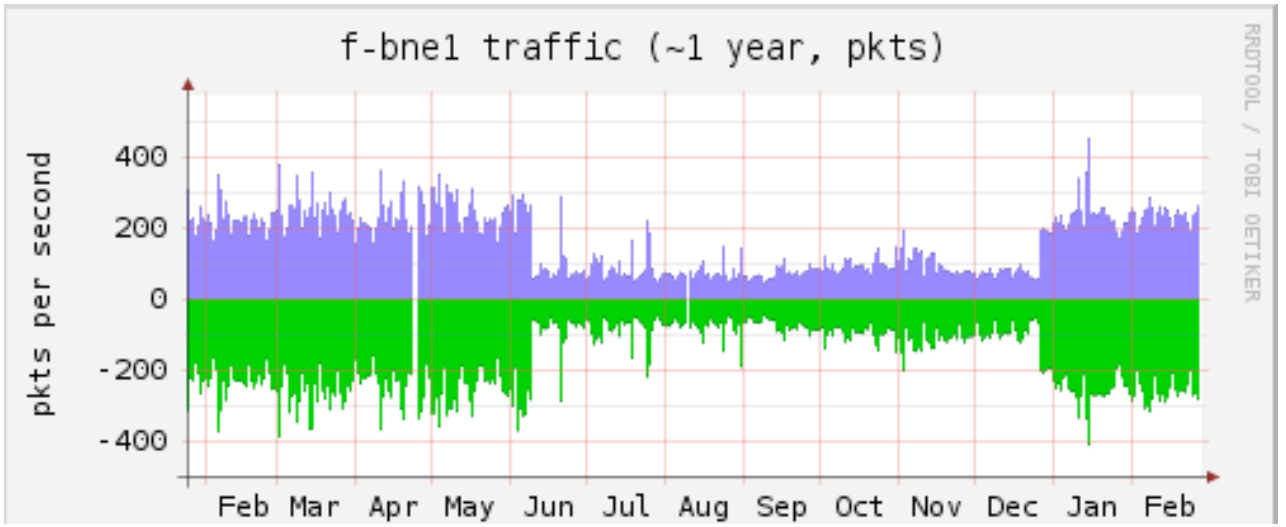
Taiwan earthquake



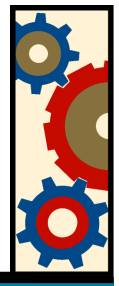
Taiwan earthquake



Taiwan earthquake

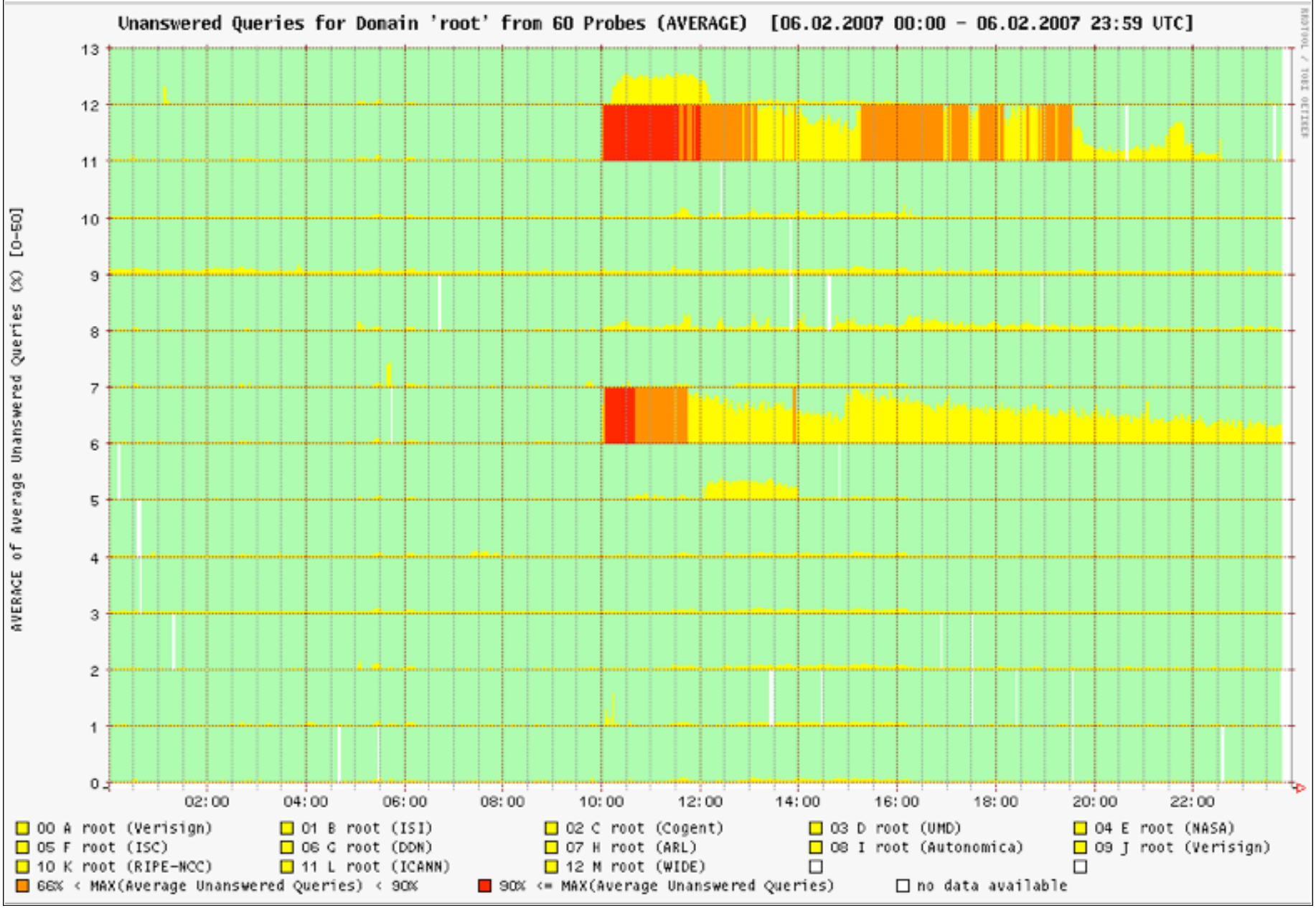


February DDoS

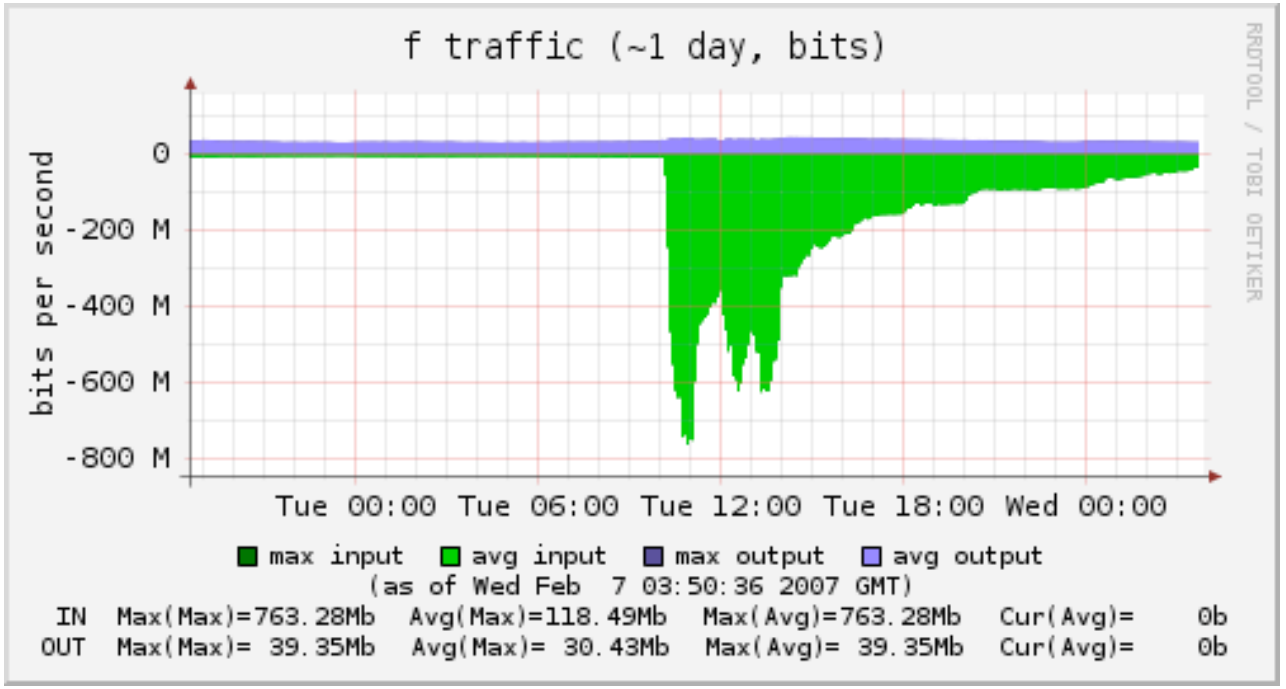


A number of the Internet root and TLD name servers sustained a DDoS attack. While this attack didn't have an impact on the service to end-users it was measured and we'll share the preliminary observations made at F-root including the type, quantity and distribution of attack traffic and how we coped.

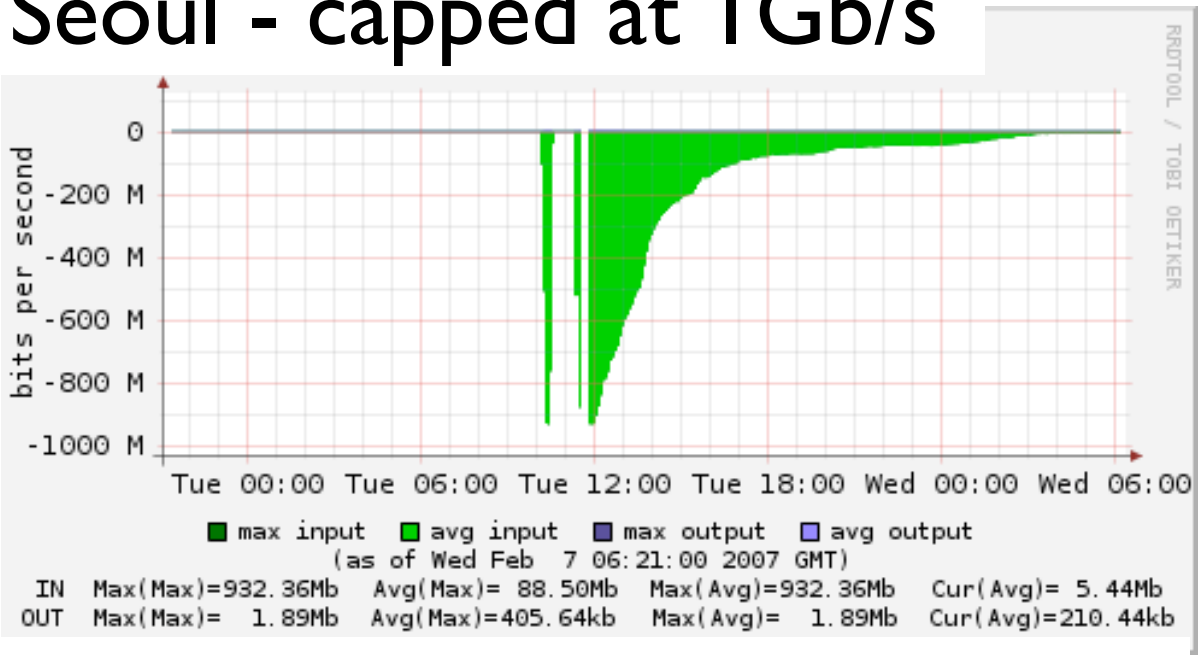
http://dnsmon.ripe.net



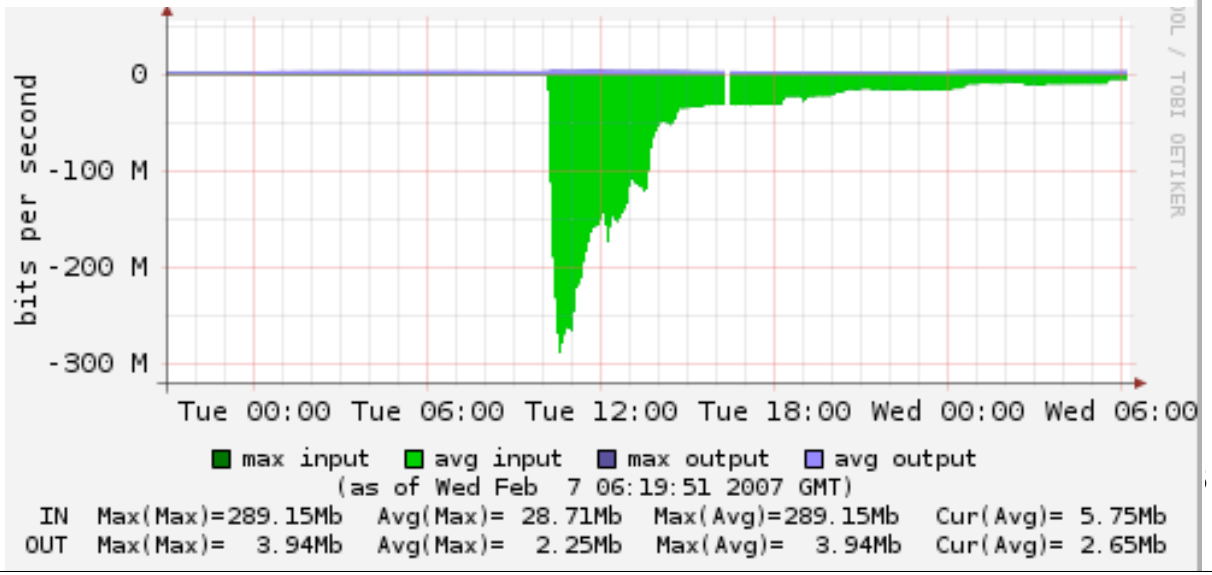
Aggregated traffic on F root



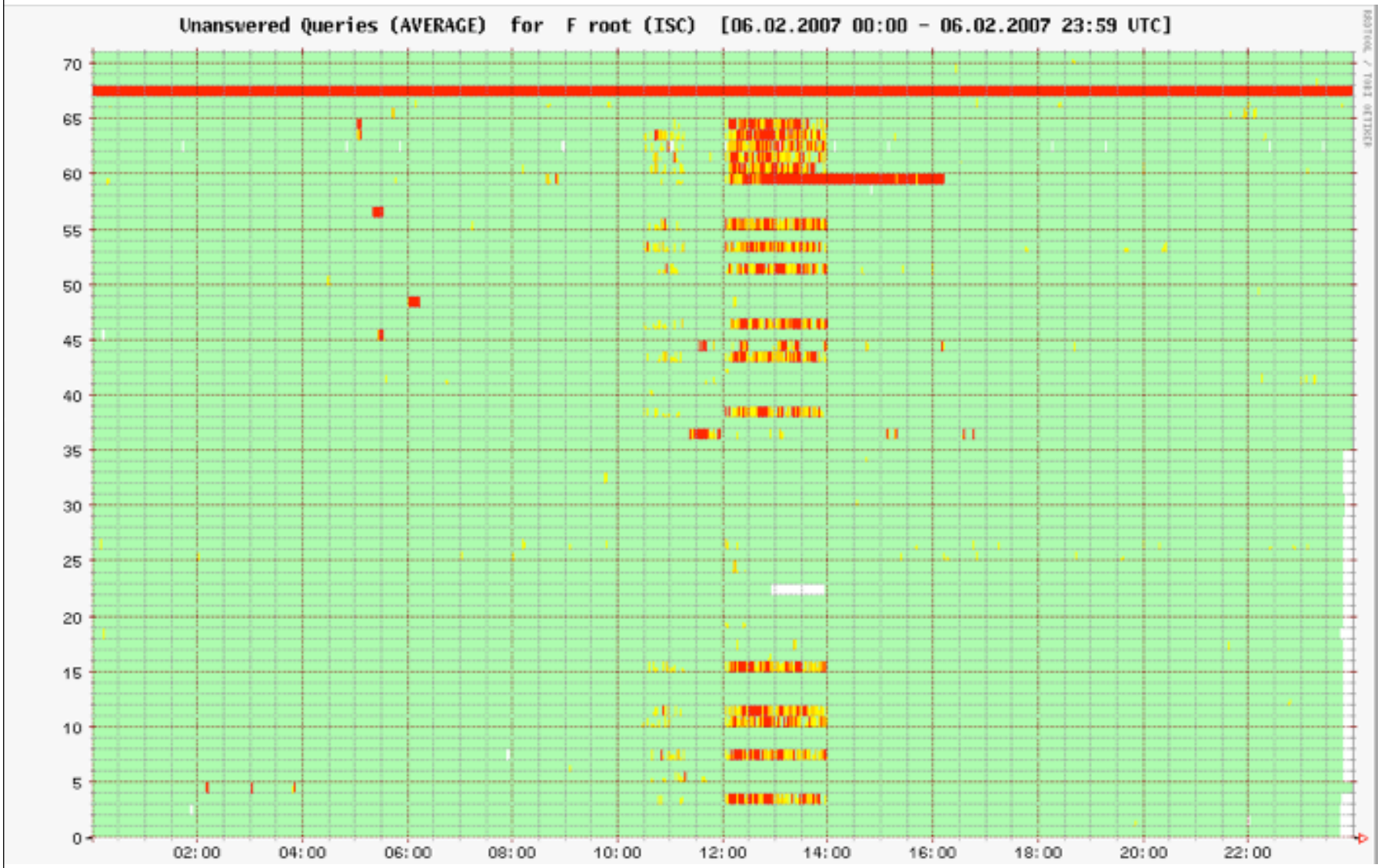
Seoul - capped at 1Gb/s



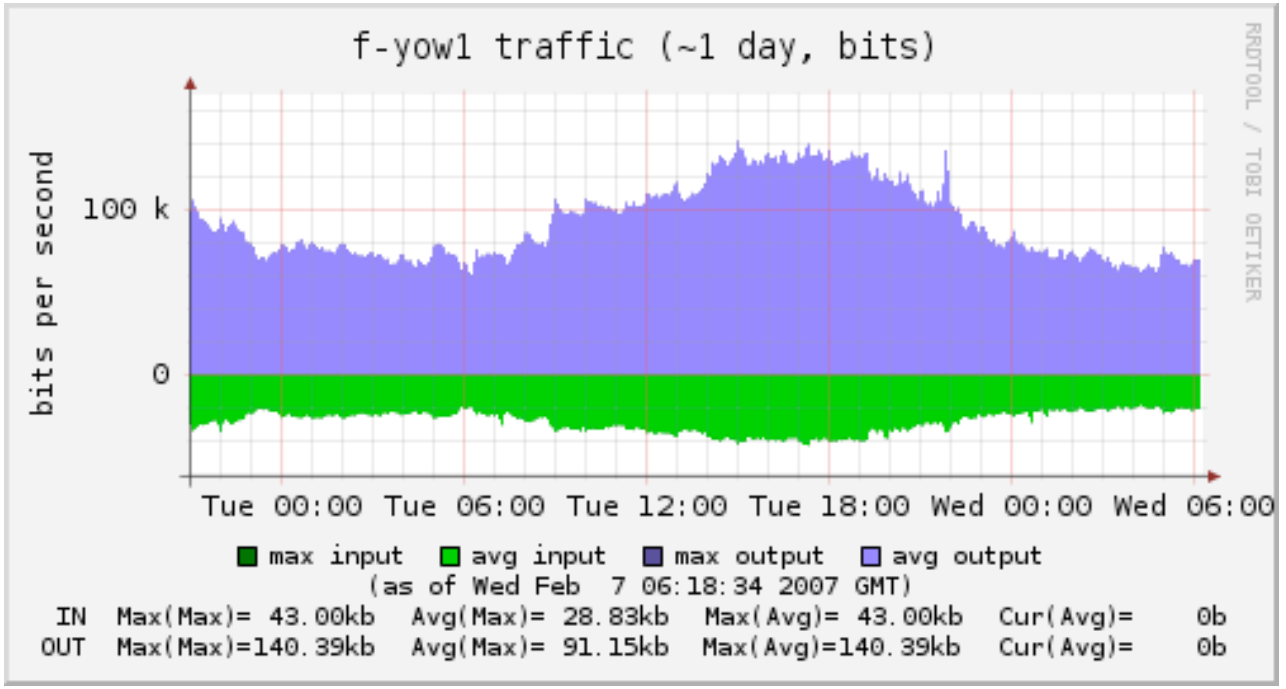
Beijing - peaked at 300Mb/s



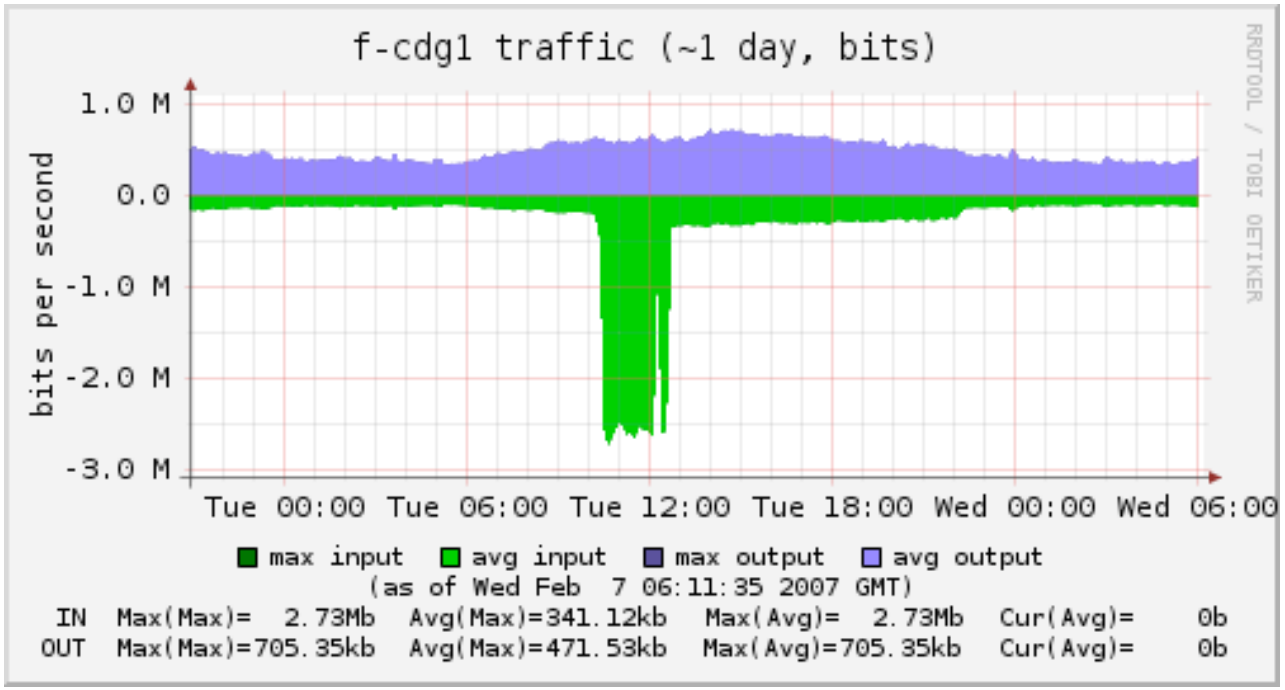
Service impact

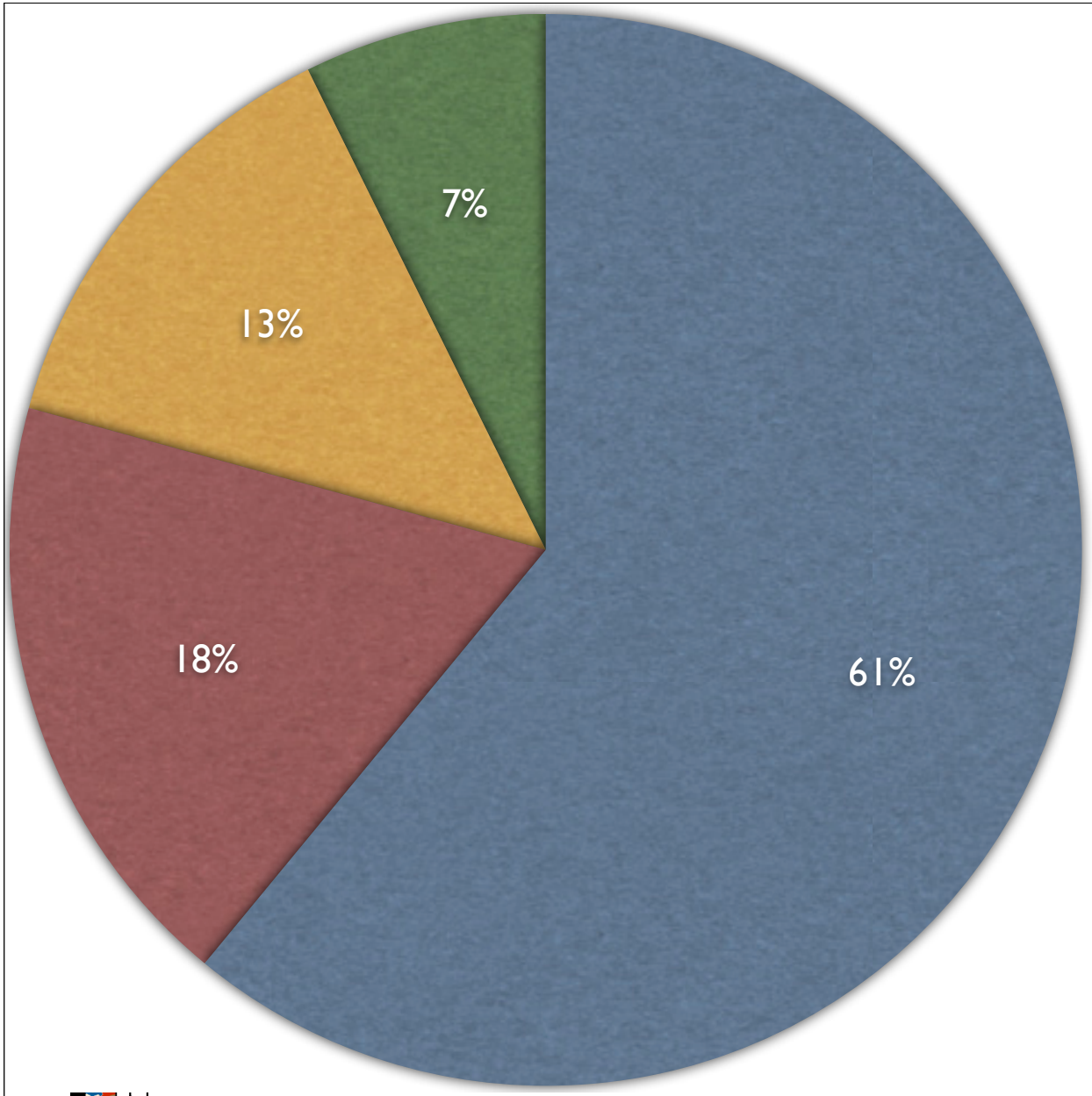


Some nodes got nothing



Others saw peculiar patterns

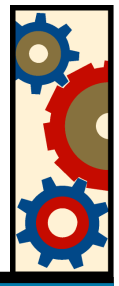




Seoul
Beijing
San Francisco
Other

Other equates to 35 F-root anycast nodes

Packet analysis



- Average size was bigger than normal traffic
- Most were more than 350 bytes
- Some were malformed DNS messages
- Contained random QTYPEs (updates, unknown, etc)

Questions?