IRNC-SP: Sustainable data-handling and analysis methodologies for the IRNC networks

PI: k claffy

CAIDA/UCSD
NSF – IRNC PI Meeting

Honolulu, HI
17 January 2013

Overview/Summary

We seek to improve availability of operational network data for the research community.

(1) foster and distill discussion of how to best make IRNC data and statistics available,

(2) adapt two CAIDA measurement technologies for IRNC community needs, and

(3) experiment with two innovations in data-handling procedures applied to existing IRNC measurements.

Current Status

- Ark active measurement infrastructure
  - 63 deployed monitors, 28 w/ IPv6

•monitors associated with the IRNC rolodex

  - sao-br2 Sao Paulo, Brazil, Rede ANSP / Projeto NARA
  - syd-au Syndey, Australia, AARNET
  - per-au Perth, Australia, AARNET
  - bjl-gm Serrekunda, GM, QCell
  - hnl-us Honolulu, HI, US, University of Hawaii

- Passive measurement infrastructure
  - AMPATH, Florida International University
    - Coralreef measurements and report generator
      - Customizations for reporting top AS flows

Note of thanks

We want to thank Von Welch, Doug Pearson, Brian Tierney, and Jim Wiliams for organizing and hosting the Security at the Cyberborder Workshop.

The workshop offered an honest discussion of the realities and challenges of measurement and, in particular, sharing of operational IRNC ProNet data.

Coralreef

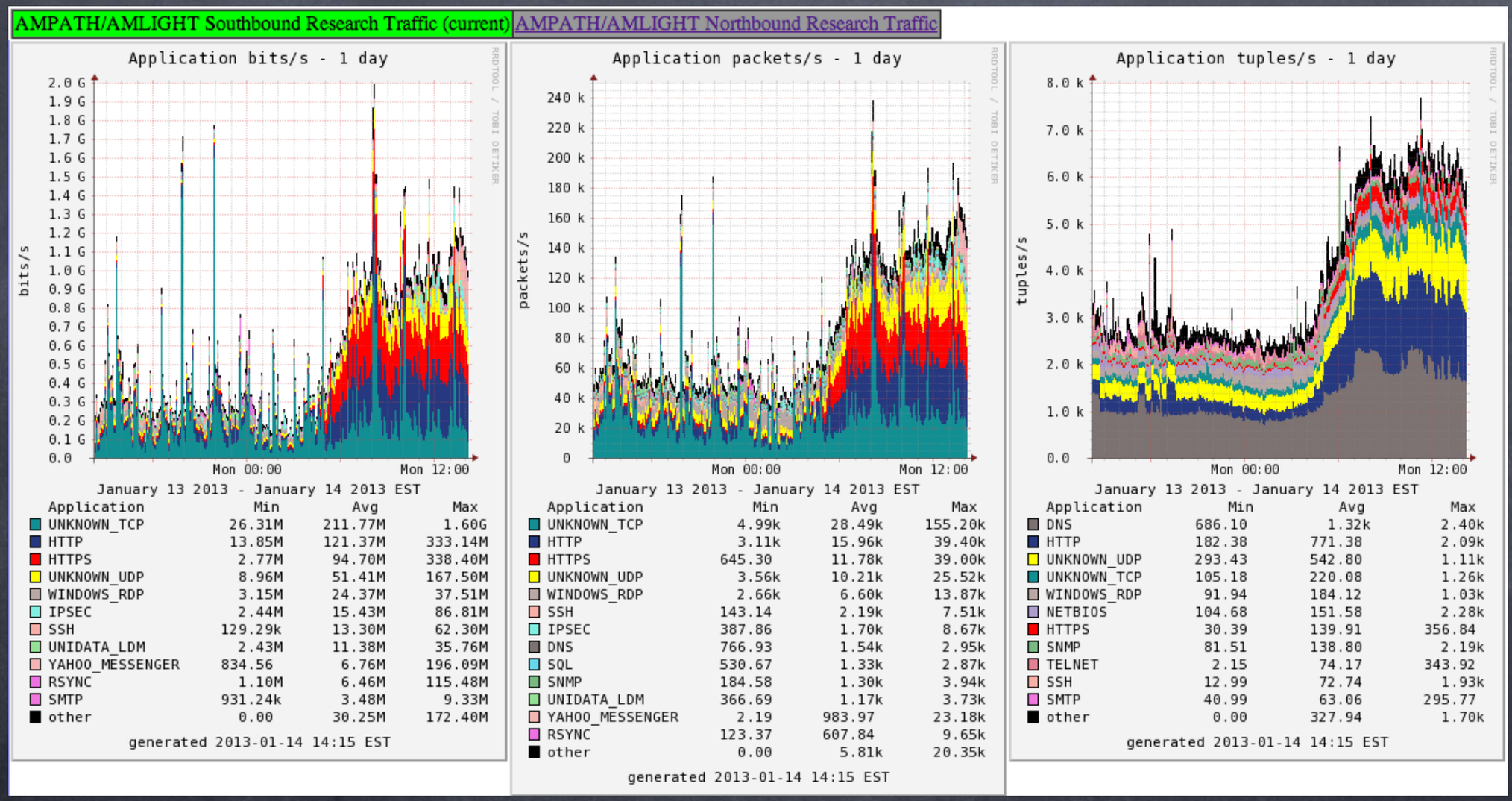
CoralReef Improvements:

- added IPv6 support to crl_flow (an app that counts packets, bytes, and flows, and is used as the back end to the report generator)
- added IPv6 support to crl_anf (a faster alternative to crl_flow that samples packets)
- improved decoding (printing) of IPv6 headers
- Working with Julio Ibarra and James Grace, added src/dest pairs sorted by volume
- netflow import to report generator

Coralreef (cont)

- added IPv6 address anonymization
  - prefix preserving anonymization with generalized Crypto-PAn algorithm
  - or zero-out some or all bits of address
  - option to apply IPv4 anonymization policy to IPv4 addresses embedded within IPv6 addresses (IPv4-mapped, SIIT, Teredo, 6to4, 6over4, ISATAP)
  - option to leave multicast addresses intact
  - anonoymizes IP addresses not just in the top IP header, but also in nested headers (e.g., IPIP, or the original IP header in an ICMP error message)
  - In unreleased Coralreef 3.9.0

Coralreef (cont)



http://coralreef.ampath.net/cgi-bin/display_report

Other Links

- IRNC-SP: Sustainable data-handling and analysis methodologies for the IRNC networks
http://www.caida.org/funding/irnc/

- Archipelago (Ark) network measurement platform
http://www.caida.org/projects/ark/

- Archipelago Monitor Statistics
http://www.caida.org/projects/ark/statistics/

- Coralreef
http://www.caida.org/tools/measurement/coralreef/

- New Raspberry Pi monitor platform
http://www.caida.org/projects/ark/ark-raspi-monitor-20130102.png