coral

a flexible platform for passive network monitoring

kc@caida.org

outline

- niche in ‘measurement space’
- hardware
- collection software
- analysis software
- manageability and future
- conclusions

niche in measurement space

- non–intrusive, passive monitoring
- full trace capture or summaries
- user modifiable
- analysis: real time or from traces
- unix (or dos) host, external to router

hardware

- passive fiber monitoring
  - optical splitter
  - collection on interface cards
  - non-intrusive, no performance impact
- ocXmon (mci)
  - atm aal5, oc3, oc12 -> oc48
  - subsets of packets: 1,2,3,last,all cells
- other related implementations
  - ds3mon, other ocNmon, "tcpdump"

collection software

- platforms: Unix and DOS
- raw packet traces
- flows collection
  - packet train (timeout) definition
  - flows analysis on host
  - support for different encapsulations
  - OS impact not determined

analysis software

- flows based
  - basic traffic characterization
  - AS matrices
  - country matrices
  - traffic import and export
  - routing/address space coverage
- non-flows based
  - interarrival time behavior
  - protocol-relevant (dups, packet sizes)
  - security/vulnerability protection

analysis s/w:

- interarrival times
  - packet run lengths
  - interarrival time distributions
- protocol-relevant
  - TCP: retransmissions/dup acks
  - packet size distributions
- security related
  - DOS attack traces
  - on-card kernel packet filtering, a la bpf

standalone vs in-router module

- in-router limitations
  - need external nearby host w disk
    - anyone have stats on flows/sec?
  - effect on forwarding
    - point of failure in network
    - upgrades mean network downtime
- in-router advantages
  - already in box
  - commercial support
  - can do > 1 i/f
- other issues
    - src code control
    - payload sniffing
    - UDP export
    - benchmarking/calibration (cross-router)

future needs

h/w
- POS for oc3 & oc12
- OC48 version

manageability
- easy installation
- other link-level encapsulations (POS, ???)
- automation
- security
- integrate w active/routing data sources

use
- plug-n-play features
- analysis software
- technical support for h/w

conclusions

coral: flexible standalone framework
for doing network measurement

community participation
in development welcome

coral-dev@caida.org

acknowledgments

- MCI: Joel Apisdorf, Kevin Thompson, Keith Burden
- NLANR: Hans-Werner Braun
- CAIDA: k claffy, Sean McCreary, Mike Tesch, Brad Huffaker, David Moore

- lots of external collaborators