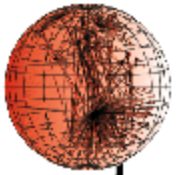


predictability of high performance networks: monitoring, analysis, & visualization

DARPA ITO PI meeting, 15–17 december 1999

scientific apparatus offers a window to knowledge,
but as they grow more elaborate,
scientists spend ever more time washing the windows.
-- Isaac Asimov

kc claffy, UCSD/SDSC/CAIDA
kc@caida.org
www.caida.org

focus

- advance capacity to monitor, depict and predict traffic behavior on current and advanced networks
- identify traffic anomalies in real time

how

- develop/deploy tools (coral oc48, skitter) to better engineer and operate networks
- analysis and visualization of data
- develop security features for coral OC3/12 monitors

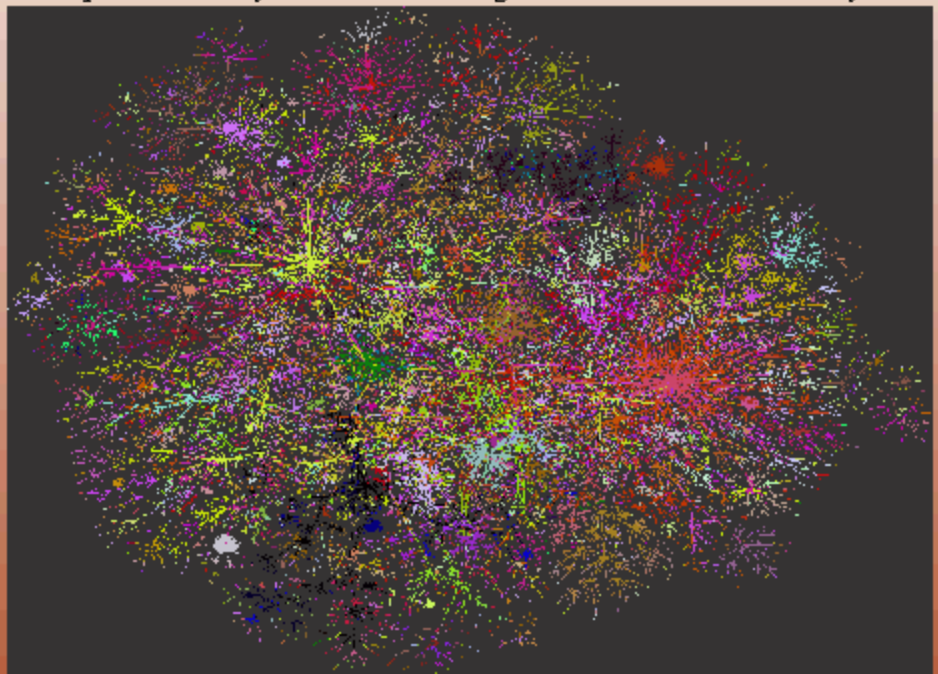
infrastructure–wide measurem't & analysis

- topology (mapping)
- workload characterization (passive)
- performance evaluation (active)
- routing (dynamics)

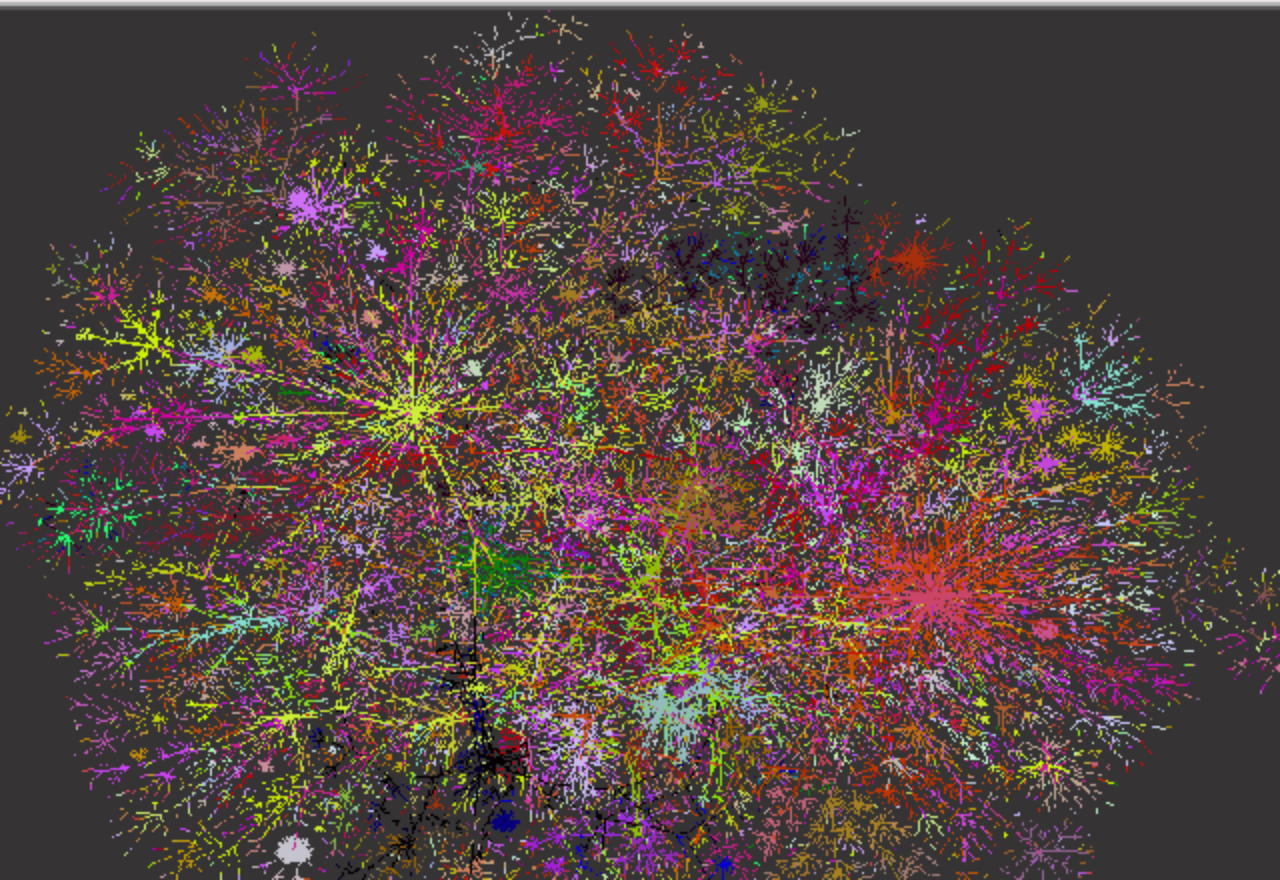
skitter: macroscopic topology mapping

- 18 monitors (inc. 1 root name server)
- multiple dest. lists 29k servers/36k root clients
- 52–byte ICMP probes, kernel timestamps, ssh/kerberos
- goal: insights into inter–SP connectivity, routing, perf.

updated daily: www.caida.org/Tools/Skitter/Summary/

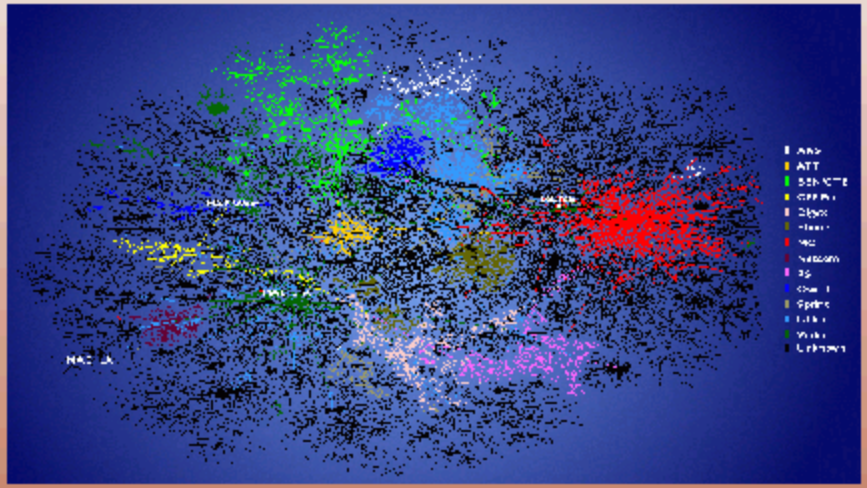


skitter: colored by IP address

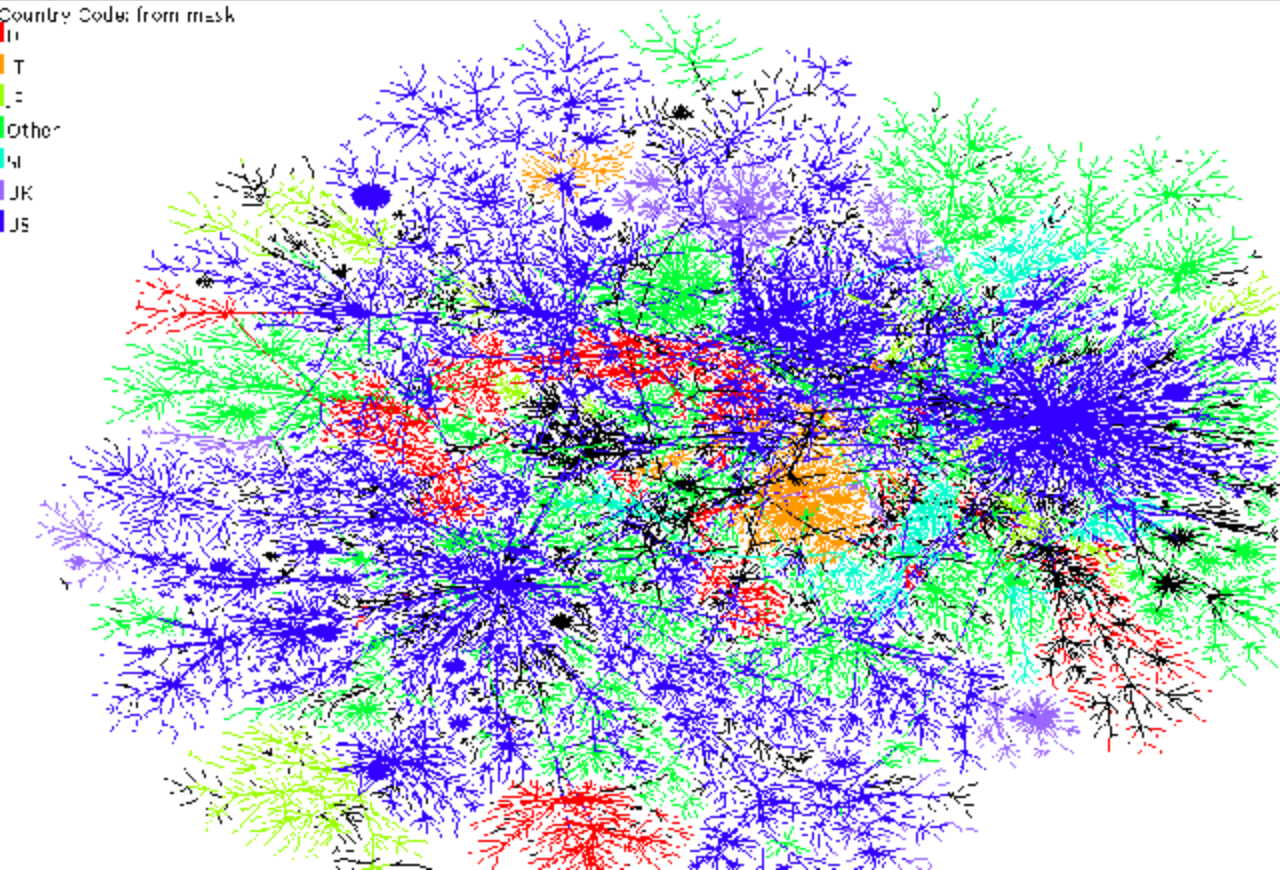


skitter: topology discovery/depiction

- correlate effects with BGP routing changes
- correlate path performance with specific events
- identify critical infrastructure within the Internet



skitter: colored by country



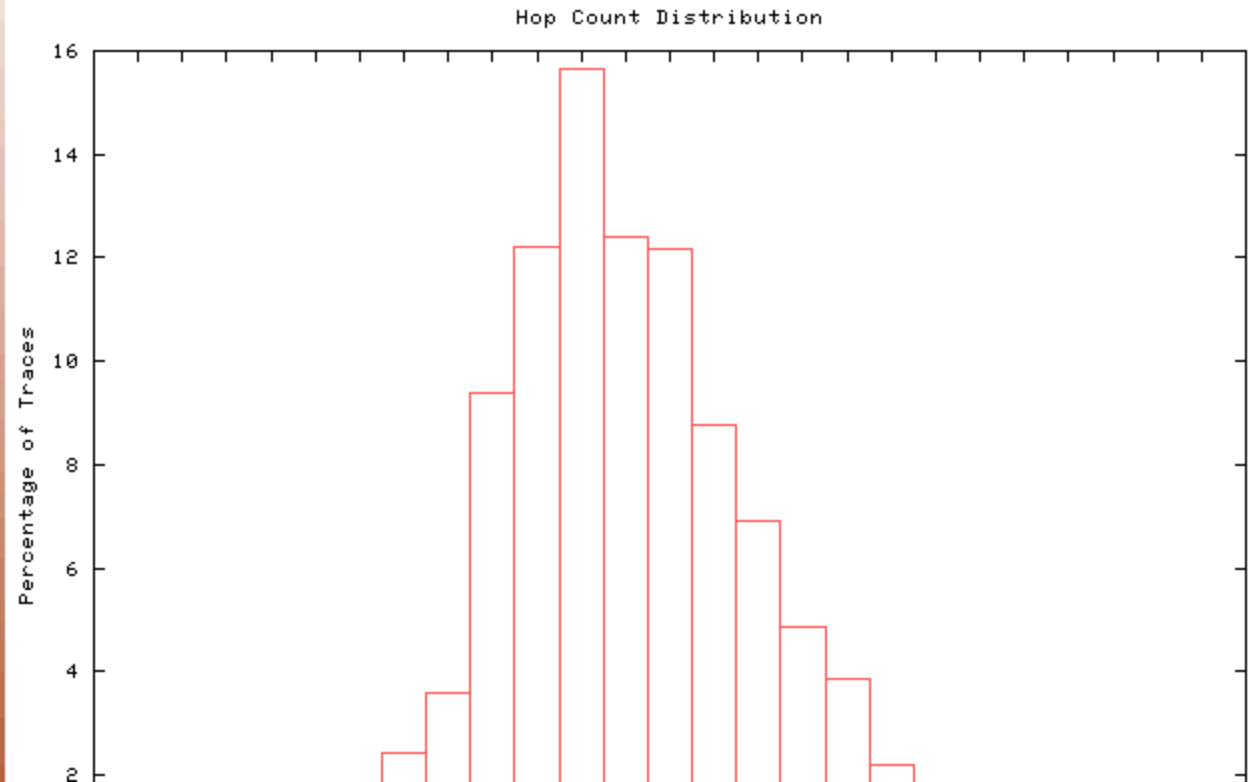
infrastructure: DNS roots

- RSSAC, DNS technical advisory committee to ICANN
- co–locate skitter hosts w root servers
- demonstrate root server performance in serving target community
- develop techniques for evaluating architectual optimality for root server placement

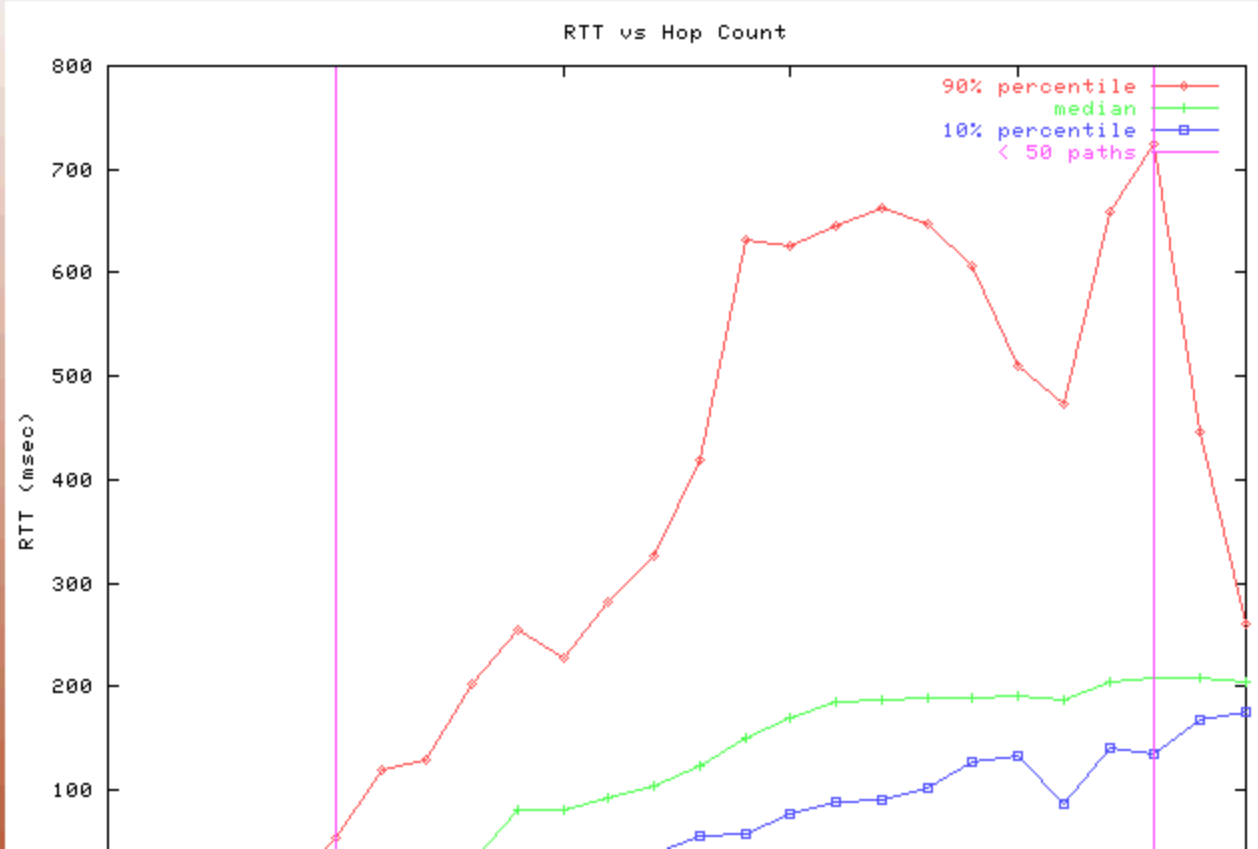
(www.caida.org/Tools/Skitter/RSSAC/)

skitter: macroscopic study

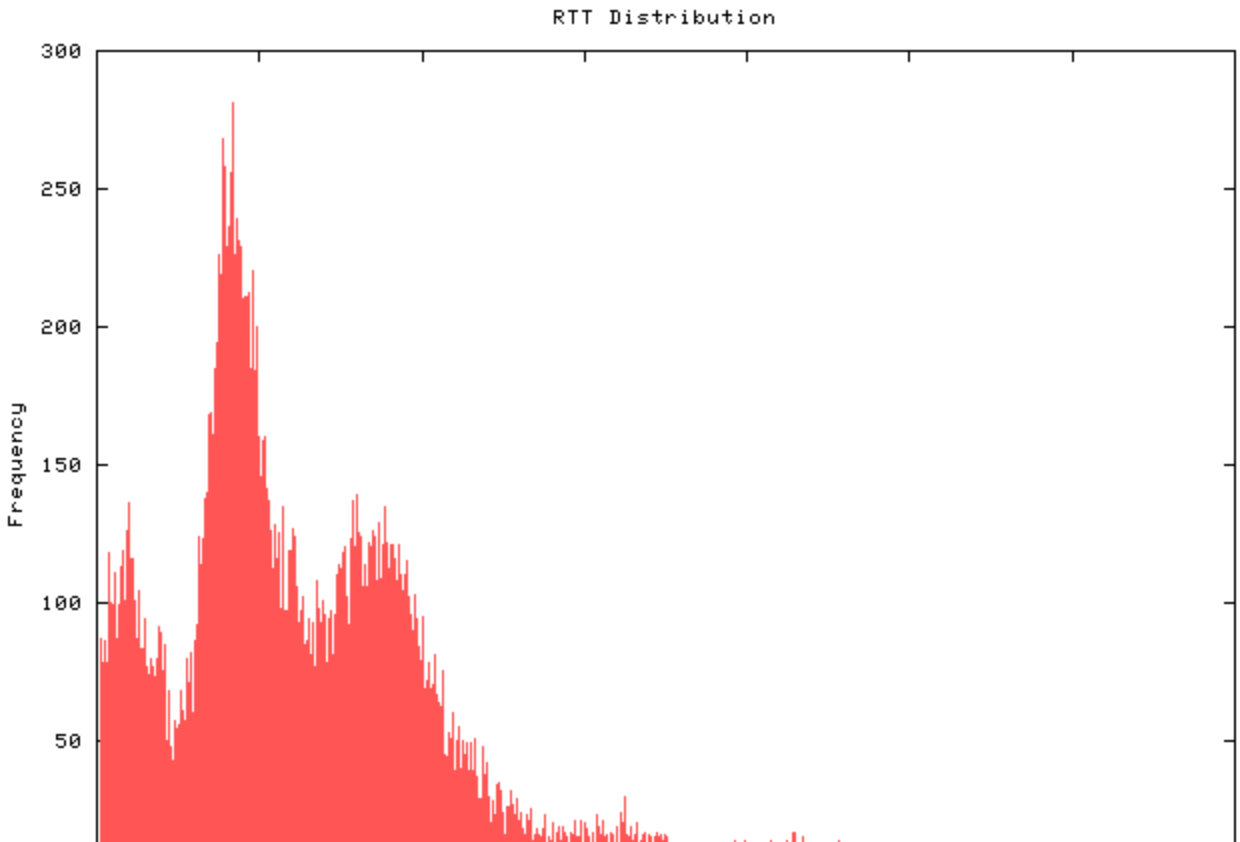
DNS f root server (pv's): path wingspans



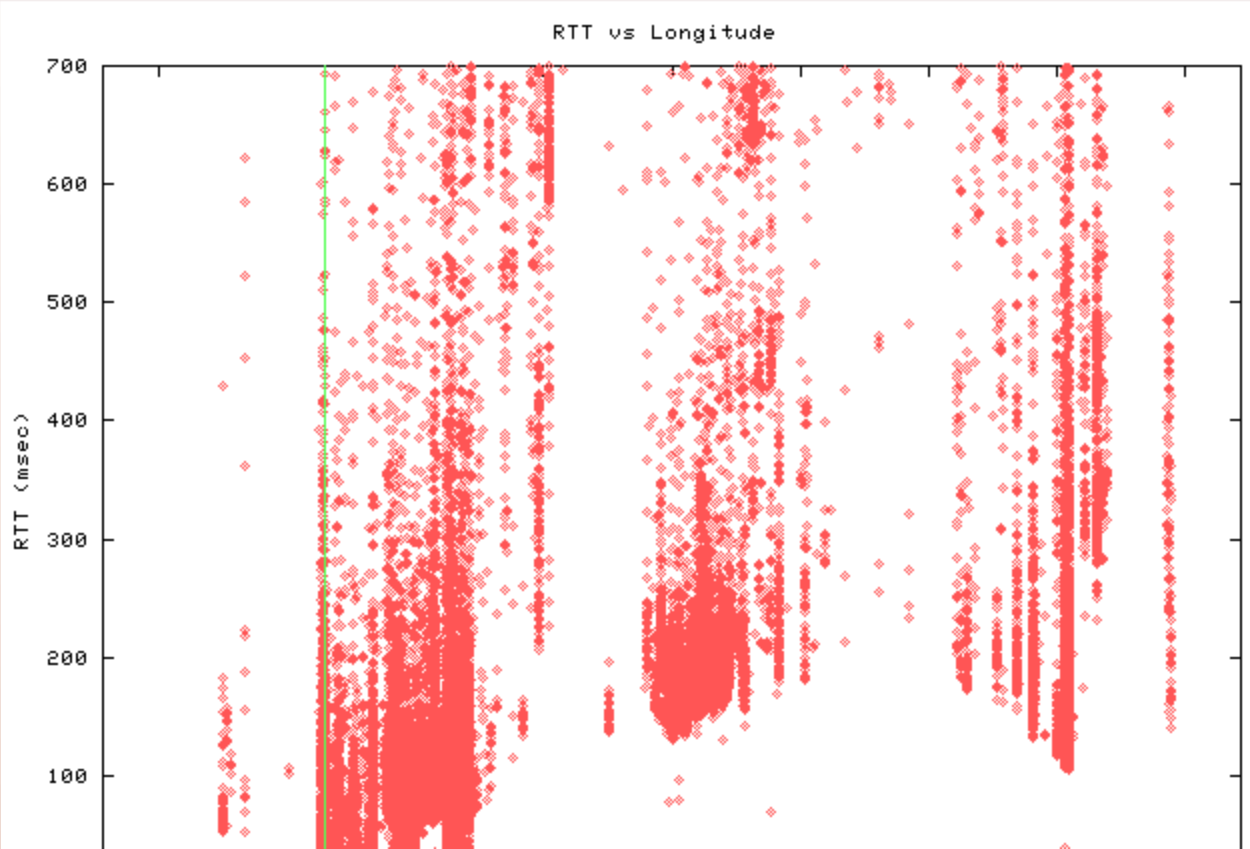
skitter: rtt vs hopcount (correlation?)



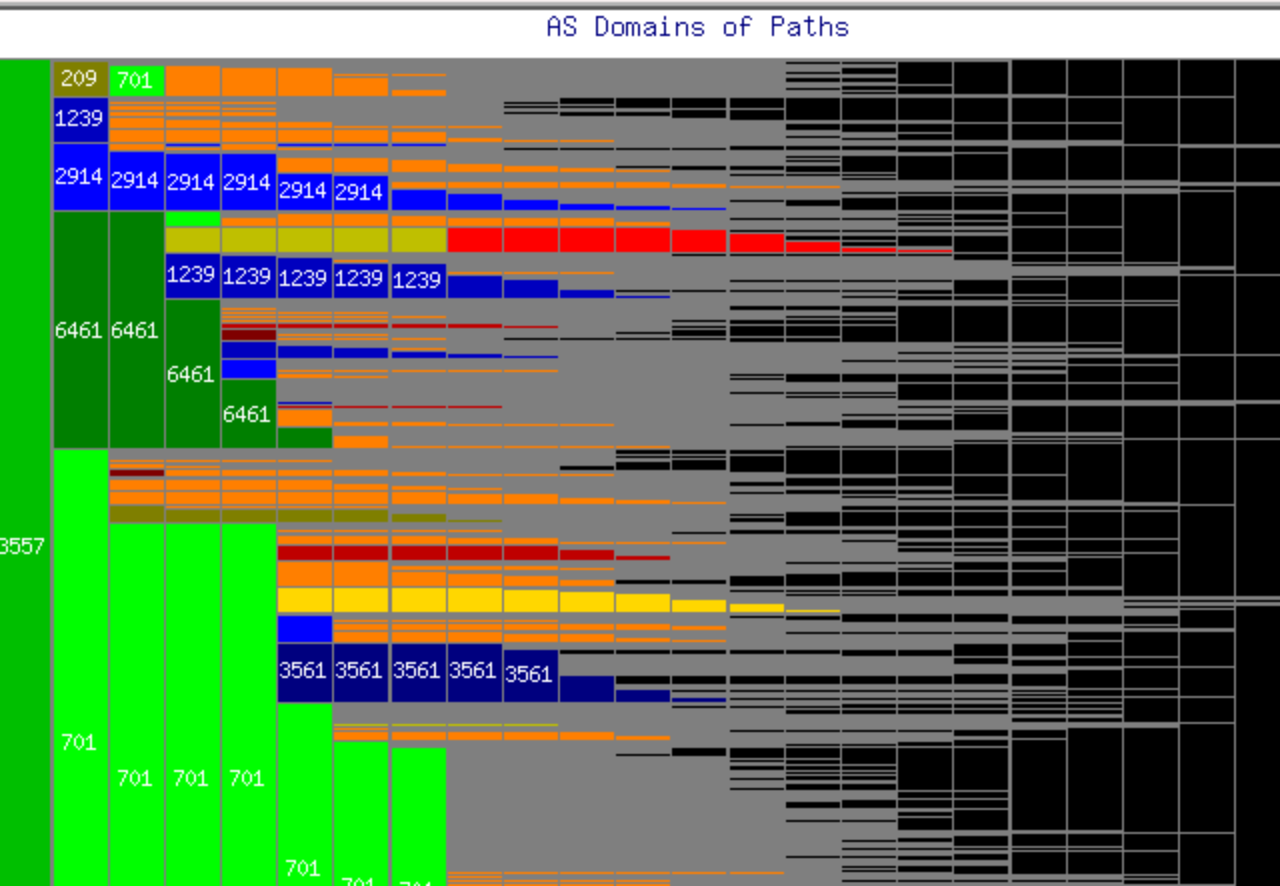
skitter: rtt distribution: tri-modal



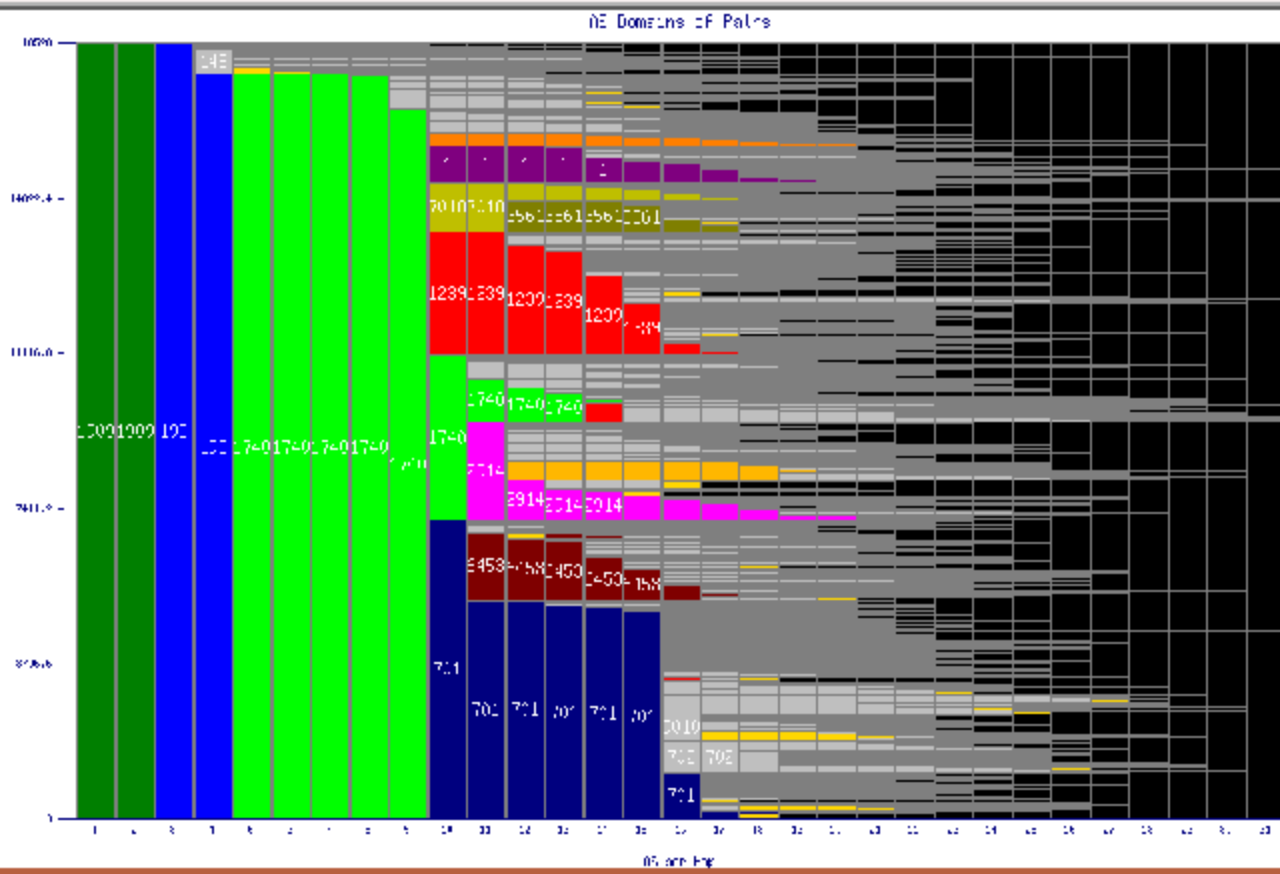
skitter: rtt vs longitude (light cone)



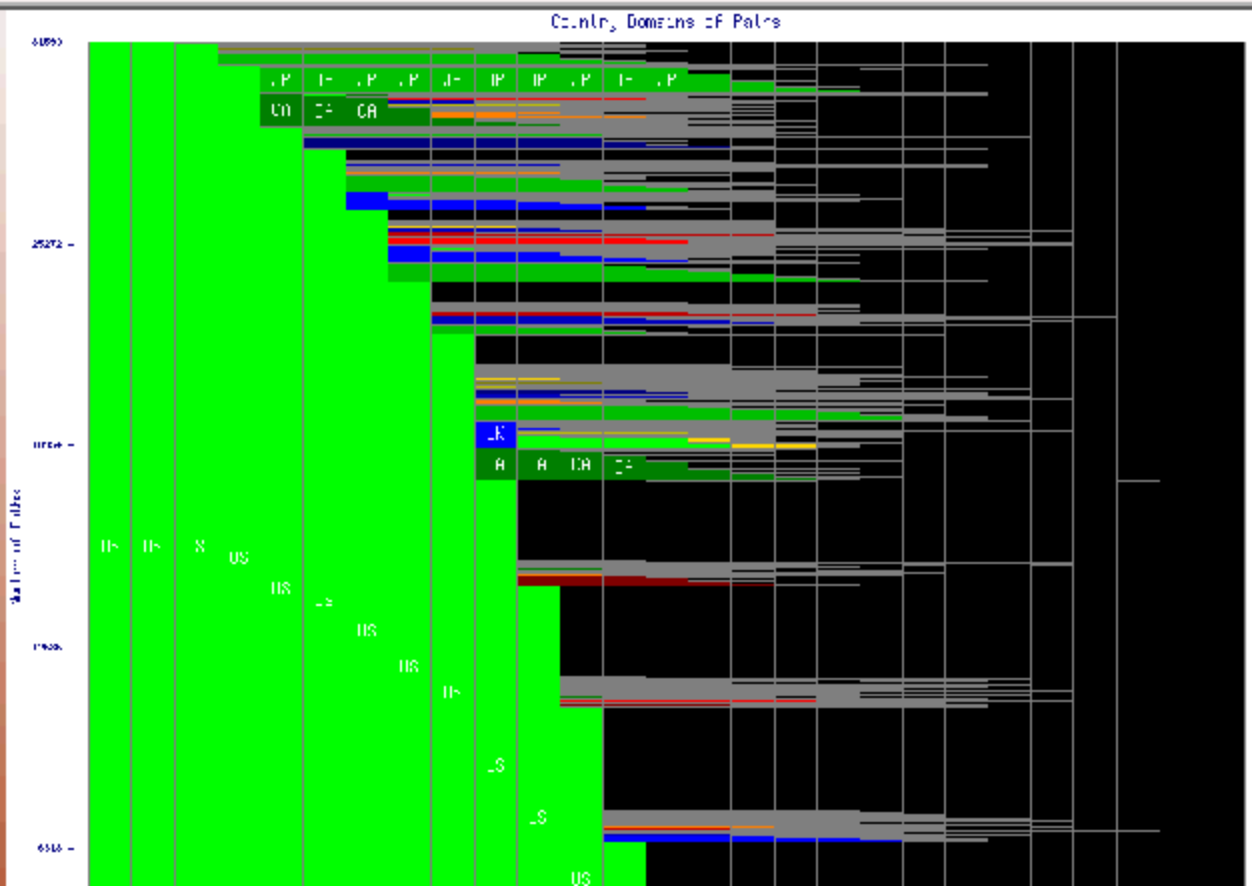
skitter: dispersion among ASes across paths



skitter: AS dispersion across paths (sdsc)



skitter: country dispersion across paths



skitter analyses – preliminary findings

- ~1% IP destinations disappearing monthly (re-addressing, firewalls)
- route announced path not matching forward path
- indication of potential routing configuration errors (by no means automatic)
- persistence of paths
- methods to identify critical infrastructure
- is there an Internet "core"?

datasets available to researchers

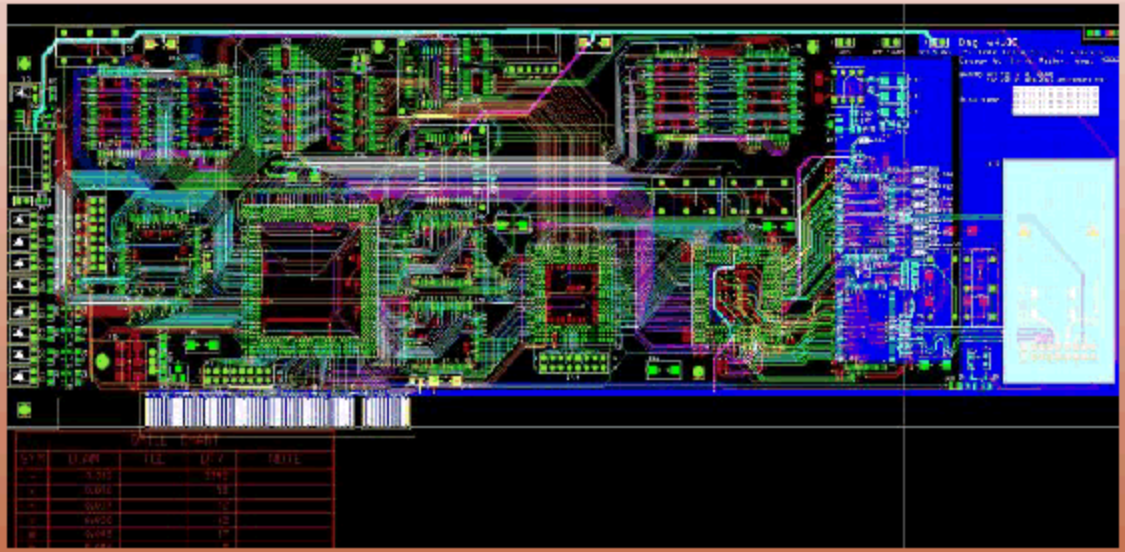
monitoring high perf. networks

priorities:

- monitor/characterize traffic on high speed nets (OC48, gigether)
- insights for
  - developing emerging hw/sw, protocols, applications
  - capacity/network planning and peering
  - network control and management
  - billing and accounting

monitoring high perf. networks

- coral/ocXmon testing (oc3,12,48,gE)
- persistent real-time full frame collection
- integration w coralreef analysis s/w
- dag4.0 testing planned 1/00



security of high perf. networks: coralreef

- CoralReef 3.2 release 12/16/99
- ATM: Applied Telecom and Fore OC3 (OC12 App. Tel. only)
- ATM/POS:OC3/12 (DAG3.2 testing 1/00)

- crl_portmap s/w module
  - listens for RPC portmap access
  - adds suspicious probing host to list
  - records all send-rec'd packets
  - full payload capture (default)
  - tcpdump output format

security of high perf. networks: coralreef

- crl_filter
  - ATM reassembly
  - tcpdump output format
  - pipes to existing security tools
- future
  - OC12 (full line rates), OC48 need card support
  - active enforcement module (yr 2000)
  - getting ISPs to use them

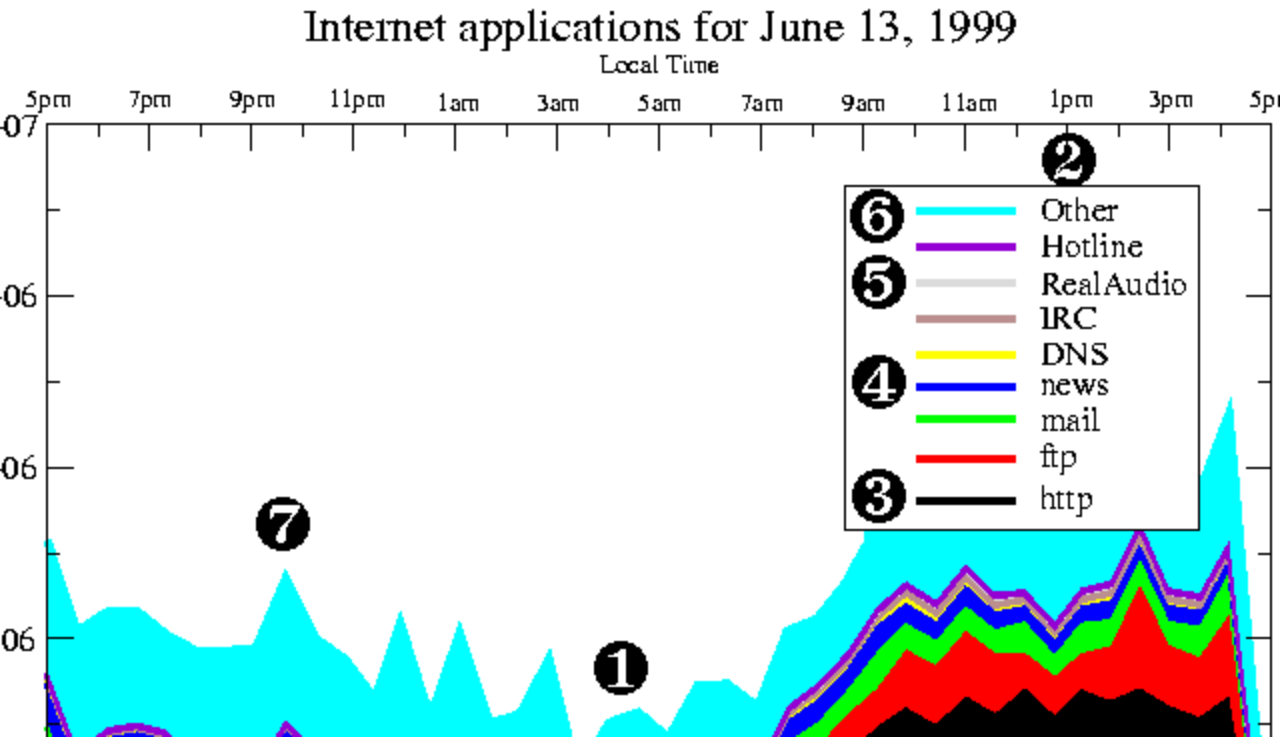
www.caida.org/Tools/CoralReef

visualization ('big viz')

- massive datasets (terabytes)
- many data attributes (complex)
- multiple viz strategies/modalities
  - workload
  - geographical
  - logical
  - chronological
  - 2D vs 3D
  - animation
- distributed acquisition, data reduction, rendering technologies
  - what is meaningful?
  - aggregation granularity
- integration into ISP utilities

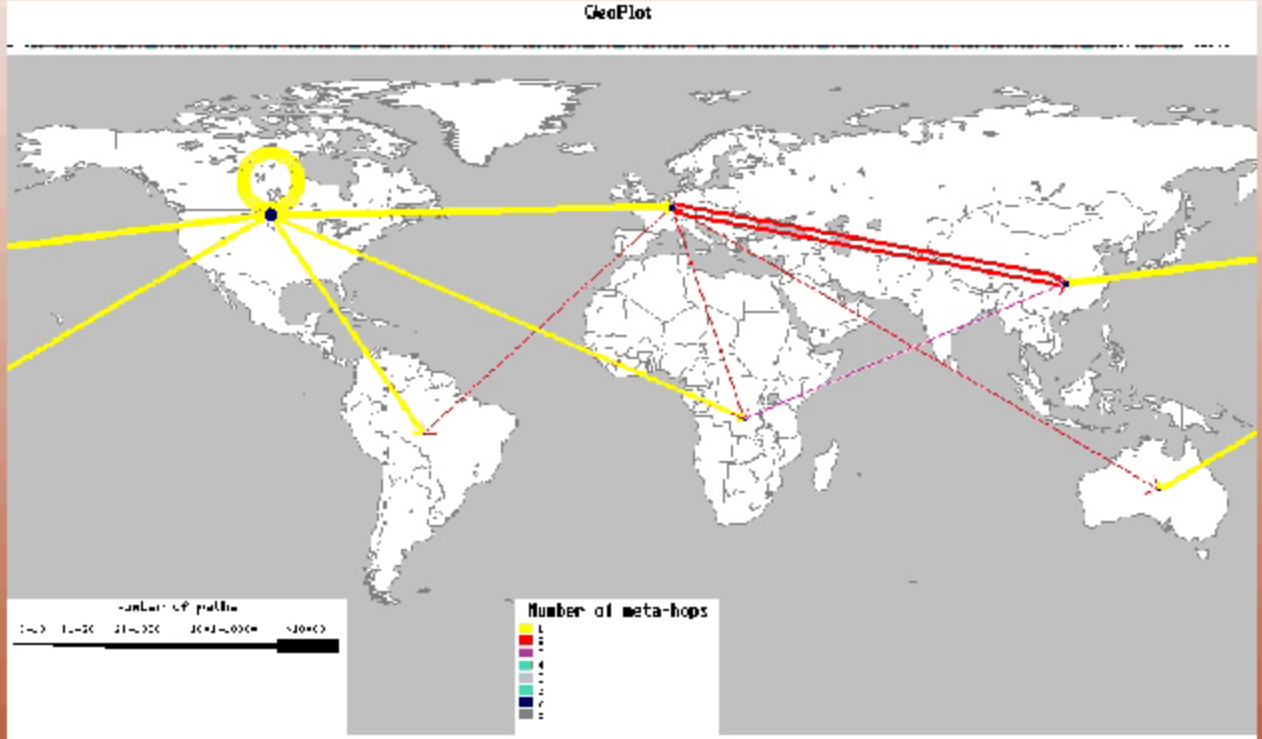
visualization: workload (protocol)

from caida traffic analysis cd, iec.caida.org



visualization: geographical

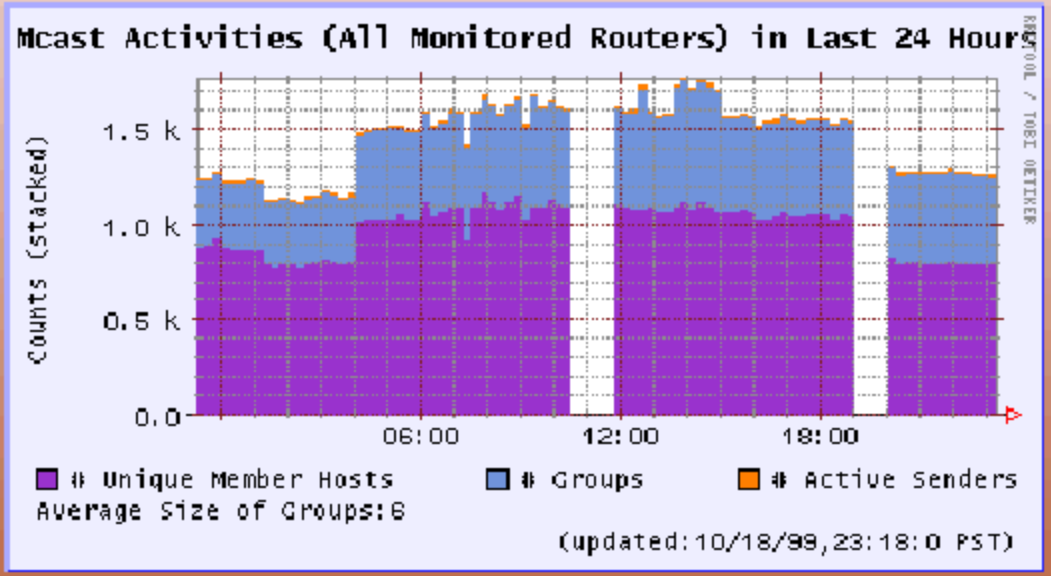
www.caida.org/Tools/GeoPlot/
[www.caida.org/Tools/NetGeo/]



visualization: chronological

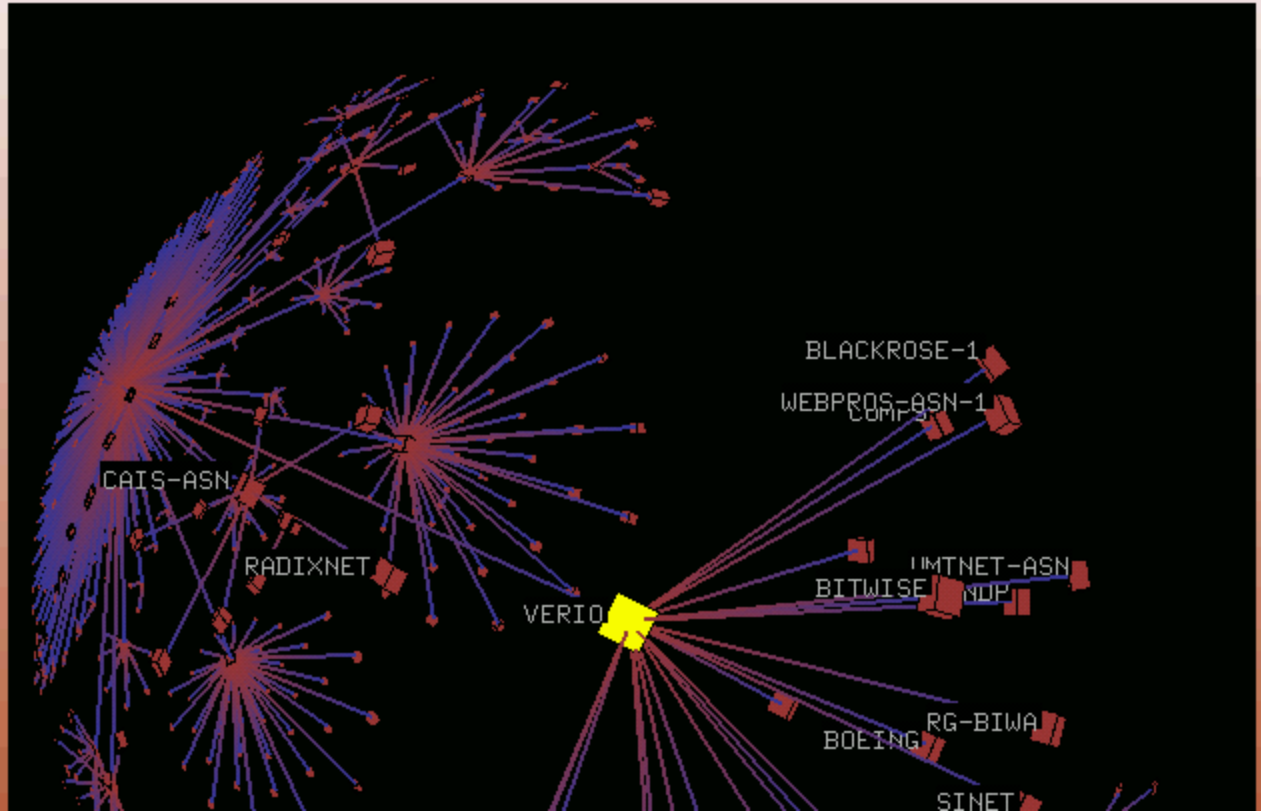
www.caida.org/Tools/Mantra
www.caida.org/Tools/RRDTool

18 oct 99, fix-west.mbone.nasa.gov



visualization: logical

BGP routing table data (connectivity among ASes)



visualization: research priorities

- latency
- key routers/networks
- AS granularity
- geographic
- integration w mgt tools

obstacles:

mapping IP addresses to

- router
- geography
- AS
- service provider
- anything...

topology changes faster than can measure

how (repeat)

- develop/deploy tools (coral oc48, skitter) to better engineer and operate networks
- get ISPs to use them (security, accounting, useful analysis & visualization)

www.caida.org/Presentations/

kc claffy
UCSD/SDSC/CAIDA
kc@caida.org
www.caida.org