

1 Proposal Title

ANALYSIS & VISUALIZATION OF BGP CONNECTIVITY AMONG AUTONOMOUS SYSTEMS

2 Primary Investigators

k claffy, Ph.D. UCSD Computer Science & Engineering, 1994

Bradley Huffaker, M.S. UCSD Computing Science & Engineering, 1998

3 Project Summary

Based on the success of last year's URB project we would like to continue and extend our research and analysis of connectivity among autonomous systems. For 2003-2004 our research agenda would involve both analysis and visualization components. First, we would like to evaluate inter-AS connectivity based on prefix-level granularity as well as AS granularity. We also want to develop a publicly available set of tools for analyzing peering, transit, and customer relationships based on Cisco BGP output. Finally, our analysis groundwork renders us in a strong position to develop much more powerful visualization tools customized for BGP tables. Results of this research will offer not only novel and innovative visualization and mapping techniques, but also key data for any infrastructure protection center involved in warning, analysis, and coordinating emergency response to infrastructure threats. Both the PSIRT and CIAG [1] groups within Cisco have expressed strong interest in continuation of this work and recommended the URB program as the most appropriate vehicle at this time.

4 Description of Research and Goals

Based on the success of last year's URB project we would like to continue and extend the work in analysis of connectivity among autonomous systems. Last year we developed an analysis methodology for ranking the richness of connectivity of ASes [2, 3] based on massive topology data as measured by CAIDA's macroscopic IP topology monitoring project [4] and observed by RouteViews BGP table snapshots [5, 6]. The coverage of these topology probes is unprecedented, dramatically higher than any previous work in this area, and the data yield significant insight into the relative richness of IP connectivity of different ASes. This work has already been enthusiastically received both internally at Cisco¹ and by the wider community, as there is great marketing-inspired speculation and little sound methodology regarding macroscopic Internet connectivity analysis. The interactive web page for AS ranking is at <http://as-rank.caida.org/cgi-bin/main.pl> and is updated with new topology data daily.²

In addition to maintaining this web site for 2003-2004, this year we would like to leverage Cisco's investment into this research area by extending the research and analysis agenda in three ways:

1. evaluate inter-AS connectivity based on prefix-level granularity as well as AS granularity
2. develop a publically available set of utilities for heuristically analyzing peering, transit, and customer relationships based on Cisco (and zebra) BGP output. Although these inferences are inherently heuristic in nature, CAIDA will build on current work in the field [7, 8, 9] to create tools for more public use by Cisco customers
3. develop a publically available visualization tool and library customized for navigating BGP tables

Results of this research will offer not only novel and innovative visualization and mapping techniques, but also key data for any infrastructure protection center involved in warning, analysis, and coordinating emergency response to threats.

¹Both the PSIRT and CIAG [1] groups at Cisco have expressed strong interest in continuation of this work and recommended the URB program as the most appropriate vehicle at this time.

²Claffy will be presenting an overview of this work at a seminar at Cisco on 29 April 2003.

4.1 Visualizing BGP tables

CAIDA has a reputation for extensive experience in macroscopic Internet visualization techniques, which unfortunately only reflects the lack of experience of anyone else in the field. Visualization of systems as massive, dynamic, and distributed as the Internet is a field with few breakthroughs since Internet topology growth careened out of control by available visualization technologies. In 2002 we focused on analysis techniques, from which we can now draw on to build the next generation of more capable and insightful visualization tools. Existing CAIDA network visualization tools, e.g., *otter* [10], *walrus* [11], and *plotpaths* [12], have been used for a variety of network visualization tasks but unfortunately lack funding for support or extension. Based on our experience with these tools, we would like to (reuse existing software where appropriate to) develop a new more sophisticated tool that:

- uses a more current graphic API (swing)
- can handle hundreds if not millions of nodes using the recently CAIDA-developed powerful *libsea* graphics library [13]
- supports an optional client server model so it can act as a generalized GUI interface and leave data-centric processing to one or more servers, e.g., *beluga* [14], traceroute. BGP looking glasses and routers.
- supports a more flexible approach to graph layout than can adapt to changing network conditions.
- allows for graceful drill-down into nodes, e.g., when AS nodes represent entire network clouds.

We list development milestones below in section 5.

4.2 Impact

Cisco specifically requested the AS ranking analysis from CAIDA last year, and has made use of it in 2002. From Wendy Garvin of Cisco's PSIRT team:

The Cisco PSIRT team uses the data provided by CAIDA's skitter and AS ranking tool during situations where a vulnerability on a Cisco product may affect the critical infrastructure of the Internet. In such cases we have a 'tiered' notification process where we notify the service providers responsible for the 'core' before we propagate the vulnerability information to other service providers and enterprise customers. CAIDA's analysis tool allows us to accurately define the current top providers based on the current state of the Internet rather than on Cisco marketing or revenue data. This facilitates an unbiased approach to what is a difficult and politically sensitive determination, which is valuable to us from a customer support perspective as well as improving our position as a responsible player in protection of critical Internet infrastructure.

From Barry Greene, CTO Consulting Engineering:

CIAG and PSIRT are two of several groups inside Cisco who have expressed interest. Several members of our Executive Staff (Mike Volpi, Tony Bates, and Roland Acra) have express interest from the POV of understanding how the Internet is currently interconnected. Field engineers working on IXPs through out the world find it valuable as a tool to understand interconnectivity levels. Field Engineering Teams find it valuable as a new replacement analogy to the 'Tier N' model. You frequently hear people refer to the "Skitter Core" as a reference tool to describe hierarchy in the Internet.

We intend to not only maintain the interactive asrank data interface throughout this year, but also leverage Cisco's investment by extending the research and analysis agenda in 2004 to offer three payoffs to Cisco and the larger community: (1) analysis approaches for drawing high integrity inferences of economic relationships from BGP data samples; (2) novel and innovative massive Internet visualization and mapping techniques; and (3) key data for any infrastructure protection center involved in warning, analysis, and coordinating emergency response to Internet infrastructural threats. Tools that can yield insight into macroscopic Internet connectivity have been of interest for years, but successful development of such tools remains elusive and yet of increasing importance to Internet infrastructural protection. In the short term this project will continue to facilitate's Cisco incident notification process in the face of learned vulnerabilities (e.g., viruses, protocol

weaknesses), as well as increased awareness of potential vulnerabilities deriving from excessive concentration of connectivity provided by a single or few ASes or exchange points. In the long term we hope to provide visualization tools that can offer a better framework for exploratory data analysis of potential future interdomain routing systems.

5 Timeframes for Funding and Research Completion

Funding (\$100,000) to begin 15 July 2003. (or whenever possible)

Research Milestones

- **15 July 03** Begin implementation of asrank by prefixes as another (finer-grained than ASes) measure of connectivity richness
- **15 October 03** Initial set of utilities for inferring peering, transit, and customer relationships based on Cisco (and zebra) BGP output
- **15 November 03** Complete prefix-based version of asrank
- **15 December 03** Test and evaluate integrity of new asrank methodology.
- **15 March 04** Integrate visualization tool with libsea library; handle visualization of at least half a million nodes. Include graceful drill-down into nodes e.g., when AS nodes represent entire network clouds.
- **15 April 04:** prototype client/server model, so tool can be GUI client for alternative servers (server could also be run locally)
- **15 May 04:** release improved graph layout modules that can adapt to real-time BGP dynamics
- **15 June 04:** report on results of testing visualization tool to handle live BGP feed graph, highlighting areas that are changing
- **15 July 04** report on results of testing visualization tool to handle traceroute-like path and per-hop performance (RTT or bandwidth) data passed on for rendering.

5.1 Required/expected Research Cooperation with Cisco

Researchers are available to meet with Cisco staff to discuss methodologies and the implications of analysis results, in particular with respect to Cisco's incident notification process or router instrumentation that might improve the quality of data gathered.

6 SUPPORT REQUIREMENTS

6.1 Total Budget

\$100,000

6.2 Duration

1 July 2003 - 30 June 2004 (or whatever Cisco can do)

6.3 Breakdown

SALARIES & BENEFITS:

k claffy, Ph.D., P.I.	10% effort	\$15,500
Brad Huffaker, M.S.	25% effort	\$12,952
2 graduate student	50% effort with tuition remission	\$69,548

DOMESTIC TRAVEL:

4 meetings (as requested by Cisco engineers): approximately \$2000, where one CAIDA researcher travels from San Diego to San Jose for two days (airfare, one day hotel) for \$500

GRADUATE TUITION:

\$22,212

7 GRADUATE STUDENTS INVOLVED

Two graduate students will be selected by January 2003.

8 OTHER CURRENT OR ANTICIPATED MATCHING FUNDS

Research on this project will draw cost-sharing support from NCS and NSF.

9 Short biographies of the researchers

kc claffy, Ph.D. is principal investigator for the distributed Cooperative Association for Internet Data Analysis (CAIDA), and resident research scientist based at the University of California's San Diego Supercomputer Center. kc's research interests include Internet workload/performance data collection, analysis and visualization, particularly with respect to commercial ISP collaboration/cooperation and sharing of analysis resources. kc received her Ph.D. in Computer Science from UCSD in 1994.

Brad Huffaker, M.S. serves as technical manager for several tool development and traffic analysis efforts at CAIDA. He specializes on efforts to develop analytical and visualization techniques suitable for insight on the configuration, evolution and occurrence of network events in large network topologies. Brad received both the B.S. and M.S. degrees in Computer Science from UCSD.

10 Name of Cisco Champion

Fred Baker, Barry Greene, Wendy Garvin, Jim Duncan

11 Relevant University Administrative Contact

(Check may be sent here. Only wording required is 'unrestricted gift' per the URB web page.)

Darlene Piche
CAIDA SDSC 0505
9500 Gilman Drive
La Jolla, CA 92093-0505
858.534.5109
piche@sdsc.edu

References

- [1] C. System, “Critical Infrastructure Assurance Group (CIAG),” 2003. http://www.cisco.com/security_services/ciag/.
- [2] kc claffy and B. Huffaker, “Cisco URB 2002 proposal: Connectivity Ranking of Autonomous Systems,” April 2002. <http://www.caida.org/projects/cisco02autorank/>.
- [3] kc claffy and B. Huffaker, “Connectivity Ranking of Autonomous Systems (using large topology sample) as viewed by CAIDA’s macroscopic topology mapping project,” 2003. http://www.caida.org/analysis/topology/rank_as/.
- [4] M. Fomenkov and B. Huffaker, “Macroscopic Topology measurements,” 2003. <http://www.caida.org/analysis/topology/macroscopic/>.
- [5] D. Meyer, “RouteViews,” 2002. <http://www.routeviews.org>.
- [6] A. Broido and k claffy, “Analysis of RouteViews BGP data: policy atoms,” in *Network Resource Data Management Workshop, Santa Barbara, CA*, May 2001. <http://www.caida.org/outreach/papers/2001/NdrmBgp/>.
- [7] L. Gao, “On Inferring Autonomous System Relationships in the Internet.” <http://www.caida.org/outreach/isma/0012/talks/lixin/>.
- [8] L. Subramanian and S. Agarwal and J. Rexford and R. H. Katz, “Characterizing the Internet hierarchy from multiple vantage points,” in *Proc. IEEE INFOCOM*, June 2002.
- [9] David Andersen and Nick Feamster and Steve Bauer and Hari Balakrishnan, “Topology Inference from BGP Routing Dynamics,” in *2nd Internet Measurement Workshop*, November 2002.
- [10] B. Huffaker, k claffy, and E. Nemeth, “Otter: A General-purpose Network Visualization Tool,” in *Proc. of INET’99*, June 1999. <http://www.caida.org/tools/visualization/otter/paper/>.
- [11] Y. Hyun and D. Moore, “Walrus tool,” 2002.
- [12] B. Huffaker and J. Gallagher, “plotpaths,” 2002.
- [13] Y. Hyun, “libsea graphics library,” 2002. <http://www.caida.org/tools/visualization/libsea/>.
- [14] R. Koga, “beluga: per hop performance visualization tool,” 2002.