Nick Feamster

MIT Computer Science and Artificial Intelligence Laboratory
32-G982, The Stata Center
32 Vassar Street
Cambridge, MA 02139

Phone: (617) 253-7341
Fax: (617) 253-8460
`feamster@csail.mit.edu`
`http://nms.csail.mit.edu/~feamster/`

Research Interests

Networked computer systems: network protocols, routing, security, and management

Education

MASSACHUSETTS INSTITUTE OF TECHNOLOGY — *Cambridge, MA*

Ph.D. candidate in Computer Science. (Expected Summer 2005)
Dissertation: Robust and Predictable Internet Routing
Advisor: Hari Balakrishnan
Minor in Game Theory

M.Eng. in Computer Science, 2001
Thesis: Adaptive Delivery of Real-Time Streaming Video
Advisor: Hari Balakrishnan
William A. Martin Memorial Thesis Award (MIT M.Eng. thesis award)

S.B. in Electrical Engineering and Computer Science, 2000
Concentration in Economics

Professional Experience

2000– **Research Assistant** — MIT, *Cambridge, MA*

Research assistant at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL). Projects include work on interdomain routing robustness, circumventing Web censorship (Infranet), and the Congestion Manager project. More details are available on Page 5.

2001– **Technical Intern and Consultant** — AT&T Labs–Research, *Florham Park, NJ*

Research on interdomain traffic engineering and modeling. More details are available on Page 5.

1999 **Technical Associate** — Bell Laboratories, Lucent Technologies, *Murray Hill, NJ*

Designed and implemented a JavaBeans-based call filtering/disposition system which allows end users to easily design a call flow based on various criteria.

1998–2000 **Intern** — Hewlett-Packard Laboratories, *Palo Alto, CA*

Designed and implemented a transcoding algorithm for real-time conversion of MPEG-2 to H.263 bitstreams. More details are available on Page 6.

1997 **Technical Staff** — LookSmart Ltd., *San Francisco, CA*

Designed and implemented Web crawler, as well as monitoring and testing scripts for production search engine system.

Teaching Experience

2002 Teaching Assistant, MIT Course 6.829, Computer Networks.
Contributed new problems to problem sets and quizzes, gave two lectures, and taught recitations covering advanced topics.

2002–2003 M.Eng. research supervisor, MIT.
With Hari Balakrishnan, supervised Winston Wang, whose thesis on an implementation of the Infranet anti-censorship system received MIT's Charles and Jennifer Johnson Thesis Prize.

Refereed Publications

Note: Papers are listed in reverse chronological order by topic area.

Internet Routing

[1] Nick Feamster, Ramesh Johari, and Hari Balakrishnan. The implications of autonomy for stable policy routing. In *Proc. ACM SIGCOMM*, Philadelphia, PA, August 2005.

[2] Nick Feamster and Hari Balakrishnan. Detecting BGP Configuration Faults with Static Analysis. In *Proc. 2nd Symposium on Networked Systems Design and Implementation*, Boston, MA, May 2005. *Best paper award.*

[3] Matthew Caesar, Don Caldwell, Nick Feamster, Jennifer Rexford, Aman Shaikh, and Kobus van der Merwe. Design and Implementation of a Routing Control Platform. In *Proc. 2nd Symposium on Networked Systems Design and Implementation*, Boston, MA, May 2005.

[4] Nick Feamster, Hari Balakrishnan, and Jennifer Rexford. Some foundational problems in interdomain routing. In *Proc. 3nd ACM Workshop on Hot Topics in Networks (Hotnets-III)*, San Diego, CA, November 2004.

[5] Nick Feamster, Hari Balakrishnan, Jennifer Rexford, Aman Shaikh, and Kobus van der Merwe. The case for separating routing from routers. In *ACM SIGCOMM Workshop on Future Directions in Network Architecture*, Portland, OR, September 2004.

[6] Nick Feamster, Jared Winick, and Jennifer Rexford. A model of BGP routing for network engineering. In *Proc. ACM SIGMETRICS*, New York, NY, June 2004.

[7] Nick Feamster. Practical verification techniques for wide-area routing. In *Proc. 2nd ACM Workshop on Hot Topics in Networks (Hotnets-II)*, Cambridge, MA, November 2003.

[8] Nick Feamster, Jay Borkenhagen, and Jennifer Rexford. Guidelines for interdomain traffic engineering. *ACM Computer Communications Review*, 33(5):19–30, October 2003.

[9] Nick Feamster and Hari Balakrishnan. Towards a logic for wide-area Internet routing. In *ACM SIGCOMM Workshop on Future Directions in Network Architecture*, Karlsruhe, Germany, August 2003.

Internet Measurement

[10] Michael Freedman, Mythili Vutukuru, Nick Feamster, and Hari Balakrishnan. Geographic locality of ip prefixes. In *Proc. ACM SIGCOMM Internet Measurement Conference*, New Orleans, LA, October 2005.

[11] Nick Feamster, Jaeyeon Jung, and Hari Balakrishnan. An empirical study of "bogon" route advertisements. *ACM Computer Communications Review*, November 2004.

[12] Nick Feamster, Zhuoqing Morley Mao, and Jennifer Rexford. BorderGuard: Detecting cold potatoes from peers. In *Proc. ACM SIGCOMM Internet Measurement Conference*, Taormina, Sicily, Italy, October 2004.

[13] Nick Feamster, David Andersen, Hari Balakrishnan, and M. Frans Kaashoek. Measuring the effects of Internet path faults on reactive routing. In *Proc. ACM SIGMETRICS*, San Diego, CA, June 2003.

[14] David G. Andersen, Nick Feamster, Steve Bauer, and Hari Balakrishnan. Topology inference from BGP routing dynamics. In *Proc. ACM SIGCOMM Internet Measurement Workshop*, Marseille, France, November 2002.

Network Security

[15] Nick Feamster and Roger Dingledine. Location diversity in anonymity networks. In *ACM Workshop on Privacy in the Electronic Society*, Washington, DC, October 2004.

[16] Nick Feamster, Magdalena Balazinska, Winston Wang, Hari Balakrishnan, and David Karger. Thwarting Web censorship with untrusted messenger discovery. In *3rd Workshop on Privacy Enhancing Technologies*, Dresden, Germany, March 2003.

[17] Nick Feamster, Magdalena Balazinska, Greg Harfst, Hari Balakrishnan, and David Karger. Infranet: Circumventing Web censorship and surveillance. In *Proc. 11th USENIX Security Symposium*, San Francisco, CA, August 2002.
Best student paper award.

[18] Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. Dos and don'ts of client authentication on the Web. In *Proc. 10th USENIX Security Symposium*, Washington, DC, August 2001.
Best student paper award.

Adaptive Streaming Media Protocols

[19] Nick Feamster and Hari Balakrishnan. Packet loss recovery for streaming video. In *Proc. 12th International Packet Video Workshop (PV 2002)*, Pittsburgh, PA, April 2002.

[20] Nick Feamster, Deepak Bansal, and Hari Balakrishnan. On the interactions between congestion control and layered quality adaptation for streaming video. In *11th International Packet Video Workshop*, Kyongju, Korea, May 2001.

[21] Susie Wee, John Apostolopoulos, and Nick Feamster. Field-to-frame transcoding with temporal and spatial downsampling. In *IEEE International Conference on Image Processing*, October 1999.

[22] Nick Feamster and Susie Wee. An MPEG-2 to H.263 transcoder. In *SPIE Voice, Video, and Data Communications Conference*, Boston, MA, September 1999.

Submitted Publications and Works-in-progress

[23] Feng Wang, Nick Feamster, and Lixin Gao. Quantifying the causes of end-to-end Internet path failures, February 2005. Submitted for publication.

[24] Nick Feamster and Jennifer Rexford. Modeling BGP route selection within an AS. *IEEE/ACM Transactions on Networking*, July 2004. Earlier version appears in *ACM SIGMETRICS 2004*.

[25] Claire Monteleoni, Hari Balakrishnan, Nick Feamster, and Tommi Jaakkola. Managing the 802.11 energy/performance tradeoff with machine learning. Technical Report MIT-LCS-TR-971, Massachusetts Institute of Technology, 2004.

Unrefereed Papers and Technical Reports

[26] Nick Feamster, Jennifer Rexford, and Jay Borkenhagen. Controlling the impact of BGP policy changes on IP traffic. Technical Report 011106-02, AT&T Labs–Research, Florham Park, NJ, November 2001.

[27] Nick Feamster and Jennifer Rexford. Network-wide BGP route prediction for traffic engineering. In *Proc. SPIE ITCom*, Boston, MA, August 2002.

[28] Nick Feamster. Rethinking routing configuration: Beyond stimulus-response reasoning. In *Workshop on Internet Routing Evolution and Design (WIRED)*, Mt. Hood, OR, October 2003.

[29] Nick Feamster and Hari Balakrishnan. Verifying the correctness of wide-area Internet routing. Technical Report MIT-LCS-TR-948, Massachusetts Institute of Technology, May 2004.

[30] Russ White and Nick Feamster. *Considerations in Validating the Path in Routing Protocols*. IETF, April 2004. Internet Draft. Expires October 2004.

Invited talks at the North American Network Operators Group (NANOG), Cooperative Association for Internet Data Analysis (CAIDA), Boston University, Carnegie Mellon SDI seminar, New York University, Harvard University, University Catholique de Louvain (Belgium), AT&T Research, Hewlett-Packard Laboratories, and Agilent Technologies.

Awards and Honors

2005	Best Paper, 2nd Usenix Symposium on Networked Systems Design and Implementation
2004	Cisco URP Grant Recipient
2002–	NSF Graduate Research Fellow

2002	Best Student Paper, 11th Usenix Security Symposium
2001	Best Student Paper, 10th Usenix Security Symposium
2001	MIT William A. Martin Memorial Thesis Award
1999–	Tau Beta Pi Engineering Honor Society
1999–	Eta Kappa Nu Honor Society
1999	Letter of Commendation for Outstanding Performance, MIT Digital Design Laboratory
1998–1999	Phi Sigma Kappa Scholarship Award
1997	National Merit Scholar
1997	Rotary Club Scholarship
1996	AP Scholar with Distinction

Service and Other Activities

Reviewer for *IEEE/ACM Transactions on Networking*, *SIGCOMM* (2002, 2003, 2004), *SOSP* (2001, 2003), *Infocom* (2004), *HotNets* (2003), *HotOS* (2001), *USENIX Security Symposium* (2002), *ACM Computer Communication Review*, *IEEE Network Magazine*, *Image Communication* (EURASIP), *ASPLOS* (2004), *MobiSys* (2004), *USENIX* (2005), *NSDI* (2005), *IPTPS* (2005).

References

Prof. Hari Balakrishnan
MIT Computer Science & AI Lab
32 Vassar Street, 32G-940
Cambridge, MA 02139
(617) 253-8713
hari@csail.mit.edu

Prof. M. Frans Kaashoek
MIT Computer Science & AI Lab
32 Vassar Street, 32G-992
Cambridge, MA 02139
(617) 253-7149
kaashoek@csail.mit.edu

Prof. Jennifer Rexford
Princeton University
Department of Computer Science
35 Olden Street, CS 306
Princeton, NJ 08544
(609) 258-5182
jrex@cs.princeton.edu

Prof. Ramesh Johari
Stanford University
Department of Management Science and Engineering
380 Panama Mall
Stanford, CA 94305
(650) 723-0937
ramesh.johari@stanford.edu

Prof. Lixin Gao
Department of Electrical and Computer Engineering
Knowles Engineering Building
University of Massachusetts
Amherst, MA 01002
(413) 545-4548
lgao@ecs.umass.edu

Internet Routing

The Internet is composed of more than 17,000 independently operated networks, or autonomous systems (ASes), that exchange routing information using the Border Gateway Protocol (BGP). Network operators in each AS configure routers to control the routes that the routers learn, select, and propagate. Configuring a network of BGP routers is like writing a distributed program where complex feature interactions occur both within one router and across multiple routers. This complex process is exacerbated by the number of lines of code, by the absence of useful high-level primitives in today's router configuration languages, by the diversity in vendor-specific configuration languages, and by the number of ways in which similar high-level functionality can be expressed in a configuration language. As a result, router configurations tend to have faults. Faults in BGP configuration can cause forwarding loops, packet loss, and unintended paths between hosts. Operators must be able to evaluate the effects of a configuration and be assured that the configuration is correct before deploying it. My dissertation advances the state of the art in Internet routing by devising fault detection and modeling tools for today's Internet routing protocols and proposing a new Internet routing architecture that alleviates many of the problems we uncovered in our work on fault detection and modeling.

Detecting Faults in BGP Configuration with Static Analysis MIT

rcc, the *router configuration checker*, detects faults in the BGP configurations of routers in an AS using static analysis. **rcc** detects two broad classes of faults that affect network reachability: route validity faults, where routers may learn routes that do not correspond to usable paths, and path visibility faults, where routers may fail to learn routes for paths that exist in the network. **rcc** enables network operators to test and debug configurations before deploying them in an operational network, improving on the status quo where most faults are detected only during operation. **rcc** has been downloaded by more than sixty network operators to date. I presented **rcc** to the North American Network Operators Group (NANOG), and the tool has been used by several large backbone Internet Service Providers (ISPs) to successfully detect faults in deployed configurations. This work was inspired by my work on the *routing logic* that I presented at the 2003 *ACM SIGCOMM Workshop on Future Directions in Network Architecture* and appears at the *2nd USENIX Symposium on Networked Systems Design and Implementation*. We have also studied configuration faults as part of several measurement studies. We presented an algorithm to detect route advertisements that violate peering contracts and an empirical study of their prevalence at the 2004 *ACM Internet Measurement Conference*.

Modeling Internet Routing for Network Engineering MIT/AT&T Labs–Research

Since interdomain route selection is distributed, indirectly controlled by configurable policies, and influenced by complex interactions with *intra*domain routing protocols, operators cannot predict how a particular BGP configuration would behave in practice. We devised an algorithm that computes the outcome of the BGP route selection process for each router in a *single* AS, given only a static snapshot of the network state, without simulating BGP's complex dynamics. Using data from a large ISP, I demonstrated that the algorithm correctly computes BGP routing decisions and has a running time that is efficient and accurate enough for many tasks, such as traffic engineering and capacity planning. Studying the general properties and computational overhead of modeling the route selection process in each of these cases provides insight into the unnecessary complexity introduced by various aspects of today's interdomain routing architecture. I used these insights to propose improvements to BGP that avert the negative side effects of various artifacts without limiting functionality. This work appeared in *ACM SIGMETRICS* 2004 and has also been submitted to *IEEE/ACM Transactions on Networking*.

Internet Routing Architecture: Routing Control Platform MIT/AT&T Labs–Research

The limitations in today's routing system arise in large part from the fully distributed path-selection computation that the IP routers in an AS must perform. We proposed that interdomain routing should be separated from today's IP routers, which should simply forward packets (for the most part). Instead, a separate *Routing Control Platform (RCP)* should select routes on behalf of the IP routers in each AS and exchange reachability information with other domains. RCP could both select routes for each router in a domain (*e.g.*, an AS) and exchange routing information with RCPs in other domains. By selecting routes on behalf of *all* routers in a domain, RCP can avoid many internal BGP-related complications that plague today's mechanisms for disseminating and computing routes within an AS. RCP facilitates traffic engineering, simpler and less error-prone policy expression, more powerful diagnosis and troubleshooting, more rapid deployment of protocol modifications and features, enforceable consistency of routes, and verifiable correctness properties. The architectural proposal for RCP appeared at the 2004 *ACM SIGCOMM Workshop on Future Directions in Network Architecture*; the design and implementation of an RCP prototype won the best paper award at the *2nd USENIX Symposium on Networked Systems Design and Implementation (NSDI)*.

Internternet Measurement

Understanding End-to-End Internet Path Failures MIT

Empirical evidence suggests that reactive routing systems, which detect and route around faulty paths based on measurements of path performance, improve resilience to Internet path failures. We studied *why* and under *what circumstances* these techniques are effective by correlating end-to-end active probes, loss-triggered traceroutes of Internet paths, and BGP routing messages. This work was the first known study to correlate routing instability with degradations in *end-to-end* reachability. We found that most path failures last less than fifteen minutes. Failures that appear in the network core correlate better with BGP instability than failures that appear close to end hosts. Surprisingly, there is often increased BGP traffic both before and after failures. Our findings suggest that reactive routing is most effective between hosts that have multiple connections to the Internet and that reactive routing systems could pre-emptively mask about 20% of impending failures by using BGP routing messages to predict these failures before they occur. This work appeared at *ACM SIGMETRICS* 2003.

End-to-end path failures are typically attributed to either congestion or routing dynamics. Unfortunately, the extent to which congestion and routing dynamics cause end-to-end failures, and the effect of routing dynamics on end-to-end performance, are poorly understood. In a follow-up study, we used similar techniques to find that routing dynamics contribute significantly to end-to-end failures and, in particular, routing dynamics are responsible for most long-lasting path failures. The study also finds that long-lived end-to-end path failures that involve routing dynamics are typically caused by BGP convergence or instability. This work is the first to quantify the impact of routing dynamics on end-to-end path availability; it was submitted to *ACM SIGMETRICS* 2005.

Network Security

Infranet: Circumventing Web Censorship MIT

An increasing number of countries and companies routinely block or monitor access to parts of the Internet. To counteract these measures, we designed and implemented *Infranet*, a system that enables clients to surreptitiously retrieve sensitive content via cooperating Web servers distributed across the global Internet. These Infranet servers provide clients access to censored sites while continuing to host normal uncensored content. Infranet uses a tunnel protocol that provides a covert communication channel between its clients and servers, modulated over standard HTTP transactions that resemble innocuous Web browsing. In the upstream direction, Infranet clients send covert messages to Infranet servers by associating meaning to the *sequence* of HTTP requests being made. In the downstream direction, Infranet servers return content by hiding censored data in uncensored images using steganographic techniques. This work appeared at the *11th USENIX Security Symposium*.

Adaptive Streaming Media Protocols

Reliable, Adaptive Video Streaming MIT

Video compression exploits redundancy between frames to achieve higher compression, but packet loss can be detrimental to compressed video with interdependent frames because errors potentially propagate across many frames. In my Master's thesis, I quantified the effects of packet loss on the quality of MPEG-4 video, developed an analytical model to explain these effects, and presented an RTP-compatible protocol, called *SR-RTP*, that *adaptively* delivers higher quality video in the face of packet loss. This work appeared at the *12th International Packet Video Workshop* and was later implemented as part of a streaming video server for MIT Project Oxygen. We also designed a scheme for performing quality adaptation of layered video for a general family of congestion control algorithms called *binomial congestion control*. This work appeared at the *11th International Packet Video Workshop*.

Video Transcoding Hewlett-Packard Laboratories

We designed and implemented an algorithm that transcoded MPEG video input to a lower-bitrate H.263 progressive bitstream, facilitating the transmission of a digital television signal over a wireless medium. This algorithm was the first to use both spatial and temporal downsampling in an MPEG-2 to H.263 field to frame transcoder to achieve substantial bitrate reduction. The proposed algorithm exploits the properties of the MPEG-2 and H.263 compression standards to perform interlaced to progressive (field to frame) conversion with spatial downsampling and frame-rate reduction in a CPU and memory efficient manner, while minimizing picture quality degradation. This work appeared at the *IEEE International Conference on Image Processing* in 1999.