



Volume 1, Number 2

2nd Quarter, 2008

The State of the Internet

REPORT





Executive Summary

Each quarter, Akamai will be publishing a quarterly "State of the Internet" report. This report will include data gathered across Akamai's global server network about attack traffic and broadband adoption, as well as trends seen in this data over time. It will also aggregate publicly available news and information about notable events seen throughout the quarter, including Denial of Service attacks, Web site hacks, and network events.

During the second quarter of 2008, Akamai observed attack traffic originating from 139 unique countries around the world. Japan and the United States were the two largest attack traffic sources, accounting for over 50% of observed traffic in total. Akamai observed attack traffic targeted at over 400 unique network ports. Many of the ports that saw the highest levels of attack traffic were targeted by worms, viruses, and bots that spread across the Internet several years ago. In addition, "SQL injection" Web site hacks continued to spread, infecting hundreds of thousands of Web pages.

Several significant Web site outages occurred during the second quarter, including problems at Amazon.com's e-commerce site, Slashdot.org, and several large shared hosting providers, as well as the "cloud computing" platforms delivered by Google and Amazon.com.

Akamai observed that from a global perspective, South Korea continued to have the highest measured levels of "high broadband" (>5 Mbps) connectivity. In the United States, Delaware once again topped the list, with over 65% of connections to Akamai occurring at 5 Mbps or greater. At the other end of the bandwidth spectrum, Rwanda and the Solomon Islands continued to top the list of slowest countries, with 93% or more of the connections to Akamai from both countries occurring at below 256 Kbps. In the United States, Washington State and the District of Columbia turned in the highest percentages of sub-256 Kbps connections. However, in contrast to the international measurements, these states only saw 21% and 16% of connections below 256 Kbps, respectively.

Table of Contents

1: INTRODUCTION	3
2: SECURITY	4
2.1 Attack Traffic, Top Originating Countries	4
2.2 Attack Traffic, Top Target Ports	5
2.3 Distributed Denial of Services (DDoS) Attacks	6
2.4 Web Site Hacks	7
2.5 DNS Hijacks	8
3: NETWORKS AND WEB SITES: ISSUES & IMPROVEMENTS	10
3.1 Network Outages	10
3.2 Web Site Outages	10
3.3 Routing Issues	11
3.4 Significant New Connectivity	12
3.5 DNS Expansion	13
3.6 IPv6	13
4: INTERNET PENETRATION	14
4.1 Unique IP Addresses Seen By Akamai	14
4.2 Internet Penetration	15
5: GEOGRAPHY	16
5.1 High Broadband Connectivity: Fastest International Countries	16
5.2 High Broadband Connectivity: Fastest U.S. States	18
5.3 Broadband Connectivity: Fast International Countries	19
5.4 Broadband Connectivity: Fast U.S. States	21
5.5 Narrowband Connectivity: Slowest International Countries	22
5.6 Narrowband Connectivity: Slowest U.S. States	23
APPENDIX: SELECTED INTERNATIONAL DATA	24

Introduction

Akamai's globally distributed network of servers allows us to gather massive amounts of information on many metrics, including connection speeds, attack traffic, and network connectivity/availability/latency problems, as well as user behavior and traffic patterns on leading Web sites.

In the second quarter of 2008, distributed denial of service (DDoS) attack traffic continued to target exploits that were identified years ago, suggesting that there is still a significant population of insufficiently patched systems connected to the Internet, and that the Slammer, Sapphire, and Sasser worms may still be active, particularly in Japan, the United States, and China. A number of DNS hijackings were reported during the quarter as well, with Comcast, Photobucket, and ICANN all falling victim. In addition, a number of high profile Web sites and several large shared hosting providers all experienced outages. These problems impacted thousands of Web sites.

The percentage of high-speed (>5 Mbps) connections to Akamai grew rapidly during the second quarter, with significant growth seen both internationally and in the United States. Decreases in the percentage of narrowband (<256 Kbps) connections to Akamai were also seen both internationally and in the United States, likely due, in part, to the growth in availability of, and options for, broadband connectivity.

Section 2: Security

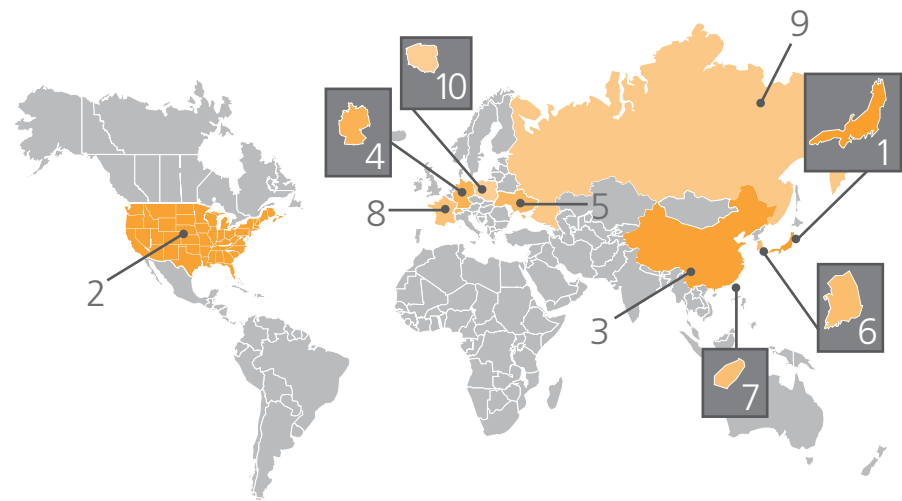
Akamai maintains a distributed set of agents deployed across the Internet that serve to monitor attack traffic. Based on the data collected by these agents, Akamai is able to identify the top countries from which attack traffic originates, as well as the top ports targeted by these attacks. (Ports are network layer protocol identifiers.) This section, in part, provides insight into Internet attack traffic, as observed and measured by Akamai, during the second quarter of 2008. While some quarter-over-quarter trending may be discussed, it is expected that both the top countries and top ports will change on a quarterly basis.

This section also includes information on selected DDoS attacks, Web site hacking attempts, and DNS hijackings as published in the media during the second quarter of 2008. These published reports indicate that DDoS attacks and Web site hacking attempts continued unabated in the second quarter. There were also a number of high-profile DNS hijackings. Note that Akamai does not release information on attacks on specific customer sites and that selected published reports are simply compiled here.

2.1 Attack Traffic, Top Originating Countries

During the second quarter of 2008, Akamai observed attack traffic originating from 139 unique countries around the world, up from 125 countries in the first quarter. Japan, the United States, and China were the three largest traffic sources respectively. Japan jumped to first place in the second quarter, up from seventh in the first quarter. China fell from first place to third place, and the United States maintained the second-place spot, originating 50% more attack traffic than in the first quarter. The trend in attack traffic distribution appears to be fairly consistent with the first quarter, as the top 10 countries were again responsible for just over three-quarters of the measured attack traffic.

Country	% Traffic	Q1 08 %
1 Japan	30.07	3.56
2 United States	21.52	14.33
3 China	8.90	16.77
4 Germany	5.56	1.58
5 Ukraine	2.34	0.41
6 South Korea	2.25	3.43
7 Taiwan	2.21	11.82
8 France	1.89	0.89
9 Russia	1.64	0.93
10 Poland	1.58	0.83
- OTHER	22.04	-



¹ http://www.grc.com/port_445.htm

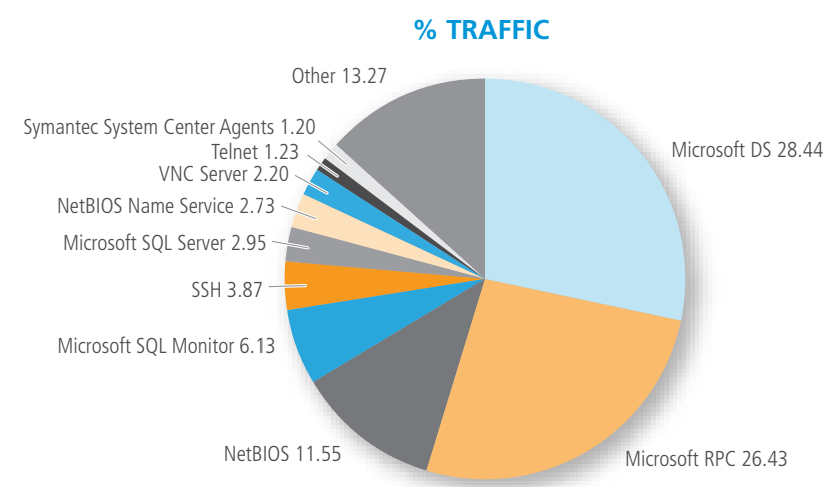
² <http://isc.sans.org/port.html?port=445>

While it is likely a contributing factor, there does not appear to be a clear and obvious link between the availability of high-speed connectivity and the likelihood that a country is a leading source of attack traffic. Of the top 10 countries listed in the table above, only Japan, the United States, and South Korea are also included in the Top 10 lists for High Broadband (>5 Mbps, Section 5.1) or Broadband (>2 Mbps, Section 5.3) International Countries. However, greater levels of Internet usage may account for higher levels of attack traffic, as six countries in the list above (the United States, China, Japan, Germany, France, and South Korea) can also be found in the Top 10 list of unique IP addresses seen by Akamai (Section 4.1).

2.2 Attack Traffic, Top Target Ports

During the second quarter of 2008, Akamai observed attack traffic targeted at over 400 unique ports, a nearly twenty-fold increase from the first quarter. Some of the attack traffic targeted services on well known ports, with others appearing to be more arbitrarily selected. Although the port distribution was fairly large, the bulk of the traffic was fairly concentrated, as the Top 10 targeted ports saw over 85% of the observed attack traffic.

The most attacked port in the first quarter, Port 135, fell to second place in the second quarter. This quarter, Port 445 took the top spot, seeing just over 28% of the observed attack traffic. This port is used for directory services on Microsoft operating systems (hence, the Microsoft-DS designation), and was intended to replace the NetBIOS trio of ports (137-139), for all versions of Windows after NT, as the preferred port for carrying Windows file sharing and numerous other services.¹ Back in 2005, a number of worms generated heavy traffic to this port, effectively creating Denial of Service (DoS) attacks, and the port was also probed by the Sasser worm in 2004 in an effort to exploit a known vulnerability.²



Destination Port	Port Use	% Traffic	Q1 08 %
445	Microsoft-DS	28.44	11.02
135	Microsoft-RPC	26.43	29.66
139	NetBIOS	11.55	13.27
1434	Microsoft SQL Monitor	6.13	NA
22	SSH	3.87	12.08
1433	Microsoft SQL Server	2.95	6.12
137	NetBIOS Name Service	2.73	NA
5900	VNC Server	2.20	1.65
23	Telnet	1.23	NA
2967	Symantec System Center Agents	1.20	2.93
Various	OTHER	13.27	-

Section 2: Security (continued)

Interestingly, while the services on Port 445 were intended to replace the NetBIOS services on Ports 137-39, these latter ports were still the target of over 14% of observed traffic. Observed attack traffic to Port 445, however, more than doubled quarter-over-quarter, from 11% in the first quarter of 2008 to over 28% in the second quarter. The largest number of attempted connections to this port came from Japan, followed by the United States.

For traffic coming from China, the highest percentage of attempted connections was directed at Port 1434, used for the Microsoft SQL Monitor. In 2003, this was the port used by the Slammer/Sapphire worm. In 2008, there are still reports on security forums of Slammer-profile traffic, so it is likely that this worm is still active, in some fashion, in China.

2.3 Distributed Denial of Service (DDoS) Attacks

In April, SlideShare, a startup that lets customers upload and embed Microsoft PowerPoint presentations on the Web, experienced multiple DDoS attacks from IP addresses originating in China. Attack vectors included a SYN-flood attack and a brute-force SSH attack.³ (As noted in Section 2.2, SSH continues to be one of the Top 10 ports targeted by attacks, with Akamai seeing nearly 4% of attack traffic targeting this port in the second quarter.)

In late June, a DDoS attack on the Marshall Islands' only ISP left the tiny country without the capability to receive incoming e-mail. While messages could be sent between customers of the National Telecommunications Authority (NTA), email from other ISPs was blocked from making its way to NTA customers.⁴ Reports indicated that the ISP's systems were hit by a four-fold increase in traffic, and that their mail gateways were seeing attempted connection rates as high as 500 per second.

In contrast to the DDoS attacks that are frequently traced back to malicious "botnets," online video site Revision3 suffered an attack in late May that was found to be originating from MediaDefender, a company involved in anti-piracy efforts. It is believed that the SYN-flood attack was related to issues concerning the use of a BitTorrent tracker being operated by Revision3 to facilitate the distribution of its own files.⁵

In another twist on DDoS attacks, Web sites in Japan are being flooded with traffic from botnets, with the attackers demanding money in return for stopping the attacks.⁶ While DDoS attacks are frequently transient, or short-lived, these attacks continue for as long as a week, causing significant financial damage to the targets. (Not including the demanded extortion fees.) As with many other DDoS attacks, and in line with the data shown in Section 2.1, the attacks appeared to originate in China.

³ <http://radar.oreilly.com/2008/05/slideshare-and-china.html>

⁴ <https://www.sans.org/newsletters/newsbytes/newsbytes.php?vol=10&issue=51#siD310>

⁵ http://www.datacenterknowledge.com/archives/2008/May/29/revision3_blames_mediadefender_for_attack.html

⁶ <http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1817>

⁷ <http://www.f-secure.com/weblog/archives/00001427.html>

⁸ <http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080424>

⁹ <http://www.eweek.com/c/a/Security/Botnet-Installs-SQL-Injection-Tool/>

¹⁰ http://news.cnet.com/8301-10784_3-9939297-7.html

¹¹ http://www.informationweek.com/blog/main/archives/2008/05/facebook_vulner.html

¹² http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9086700&intsrc=hm_list

¹³ http://us.mcafee.com/en-us/local/docs/Mapping_Mal_Web.pdf?cid=45044

2.4 Web Site Hacks

SQL injection continued to be an extremely popular vector for Web site hacks during the second quarter. According to an April 24 post on the F-Secure Weblog, "There's another round of mass SQL injections going on which has infected hundreds of thousands of websites. Performing a Google search results in over 510,000 modified pages." (Akamai's State of the Internet Report for the 1st Quarter, 2008 noted that a similar attack infected 10,000 Web pages in March 2008.) According to F-Secure, only Web sites using Microsoft IIS Web Server and Microsoft SQL Server were being targeted, and they noted that poorly written ASP and ASPX (.net) code that does not 'sanitize' user input was what made the attacks possible, not flaws in the server software.⁷ According to a post on the ShadowServer wiki,⁸ visiting an infected Web site would generate an attempt to download a piece of malware that steals passwords. A similar set of SQL injection attacks by the Asprox botnet in May was believed to have compromised approximately 1,000 Websites, according to researchers at SecureWorks.⁹

In May, hackers exploited a security hole in the publishing software used for the support forums on the Epilepsy Foundation Web site. The attackers posted hundreds of flashing images and links to other similar images, designed to cause seizures in site visitors with photosensitive epilepsy.¹⁰

Cross-site scripting (XSS) attacks also continued to be a problem for high-profile Web sites in the second quarter. In May, an XSS vulnerability was discovered on Facebook,¹¹ and PayPal announced that it had patched an XSS hole that could have undermined the security mechanisms that it had put into place.¹² In addition, an XSS vulnerability discovered in April on the Web site of presidential candidate Barack Obama redirected some site visitors to the Web site of opponent Hillary Clinton.

In June, security firm McAfee issued a report titled "Mapping the Mal Web, Revisited,"¹³ updating a March 2007 report that examined the distribution of malicious Web sites around the world, grouped by top level domain (TLD). The site safety assessments for the report came from the McAfee® SiteAdvisor® Web safety database, and are based on nearly 10 million site reports.

Section 2: Security (continued)

KEY FINDINGS FROM THE REPORT INCLUDED:

- Hong Kong (.hk) became the most risky country TLD, with 19.2 percent of all sites tested rated red (avoid) or yellow (use caution). China (.cn) was second with 11.8 percent.
- The most risky generic TLD remained .info, with 11.8 percent of all sites tested rated red or yellow. .com, the most popular generic TLD, is rated ninth riskiest overall with 5.3 percent, and is the fourth riskiest generic TLD.
- In the Europe, Middle East, and Africa regions, Romania (.ro) and Russia (.ru) are risky surfing destinations, with 6.8 percent of Romanian and 6.0 percent of Russian domains rated risky.
- In the North, South, and Latin America regions, the United States (.us) domain is the riskiest, with 2.1 percent. However, the Americas TLDs remain relatively safe to surf.
- The five least-risky TLDs are Slovenia (.si), Norway (.no), Japan (.jp), Governmental (.gov), and Finland (.fi), each with 0.2 percent or fewer domains rated risky.

2.5 DNS Hijacks

DNS celebrated its 25th birthday on June 23, 2008. On that date in 1983, Paul Mockapetris and the late Jon Postel ran the first successful test of the automated, distributed Domain Name System, which served to replace manually maintained “host tables,” which were text files that served as a phone book, enabling users on the Internet of the time to contact other systems by typing in names, instead of looking up the IP address of the remote system. As would be expected, maintaining these host tables as the Internet grew became increasingly challenging, and a growing operational nightmare.¹⁴ While the development of DNS has arguably facilitated the rapid growth of the Internet during the last quarter century, it still has its fair share of operational nightmares, as described below.

Comcast is one of the top three residential broadband service providers in the United States. On May 28, hackers changed the DNS registration records for the Comcast.net domain, redirecting visitors to IP addresses in Germany and elsewhere. The problem impacted user access to the Comcast portal, Webmail, and the official Comcast forums throughout the day on May 29, as corrected DNS information propagated through DNS servers across the Internet.¹⁵

¹⁴ http://www.wired.com/science/discoveries/news/2008/06/dayintech_0623

¹⁵ http://news.cnet.com/8301-10784_3-9954785-7.html

¹⁶ http://www.theregister.co.uk/2008/06/18/photobucket_dns_hack/

¹⁷ <http://blog.wired.com/27bstroke6/2008/06/icann-and-iana.html>

¹⁸ http://www.renesity.com/blog/2008/05/identity_theft_hits_the_root_n_1.shtml

¹⁹ <http://www.infoblox.com/library/pdf/2007-survey-executive-summary.pdf>

²⁰ http://www.renesity.com/blog/2008/06/securing_the_root_1.shtml

Popular photo-sharing site Photobucket was targeted by a DNS hack on June 17 that redirected requests from some users to a greeting and message from a Turkish hacking group.¹⁶ These same hackers also took control of several domain names belonging to ICANN and IANA for approximately 20 minutes on June 27, redirecting visitors to their Web sites to an alternative site that contained a message taunting the Internet governing bodies.¹⁷ (The Internet Assigned Numbers Authority [IANA] globally coordinates the DNS Root servers and IP address assignment. The Internet Corporation for Assigned Names and Numbers [ICANN] supervises the distribution of the world’s Internet domain names, IP addresses, and protocol port numbers.)

While not an intentional DNS hijack, many DNS servers that were contacting the L root name server were using an unauthorized L root name server due to a change in the IP address of the legitimate L root name server. These unauthorized servers were answering queries destined for the L root name server for nearly six months between November 2007 and May 2008. The IP addresses of the root name servers are stored in a static configuration file that is rarely updated; as a result, as systems around the world continued to send requests to the old IP address, they were being answered by unauthorized root name servers.¹⁸ (The configuration file change would need to be made in over 11 million name servers according to figures published by Infoblox in their “2007 DNS Survey.”¹⁹) While they were believed to have been providing correct responses, these name servers could have been easily used for more nefarious purposes, intentionally replying with incorrect information. A post on the Renesity blog highlights this issue, noting “While there is no evidence of foul play with regard to the bogus L root servers, the duration of this event, the potential for mayhem, and the complete absence of any controls whatsoever should give us all reason for concern.”²⁰

Finally, Internet security researcher Dan Kaminsky announced that he had discovered a vulnerability in the DNS protocol, and urged organizations running BIND and many other name servers to upgrade immediately to the most recent versions of the software. Mr. Kaminsky did not release detailed information about the vulnerability, so as to give providers time to secure their systems. He planned to make an announcement with additional details on August 5th at the Black Hat security conference. (This vulnerability, and the impact to the Internet, will be covered in more detail in next quarter’s State of the Internet report.)

Section 3: Networks and Web Sites: Issues & Improvements

The second quarter of 2008 saw few reported large-scale network outages, but there was a significant increase in reported Web site outages, including those affecting several large shared hosting providers, as well as nascent cloud computing services. Several new submarine fiber initiatives were announced during the quarter, which, when completed, will improve Internet connectivity between Europe, India, and the Middle East. From a protocol perspective, the second quarter saw increased DNS resolution capacity, steps towards additional generic top-level domains, and key IPv6 deadline for the U.S. federal government.

3.1 Network Outages

Unlike the first quarter of 2008, there were no large-scale network outages that were significant enough to be covered in the mainstream press. Instead, outages in the second quarter tended to be more transient and localized.

Businesses in Vermont found their Internet service interrupted in both May and June due to damage to fiber maintained by Level 3 Communications. A spokesperson for Level 3 noted that the outages were due to cuts on both sides of a “fiber ring” serving the area — the spokesman said that “To have outside influences cause outages on both sides of a fiber ring at the same time is extremely rare.”²¹

In the Netherlands, thousands of DSL customers using the KPN network were unable to access the Internet. KPN is the Dutch PTT (last mile provider), and it is believed that configuration problems with their ATM switches were the cause of the problem.²² Also in Europe, the London Internet Exchange (LINX) experienced several outages — a published report indicates that outages happened in late April, early May, and late May.²³

3.2 Web Site Outages

Hosting customers experienced a rough second quarter, as outages at major hosting providers forced thousands of sites off the Web for extended periods of time. On April 15, a number of dedicated server customers at Fasthosts were taken offline due to a hardware failure in a core network switch.²⁴ Web hosting providers Valueweb and Affinity Hosting, both operated by Hostway, were offline for more than 6 hours on May 27-28. This outage followed an extended multi-day outage that occurred in July 2007, as the migration of ValueWeb customer servers to Hostway encountered problems.²⁵ Power issues at a data center operated by HostDime took thousands of customer sites offline for a three-hour period on May 23.²⁶ On May 31, an explosion and fire at the primary data center of hosting provider The Planet caused a significant outage, impacting approximately 9,000 servers and 7,500 customers, as well as DNS, service management, and support servers.²⁷

²¹ http://www.vpr.net/news_detail/80930/

²² <http://webwereld.nl/articles/51048>

²³ http://www.theregister.co.uk/2008/05/28/linux_problems/

²⁴ http://www.datacenterknowledge.com/archives/2008/Apr/15/major_outage_at_fasthosts.html

²⁵ http://www.datacenterknowledge.com/archives/2007/Jul/31/data_center_migration_goes_awry_at_valueweb.html

²⁶ http://www.datacenterknowledge.com/archives/2008/May/23/power_outage_affects_hostdime_data_center.html

²⁷ <http://forums.theplanet.com/index.php?showtopic=90185&view=findpost&p=592355>

²⁸ <http://royal.pingdom.com/?p=285>

²⁹ <http://gigaom.com/2008/06/06/why-amazon-went-down-and-what-it-means-to-you/>

³⁰ <http://www.narus.com/blog/2008/06/06/amazon-outage-today/>

³¹ <http://www.destructoid.com/rumortoid-mgs-4-pre-order-bots-responsible-for-amazon-downtime-89492.phtml>

³² <http://bit.ly/20qpUX>

³³ http://www.datacenterknowledge.com/archives/2008/Jun/05/brief_outage_for_amazon_web_services.html

³⁴ http://www.renesys.com/blog/2008/05/identity_theft_hits_the_root_n_1.shtml

High profile Web sites also had a tough second quarter, with several of them experiencing multi-hour outages. According to Pingdom, a server monitoring service, the Slashdot.org Web site was down for more than five hours in the early morning of April 30.²⁸ Amazon.com’s namesake retail site experienced several availability challenges in early June, with a two-hour outage on the 6th²⁹, and additional outages on the 10th. Speculation on reasons for the outages ranged from a DDoS attack on IMDB.com³⁰ (a site owned and operated by Amazon) to bot activity related to the sale of some highly anticipated gaming system/game bundles.³¹

While not suffering full-blown outages that took the site completely off the Web, microblogging service Twitter suffered a number of well-reported problems during the second quarter. These problems generally resulted in users being unable to post new messages or view messages from others on the service. The problems were generally attributed to scalability issues that the service faces as it grows.

In addition, the silver lining was hard to find for customers of some cloud computing services, as outages hit their platforms during the second quarter. Google’s new “App Engine” utility computing platform saw several outages over the course of a twelve-hour period on June 17.³² Weather was the apparent cause of some downtime experienced by Amazon’s EC2 utility computing platform on June 4, as severe weather caused a power outage near one of Amazon’s data centers, believed to be in Ashburn, Virginia.³³

3.3 Routing Issues

Regarding the L root name server issue discussed in Section 2.5, a post on the Renesys blog asks, “So, what mechanisms are in place today to keep this from happening again?” and points out that the answer is “none”.³⁴ They do note that the L root name server issue is similar to the issue that impacted YouTube during the first quarter, and that similar to the solution to the YouTube problems, network providers need to be vigilant in filtering routing announcements, rejecting those that do not come from the proper sources.

Section 3: Networks and Web Sites: Issues & Improvements (cont'd)

3.4 Significant New Connectivity

In April, Reliance Globalcom announced plans to land their “Hawk” cable on Cyprus.³⁵ The cable will connect Cyprus to key European and Middle Eastern markets, and is expected to help the telecommunications industry, and the economy, in this island nation of 792,000 people.

A consortium of 16 telecommunications firms has contracted to build a 15,000 km submarine cable system linking India with Europe via the Middle East. The Europe India Gateway (EIG) will cost \$700 million and add 3.84 Tbps of capacity. The EIG consortium includes firms from the US, Europe, Africa, the Middle East and India – including AT&T, Verizon, BT, Cable & Wireless, MTN, Telecom Egypt, Omantel, Saudi Telecom Company, du, Bharti Airtel, Gibraltar’s Gibtelecom, PT Comunicacoes of Portugal, Djibouti Telecom, Maroc Telecom, Libya Telecom and Technology, and Telkom South Africa. Initial landings are for the cable are planned for the UK, Portugal, Gibraltar, Morocco, Monaco, France, Libya, Egypt, Saudi Arabia, Djibouti, Oman, the United Arab Emirates, and India.

At least two other new cables serving much the same route as the EIG are also currently being planned. Tata Communications is leading the consortium behind the IMeWe system, due to add another potential 3.84 Tbps to the route when it goes live in 2009. Also backing IMeWe are Etisalat, France Telecom, Ogero of Lebanon, PTCL of Pakistan, TIS Sparkle of Italy, as well as EIG investors Bharti Airtel, Telecom Egypt and STC. Tata is also behind the TGN Eurasia Cable System, set to link Mumbai with Paris, London and Madrid via Egypt, with Seacom and Telecom Egypt as fellow sponsors.³⁶

Along these lines, research firm Telegeography’s annual Global Bandwidth Research Service noted that 25 new submarine cables will be built over the next three years.³⁷

The need for continued capacity growth was underscored in statements made by AT&T’s vice president of legislative affairs, Jim Cicconi, in April. During a speech at a Web 2.0-related forum, Cicconi claimed, “We are going to be butting up against the physical capacity of the Internet by 2010” due to the growth in the consumption of high-definition video. Cicconi went on to claim that video will comprise 80% of all traffic by 2010, up from 30% today.³⁸ However, the veracity of these claims was widely contradicted by networking experts, including a long thread on David Farber’s Interesting People mailing list.³⁹ Regardless, predictions about future Internet traffic tend to point toward significant growth, with a presentation by Andrew Odlyzko of the University of Minnesota’s Digital Technology Center citing industry three industry white papers that predict 40%, 55%, and 100% cumulative annual growth rates in traffic.⁴⁰

³⁵ <http://www.rediff.com/money/2008/apr/17reliance2.htm>

³⁶ http://www.capacitymedia.com/images/library/files/JUNE_08_News_Views_pg_4-6+8+10+12+14-15+18_v6.pdf

³⁷ http://www.telegeography.com/cu/article.php?article_id=22700

³⁸ http://news.cnet.com/2100-1034_3-6237715.html

³⁹ <http://www.interesting-people.org/archives/interesting-people/200804/msg00151.html>

⁴⁰ <http://www.dtc.umn.edu/~odlyzko/talks/gilder2008.pdf>

⁴¹ http://www.verisign.com/press_releases/pr/page_043950.html

⁴² <http://www.networkworld.com/news/2008/062608-board-opens-way-for-new.html>

⁴³ <http://www.networkworld.com/news/2008/062608-ipv6-federal-government.html>

3.5 DNS Expansion

In June, VeriSign announced that it had completed additional infrastructure deployments in Europe for its Project Titan initiative, which is intended to improve the performance, redundancy, and security of core Internet DNS infrastructure that it manages. According to VeriSign, “Under Project Titan, VeriSign will increase its daily DNS query capacity from 400 billion queries a day to over 4 trillion queries a day and will increase the aggregate network bandwidth of its primary resolution centers around the world from more than 20 gigabits per second (Gbps) to greater than 200 Gbps per second.”⁴¹

At its meeting in late June, The Internet Corporation for Assigned Names and Numbers (ICANN) relaxed the rules for the introduction of new generic top-level domains (gTLDs, such as .com, .net, etc.). The action taken at the Paris meeting does not specifically create any new gTLDs at this time, but instead paves the way for the development of a set of rules governing the creation and management of new gTLDs.⁴² The decision is significant in that it will enable the creation of new “internationalized domain names,” using non-English scripts, as well as the potential creation of large numbers of commercial (.companyname) top level domains.

3.6 IPv6

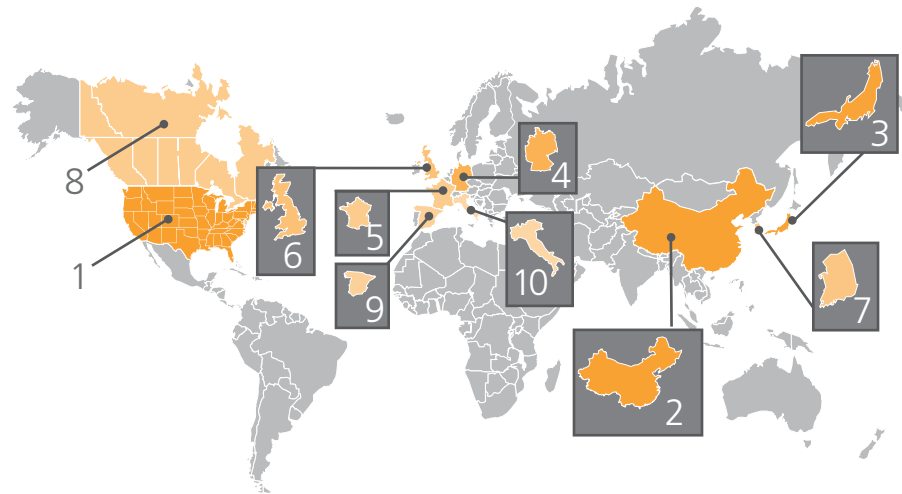
June 30, 2008 marked the deadline for all U.S. government networks to be IPv6 capable.⁴³ IPv6 is an upgrade to the Internet’s main communications protocol that provides virtually unlimited address space (2 to the 128th power, or $3.40282367 \times 10^{38}$, IP addresses), built-in security and simplified network management. Created by the Internet Engineering Task Force in 1998, IPv6 replaces IPv4, which supports 4.3 billion individually addressed devices on the network. Under a White House policy directive issued in August 2005, all federal agencies had to demonstrate the ability to pass IPv6 packets across their backbone networks by the June 30 deadline.

Section 4: Internet Penetration

4.1 Unique IP Addresses Seen By Akamai

Through a globally-deployed server network, and by virtue of the billions of requests for Web content that it services on a daily basis, Akamai has a unique level of visibility into the levels of Internet penetration around the world. In the second quarter of 2008, over 346 million unique IP addresses connected to the Akamai network – five percent more than in the first quarter. Similar to the first quarter, nearly 30% of those IP addresses came from the United States and fewer than 10% came from China.

Country	Q2 08 Unique IP's	Q1 08 Change	Q4 07 Change
- Global	346,151,241	+5.2%	+11%
1 United States	102,006,996	+5.2%	+11%
2 China	34,004,601	+4.8%	+13%
3 Japan	25,456,816	+2.8%	+4.9%
4 Germany	23,826,611	+5.1%	+18%
5 France	16,909,729	+2.9%	+6.3%
6 United Kingdom	16,552,605	+4.2%	+11%
7 South Korea	13,249,291	-2.2%	+0.3%
8 Canada	10,144,269	+3.5%	+7.8%
9 Spain	8,472,640	+3.7%	+7.8%
10 Italy	6,977,409	+5.3%	+13%



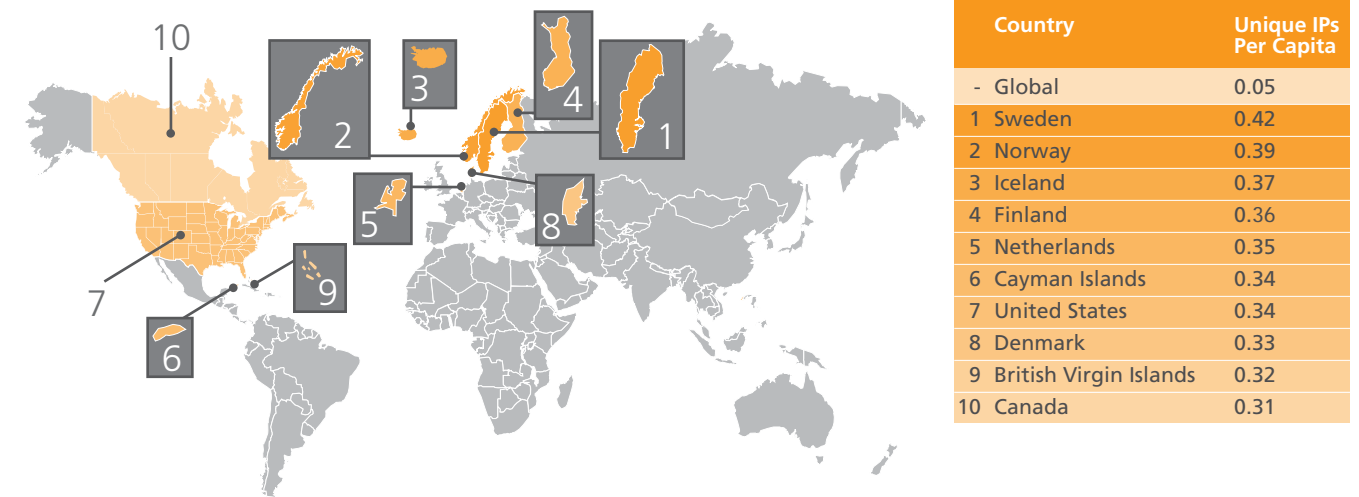
Every country in the top 10, with the exception of South Korea, showed an increase in the number of IP addresses connecting to Akamai's network in the second quarter. It is not clear why the number of unique IP addresses seen from South Korea decreased by approximately 300,000 in Q2, as there were no widely reported shutdowns of Internet cafes, or other wide-scale problems that would have prevented users in the country from accessing the Internet. In addition, over the first half of 2008, the number of IP addresses from all of the countries in the top 10 increased – Germany saw the most significant increase at 18%.

Looking at the "long tail," there were 185 countries with fewer than 1 million unique IP addresses connecting to Akamai in the second quarter of 2008, 149 with under 100,000 unique IP addresses, and 38 with fewer than 1,000 unique IP addresses. These country counts all decreased quarter-over-quarter, which likely speaks to growth in Internet connectivity on a global basis.

Interestingly, the *22nd Statistical Report on the Internet Development in China*⁴⁴ notes that at the end of the second quarter, China had 253 million "netizens" (Internet users). This count results in an Internet user-to-unique IP ratio of just over 7:1. In contrast, the latest Nielsen//NetRatings data suggests that the United States had over 219 million Internet users as of the end of May 2008,⁴⁵ resulting in Internet user-to-unique IP ratio of just over 2:1. One possible explanation for the large difference in these ratios may be how these users are accessing the Internet. Shared Internet cafes are extremely popular in China, with a March 2007 *Business Week* article noting "The country has about 113,000 licensed Internet cafes, and there are many more that operate illegally."⁴⁶ In the United States, Internet users are more likely to be connecting to the Internet from a personal computer used by a single user, or shared among a small number of household members.

4.2 Internet Penetration

How does the number of unique IP addresses seen by Akamai compare to the population of each of those countries? Asked another way, what is the level of Internet penetration in each of those countries? Using 2008 global population data from the United States Census Web site⁴⁷ as a baseline, levels of Internet penetration for each country around the world were calculated. The largest increase in the number of unique IP addresses per capita from the first quarter of 2008 was in the British Virgin Islands, with a 7% increase. Overall, the Top 10 countries did not change quarter-over-quarter.



These per capita figures should be considered as an approximation, as the population figures used to calculate them are static estimates – obviously, they will change over time, and it would be nearly impossible to obtain exact numbers on a quarterly basis. In addition, individual users can have multiple IP addresses (handheld, personal/home system, business laptop, etc.). Furthermore, in some cases, many individuals are represented by a single IP address (or small number of IP addresses), as they access the World Wide Web through a firewall proxy server. Akamai believes that it sees approximately 1 billion users per day, though we see only see approximately 350 million unique IP addresses.

⁴⁴ <http://www.cnnic.cn/html/Dir/2008/07/31/5247.htm>

⁴⁶ http://www.businessweek.com/globalbiz/blog/eyeonasia/archives/2007/03/no_new_internet.html

⁴⁷ <http://www.census.gov/ipc/www/idb/tables.html>, <http://www.census.gov/ipc/www/popclockworld.html> (03/01/08 estimate)

⁴⁵ <http://www.internetworldstats.com/am/us.htm>

