Akamai Volume 1, Number 3

3rd Quarter, 2008

The State of the Internet

REPORT

The "spinning globe" featured in the Akamai NOCC represents where Akamai servers are located and how much traffic they are seeing.

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, including outages and new connections.

During the third quarter of 2008, Akamai observed attack traffic originating from 179 unique countries around the world. China and the United States were the two largest attack traffic sources, accounting for over 45% of observed traffic in total. Akamai observed attack traffic targeted at nearly 2,400 unique ports, with the top 10 ports seeing over 85% of the observed attack traffic. Web site and Internet security were regularly in the news during the quarter, as several proof-of-concept attack vectors were announced, targeting social networking Web sites, as well as DNS, BGP and TCP, all core underlying Internet protocols.

Hurricanes Gustav and Ike, which made landfall in the United States in September, caused Internet outages in the states that they swept through. Notable Web site outages in the third quarter were attributed to increased traffic, human error and power outages.

Global connectivity saw big advances in the third quarter, with various undersea cable projects getting underway or nearing completion, the commercial launch of WiMAX services in a number of countries, and the announcement of fiber-to-the-premises services that will bring gigabit-speed connections to subscribers in Japan, the Ukraine and the Netherlands.

Akamai observed a nearly ten percent increase globally in the number of unique IP addresses connecting to Akamai's network, and this increase may be attributable to more people turning to the World Wide Web for news and video content related to the Beijing Olympic Games, which took place in August. From a global connection speed perspective, South Korea had the highest levels of "high broadband" (>5 Mbps) connectivity for the third straight quarter. In the United States, Delaware also maintained its top position, with 55% of connections to Akamai occurring at 5 Mbps or greater. Looking at observed "narrowband" (<256 Kbps) connections, Mayotte and Equatorial Guinea were the "slowest" countries, with 97% and 94% of connections to Akamai, respectively, occurring at speeds below 256 Kbps. In the United States, the District of Columbia and Washington State continued to have the highest percentages of observed connections below 256 Kbps. However, these regions also saw a significant quarter-over-quarter decline in narrowband connection percentages, down 25% and 46% respectively as compared to the second quarter.

Table of Contents

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 third quarter of 2008, observed Distributed Denial of Service (DDoS) attack traffic continued to target a consistent set of ports, likely indicating continued activity by malware targeting exploits that were identified several years ago. Several proof-of-concept attack vectors were announced, targeting social networking Web sites, as well as DNS, BGP and TCP, all core underlying Internet protocols. Exploitation of the vulnerabilities described within these announcements could cause significant problems for systems connected to the Internet.

Several network outages in the United States, due to hurricanes, were observed in the third quarter, though global connectivity continued to become more robust, with various undersea cable projects getting underway or nearing completion, the commercial launch of WiMAX services in a number of countries, and the announcement of fiber-to-the-premises services bringing gigabit-speed connections to subscribers in several countries.

The percentage of high-speed (>5 Mbps) connections to Akamai continued to grow during the third quarter, though growth rates in several countries, as well as the United States, were lower than in the second quarter. 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 third 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, Web-based exploits and DNS-, BGP- and TCP-based attacks as published in the media during the third quarter of 2008. As noted below, a number of new high-profile attack vectors were discovered or announced during the quarter. 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 third quarter of 2008, Akamai observed attack traffic originating from 179 unique countries around the world, up nearly 30% from the second quarter count of 139 countries. This quarter, China moved back into the first place slot, which it held in the first quarter as well, and the United States maintained its second place position. Japan's percentage of attack traffic dropped back to first quarter levels, moving them into fifth place this quarter. It's not clear what drove the surge in attack traffic that was observed to originate from Japan during the second quarter — continued observation over time should help determine if it was an anomaly, or if there are other factors that may have influenced it.

The trend in attack traffic distribution continues to be consistent with the previous two quarters, with the top 10 countries continuing to be the source for just over three-quarters of observed attack traffic. However, the list of countries that make up the top 10 continues to be dynamic, as expected — France, Poland and the Ukraine dropped out of the top 10 quarter-over-quarter, while Brazil reappears in sixth place, as it did in the first quarter.

	Country	% Traffic	Q2 08 %
1	China	26.85	8.90
2	United States	19.68	21.52
3	South Korea	9.37	2.25
4	Sweden	3.86	0.48
5	Japan	3.13	30.07
6	Brazil	2.64	1.53
7	Taiwan	2.54	2.21
8	Hong Kong	2.26	0.46
9	Germany	2.20	5.56
10	Russia	1.94	1.64
–	OTHER	25.53	–

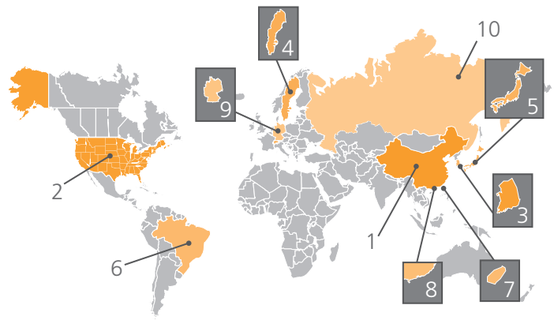


Figure 1: Attack Traffic, Top Originating Countries

Akamai's observations are supported by other industry findings as well. Security service provider SecureWorks issued a press release[1] on September 22 that listed the top 10 countries responsible for attacks attempted against the company's clients in 2008. According to the release, the top 10 countries were the United States, China, Brazil, South Korea, Poland, Japan, Russia, Taiwan, Germany and Canada. With the exception of Canada, the other nine countries have appeared in Akamai's top 10 list at least once during the last three quarters. (Canada is No.11 on the third quarter list, up from No.16 in the second quarter.)

2.2 Attack Traffic, Top Target Ports

During the third quarter of 2008, Akamai observed attack traffic targeted at nearly 2,400 unique ports, a nearly six-fold increase from the second quarter. Consistent with the prior quarter, some of the attack traffic targeted services on well-known ports. While the distribution of target ports was very broad, the bulk of the traffic was fairly concentrated, as the top 10 targeted ports saw over 85% of the observed attack traffic, which is also consistent with second quarter measurements. It is not clear what is driving the rapid quarter-over-quarter increases in target port counts.

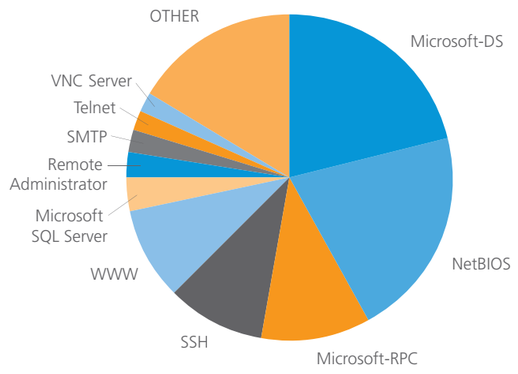


Figure 2: Attack Traffic, Top Target Ports

For the second quarter in a row, Port 445 (Microsoft-DS) held the first place spot, though with a smaller percentage of the overall observed traffic than in the second quarter. Ports 139 and 135 remained in the top three, though they switched places quarter-over-quarter. New to the top 10 in the third quarter is port 25 (SMTP) — this may be due to attackers or botnets scanning for open mail relays through which to send spam. Returning to the list are port 80 (WWW) and port 4899 (Remote Administrator), which both appeared on the list in the first quarter as well. As the name suggests, the Remote Administrator service (radmin) listens on port 4899, and is used to provide remote access to Microsoft Windows systems. While there have been no recently published exploits for radmin, attackers may be attempting to find and exploit systems with weak default passwords, which would provide them the ability to remotely monitor, control and transfer files to and from the compromised system.

Interestingly, though it didn't make it into the global top 10, the top target port seen from China was Port 7212, accounting for 16% of the observed attack traffic from the country. While not previously used to spread malware in the past, it appears that the port is used by a program

Destination Port	Port Use	% Traffic	Q2 08 %
445	Microsoft-DS	21.12	28.44
139	NetBIOS	21.09	11.55
135	Microsoft-RPC	10.68	26.43
22	SSH	9.73	3.87
80	WWW	9.18	0.91
1433	Microsoft SQL Server	3.20	2.95
4899	Remote Administrator	2.56	0.89
25	SMTP	2.28	0.70
23	Telnet	2.05	1.23
5900	VNC Server	1.93	2.20
Various	OTHER	16.17	–

called GhostSurf.[2] Older versions of the software, when run, created open proxy relays. A published security advisory[3] notes "Users may inadvertently be subject to forwarding data for those with malicious intent." It may be the case that attackers in China are attempting to identify available open proxies that they can relay malicious traffic through, potentially covering their tracks. In addition, Akamai observed that port 80 (the default port used for Web servers) was responsible for a disproportionately large percentage of detected attack traffic in the United States, Sweden and Russia. Given the continued growth in SQL injection attacks (see below), this traffic may have been, at least in part, attempts to identify Web servers with SQL injection vulnerabilities.

2.3 Distributed Denial of Service (DDoS) Attacks

While just a proof-of-concept, researchers at the Institute of Computer Science created a Facebook application that can create a botnet capable of launching a DDoS attack against a target system.[4] This proof-of-concept attack was created, in part, to expose the risks that the inherent trust of others plays in a social network. By exploiting the viral nature of application distribution on the Facebook platform, the researchers demonstrated that a botnet with thousands of users could easily be created, flooding a target with a large number of Web requests, causing it to become overloaded and ultimately unavailable. It is important to note that Akamai's services would help customers mitigate the effects of such an attack, as the requests could be absorbed or deflected by Akamai's servers at the edge of the Internet.

During the third quarter, Facebook and MySpace users were the target of a newly discovered worm, dubbed Net-Worm.Win32.Koobface, according to researchers at Kaspersky Lab.[5] The worm e-mails friends of Facebook and MySpace users, and includes a link to a bogus YouTube site. If a user attempts to access the link, they are prompted to download and install what claims to be a new version of the Adobe Flash player. Instead, the code downloaded is a network worm that recruits victim's machines into botnets.

While it is not clear how many machines were recruited into botnets by the "Koobface" worm, the number of hijacked systems ("zombies") that belong to botnets responsible for some DDoS attacks surged over the third quarter. The Shadowserver Foundation[6] (a group of security professionals who volunteer their time to track and measure botnets to help law enforcement investigations) reported a significant increase, based on their monitoring, which is likely indicative of the general trend. In June 2008, the Shadowserver Foundation were aware of about 100,000 machines that were part of a botnet, and by late August this number had more than quadrupled to over 450,000 machines. According to "Bot Count" statistics[7] on the Shadowserver Web site, this climbed to over 500,000 machines in early September before beginning to decline to approximately 350,000 by the end of the quarter, as shown in Figure 3. The growth in the number of infected machines, according to the Internet Storm Center,[8] could be related to an increase in SQL injection attacks observed during the same time frame.

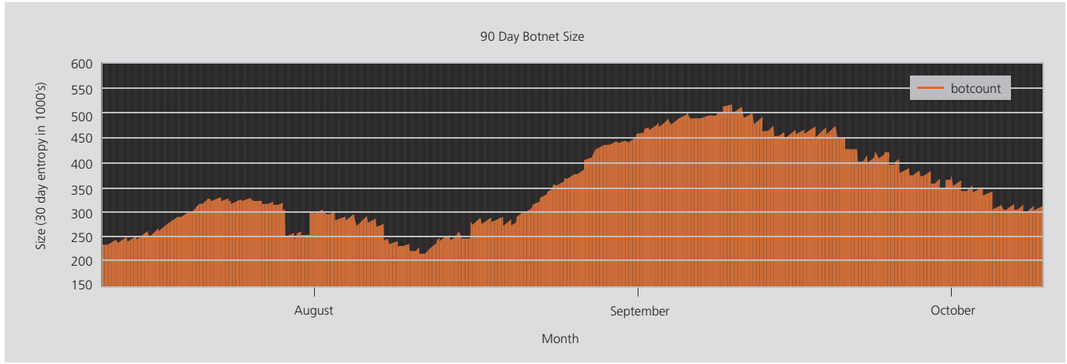


Figure 3: Botnet sizes grew significantly during the third quarter of 2008, reaching over a half-million machines during September. (Graph courtesy of The Shadowserver Foundation)

No discussion of DDoS attacks for the third quarter of 2008 would be complete without looking at those that occurred in July and August, related to the Russian-Georgian political conflict. DDoS attacks and site defacements targeted the Web sites of Georgia's President, the Georgian Ministry of Foreign Affairs and the Georgian Ministry of Defense. The President's Web site was ultimately moved to a hosting company based in Atlanta, Georgia (in the United States), and the Georgian Ministry of Foreign Affairs chose to provide updates using a site hosted on Google's Blogger service.[9] SQL injection attacks were another attack vector used against Georgian sites, as it was reported that Russian hackers were distributing lists of Georgian Web sites that were vulnerable to SQL injection attacks, enabling site defacement to be automated.

Georgian hackers fought back, targeting Web and DNS servers at the Russian News and Information Agency (RIA Novost) with DDoS attacks. In addition, Estonian officials offered their support to Georgia, noting that the attacks targeting Georgia were similar to those made against Estonian Web sites in 2007. Specifically, according to the Shadowserver Foundation, similar to the attacks against Estonia, a number of Russian blogs, forums and Web sites spread a Microsoft Windows batch script that was designed to attack Georgian Web sites by continually sending ICMP traffic via the 'ping' command to several Georgian websites, the vast majority of which are government-related.[10]

2.4 Web Site Hacks & Web-Based Exploits

A research report[11] published on the "insecurity iceberg" analyzed browser type (user-agent) data collected by Google between January 2007 and June 2008 in an effort to measure what the authors termed the "worldwide vulnerable browser population." After reviewing this user-agent data, the report's authors concluded, "The tip of the Web browser insecurity ice-berg was measured to be 637 million (or 45.2%) Internet users at risk worldwide due to not running the latest, most secure browser version. Meanwhile, hidden below the surface, the iceberg extends further, encompassing users that rely on outdated vulnerable browser plug-ins." Ultimately, these findings indicate that targeted exploitation of a known security problem in an older version of a Web browser could ultimately impact millions of Internet users, resulting in potential compromise of end-user systems, or the creation of a so-called botnet used to implement large-scale DDoS or SQL injection attacks, such as those described in Akamai's *1st Quarter, 2008* and *2nd Quarter, 2008 State of the Internet* reports.

In late September, word began to spread about a new Web-based attack vector known as "clickjacking" that affects all the major desktop platforms, including Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, Opera and Adobe Flash. Published descriptions[12] of clickjacking note, "With this exploit, once you're on the malicious web page, the bad guy can make you click on any link, any button, or anything on the page without you even seeing it happening." Browser vendors including Microsoft and Mozilla "concur independently that this is a tough problem with no easy solution at the moment," according to one of the researchers that discovered the exploit.

Also in late September, Princeton University researchers revealed that a number of popular Web sites, including those belonging to ING, MetaFilter, YouTube and the New York Times, were vulnerable to "cross-site request forgery" (CSRF) flaws.[13] By exploiting these flaws, an attacker can force the user's browser to request a page or action without the user knowing, or the Web site recognizing the request didn't come from the actual legitimate user. The flaw on the ING site would have let an attacker move funds from the victim's account to another account, while the flaws on the Metafilter and YouTube sites would have let the attacker essentially take over a victim's account. The flaw on the New York Times site let an attacker grab e-mail addresses of users registered on the site and use them for spamming or other malicious purposes. As of October 1, all of these sites had addressed their CSRF vulnerabilities.[14]

System "clipboards" were also getting hijacked by an attack discovered in August. According to a post[15] on ZDNet's Zero Day security blog, "In the Web attacks, which target Mac, Windows and Linux users running Firefox, IE and Safari, hackers are seizing control of the machine's clipboard and using a hard-to-delete URL that points to a fake anti-virus program. According to victims on several Web forums, the attack is coming from Adobe Flash-based advertising on legitimate sites — including Newsweek, Digg and MSNBC.com." According to a September 19 post[16] on the same blog, Adobe will mitigate these attacks in the final version of the upcoming release of Flash Player 10 by demanding user interaction when a Shockwave (.swf) file attempts to set data on a user's clipboard.

SQL injection attacks continued during the third quarter, and one high-profile site that became infected belonged to BusinessWeek. According to a report[17] from anti-virus firm Sophos, in September, hundreds of pages were affected on a section of BusinessWeek's Web site which offers information about where MBA students might find future employers. In addition, according to an August 7 article in The Register,[18] a new round of SQL injection attacks has infected millions of Web pages belonging to businesses and government agencies, including those that belong to the National Institute of Health and Department of Education in the United States, as well as UK Trade & Investment. A search highlighted in the article noted that at least 1.45 million Web pages had been infected as part of this new round of attacks. A post[19] on SecureComputing's TrustedSource™ blog on August 10th also reported the appearance of a new SQL injection attack; noting that it was targeting machines running Microsoft SQL Server, and possibly also Web servers with Sybase database backends, as they use a similar SQL syntax and table structure to Microsoft's SQL Server. The post's authors also stated that infected Web pages were found on government sites, sales sites, real estate sites and financial information sites.

In addition to the Russian/Georgian aggression that resulted in DDoS attacks on Georgian Web sites and Georgian network infrastructure, Russian hackers also targeted Lithuanian Web sites. According to the Web Host Industry News,[20] the 300 affected Web sites were hosted at Hostex, and the sites were defaced with recently banned Soviet symbols and profane messages. It is believed that the Web site defacements may have been a precursor to a planned DDoS attack against sites in Latvia, Ukraine, Lithuania and Estonia, according to a report from an Estonian television network.

2.5 DNS-Based Attacks

In the *2nd Quarter, 2008 State of the Internet* report, Akamai noted that Internet security researcher Dan Kaminsky had 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. According to multiple published descriptions, exploitation of the vulnerability would allow attackers to "poison" DNS caches by maliciously causing DNS servers to cache incorrect information. If this were to occur, users could be sent, unbeknownst to them, to fake Web sites controlled by an attacker, where usernames, passwords and other personally identifiable information could potentially be stolen. In addition to simply sending users to fake Web sites, other targets could include FTP services, mail servers, spam filters and SSL, which is used to make Web-based transactions more secure.

Described in Kaminsky's presentation[21] to the Black Hat conference in August, as well as in multiple published reports related to Kaminsky's findings, the vulnerabilities in DNS that he found concerned two key points:

1. Randomized DNS request transaction IDs — if the pool of random numbers used for transaction IDs is smaller than is defined in the DNS protocol specification, or transaction IDs are insufficiently random (and thus, more easily predictable), it becomes significantly easier for an attacker to return a forged reply to a query before the genuine reply arrives.
2. Source port randomization — some DNS server implementations use a fixed port for all outgoing queries, or insufficiently randomize the source port used. This too makes it easier for an attacker to inject a fraudulent reply that is accepted by the resolving nameserver as legitimate.

In each case, the attacker's reply then pollutes the cache of the resolving nameserver. Notably, just one type of forged reply can cause all future DNS queries to be directed to the attacker's nameservers so that it is not necessary to continually compromise the resolver's cache for other names in the target domain. For instance, an attacker could poison www.google.com, and give the "false" record a time-to-live (TTL) value lasting several years, so the resolving nameserver effectively never needs to ask Google again for the "real" IP address.

According to CNET,[22] Kaminsky first warned security software vendors about the problem in March, so they could start writing patches to address the problem. In an unprecedented, synchronized multivendor effort, many leading vendors of DNS server software and other Internet infrastructure components all released patches on July 8. Exploit code for the Metasploit Framework (a development platform for creating security tools and exploits) became available in late July,[23] and security firm MessageLabs recorded a 52 percent increase in suspicious DNS traffic between July and August.[24] Akamai advised customers that our Enhanced DNS and Global Traffic Management services were not affected by the vulnerabilities described by Kaminsky.

Enterprises and Internet Service Providers scrambled to patch their DNS servers, while many end user systems were patched automatically. An article published on InternetNews.com[25] noted, "Based on data from a tool that Kaminsky posted on July 8th, when the first patches for the DNS server were made available, 86 percent of people that came to his site were vulnerable. As of July 24th that number had dropped down to 52 percent." Based on data from Kaminsky's research, Clarified Networks developed a "DNS Repair Visualization"[26] video that illustrated where patches were being applied over time.

While the patches issued by software vendors addressed the immediate issue, longer-term fixes are required, and one technology that will help drive such longer-term fixes is known as DNSSEC. DNSSEC is short for DNS Security Extensions which, as the name suggests, are a set of extensions used to add an additional layer of security to the Domain Name System by providing a form of cryptographically signed verification for DNS information, which is intended to assure the authenticity of DNS responses.[27] .ORG and .GOV are the first generic top level domains to take steps toward implementing DNSSEC. According to a July 22 press release[28] from the Public Interest Registry, "A request by .ORG, The Public Interest Registry to bolster Internet security via the implementation of Domain Name Security Extensions (DNSSEC) was unanimously approved by the board of the Internet Corporation for Assigned Names and Numbers (ICANN) at the recent Paris meeting." Similarly, according to an August 22 memorandum[29] from the Office of Management and Budget in the Executive Office of the President, "The Federal Government will deploy DNSSEC to the top level .gov domain by January 2009. The top level .gov domain includes the registrar, registry and DNS server operations. This policy requires that the top level .gov domain will be DNSSEC signed and processes to enable secure delegated sub-domains will be developed." Country domains for the United Kingdom (.UK), Sweden (.SE), Brazil (.BR) and Bulgaria (.BG) have already adopted DNSSEC, according to Internet infrastructure news site CircleID.[30]

2.6 BGP-Based Attacks

A presentation[31] by Alex Pilosov and Tony Kapela at Defcon 16 in August was titled "Stealing the Internet: An Internet-Scale Man In The Middle Attack", and illustrated the exploitation of a design vulnerability in BGP that has existed since the protocol's inception: if not properly filtered by its service provider, a customer can inject whatever routes it wishes into the global Internet routing table. The described attack exploits BGP to fool routers into re-directing data to an eavesdropper's network, allowing the attacker to intercept data headed to a target IP address or group of addresses. The innovation in this attack, as noted on Wired's "Threat Level" security blog,[32] is that the intercepted data is silently forwarded to the actual destination, so that no outage occurs.

Ultimately, the issue highlighted by Pilosov and Kapela exists because the underlying architecture of BGP is based on trust — that is, when a router says that it is the best path to a given destination network, BGP assumes that it is telling the truth. A rogue router could advertise a more specific path to a destination network, and other routers, as directed by BGP, would begin directing traffic through that rogue router, where it could be intercepted, or in the case of the Pakistan Telecom/YouTube incident described in the *1st Quarter, 2008 State of the Internet* report, simply black-holed.

Several recognized Internet security experts, including Peiter "Mudge" Zatko and Stephen Kent, both currently with BBN Technologies, noted that they had described similar attack models for United States government agencies a number of years ago. Solutions to the problem, as described[33] by Kapela, Kent and others, include:

- ISPs aggressively filtering to allow only authorized peers to draw traffic from their routers, and only for specific IP prefixes
- Implementation of processes to authenticate ownership of IP blocks, and validation of the advertisements that ASes send to routers so they don't just send traffic to whomever requests the traffic

However, it is likely that it will take some time for any true solution to be implemented. Filtering, as described above, is labor intensive, and if just one ISP decides not to filter, then the system breaks down. One implementation of the authentication solution, as described above, would require the use of Secure BGP, developed by Kent and colleagues at BBN Technologies. Unfortunately, many current routers lack the memory and processing power to generate and validate signatures. In addition, router vendors have resisted upgrading the hardware because their customers (ISPs) haven't demanded it, due to the cost and effort involved in replacing existing deployed routers. (While Secure BGP would fix the problem, it is not the only possible solution.)

2.7 TCP-Based Attacks

In late September, Outpost24, a Swedish vulnerability firm, publicized an attack framework developed by their researchers that exploits several fundamental issues with TCP (Transmission Control Protocol — one of the key foundational protocols of the Internet) to cause denials of service and resource consumption on virtually any remote machine that has a TCP service listening for remote connections.[34] According to the researchers, the problem stems from issues in the way that Internet-connected devices (routers, computers, etc.) handle TCP connection requests from unknown, remote systems. While the underlying issues with TCP are well known within the networking and security community, the development of the attack framework received publicity, as expected, on industry Web sites and blogs.

The attack framework developed by the researchers, called "Sockstress", enabled them to produce DoS attacks on target systems, exploiting these flaws in TCP. One of the researchers noted that the attack, which can be carried out in less than five minutes, takes advantage of the way resources are allocated immediately after a successful three-way handshake, making it possible to claim so many resources that the compromised system crashes as a result. The researchers noted that this makes conventional measures to counteract DoS attacks ineffective.[35]

Section 3: Networks and Web Sites: Issues & Improvements

The third quarter of 2008 saw network outages in the United States caused by two major hurricanes, as well as outages in Georgia due to its military conflict with Russia. "Cloud" services continued to experience availability problems, and high traffic levels took down sites belonging to an Olympic gymnast and the United States House of Representatives. Announcements of new connectivity were numerous during the quarter, including more submarine cables, plans for satellite connectivity to developing regions, the launch of new WiMAX wireless services and gigabit speed connections for consumers and businesses.

3.1 Network Outages

Two major hurricanes battered the United States in September — Gustav primarily impacted Louisiana (as Katrina had three years prior), while Ike made landfall in Texas, but moved northeast through Arkansas, Missouri, Illinois, Indiana, Ohio and Pennsylvania.

In a blog post[36] covering the impact of Hurricane Gustav on Internet infrastructure in Louisiana, Renesys noted that it had identified more than 1,500 network prefixes that geo-located to Louisiana.

As shown in Figure 4, network outages peaked on September 2nd, when approximately one-seventh (14%) of the network prefixes monitored in the geographic area were unavailable. Renesys noted in its blog post that the peaks in the graph largely correspond to Bell South outages in the Baton Rouge area, and that the prevalence of Bell South outages was not surprising, as it originates over one-third of the network prefixes that geo-locate to Louisiana.

Hurricane Ike didn't batter the Gulf region as Gustav did, but had a nearly immediate impact on networks in Texas as it made landfall in Galveston and moved through Houston and Harris County.[37]

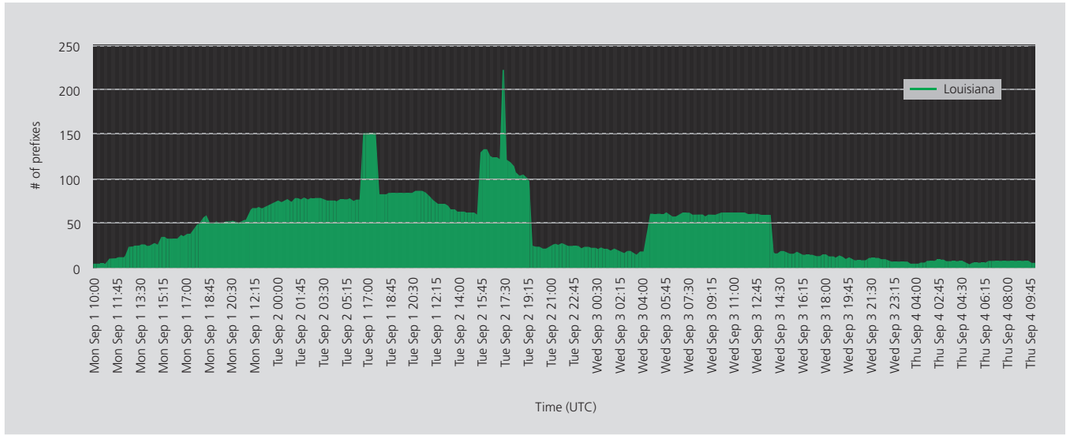


Figure 4: Network outages in Louisiana caused by Hurricane Gustav peaked on September 2. (Data courtesy of Renesys)

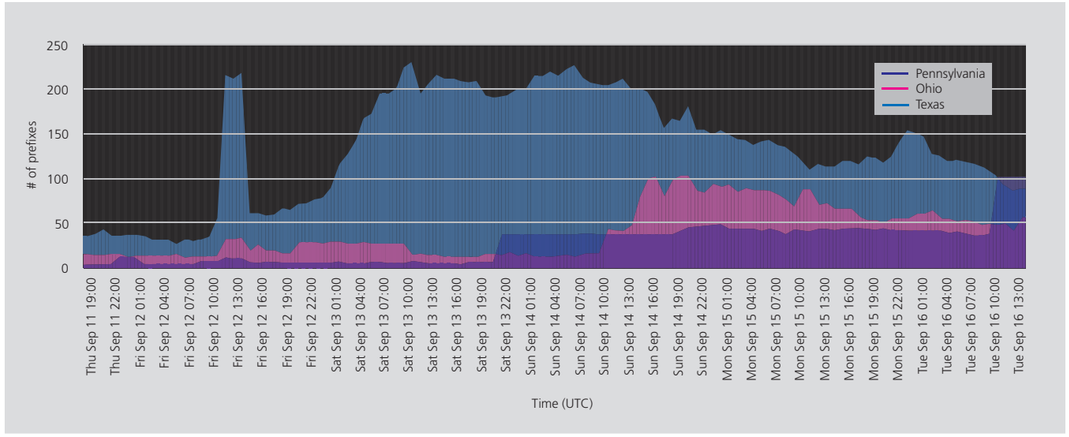


Figure 5: Network outages in Ohio and Pennsylvania grow as Ike moves northeast from Texas. (Data courtesy of Renesys)

As shown by the Renesys data in Figure 5, the number of network prefixes geo-located in Texas that became unavailable increased as Hurricane Ike moved across the state. As network connectivity returned in Texas, the number of outages detected in Ohio and Pennsylvania grew as the hurricane moved northeast across the Midwest. A Renesys blog post[38] noted that outages in Arkansas, Illinois, Indiana, Kentucky and Missouri were much less noticeable than those in Texas, Ohio, and Pennsylvania.

While targeted DDoS attacks were part of the Russian-Georgian conflict, as discussed in Section 2.3, a post[39] on the Renesys blog noted that the anticipated wide-spread, long-term outages had apparently not materialized. (Renesys identified 309 prefixes (networks) that geo-located to Georgia).[40] One noteworthy outage, according to Renesys, occurred over a five-hour period on August 15, where approximately one-third of the monitored networks became unavailable or unstable. In addition, Renesys also noted that during the three-day period from August 8 to August 10, up to 35% of Georgia-based prefixes disappeared from the Internet, as highlighted in Figure 6, and up to 60% of them were unstable. The resilience of the Internet was reinforced by the fact that none of the observed outages appeared to be permanent.

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

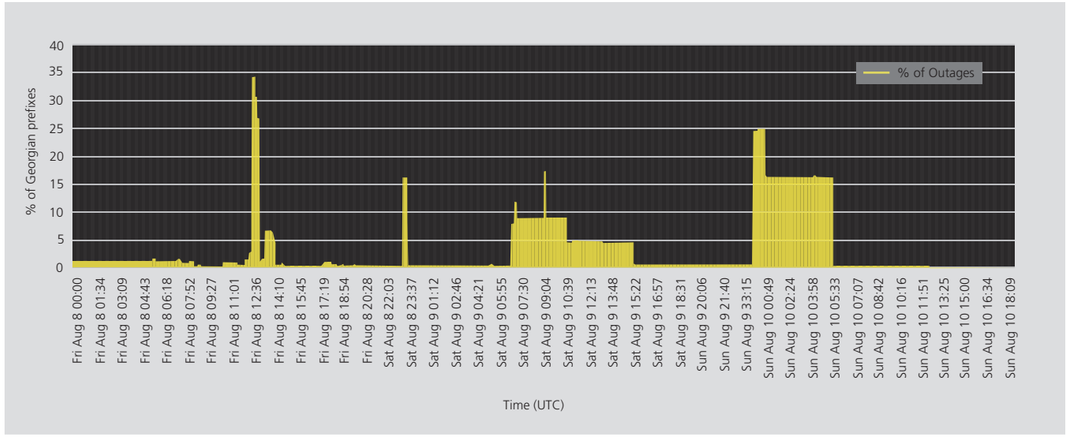


Figure 6: Between August 8 and August 10, up to 35% of networks in Georgia experienced outages. (Data courtesy of Renesys)

3.2 Web Site Outages

Google's Apps and Gmail services continued to experience availability issues during the third quarter, with multi-hour service availability issues noted on July 8, August 7 and August 11.[41] In addition, micro-blogging service Jaiku, acquired by Google in October 2007, saw a multi-hour outage on August 18.[42] The outage was related to a power failure at the data center where the site's servers are hosted, and impacted the sites of nearly 8,000 customers, including Jaiku itself.

XCalibre Communications' FlexiScale utility computing service saw a multi-day outage in late August. The company indicated human error related to the accidental deletion of one of its main storage volumes was the cause of the outage,[43] but did not provide any details on how many customers were impacted. Amazon's Simple Storage Service (S3) experienced a nearly eight-hour outage on July 20, caused by message corruption in server-to-server communications.[44] While Amazon.com did not release figures on the number of customers impacted, many Web 2.0 sites and services rely on Amazon's utility services, including S3.

In early September, Thailand's Information and Communications Technology Ministry sought court orders to shut down about 400 Web sites and advised Internet Service Providers to block another 1,200 Web sites it considers socially disturbing or dangerous to national security.[45]

After suffering a number of high-profile problems, as reported in the *2nd Quarter, 2008 State of the Internet* report, micro-blogging service Twitter greatly improved its uptime in the third quarter. According to monitoring service Pingdom,[46] Twitter saw less than an hour of downtime during each month of the past quarter, with an average availability of 99.88% for the quarter.

While the main Web sites supporting the 2008 Summer Olympic Games in Beijing remained available throughout the course of the event, NastiaLiukin.com, the official Web site for the United States gymnast who won a gold medal in the women's all-around finals, failed as a surge of traffic overwhelmed the shared server at DreamHost that supported the gymnast's Web site.[47]

Finally, at the end of September, performance and availability problems with the Web site for the United States House of Representatives stemmed from users attempting to download the text of a $700 billion emergency "bailout" bill and attempting to use the e-mail form on the site to contact their representatives. According to a spokesperson for the House Chief Administrative Officer, the site was seeing three to four times its normal traffic, which ultimately caused the performance and availability problems.[48]

3.3 Significant New Connectivity — Undersea Cables

Undersea cable projects continued to see significant growth around the world during the third quarter. A number of cables were completed and initial connections were made for other cable projects. Funding for still more cables was announced, in an effort to address the growing need for bandwidth in both developed and developing countries around the world.

Undersea capacity to and from Asia continues to grow rapidly. In addition to its investment in the Unity trans-Pacific submarine cable, Google is working with a consortium of carriers planning to build an intra-Asian submarine cable system. The new cable, dubbed the Southeast Asia Japan Cable (SJC), would link Unity's landing station in Japan to Guam, Hong Kong, the Philippines, Thailand and Singapore. The cable is still in the planning stage, and it is estimated that it will probably not be ready for service until 2011 at the earliest. Companies that are cooperating on both the Unity and SJC cables include Google, Bharti, SingTel, KDDI and Global Transit. Globe Telecom of the Philippines and TOT of Thailand are also members of the SJC consortium.[49]

A new undersea fiber-optic cable linking Japan and Russia went into service in early July, providing the first direct link between the two countries and an alternate cable route between Europe and Asia. Known as the Hokkaido-Sakhalin Cable System (HSCS), the 570 kilometer connection runs between Japan's Hokkaido Island and Russia's Sakhalin Island, and has a capacity of 640 Gbps. Construction of the 570 kilometer cable was carried out

by Japan's NTT Communications and Russia's TransTeleCom Company and was both started and completed in 2007. Prior to the activation of the HSCS, traffic between Japan and Russia, which share a sea border in the Russian Far East, travelled via traditional cable routes through Southeast Asia and the Indian Ocean to Europe. The new cable provides a shorter route and is expected to reduce latency by 20 percent to 30 percent.[50]

Also in the Asia Pacific region, the 18,000 kilometer "Trans-Pacific Express" cable linking the U.S., China, South Korea and Taiwan was completed in September. Initially covered in the *1st Quarter, 2008 State of the Internet* report,[51] the new cable will provide significantly more network capacity to the region. Interestingly, the driver for deployment of the "Trans-Pacific Express" cable was a December 2006 earthquake off Taiwan's coast that severed several undersea data cables, disrupting communications throughout much of Asia. AT&T and Japan's NTT Communications also joined the "Trans-Pacific Express" consortium, and plan to invest to extend the cable to Japan.[52]

In Africa, Moroccan provider Medi Telecom (Meditel) and Telefonica completed Africa Gate, which provides international connectivity via an undersea section between Morocco and Spain.[53] The government of Botswana, a landlocked country in Southern Africa, invested $100 million in the East Africa Submarine Cable System (EASSY), Africa's second biggest submarine cable, in order to improve its communications with North America and Europe, as well as the rest of the continent. The cable runs up the east coast of the continent in the Indian Ocean, touching several countries between Mtunzini, South Africa and Port Sudan.[54] Private equity venture SEACOM's 15,000 kilometer undersea cable linking east Africa to Europe and Asia will be launched in June 2009, ahead of South Africa's hosting of the World Cup in 2010. Laying cable was scheduled to begin in October 2008, with work on connecting sections of the cable scheduled to begin in April 2009. The cable will provide 1.28 Tbps of broadband capacity, and will cost $650 million.[55] On the other side of the continent, a group of African telecom firms have agreed to cooperate on the deployment of a $400 million undersea cable along the western coast of Africa. Cooperating firms include South African operators such as Telkom, Vodacom, MTN and Neotel.[56]

In Europe, Alcatel-Lucent announced that its cable ship landed a 2,100 kilometer section of Tele Greenland's new submarine cable, Greenland Connect, at Nuuk, connecting Greenland with Iceland. The cable will offer capacity of up to 960 Gbps, and it is expected to be completed "before the winter season."[57]

Across the Atlantic Ocean, the new 1,200 kilometer Challenger cable, deployed by the Cable Co consortium and linking Bermuda to the rest of the world, was officially connected at Devonshire Bay in mid-September. The Cable Co consortium, which includes telecom firms KeyTech, North Rock and Transact, invested $26 million in the project. The Challenger cable is scheduled to be activated in early 2009 and will initially have capacity of 20 Gbps, increasing over time to 320 Gbps.[58]

Costa Rican state-run telecommunications provider Instituto Costarricense de Electricidad (ICE) signed an agreement with Columbus Networks to connect to the new 2,400 kilometer CFX-1 submarine cable linking Florida with Colombia via Jamaica. Under the agreement with ICE, CFX-1 will land at Puerto Limon in Costa Rica, and will also connect other Central American countries including Panama.[59] Also in Costa Rica, Global Crossing inaugurated a new submarine cable connecting the Pacific coast of Costa Rica to the Pan American Cable (PAC). The PAC connects the West Coast of the United States, Mexico, Panama, Venezuela and the Virgin Islands. The new submarine cable, constructed and operated by Global Crossing, will provide state-run Costa Rican telecommunications providers ICE and Radiografica Costarricense (RASCA) with increased international capacity and additional connection redundancy.[60]

In mid-July, Web site Wikileaks published[61] documents that were signed in 2006 by officials in Cuba and Venezuela that described plans for a new undersea cable connecting the two countries. This new cable will help provide high-speed Internet access to Cuban citizens by 2010. The United States economic embargo against the island nation has forced the communist country to rely on slow and expensive satellite links for Internet connectivity, according to the Wikileaks article.[62] Even though it would be less costly and more efficient to deploy a new cable between Cuba and the United States, which are only 120 kilometers apart, Cuba is instead working with Venezuela to lay a 1,500 kilometer cable to get high-speed Internet connectivity. The proposed cable will be deployed by CVG Telecom (Corporacion Venezolana de Guyana) and ETC (Empresa de Telecomunicaciones de Cuba), and will also provide high-speed Internet access to Jamaica, Haiti and Trinidad.[63]

As all of these new cables are deployed, bringing a significant increase in capacity to countries around the world, the idea of a global bandwidth exchange is gaining interest. According to a July 23 article[64] published on BusinessWeek.com, Neil Tagare is launching buysellbandwidth.com. Tagare has a long history with global connectivity projects, as he was involved with international fiber network FLAG Telecom, as well as Project Oxygen, which he originally envisioned as a submarine and terrestrial fiber network spanning the globe and connecting 175 countries.[65] In the article, Tagare notes that he first started to think about buysellbandwidth.com earlier in 2008, when five cables were simultaneously cut in the Middle East. (See Section 3.1 of the *1st Quarter, 2008 State of the Internet* report for additional discussion on the impact of these cable cuts.) Buysellbandwidth.com is positioned as a global bandwidth exchange and counts major global telecommunications firms including PCCW, KPN, PLDT, Globe Telecom, Cable & Wireless, Reach and Tata Communications among its initial participants.

3.4 Significant New Connectivity — Wireless

While undersea cable projects made a big splash in the third quarter, satellite and WiMAX initiatives got a significant amount of press as well. The big satellite-related news was related to O3b Networks, a startup looking to offer Internet services to areas that are too far from undersea network cables and major backbones to take advantage of them. According to an article[66] in the Wall Street Journal, O3b Networks took an initial investment of approximately $60 million from investors including Google, HSBC Holdings PLC, Allen & Company and Liberty Global Inc. The company announced plans to launch as many as 16 satellites that could provide service to Africa, the Middle East and parts of Latin America by the end of 2010. The project is expected to cost approximately $650 million. O3b won't sell access directly to end users, but instead will sell service to local Internet service providers, which can then offer connectivity over their own networks.

According to an interview[67] with O3b's founder Greg Wyler, the satellites will orbit the Earth around the equator, and he notes that "Because they're approximately five times closer to the earth than geo-satellites, the latency is reduced by approximately five times." Wyler claims that the service will provide multi-Gbps speeds, and will cost in the range of $500/Mbps or below.

A number of commercial WiMAX services debuted in the third quarter, offering wireless broadband connectivity to both mobile and home users. In the United States, Sprint Nextel Corp. launched its "Xohm"-branded WiMAX service in Baltimore, Maryland in late September, claiming to provide download speeds of 2-4 Mbps for $25-30/month (for the first six months).[68] According to the Xohm Web site,[69] the service will be coming soon to Chicago and Washington, D.C., while Dallas, Fort Worth, Boston, Providence and Philadelphia are "in the works". Puerto Rican communications services provider Neptuno announced that it had selected Airspan Networks to supply WiMAX base stations for a planned island-wide WiMAX network rollout, with installation expected to be completed by the end of 2008.[70]

Internationally, in Uzbekistan, joint venture Super iMAX launched a commercial WiMAX service for enterprise customers in the capital Tashkent, Ferghana and Samarkand.[71] Scartel launched WiMAX trials in Moscow and St. Petersburg, Russia, with plans to deploy 1,600 access points by early 2009.[72] Also in Russia, Enforta announced in September that it planned to expand its WiMAX services to 13 additional cities (Armavir, Artem, Birobidzhan, Vanino, Dzerzhinsk, Zlatoust, Miass, Novorossiysk, Novotroitsk, Sochi, Sterlitamak, Syzran and Ulan-Ude), increasing its total coverage to 68 cities.[73]

In Saudi Arabia, cellular operator Mobily launched a new WiMAX service called "broadband@home" for residential users in Riyadh, Jeddah, Dammam and Khobar. Customers can expect download speeds of up to 2Mbps on the service, which costs SAR250 ($66.56) per month.[74] South African cellular operator Vodacom announced in August that it was aiming to launch commercial WiMAX services in partnership with Wireless Business Solutions (iBurst) at the beginning of October for business customers in the Western Cape, Kwazulu-Natal and Gauteng regions.[75]

Malaysian WiMAX network operators Redtone-CNX Broadband and Packet One Networks launched commercial WiMAX services in mid-August.[76] The first phase of Redtone's network covers the Kota Kinabalu business district in the state of Sabah, and was expected to be expanded to Kuching in October. Packet One is aiming to cover 65% of the population in the west coast of Peninsular Malaysia by 2012. The Malaysian government issued four WiMAX licenses in March 2007 to Redtone, Packet One, Bizsurf and Asiaspace and gave the providers a 2008 year-end deadline to roll out WiMAX services; otherwise they risked having their licenses revoked. In India, state-run telecommunications firm Bharat Sanchar Nigam Ltd (BSNL) plans a rural WiMAX expansion and aims to provide high speed Internet access to 25,000 villages by the end of the fiscal year.[77]

3.5 Significant New Connectivity — Fixed Broadband

In late September, KDDI announced that it would be launching a new high-speed broadband service in Japan, with upload and download speeds each of up to one gigabit per second.[78] The company noted that it plans to target residents living in single-family homes and low-rise apartment buildings and that its service would offer the fastest speeds in eastern Japan, a 10x increase from the 100 Mbps currently available to broadband subscribers. While not expressly targeted at consumer subscribers, one gigabit per second speeds are also available through the new "Beeline" service, launched in the Ukraine by sister companies Golden Telecom and Ukranian Radio Systems.

Gigabit speeds are also moving into Europe, as CityNet, along with Netherlands telecommunications firms GNA, BBned and InterNLnet, announced that they concluded a 3-day test in early September of one gigabit per second connectivity for residential consumers over their network.[79] However, a study done by the United Kingdom's government broadband advisory group highlighted the significant expense that would be required to bring gigabit speed connections to every home or business. According to a BBC News article[80] on the study's results, bringing a dedicated cable delivering one gigabit per second to every home or business could cost up to £28.8bn (nearly $50 billion), and was the most costly of the three options considered. The study also noted that bringing fiber to homes in more rural areas would carry disproportionately higher costs — the more isolated a home, the more it would cost to reach it.

The growth in number and reach of gigabit speed connections will serve to improve end-user experiences. However, this growth will also serve to highlight a key issue in the Internet's architecture — the bandwidth bottleneck in the Internet's "middle mile" — the points where network providers interconnect. Investments in these connections have not kept pace with the growth in end-user connectivity speeds and, as such, will come under increasing strain from growing amounts of traffic at higher and higher speeds. Akamai's distributed network architecture can help content providers make the most of these higher speed last-mile connections, largely avoiding these middle-mile bottlenecks and delivering content directly from within end-user networks.

Section 4: Internet Penetration

	Country	Q3 08 Unique IP's	Q3-Q2 Change	Q2-Q1 Change	Q1-Q4 Change
-	Global	379,757,053	+9.7%	+5.2%	+5.3%
1	United States	109,333,753	+7.2%	+5.2%	+5.5%
2	China	37,591,948	+10.5%	+4.8%	+7.6%
3	Japan	27,513,814	+8.1%	+2.8%	+2.1%
4	Germany	25,888,158	+8.7%	+5.1%	+12.6%
5	France	17,816,002	+5.4%	+2.9%	+3.3%
6	United Kingdom	17,304,827	+4.5%	+4.2%	+6.4%
7	South Korea	14,855,171	+12.1%	-2.2%	+2.6%
8	Canada	10,298,798	+1.5%	+3.4%	+4.2%
9	Spain	8,989,657	+6.1%	+3.7%	+4.0%
10	Brazil	8,777,278	+27.1%	+4.7%	+2.0%

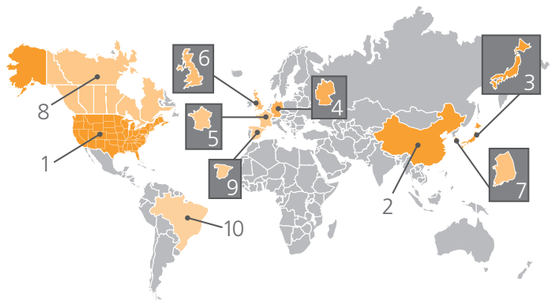


Figure 7: Unique IP Addresses Seen By Akamai

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 unique visibility into the levels of Internet penetration around the world. In the third quarter of 2008, nearly 380 million unique IP addresses connected to the Akamai network – almost ten percent more than in the second quarter. Similar to the prior two quarters, nearly 30% of those IP addresses came from the United States and just below 10% came from China.

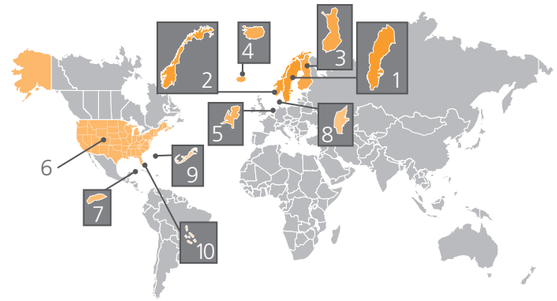
Three countries among the top 10 saw double-digit percentage increases quarter-over-quarter: China (10.5%), South Korea (12.1%), and Brazil (27.1%). Brazil's increase is fairly significant, and one possible explanation may be related to demand for online broadcasting of the Beijing Olympic Games in August, according to TeleGeography.[81] As the Olympic Games were hosted by China, it is likely that the large increase in unique IP addresses seen in that country was also related to demand for online broadcasting of the Olympics. South Korea also recovered well from their unusual second quarter decline in the number of unique IP addresses seen by Akamai.

Looking at the "long tail," there were 187 countries with fewer than 1 million unique IP addresses connecting to Akamai in the third quarter of 2008, 148 with under 100,000 unique IP addresses, and 38 with fewer than 1,000 unique IP addresses. As compared to the second quarter, these country counts remained fairly stable; Akamai did not see the more significant changes that occurred between the first and second quarters.

4.2 Internet Penetration, Global

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 updated 2008 global population data from the United States Census Web site[82] as a baseline, levels of Internet penetration for each country around the world were calculated. Most of the countries in the top 10 remained stable from quarter-to-quarter, with the exception of one — Canada ceded its place on the list to Bermuda this quarter, and dropped to No.13 overall. (Bermuda was No.15 for the second quarter, with 0.28 unique IP's per capita.)

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. (For this report, the population estimates used were for July 1, 2008, updated from the March 1, 2008 estimates used for the prior two *State of the Internet* reports.) In addition, individual users can have multiple IP addresses (handheld, personal/home system, business laptop, etc.). Furthermore, in some cases, multiple individuals may be 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 380 million unique IP addresses.



	Country	Unique IP's Per Capita
-	Global	0.06
1	Sweden	0.42
2	Norway	0.39
3	Finland	0.38
4	Iceland	0.38
5	Netherlands	0.36
6	United States	0.36
7	Cayman Islands	0.35
8	Denmark	0.35
9	Bermuda	0.34
10	British Virgin Islands	0.33

Figure 8: Global Internet Penetration

4.3 Internet Penetration, United States

This quarter, Akamai will also begin to examine Internet penetration within the United States. Using the most recent population estimates available from the United States Census Web site[83] and the number of unique IP addresses from each state that Akamai saw during the third quarter, we calculated the levels of Internet penetration on a state-by-state basis. The same caveats noted immediately above in section 4.2, regarding per capita figures as an approximation, apply here as well.

It is not surprising that the top three states are Virginia, New Jersey, and Massachusetts, for a variety of reasons. All three states have a strong base of high-tech companies that are headquartered or have a major presence within the state, potentially making for a population more likely to use, and more comfortable with using, the Internet on a regular basis. In addition, over 200 colleges and universities are located in each state[84] — the large academic populations are known to be frequent Internet users. Finally, New Jersey and Massachusetts are among the top 3 states in population density, while Virginia is in the top 15.[85] Higher population densities often make it easier to bring Internet connectivity to larger numbers of people.

Many may be surprised that California did not rank within the top 10, as the three points above apply to the state as well. California was just barely edged out of the top 10, coming in at No.12, with 0.37 unique IP's per capita, just behind Texas.

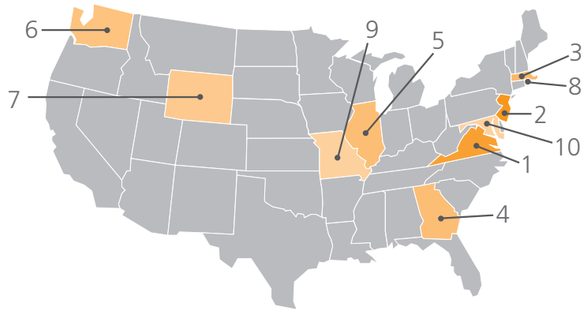


Figure 9: Internet Penetration in the United States

	State	Unique IP's Per Capita
1	Virginia	0.82
2	New Jersey	0.75
3	Massachusetts	0.51
4	Georgia	0.50
5	Illinois	0.49
6	Washington	0.46
7	Colorado	0.45
8	Rhode Island	0.43
9	Missouri	0.40
10	Maryland	0.38

Through its globally deployed server network and the billions of requests for Web content that it services on a daily basis, Akamai has a unique level of visibility into the connection speeds of those systems issuing the requests, and as such, of broadband adoption around the globe. Because Akamai has implemented a distributed network model, deploying servers within Edge networks, it can deliver content more reliably and more consistently at those speeds, in contrast to centralized competitors that rely on fewer deployments in large data centers. For more information on why this is possible, please see Akamai's *How Will The Internet Scale?* white paper.[86]

The data presented was collected during the third quarter of 2008 through Akamai's globally-deployed server network and includes all countries and U.S. states having more than 1,000 average monthly unique IP addresses make requests to Akamai's network during the second quarter. For the purposes of classification in this report, the "broadband" data included below is for connections greater than 2 Mbps, and "high broadband" is for connections 5 Mbps or greater. In contrast, the "narrowband" data included below is for connections slower than 256 Kbps. Note that the percentage changes reflected below are not additive — they are relative to the prior quarter(s). (That is, a Q2 value of 50%, and a Q3 value of 51%, would be reflected here as a +2% change.) Quarter-over-quarter changes are shown within the tables in an effort to highlight general trends.

As the quantity of HD-quality media increases over time, and the consumption of that media increases, end users are likely to require ever-increasing amounts of bandwidth. A connection speed of 2 Mbps is arguably sufficient for standard-definition TV-quality video content, and 5 Mbps for standard-definition DVD-quality video content, while Blu-Ray (1080p) video content has a maximum video bit rate of 40 Mbps, according to the Blu-Ray FAQ.[87]

5.1 High Broadband Connectivity: Fastest International Countries

For the third consecutive quarter, South Korea tops the list of countries with the greatest levels of high broadband (>5 Mbps) connectivity. However, South Korea is also the only country within the top 10 that experienced a quarter-over-quarter decrease. Over the past three quarters, South Korea's high broadband connectivity levels, as observed by Akamai, have dropped from 64% to 58%. Romania jumped up the list, with a near doubling quarter-over-quarter, moving into third place, and newcomer Singapore pushed Canada off of the top 10 list and down to No.12.

Country	% above 5 Mbps	Q3–Q2 Change	Q2–Q1 Change	Q1–Q4 Change
- Global	19%	+0.3%	+20%	-2.9%
1 South Korea	58%	-10%	+9.3%	-10%
2 Japan	55%	+4.6%	+12%	+6.5%
3 Romania	43%	+92%	+11%	+0.8%
4 Hong Kong	38%	+2.6%	+6.6%	-8.6%
5 Sweden	37%	+16%	+11%	-6.7%
6 Belgium	29%	+9.4%	+30%	25%
7 Denmark	27%	+50%	+26%	20%
8 United States	26%	+0.2%	+29%	0.9%
9 Singapore	26%	+80%	+33%	-8.4%
10 Netherlands	25%	+14%	+11%	-3.2%

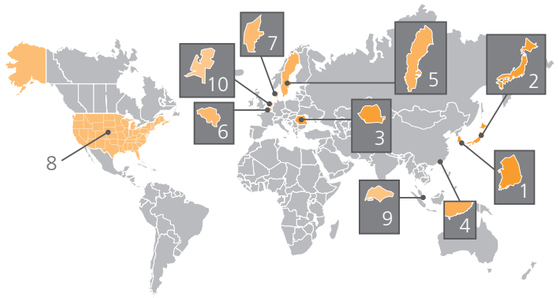
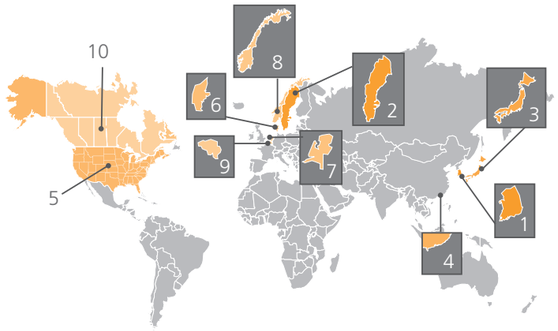


Figure 10: High Broadband Connectivity, Fastest International Countries



	Country	High Broadband IP's Per Capita
-	Global	0.01
1	South Korea	0.18
2	Sweden	0.16
3	Japan	0.12
4	Hong Kong	0.10
5	United States	0.09
6	Denmark	0.09
7	Netherlands	0.09
8	Norway	0.08
9	Belgium	0.07
10	Canada	0.07

Figure 11: Global High Broadband Penetration

Some published reports in the third quarter claimed that the United States has fallen to 15th place in terms of average download speeds, as compared to other countries. The source data for these claims is the 2008 ITIF Broadband Rankings, published by the Information Technology and Innovation Foundation.[88] This data claims that South Korea tops the list at an average speed of 63.6 Mbps, while the United States only manages a comparatively anemic 4.9 Mbps on average. However, the report also notes that their methodology for calculating broadband speed involved calculating a weighted average of the speeds of the incumbent DSL, cable and fiber offerings provided in the OECD's April 2006 "Multiple Play" report. While Akamai does not currently calculate statistics on average connection speeds by country, our rankings are based on actual observed connections to the Akamai network, and are accurate as of the most recent quarter.

From an Internet penetration perspective (unique IPs per capita), eight countries can also be found in the High Broadband Top 10, as would be expected. Canada and Norway did not make the High Broadband Top 10, though they were in the top 15.

As in the second quarter of 2008, South Korea, Sweden, Japan, Hong Kong and the United States once again round out the five top slots. In the third quarter, Hong Kong joined South Korea, Sweden and Japan in having more than 0.10 high broadband IP's per capita — in other words, an observed high broadband penetration of greater than 10%.

5.2 High Broadband Connectivity: Fastest U.S. States

While high broadband usage in the United States lags behind countries in Europe and Asia, as discussed in Section 5.1, the availability of high-speed Internet access is becoming increasingly important. An August 19 article published in USA Today quoted Federal Communications Commission Chairman Kevin Martin, noting "High-speed Internet access is so important to the welfare of U.S. consumers that America can't afford not to offer it — free of charge — to anybody who wants it. There's a social obligation in making sure everybody can participate in the next generation of broadband services because, increasingly, that's what people want."

Continuing the trend from the first two quarters of 2008, the East Coast of the United States was once again very well represented in the Top 10 list of U.S. states with the greatest levels of high broadband (>5 Mbps) connectivity, taking seven of the top 10 slots.

Looking at the trends over time, only Oklahoma and Kentucky have seen consistent quarterly growth since Q4 2007, with Kentucky seeing significant increases over the last two quarters. This consistent and significant growth in Kentucky may be due in part to the efforts of ConnectKentucky, a nonprofit with a roughly $2 million annual budget that has worked for the past four years to expand the availability and use of broadband Internet connections in the state's rural areas. An article in the Wall Street Journal[89] notes that according to ConnectKentucky, 95% of the state's households can now buy high-speed Internet service, up from 60% in 2004. The article also highlights education benefits and job growth that have resulted from the availability of high-speed Internet connectivity within the state. While not in the top 10, Tennessee, West Virginia and Ohio are also pursuing similar programs, according to Connected Nation.[90]

In August, the Communications Workers of America union released its second annual survey of Internet speeds in the United States.[91] The report notes that it gathered user connection speed data by asking users to go to speedmatters.org Web site to take the speed test available there. Interestingly, the results[92] of the speed tests show only four states (Rhode Island, Delaware, New Jersey and Virginia) with median download speeds above 5 Mbps, while Akamai's empirical data doesn't even have New Jersey and Virginia in the top 10 high broadband states.

	State	% above 5 Mbps	Q3–Q2 Change	Q2–Q1 Change	Q1–Q4 Change
1	Delaware	55%	-17%	+13%	-0.4%
2	New York	47%	+17%	+14%	-1.3%
3	Rhode Island	47%	+9.3%	+2.4%	-4.8%
4	New Hampshire	46%	+44%	+9.0%	-0.8%
5	Connecticut	41%	+18%	+10%	-4.3%
6	Massachusetts	40%	+29%	+10%	-4.1%
7	Nevada	39%	+17%	-0.3%	-2.5%
8	Oklahoma	35%	+3.7%	+3.1%	+1.1%
9	Maryland	33%	+14%	+7.0%	-6.6%
10	Kentucky	32%	+47%	+33%	+3.5%

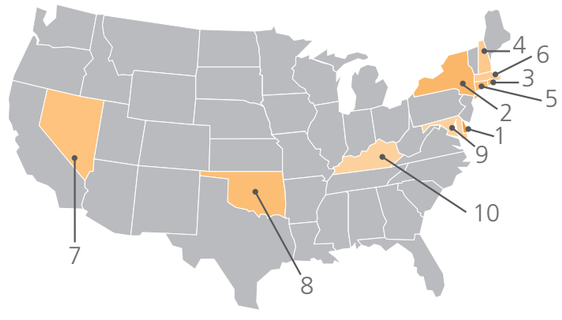
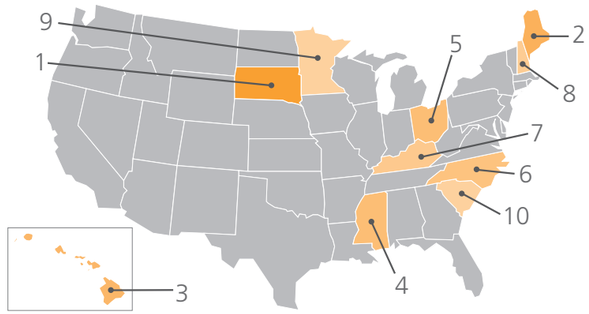


Figure 12: High Broadband Connectivity, Fastest U.S. States



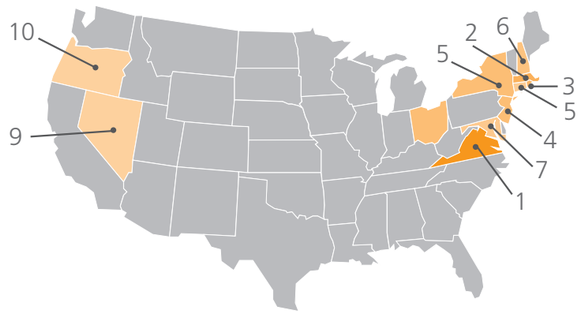
	State	% above 5 Mbps	Q3–Q2 Change
1	South Dakota	17%	+116%
2	Maine	29%	+102%
3	Hawaii	5.7%	+95%
4	Mississippi	21%	+70%
5	Ohio	22%	+59%
6	North Carolina	26%	+54%
7	Kentucky	32%	+47%
8	New Hampshire	46%	+44%
9	Minnesota	28%	+40%
10	South Carolina	23%	+40%

Figure 13: Greatest Increases in High Broadband Connectivity

It is also interesting to look at which are the top states in terms of rate of change for high broadband connectivity, as observed by Akamai? Figure 13 shows that the three states that saw the greatest quarterly increases were South Dakota, Maine and Hawaii, all of which essentially doubled second quarter levels. Arguably, the law of small numbers plays a part here, as it is easier to double the lower percentages of high broadband connectivity historically observed in these states. Further down the list, states like Minnesota may be seeing rapid growth from investments in rural broadband infrastructure. A September 17 post on the Internet Evolution blog[93] noted that Minnesota is "… committed to investing in rural infrastructure because they believe that a far-reaching broadband and Internet infrastructure can generate economic prosperity…"

Looking at high broadband penetration across the United States, we see that the top eight states are on the East Coast, with Nevada and Oregon rounding out the top 10.

As noted in Section 5.1, on a country-wide basis, the United States has 0.09 high broadband IP's per capita. From a state-wide perspective, we see that all of the states in the top 10 list above have better high broadband penetration than the country average, with more than 0.10 high broadband IP's per capita — in other words, an observed high broadband penetration of greater than 10%. Thirty states come in below the country average, with Hawaii (0.02) and Alaska (0.01) at the bottom of the list.



	State	High Broadband IP's Per Capita
1	Virginia	0.21
2	Massachusetts	0.20
3	Rhode Island	0.20
4	New Jersey	0.20
5	New York	0.17
6	New Hampshire	0.13
7	Maryland	0.12
8	Connecticut	0.11
9	Nevada	0.11
10	Oregon	0.10

Figure 14: High Broadband Penetration in the U.S.

5.3 Broadband Connectivity: Fast International Countries

Internationally, the percentage of connections to Akamai at speeds greater than 2 Mbps continues to be more clustered than the "high broadband" data, as it was in the second quarter as well. The cluster continues to tighten, with only 13% separating No. 1 Tunisia (97%) and No. 10 Denmark (84%) — the gap was 20% in the first quarter of 2008, and 15% in the second quarter of 2008. The United States dropped to No. 30 on the list, seeing a nearly 10% loss from the second quarter. Five countries in the Broadband Top 10 also appear in the High Broadband Top 10 for the second quarter of 2008: South Korea, Japan, Hong Kong, Belgium and Denmark. This is down from seven countries in the second quarter.

Quarter-to-quarter changes for many of the countries on the list above were fairly modest. However, the three newcomers to the list (Tunisia, Oman and Monaco) all experienced significant growth in broadband percentages from the second quarter, placing them all on the Broadband Top 10 list. It is not clear what drove the double digit increases in broadband percentages during the second quarter — it could be related to localized consumption of content from the Beijing Olympic Games. If that is the case, then these three countries will likely not appear in the Broadband Top 10 list for the fourth quarter — we will re-examine their ranking in the next report.

Interestingly, the United States saw a drop of over 9%, placing it slightly ahead of where it stood in the first quarter (62%). In addition, the United States saw a 29% drop in narrowband connections from the second quarter (see Section 5.5). As such, the percentage of users connecting between 256 Kbps and 2 Mbps likely increased, though this group is not tracked for the purposes of this report. It may also be the case that users who connected at average speeds just over 2 Mbps in the second quarter saw slight reductions in their connection speeds in the third quarter, to just under 2 Mbps, which would account for the drop as well.

For the third consecutive quarter, Europe was very well represented for broadband Internet penetration, remaining consistent with the second quarter, with European countries capturing seven of the top 10 slots, as shown in Figure 16.

Country	% above 2 Mbps	Q3–Q2 Change	Q2–Q1 Change	Q1–Q4 Change
- Global	57%	-1.9%	+6.8%	-2.0%
1 Tunisia	97%	+37%	-9.4%	+26%
2 South Korea	92%	+2.3%	+5.4%	-6.8%
3 Belgium	92%	+2.2%	+1.6%	+2.9%
4 Switzerland	91%	+6.8%	-2.6%	+1.0%
5 Japan	91%	+4.5%	+2.7%	+1.8%
6 Oman	90%	+25%	+34%	+25%
7 Hong Kong	88%	+1.1%	+0.3%	-0.2%
8 Slovakia	87%	+5.3%	+8.1%	+2.2%
9 Monaco	86%	+47%	-5.0%	-2.5%
10 Denmark	84%	+5.8%	+10%	+6.1%
…				
30 United States	64%	-9.3%	+13%	-2.8%

Figure 15: Broadband Connectivity, Fast International Countries

Akamai's observed broadband penetration in Europe is consistent with a report from trade group Broadband Forum, which noted that broadband subscriptions continue to grow faster in Europe than any other region in the world, according to a post on the GigaOM blog.[94] The report, prepared for the Broadband Forum by industry analysts Point Topic, shows that the European region now has nearly 120 million subscribers, a full 32 percent of the global broadband market.[95]

	Country	Broadband IP's Per Capita
-	Global	0.03
1	Sweden	0.33
2	Norway	0.33
3	Denmark	0.29
4	Netherlands	0.28
5	South Korea	0.28
6	Monaco	0.26
7	Germany	0.26
8	Switzerland	0.26
9	Iceland	0.25
10	Hong Kong	0.24
...		
11	United States	0.23

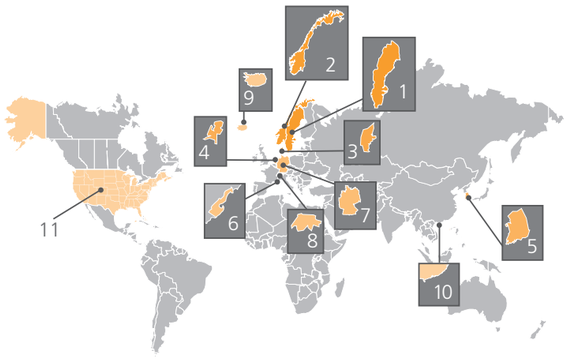


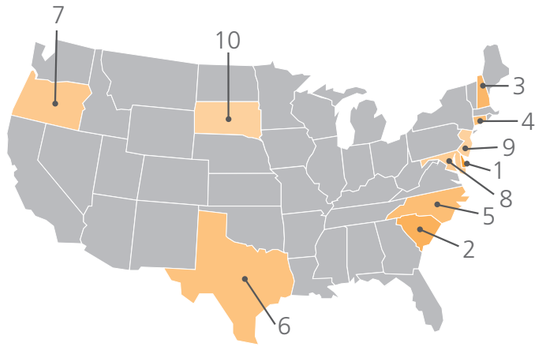
Figure 16: Global Broadband Penetration

5.4 Broadband Connectivity: Fast U.S. States

The third quarter of 2008 saw increased broadband usage across the board, as all of the states in the Top 10 showed an increase over the second quarter. Delaware continues to shed low-speed connections, with a modest increase bringing it to 97% of observed connections to Akamai at speeds over 2 Mbps. Rhode Island, which held the No. 2 slot for the prior two quarters, was pushed out of the Broadband Top 10 list entirely, as many states saw significant double-digit increases on a quarter-over-quarter basis. (It dropped to No. 28, with a nearly 22% loss to only 66% of connections at speeds above 2 Mbps.)

Four of these states (South Dakota, New Hampshire, North Carolina and South Carolina) were also on the list of states with the largest percentage gains in high broadband connections observed between the second and third quarters. As noted previously in Section 5.2, many states are investing in bringing Internet and broadband connectivity to more rural locations, as they seek to improve education, job growth and overall economic prosperity.

Going forward, more specific information about broadband deployment, adoption and benefits in the United States may become available as a result of the adoption of the Broadband Data Improvement Act, which aims to improve the quality of federal and state data regarding the availability and quality of broadband services and to promote the deployment of affordable broadband services to all parts of the United States.

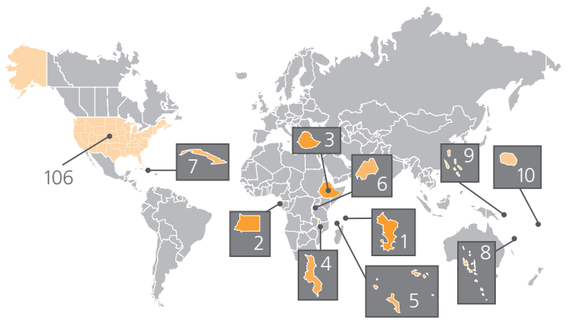


	State	% above 2 Mbps	Q3–Q2 Change	Q2–Q1 Change	Q1–Q4 Change
1	Delaware	97%	+3.5%	+0.5%	-2.4%
2	South Carolina	87%	+21.1%	-0.9%	+1.0%
3	New Hampshire	86%	+15.6%	+1.4%	+1.8%
4	Connecticut	86%	+8.2%	+0.1%	-3.0%
5	North Carolina	81%	+29.6%	+1.6%	-1.1%
6	Texas	81%	+49.8%	-4.9%	-5.1%
7	Oregon	81%	+30.1%	+1.0%	+0.2%
8	Maryland	79%	+43.0%	-6.3%	-6.6%
9	New Jersey	79%	+83.4%	-15.3%	-6.8%
10	South Dakota	79%	+19.3%	+1.5%	+1.8%

Figure 17: Broadband Connectivity, Fast U.S. States

It was passed by the United States Senate on September 26 and the United States House of Representatives on September 29, and signed into law by President Bush on October 10.[96] According to a press release[97] issued by the United States Senate Committee on Commerce, Science and Transportation, the Broadband Data Improvement Act specifically is intended to:

- Direct the Federal Communications Commission to conduct inquiries into the deployment of advanced telecommunications services on an annual, rather than periodic, basis.
- Direct the Census Bureau to include a question in its American Community Survey that assesses levels of residential computer use and dial-up versus broadband Internet subscribership.
- Direct the Government Accountability Office to develop broadband metrics that may be used to provide consumers with broadband connection cost and capability information and improve the process of comparing the deployment and penetration of broadband in the United States with other countries.
- Direct the Small Business Administration's Office of Advocacy to conduct a study evaluating the impact of broadband speed and price on small businesses.
- Establish a program that would provide matching grants to State non-profit, public-private partnerships in support of efforts to more accurately identify barriers to broadband adoption throughout the State.



	Country	% below 256 Kbps	Q3–Q2 Change	Q2–Q1 Change	Q1–Q4 Change
–	Global	5.0%	-32%	-6.8%	-8.1%
1	Mayotte	97%	+7.1%	+9.0%	+5.6%
2	Equatorial Guinea	94%	+8.8%	+6.7%	+38%
3	Ethiopia	93%	+1.8%	-1.6%	-0.7%
4	Malawi	93%	+19%	-12%	+1.8%
5	Seychelles	93%	+25%	-12%	+11%
6	Rwanda	92%	-1.7%	-0.2%	-2.0%
7	Cuba	92%	+4.8%	-4.8%	+1.5%
8	Vanuatu	90%	+2.3%	+2.1%	-3.8%
9	Solomon Islands	88%	-6.1%	+1.4%	+8.9%
10	Cook Islands	87%	+9.1%	-9.7%	-2.3%
	...				
106	United States	5.8%	-29%	+5.8%	+3.8%

Figure 18: Narrowband Connectivity, Slowest International Countries

5.5 Narrowband Connectivity: Slowest International Countries

While broadband adoption continues to increase in many countries across the world, many other countries are still stuck with low-speed Internet connections, with large percentages of their connections to Akamai occurring at speeds below 256 Kbps.

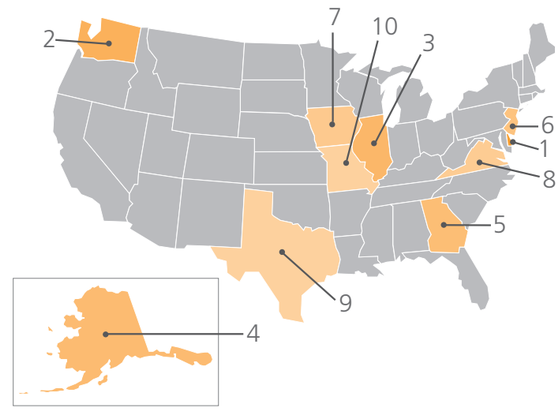
Similar to the prior two quarters, many of the countries with the largest percentages of connections to Akamai at speeds below 256 Kbps were either island nations or on the African continent. Rwanda and the Solomon Islands, which held the first two slots in the second quarter, were the only two countries in the top 10 that saw decreasing narrowband connection percentages quarter-over-quarter, moving them down to sixth and ninth place respectively.

Rwanda continues to show a declining trend in the percentage of narrowband connections over the past three quarters, and as noted last quarter, this may indicate the increasing adoption of options for higher speed connectivity. This declining trend is also occurring on a global basis, with a significant shift seen between the second and third quarters. Given the slight decline seen in global broadband (>2 Mbps) connection percentages in the third quarter, it is likely that users are moving slowly to higher speed connections, and not jumping directly to broadband or high broadband speeds.

5.6 Narrowband Connectivity: Slowest U.S. States

After holding the first place slot for the prior two quarters, Washington State experienced a significant quarter-over-quarter percentage decrease and dropped to second place. Four states in the top 10 saw a multi-quarter trend of declining percentages, while New Jersey is the only one of the top 10 that saw a multi-quarter increase.

Given New Jersey's significant quarter-over quarter increase in broadband connections, as shown in Section 5.4, it is surprising to see the significant increase in narrowband connections in the third quarter as well. However, the 62% quarter-over-quarter increase in unique IP addresses seen from New Jersey may account for both of these trends.



	State	% below 256 Kbps	Q3–Q2 Change	Q2–Q1 Change	Q1–Q4 Change
1	District of Columbia	12%	-25%	-3.7%	+5.4%
2	Washington	12%	-46%	+6.6%	+145%
3	Illinois	11%	-27%	+1.1%	+11%
4	Alaska	9.4%	+0.6%	-16%	-9.8%
5	Georgia	9.3%	-41%	+6.7%	+9.3%
6	New Jersey	9.3%	+24%	+18%	-4.4%
7	Iowa	8.7%	-6.7%	-7.8%	-2.8%
8	Virginia	7.5%	-43%	-27%	+12%
9	Texas	7.3%	-42%	+2.1%	+7.1%
10	Missouri	7.2%	-1.5%	-3.3%	-0.8%

Figure 19: Narrowband Connectivity, Slowest U.S. States

Section 6: Appendix

As we did in Section 5.2, it is also interesting to look at which are the top states in terms of rate of change — in other words, which states saw the greatest decreases in quarter-over-quarter narrowband connectivity, as observed by Akamai. Figure 20 shows that five states (Delaware, Washington, Virginia, Texas and Georgia) experienced quarterly declines of over 40%.

Delaware's drop to 0.3% of connections below 256 Kbps means that it is only one of two states that have a narrowband connection percentage below 1%. The other state is Nevada, which has also historically shown a higher percentage of connections at speeds above 2 Mbps.

	State	% below 256 Kbps	Q3–Q2 Change
1	Delaware	0.3%	-50%
2	Washington	12%	-46%
3	Virginia	7.5%	-43%
4	Texas	7.3%	-42%
5	Georgia	9.3%	-41%
6	Illinois	11%	-27%
7	District of Columbia	12%	-25%
8	New Mexico	2.6%	-24%
9	Idaho	2.9%	-19%
10	Florida	4.4%	-18%

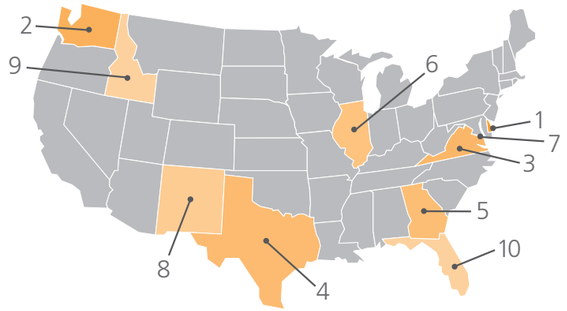


Figure 20: Greatest Decreases in Narrowband Connectivity

REGION	% ATTACK TRAFFIC	UNIQUE IP ADDRESSES	Q2 08 CHANGE	UNIQUE IPs PER CAPITA	% ABOVE 5 MBPS	HIGH BB IPs PER CAPITA	% ABOVE 2 MBPS	BB IPs PER CAPITA	% BELOW 256 KBPS
Europe									
Austria	0.06%	1,630,259	2.4%	0.20	17%	0.03	66%	0.12	1.5%
Belgium	0.27%	2,480,880	-1.4%	0.24	29%	0.07	92%	0.22	1.0%
Czech Republic	0.90%	1,291,253	2.1%	0.13	17%	0.02	69%	0.09	2.8%
Denmark	1.03%	1,892,370	4.1%	0.35	27%	0.09	84%	0.29	1.5%
Finland	1.09%	2,003,742	4.8%	0.38	17%	0.06	52%	0.20	1.7%
France	0.87%	17,816,002	5.4%	0.28	7.2%	0.02	74%	0.21	0.9%
Germany	2.20%	25,888,158	8.7%	0.31	14%	0.04	82%	0.26	1.8%
Greece	0.21%	1,216,634	15%	0.11	6.3%	0.01	44%	0.05	5.4%
Iceland	0.03%	116,276	2.2%	0.38	13%	0.05	66%	0.25	1.7%
Ireland	0.10%	915,984	-3.8%	0.22	7.7%	0.02	45%	0.10	4.8%
Italy	0.71%	6,761,785	-3.1%	0.12	7.1%	0.01	73%	0.09	3.8%
Luxembourg	0.00%	142,915	6.0%	0.29	4.0%	0.01	61%	0.18	3.2%
Netherlands	1.38%	6,068,499	3.1%	0.36	25%	0.09	78%	0.28	1.4%
Norway	0.08%	1,816,201	-0.7%	0.39	20%	0.08	83%	0.33	1.3%
Portugal	0.07%	1,450,497	5.9%	0.14	6.5%	0.01	71%	0.10	1.8%
Spain	0.86%	8,989,657	6.1%	0.22	3.3%	0.01	61%	0.14	1.8%
Sweden	3.86%	3,828,205	0.8%	0.42	37%	0.16	78%	0.33	2.5%
Switzerland	0.11%	2,132,826	9.7%	0.28	21%	0.06	91%	0.26	1.9%
United Kingdom	1.20%	17,304,827	4.5%	0.28	6.9%	0.02	79%	0.22	2.0%
Asia/Pacific									
Australia	0.17%	6,736,068	13%	0.32	9.1%	0.03	46%	0.15	6.6%
China	26.9%	37,591,948	11%	0.03	0.6%	< 0.01	4.3%	< 0.01	6.7%
Hong Kong	2.26%	1,900,672	7.4%	0.27	38%	0.10	88%	0.24	1.3%
India	1.63%	2,586,258	23%	0.00	0.6%	< 0.01	5.0%	< 0.01	26%
Japan	3.13%	27,513,814	8.1%	0.20	55%	0.12	91%	0.20	2.0%
Malaysia	0.51%	838,398	10%	0.03	0.7%	< 0.01	4.9%	< 0.01	15%
New Zealand	0.15%	1,023,133	6.3%	0.25	3.7%	0.01	62%	0.15	8.3%
Singapore	0.02%	714,014	41%	0.15	26%	0.04	60%	0.09	1.9%
South Korea	9.37%	14,855,171	12%	0.31	58%	0.18	92%	0.28	0.2%
Taiwan	2.54%	4,787,144	2.2%	0.21	13%	0.03	49%	0.10	1.6%
Middle East									
Egypt	0.03%	550,661	7.4%	0.01	0.1%	< 0.01	1.2%	< 0.01	25%
Israel	0.29%	1,550,594	0.1%	0.22	4.8%	0.01	59%	0.13	0.6%
Kuwait	n/a	123,065	18%	0.05	15%	0.01	40%	0.02	7.6%
Saudi Arabia	n/a	529,522	18%	0.02	4.0%	< 0.01	20%	< 0.01	4.8%
Sudan	n/a	13,077	37%	0.00	<0.1%	< 0.01	0.3%	< 0.01	23%
Syria	n/a	30,578	80%	0.00	0.2%	< 0.01	1.2%	< 0.01	74%
United Arab Emirates (UAE)	0.10%	341,070	91%	0.07	4.0%	< 0.01	20%	0.01	7.2%
Latin & South America									
Argentina	0.76%	2,532,185	26%	0.06	0.2%	< 0.01	10%	< 0.01	6.7%
Brazil	1.53%	8,777,278	27%	0.04	1.0%	< 0.01	9.8%	< 0.01	20%
Chile	0.27%	1,367,514	5.3%	0.08	0.3%	< 0.01	7.1%	0.01	2.1%
Colombia	0.28%	1,471,433	21%	0.03	0.2%	< 0.01	9.0%	< 0.01	8.0%
Mexico	0.68%	5,471,183	19%	0.05	0.2%	< 0.01	5.6%	< 0.01	4.1%
Peru	0.08%	488,836	21%	0.02	< 0.1%	< 0.01	2.1%	< 0.01	4.4%
Venezuela	0.20%	1,426,681	18%	0.05	< 0.1%	< 0.01	1.7%	< 0.01	7.0%
North America									
Canada	1.94%	10,298,798	1.5%	0.31	21%	0.07	74%	0.23	2.9%
United States	19.7%	109,333,753	7.2%	0.36	26%	0.09	64%	0.23	5.8%

Section 7: Endnotes

[1] http://www.secureworks.com/media/press_releases/20080922-attacks
[2] http://www.dshield.org/port.html?port=7212
[3] http://www.tenebril.com/src/advisories/open-proxy-relay.php
[4] http://blogs.zdnet.com/security/?p=1854
[5] http://www.kaspersky.com/news?id=207575670
[6] http://news.bbc.co.uk/2/hi/technology/7596676.stm
[7] http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotCount90-Days (Main Web site: http://www.shadowserver.org/)
[8] http://isc.sans.org/diary.html?storyid=4963
[9] http://blogs.zdnet.com/security/?p=1670
[10] http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080813
[11] http://www.techzoom.net/publications/insecurity-iceberg/
[12] http://blogs.zdnet.com/security/?p=1972
[13] http://www.darkreading.com/document.asp?doc_id=164854
[14] http://www.freedom-to-tinker.com/blog/wzeller/popular-websites-vulnerable-cross-site-request-forgery-attacks
[15] http://blogs.zdnet.com/security/?p=1733
[16] http://blogs.zdnet.com/security/?p=1948
[17] http://www.net-security.org/malware_news.php?id=990
[18] http://www.theregister.co.uk/2008/08/07/new_sql_attacks/
[19] http://www.trustedsource.org/blog/142
[20] http://www.thewhir.com/marketwatch/070708_Lithuanian_Sites_Hacked_by_Russians.cfm
[21] http://www.doxpara.com/DMK_BO2K8.ppt
[22] http://news.cnet.com/8301-1009_3-10022303-83.html
[23] http://news.cnet.com/8301-1009_3-9998406-83.html
[24] http://news.cnet.com/8301-1009_3-10022303-83.html
[25] http://www.internetnews.com/infra/article.php/3761216/DNS+Cache+Poisoning+Flaw+Goes+Ballistic.htm
[26] https://www.clarifiednetworks.com/Videos#head-6b86a6c80a56a57fa63271a929f7531af5b5aa81
[27] http://www.internetnews.com/security/article.php/3774131
[28] http://www.pir.org/index.php?db=content/News&tbl=Press&id=9
[29] http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf
[30] http://www.circleid.com/posts/arpa_org_and_uk_adopting_dnssec/
[31] http://eng.5ninesdata.com/~tkapela/iphd-2.ppt
[32] http://blog.wired.com/27bstroke6/2008/08/revealed-the-in.html
[33] Ibid.
[34] http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1332898,00.html
[35] http://www.heise-online.co.uk/security/Speculation-surrounds-DoS-vulnerability-in-the-TCP-protocol--/news/111651
[36] http://www.renesys.com/blog/2008/09/gustav-3-days-later.shtml
[37] http://www.renesys.com/blog/2008/09/ike-brings-biggest-multistate.shtml
[38] Ibid.
[39] http://www.renesys.com/blog/2008/08/georgia-on-my-mind-1.shtml
[40] http://www.renesys.com/blog/2008/08/georgia-clings-to-the-net.shtml
[41] http://royal.pingdom.com/2008/09/04/the-major-internet-outages-so-far-in-2008/
[42] http://www.jaiku.com/blog/2008/08/18/web-server-outage/
[43] http://www.t1r.com/client/view.php?rid=54762
[44] http://status.aws.amazon.com/s3-20080720.html
[45] http://www.guardian.co.uk/media/2008/sep/03/digitalmedia.thailand
[46] http://www.pingdom.com/reports/vb1395a6sww3/check_overview/?name=twitter.com%2Fhome
[47] http://www.datacenterknowledge.com/archives/2008/08/15/nastia-liukin-bigfoot-crash-web-servers/
[48] http://news.cnet.com/8301-13578_3-10054346-38.html
[49] http://www.telegeography.com/cu/article.php?article_id=24744
[50] http://www.pcworld.com/businesscenter/article/147958/new_cable_linking_japan_russia_goes_into_service.html
[51] http://www.akamai.com/dl/whitepapers/akamai_state_of_the_internet_q1_2008.pdf
[52] http://news.cnet.com/8301-1001_3-10053949-92.html?tag=mncol
[53] http://www.telegeography.com/cu/article.php?article_id=25135
[54] http://www.t1r.com/client/view.php?rid=54652
[55] http://www.telegeography.com/cu/article.php?article_id=24604
[56] http://www.telegeography.com/cu/article.php?article_id=24970
[57] http://www.telegeography.com/cu/article.php?article_id=25025
[58] http://www.telegeography.com/cu/article.php?article_id=25123
[59] http://www.telegeography.com/cu/article.php?article_id=24719
[60] http://www.telegeography.com/cu/article.php?article_id=24128
[61] http://wikileaks.org/leak/cuba-ve-cable-2006.zip
[62] http://wikileaks.org/wiki/Cuba_to_work_around_US_embargo_via_undersea_cable_to_Venezuela
[63] http://news.cnet.com/8301-1035_3-9994491-94.html?tag=mncol
[64] http://www.businessweek.com/technology/content/jul2008/tc20080722_084460.htm
[65] http://findarticles.com/p/articles/mi_m0UKG/is_1999_Nov_15/ai_58125101
[66] http://online.wsj.com/article/SB122091223182012137.html
[67] http://mybroadband.co.za/news/Telecoms/5379.html
[68] http://tech.yahoo.com/news/ap/20080929/ap_on_hi_te/sprint_wimax
[69] http://www.xohm.com/en_US/learn/up-next/
[70] http://www.telegeography.com/cu/article.php?article_id=24676
[71] http://www.telegeography.com/cu/article.php?article_id=25139
[72] http://www.telegeography.com/cu/article.php?article_id=24892
[73] http://www.telegeography.com/cu/article.php?article_id=24842
[74] http://www.telegeography.com/cu/article.php?article_id=24891
[75] http://www.telegeography.com/cu/article.php?article_id=24769
[76] http://www.telegeography.com/cu/article.php?article_id=24689
[77] http://www.telegeography.com/cu/article.php?article_id=24617
[78] http://www.japantoday.com/category/technology/view/kddi-to-launch-1gbps-fiber-optic-service-in-oct
[79] http://www.dslreports.com/shownews/Amsterdam-Tests-Residential-1Gbps-Fiber-97642
[80] http://news.bbc.co.uk/1/hi/technology/7600834.stm
[81] http://www.telegeography.com/cu/article.php?article_id=25443
[82] http://www.census.gov/ipc/www/idb/tables.html, http://www.census.gov/ipc/www/popclockworld.html (07/01/08 estimate)
[83] http://www.census.gov/popest/national/files/NST-EST2007-alldata.csv
[84] http://www.univsearch.com/state.php
[85] http://www.worldatlas.com/aatlas/populations/usadensityh.htm
[86] http://www.akamai.com/dl/whitepapers/How_will_the_internet_scale.pdf
[87] http://www.blu-ray.com/faq/
[88] http://www.itif.org/files/2008BBRankings.pdf
[89] http://online.wsj.com/article/SB121676442873775111.html
[90] http://www.connectednation.com/state_programs/
[91] http://www.speedmatters.org/document-library/sourcematerials/cwa_report_on_internet_speeds_2008.pdf
[92] http://files.cwa-union.org/speedmatters/state_reports_2008/CWA_Report_on_Internet_Speeds_2008_Ranking.pdf
[93] http://www.internetevolution.com/author.asp?section_id=562&doc_id=163929
[94] http://gigaom.com/2008/09/30/europe-leads-global-broadband-growth-again/
[95] http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/09-30-2008/0004894590&EDATE=
[96] http://www.govtrack.us/congress/bill.xpd?bill=s110-1492
[97] http://bit.ly/3n7WqN

The Akamai Difference

Akamai® provides market-leading managed services for powering rich media, dynamic transactions, and enterprise applications online. Having pioneered the content delivery market one decade ago, Akamai's services have been adopted by the world's most recognized brands across diverse industries. The alternative to centralized Web infrastructure, Akamai's global network of tens of thousands of distributed servers provides the scale, reliability, insight and performance for businesses to succeed online. An S&P 500 and NASDAQ 100 company, Akamai has transformed the Internet into a more viable place to inform, entertain, interact, and collaborate.

Acknowledgements

EDITOR: David Belson
CONTRIBUTOR: Jon Thompson
CONTRIBUTOR: Patrick Gilmore
CONTRIBUTOR: Alloysius Gideon
EXECUTIVE EDITOR: Brad Rinklin
EXECUTIVE EDITOR: Tom Leighton

Please send comments, questions, and corrections to stateoftheinternet@akamai.com

Akamai | Powering A Better Internet™
For more information, visit **www.akamai.com**

U.S. Headquarters
8 Cambridge Center
Cambridge, MA 02142
Tel 617.444.3000
Fax 617.444.3001
U.S. toll-free 877.4AKAMAI
(877.425.2624)

Akamai Technologies GmbH
Park Village, Betastrasse 10 b
D-85774 Unterföhrinzg, Germany
Tel +49 89 94006.0

www.akamai.com