Volume 2, Number 2

REPORT

2nd Quarter, 2009

The State of the Internet

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 publishes a quarterly "State of the Internet" report. This report includes data gathered from across Akamai's global server network about attack traffic and broadband adoption, as well as trends seen in this data over time. It also aggregates 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 second quarter of 2009, Akamai observed attack traffic originating from 201 unique countries around the world. The United States and China were the two largest attack traffic sources, accounting for nearly 45% of observed traffic in total. Akamai observed attack traffic targeted at more than 4,100 unique ports, with the top 10 ports once again seeing roughly 90% of the observed attack traffic. (The additional concentration in the second quarter was again likely related to traffic associated with the Conficker worm.) Numerous Web site hacks and Web-based exploits were reported during the quarter, as were distributed denial of service attacks targeted at DNS infrastructure.

Only minor network outages and routing issues were reported in the second quarter. Web site outages during the quarter impacted popular Google applications and Web hosting providers.

A number of new submarine cable projects were announced or deployed in the second quarter. These deployments are ultimately expected to improve Internet connectivity for countries in Africa, Northern Europe, and the Asia-Pacific region. New WiMAX projects and deployments will bring broadband wireless connectivity to countries in Europe, Africa, and Asia, as well as the United States. Fiber-to-the-home efforts announced in the second quarter will benefit users in the United Kingdom, the United States, Germany, Spain, and the Philippines.

The second quarter saw an increased push for IPv6 adoption, as ARIN adopted new requirements governing applications for additional IPv4 address space, and cable provider Comcast announced the availability of IPv6 transit services. In a number of countries around the world, funding was allocated to drive increased broadband deployment, while in the United States, the FCC began seeking comments on the creation of a national broadband plan.

Akamai observed a nominal one percent increase (from the first quarter of 2009) globally in the number of unique IP addresses connecting to Akamai's network. From a global connection speed perspective, South Korea returned to having the highest levels of "high broadband" (>5 Mbps) connectivity and also maintained the highest average connection speed, at 11 Mbps. In the United States, New Hampshire moved into the top position, with 56% of connections to Akamai occurring at 5 Mbps or greater. However, Delaware maintained the highest average connection speed in the United States, at 6.4 Mbps.

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 traffic patterns on leading Web sites.

In the second quarter of 2009, observed attack traffic continued to target a consistent set of ports, and attacks likely related to the ongoing spread of the Conficker worm were responsible for an overwhelming percentage of the observed attacks. China and the United States continued to be top sources for this observed attack traffic.

A number of leading providers experienced availability issues during the second quarter, reinforcing the need for failover services, such as those offered by Akamai.

Global connectivity continued to become more robust, with new WiMAX mobile broadband services announced or launching in a number of countries, new fiber-to-the-home initiatives bringing higher speed connectivity to subscribers in multiple countries, and new submarine cable projects increasing global Internet capacity and improving Internet connectivity around the world. Second quarter funding of broadband deployment initiatives around the world is intended to improve the availability of broadband Internet connections to users in more rural areas.

In the second quarter of 2009, the quarterly change in average connection speeds among countries around the world was mixed, though most countries continued to see increasing speeds on a year-over-year basis. In addition, the quarterly change in high broadband (connections to Akamai's network at speeds in excess of 5 Mbps) penetration was mixed, though most countries continued to see increasing high broadband penetration on a year-over-year basis as well. In spite of the growth in availability of, and options for, broadband connectivity, many countries and U.S. states unexpectedly saw increasing percentages of narrowband (<256 Kbps) connections to Akamai during the second quarter.

SECTION 2: Security

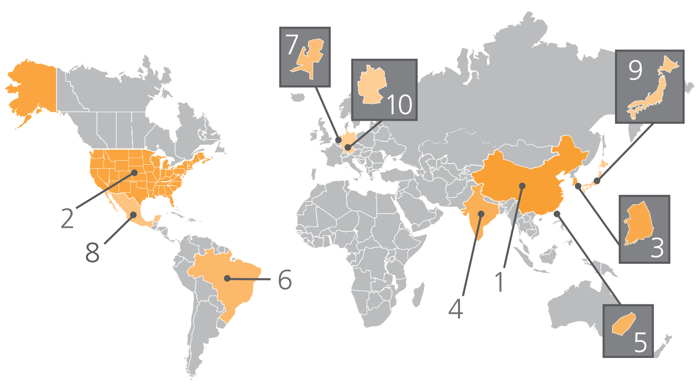
Akamai maintains a distributed set of agents deployed across the Internet that serve to monitor attack traffic. Based on the data collected by these agents, Akamai is able to identify the top countries from which attack traffic originates, as well as the top ports targeted by these attacks. (Ports are network layer protocol identifiers.) This section, in part, provides insight into Internet attack traffic, as observed and measured by Akamai, during the second quarter of 2009. 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 other attacks and events as published in the media during the second quarter of 2009. Note that Akamai does not release information on attacks on specific customer sites and that selected published reports are simply compiled here.

Akamai observed attack traffic originating from 201 unique countries around the world.

2.1 Attack Traffic, Top Originating Countries

During the second quarter of 2009, Akamai observed attack traffic originating from 201 countries. This count is up significantly from the first quarter (68 countries), and represents a return to levels seen in 2008, indicating that the significant drop in the first quarter may have been an anomaly. In the second quarter, China remained in first place, while the United States and South Korea maintained their second- and third-place positions respectively, as illustrated in Figure 1. Cumulatively, these top three countries were responsible for just over half of the observed attack traffic. A significant increase was seen in the level of observed attack traffic from India, causing the country to appear among the top 10 countries for the first time since the first quarter of 2008. In addition to India, in the second quarter, the Netherlands and Mexico also saw enough growth in attack traffic to move up into the top 10, while Sweden, Poland, and Romania all dropped out of the top 10.



	Country	% Traffic	Q1 09 %
1	China	31.35%	27.59%
2	United States	14.63%	22.15%
3	South Korea	6.83%	7.53%
4	India	3.93%	1.60%
5	Taiwan	2.32%	2.22%
6	Brazil	2.29%	2.60%
7	Netherlands	2.06%	1.16%
8	Mexico	1.96%	1.21%
9	Japan	1.95%	1.79%
10	Germany	1.93%	2.95%
–	OTHER	30.75%	–

Figure 1: Attack Traffic, Top Originating Countries

For the fifth consecutive quarter, attacks targeted at Port 445 were responsible for the highest percentage of the observed attacks.

2.2 Attack Traffic, Top Target Ports

During the second quarter of 2009, Akamai observed attack traffic targeted at over 4,100 unique ports. While approximately 80% lower than the port counts seen in the prior two quarters, it is arguably more in line with (though nearly 70% higher than) the port count seen in the third quarter of 2008. It is not clear exactly what was responsible for the significantly inflated port counts in the prior two quarters. With over two-thirds of the observed attacks once again being targeted at Port 445, likely related to continued activity around the Conficker worm and other variants/offshoots (such as Neeris), the concentration of attack traffic in the second quarter remained roughly in line with the first quarter of 2009, with the top 10 ports accounting for approximately 91% of the traffic, as shown in Figure 2. Despite some (expected) variance in percentages, the top 10 ports remained consistent with the prior quarter.

Port 445 remained the most-targeted port for the fifth consecutive quarter, and continues to be overwhelmingly responsible for the highest percentage of attacks. Unsurprisingly, the largest number of attacks was targeted at Port 445 from nine of the top 10 countries, in some cases with more than 20x as much traffic as the second place port. (The lone holdout was Mexico, where Port 5900 was the most targeted, followed closely by Port 445.) Ports 22 and/or 23 (SSH and Telnet) were among the top five most targeted ports from all of the top 10 countries, likely indicating that brute force login attempts remain a popular way to try to gain unauthorized access to Internet-connected systems.

Destination Port	Port Use	% Traffic	Q1 09 %
445	Microsoft-DS	68.47%	67.80%
23	Telnet	6.67%	2.40%
139	NetBIOS	4.36%	6.20%
135	Microsoft-RPC	3.08%	3.60%
22	SSH	2.54%	4.40%
5900	VNC Server	1.71%	1.30%
80	WWW	1.57%	1.30%
1433	Microsoft SQL Server	1.28%	1.00%
4899	Remote Administrator	0.62%	0.60%
25	SMTP	0.60%	0.80%
Various	OTHER	9.10%	–

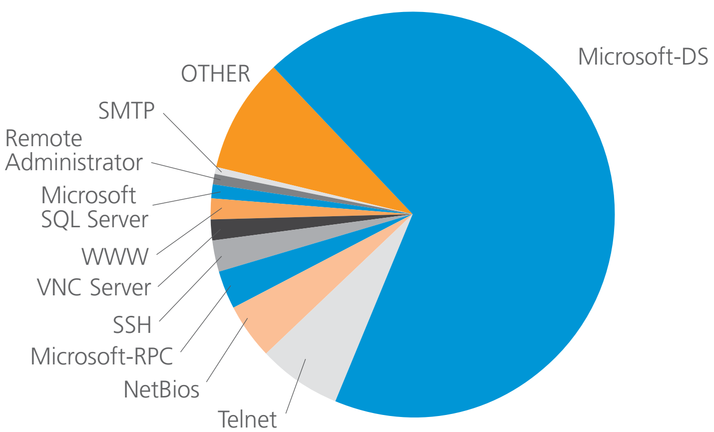


Figure 2: Attack Traffic, Top Target Ports

Monthly peaks in the second quarter were not as clearly coincidental with the publication of Microsoft Security Bulletins.

2.3 Attack Traffic, By Day

In examining a quarter-long view of attack traffic during the prior two quarters, Akamai found that peaks in attack traffic volume were roughly coincidental with the publication of Microsoft Security Bulletins for those months, potentially indicating that attackers were attempting to exploit the critical vulnerabilities described in those bulletins ahead of the patch release. However, in looking at overall global daily attack traffic patterns for the second quarter, as illustrated in Figure 3, we found that the monthly peaks were not as clearly coincidental. April's attack peak occurred on the 6th, three days before the Microsoft Security Bulletin Summary for April 2009 was originally published.[1] May's attack traffic peak occurred on the 27th, two weeks after Microsoft released their security updates. However, a secondary peak on the 7th is in fact coincident with the security bulletin advance notification originally issued that day.[2] In June, the highest level of attack traffic was recorded on the 10th — one day after Microsoft issued what was considered to be a "record" update, patching 31 vulnerabilities in Windows, Internet Explorer, Excel, Word, Windows Search and other programs.[3]

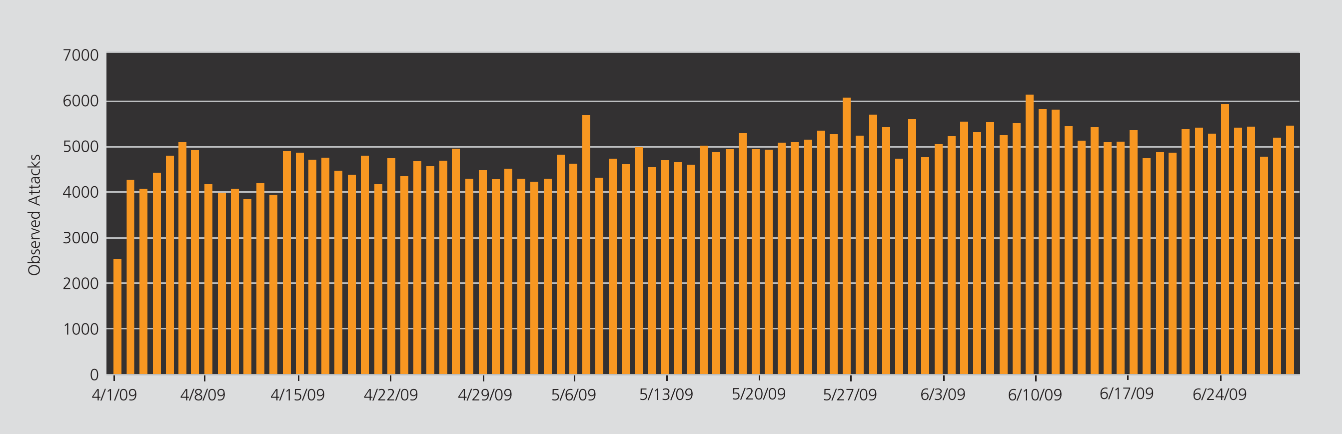


Figure 3: Attack Traffic, by Day of Quarter

2.4 Conficker

The Conficker worm caused a great deal of concern leading up to April 1, the day that it was set to "activate." However, April 1 largely came and went without any significant amount of digital pandemonium, though the worm continued to remain a menace into the second quarter. As noted above in Section 2.2, Port 445, associated with the spread of Conficker, continued to be the most heavily targeted port for attack traffic observed by Akamai in the second quarter.

It is believed that what Conficker did do on April 1 was update itself — the update may have provided instructions to infected systems for connecting to the thousands of new nodes that were registered by Conficker.C during the previous few weeks, which would effectively serve to increase the size of the botnet to a point where it would be extremely hard to stop.[4] A week later, it was also reported that the Conficker worm updated itself via P2P communications among infected systems, dropping a "mystery" payload onto these systems that hides behind a rootkit — reportedly, the worm tried to connect to several popular Web sites as a way to test for Internet connectivity, then deleted all traces of itself (but not the worm code itself) in the host machine, and was set to shut down on May 3.[5] In addition, it was reported that this update also installed fake antivirus software called Spyware Protect 2009 on infected systems, as well as an e-mail spam engine.[6]

Also in April, a four year-old worm known as Neeris re-surfaced,[7] exploiting the same MS08-067 vulnerability on Microsoft Windows-based systems that enabled Conficker to spread, causing problems for systems still not patched. It is possible that Neeris-related traffic may also have contributed to the high percentage of attacks targeted at Port 445 in the second quarter.

2.5 Distributed Denial of Service (DDoS) Attacks

In April, Web site hosting service provider and domain name registrar Register.com was targeted by a DDoS attack that lasted from the 2nd to the 5th, causing intermittent outages for the company's hosting and DNS customers.[8] On the 6th and 7th of April, name servers at The Planet were also targeted with a DDoS attack, causing Web site outages for customers of the Web hosting provider.[9]

Several DDoS attacks in the second quarter targeted DNS infrastructure.

Also in April, researchers at security firm Symantec uncovered evidence of Apple Macintosh-based malware that was being used to build a Mac OS X botnet designed to launch DDoS attacks. The malware was found in pirated copies of the iWork '09 and Adobe Photoshop software packages that were being distributed via P2P networks.[10]

In May, a DDoS attack targeted the DNS servers of Chinese domain name registrar DNSPod.com. According to published reports, Internet access was affected in five northern and coastal provinces.[11] In June, political activists launched DDoS attacks against "pro-Ahmedinejad" Iranian Web sites, including a number of news and government sites.[12] These attacks were reportedly generated through a combination of tools, including multiple iframe loading scripts, a public Web page "refresher" tool (later disabled due to abuse), and a PHP script.

Data published in May by Danny McPherson, Chief Security Officer at Arbor Networks, provided interesting insight into the attack traffic volumes generated by DDoS attacks that had been observed by Arbor during the preceding two months. According to the data, approximately 10% of the attacks generated 1 Gbps or more of traffic, while only 0.8% of the attacks generated traffic volumes in excess of 10 Gbps. In examining the data, McPherson also noted that the larger attacks typically have longer durations.[13]

Popular micro-blogging site, Twitter, came under attacks from a number of worms early in the second quarter.

More than 600 XSS vulnerability advisories were published in the second quarter.

2.6 Web Site Hacks & Web-Based Exploits

Security firm WhiteHat Security released data[14] in May that showed that most Web sites have at least one major vulnerability, and that over 80% of sites surveyed have at least one security flaw that can be classified as high/critical/urgent. Based on vulnerability data gathered from WhiteHat's own enterprise clients, the company highlighted the most common vulnerabilities that can be exploited by attackers. According to the company, approximately 30% of Web sites are likely to contain content spoofing bugs; 18%, insufficient authorization; 17%, SQL injection; 14%, predictable resource location; 11%, session fixation; 11%, cross-site request forgery (CSRF); 10%, insufficient authentication; and 9%, HTTP response-splitting flaws. In addition, they highlighted the fact that these vulnerabilities can be found on Web sites belonging to all types of companies: social networking companies have an 82% chance of having unresolved high/critical/urgent flaws in their Web sites; IT firms, 75%; financial services, 65%; insurance, 64%; retail, 61%; pharmaceutical, 59%; telecommunications, 54%; and healthcare, 47%.

Popular micro-blogging site, Twitter, came under attacks from a number of worms early in the second quarter. On Saturday, April 11, the "StalkDaily worm" exploited a cross-site scripting (XSS) vulnerability to spread rapidly across the site.[15] Users who visited the profile pages of other infected users became infected themselves — the worm reportedly modified the user's "About Me" section to include a link to the worm, and also sent unauthorized messages from infected accounts that directed users to the StalkDaily Web site.[16] The following day, the "Mikeyy" worm also spread across Twitter, posting unwanted messages from the accounts of infected users. Both worms were ultimately traced to a 17-year old high school senior, who claimed to have created the worms "out of boredom."[17] A follow-on worm dubbed "cleaningUpMikey" kept Twitter administrators busy on Monday as well, as they highlighted their efforts to secure compromised accounts and delete "tweets" that could have been used to further spread the worm(s).[18]

The Koobface virus, covered in prior issues of this report, continued to spread in the second quarter as well, despite efforts to stem its growth. In April, Microsoft announced that it was adding Koobface detection to its Malicious Software Removal Tool, in an effort to keep the virus off of Facebook.[19] However, in late May, Websense Security Labs highlighted a resurgence in Facebook-based Koobface attacks,[20] and in June, security firm Kaspersky Labs highlighted an explosion in the number of detected Koobface variants, from 324 at the end of May to nearly 1,000 by the end of June.[21]

In addition to the XSS vulnerability that led to the Twitter worms mentioned above, cross-site scripting continued to create security issues for many other sites. As was mentioned in the *1st Quarter, 2009 State of the Internet* report, XSSED.com, a Web site that tracks XSS issues, published[22] more than 600 advisories in April, May, and June and listed XSS vulnerabilities for Web sites belonging to some of the Web's most recognizable brands, including several vendors of security tools and software. However, a post[23] on June 22 to ZDNet's

In May, it was estimated that more than half of all malware found on Web sites was identified as Gumblar, and a new Web page was becoming infected every 4.5 seconds.

Zero Day security blog noted that engineers at Mozilla are working on a project, known as Content Security Policy, which is designed to shut down XSS attacks by providing a mechanism for sites to explicitly tell the browser which content is legitimate.

Malware known as Gumblar, named for the gumblar.cn domain it attempted to contact, resurfaced in April, and reports indicated that it had compromised several thousand legitimate Web sites.[24] According to security experts, Gumblar targets known flaws in software from Adobe Systems and uses them to install malware on a victim's machine. The malware steals FTP login credentials from victims, if found on the machine, and uses these logins to spread further. In addition, the malware also hijacks the victim's Web browser, replacing links in Google search results with links specified by the attackers. Cleanup of infected systems proved to be challenging, because in early May the attackers replaced the original malicious code with dynamically generated and heavily obfuscated JavaScript so that the scripts change from page to page and are difficult for security tools to spot. Later in May, it was estimated that more than half of all malware found on Web sites was identified as Gumblar, and a new Web page was becoming infected every 4.5 seconds.[25]

According to security vendor Websense, an attack known as Beladen spread across a reported 40,000 Web sites in June by using infection vectors similar to those exploited by Gumblar. Websense noted that these sites appear to have been compromised with rogue JavaScript code that redirects users to a fake Google Analytics site, after which they are directed to a site (beladen.net) that tries to exploit 15-20 different Internet Explorer or Firefox vulnerabilities to infect that system with malware.[26] Websense also issued an alert in June regarding a multi-level redirection attack it called Nine-Ball, again named after the final Web site that a victim contacts. The Nine-Ball attack reportedly compromised more than 40,000 Web sites with obfuscated JavaScript code that aims to install malware known as a trojan downloader onto a user's system.[27]

2.7 DNS Hijacks

DNS continued to not only be a popular target for DDoS attacks but was also a popular vector for attacks on specific Web sites. In April, an attack on the main DNS registrar in Puerto Rico led to the local Web sites of Google, Microsoft, Yahoo, Coca-Cola, and several other major companies being redirected for a few hours to rogue Web sites falsely claiming that the sites of these companies had been hacked.[28] Traffic to the Web sites for Google Uganda and Google Morocco was redirected to different sites for a short period in May due to unauthorized changes made to the DNS entries for both sites.[29] In addition, a DNS cache poisoning attack on Brazilian service provider NET Virtua resulted in customers of one of Brazil's biggest banks being redirected to fraudulent Web sites that attempted to install malware and steal passwords. Such cache poisoning attacks were described last year in the *3rd Quarter, 2008 State of the Internet* report.

2.8 DNSSEC

In June, the .org TLD became the first open generic TLD to implement DNSSEC, as well as the largest domain registry to implement it to date.

In the second quarter, DNSSEC adoption took several critical steps forward. In June, the United States Department of Commerce's National Telecommunications and Information Administration (NTIA) and National Institute of Standards and Technology (NIST) announced that the two agencies are working with the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign on an interim approach to deployment, by year's end, of DNSSEC at the authoritative root zone.[30] ICANN noted that details of the process were still being worked on, but that discussions between the Department of Commerce, VeriSign and ICANN have identified that VeriSign will manage and have operational responsibility for the Zone Signing Key in the interim arrangement, and that ICANN will manage the Zone Signing Key process. ICANN will work closely with VeriSign regarding the operational and cryptographic issues involved.[31] In an additional nod to the complexities of having the DNS root zone signed, the DNSSEC Industry Coalition convened a two day invitational symposium in June to identify potential issues and proposed solutions, recommended solutions, and next steps for reaching solutions.[32]

Signing of the DNS root will likely help accelerate the global deployment and implementation of DNSSEC. However, not everyone is waiting for a signed root to implement DNSSEC. As noted in the *1st Quarter, 2009 State of the Internet* report, DNSSEC was implemented on the .gov top level domain (TLD) in February. In June, the .org TLD became the first open generic TLD to implement DNSSEC, as well as the largest domain registry to implement it to date.[33] The CTO of Afilias, the technology provider for the .org TLD, noted that at the peak of effort around signing .org, a team of 30-40 people were working on it on a full-time basis, and estimated that the effort was a "multi-million dollar exercise."[34]

In May, the European Network and Information Security Agency (ENISA) published the results of a survey that it conducted around DNSSEC deployment plans. The survey found that 78% of service providers in Europe have plans to deploy DNSSEC within the next three years, though 22% do not. According to the survey, among service providers planning to deploy DNSSEC, 86% of the respondents highlighted complexity as a key barrier to deployment, while only 29% cited the lack of a signed root as a key barrier.[35]

78% of service providers in Europe have plans to deploy DNSSEC within the next three years.

SECTION 3: Networks and Web Sites: Issues & Improvements

Just over forty years ago, on April 7, 1969, the first Request for Comments (RFC) was published. Titled "RFC1 – Host Software," it established a framework for how networking technologies and the Internet itself work. The RFC model ultimately became the formal method of publishing Internet protocol standards, and today, there are more than 5,700 of them available.[36] Without the grounding provided by the RFCs, the issues and improvements highlighted within this section may not have been possible.

3.1 Network Outages

In early April, it was reported[37] that vandals were responsible for several cuts to AT&T fiber optic cables in the California cities of San Jose and San Carlos. According to published reports, the damage to the cables impacted landline and cell phone service, as well as Internet access for many in the affected areas. Some Web sites, hosted in data centers connected to the damaged fiber, also experienced time-outs and slow page loading times as traffic was re-routed.[38]

While not due to physical damage to network infrastructure, it is interesting to note that monitoring of Internet traffic from Iran showed a near complete outage for several hours on June 13, as shown in Figure 4. After the Iranian elections, it appeared that the state-owned Data Communication Company of Iran (DCI) essentially severed the upstream transit connections that carry Internet traffic for the country, according to monitoring done by security firm Arbor Networks' "Internet Observatory" project.[39] Additional analysis of the data by Arbor Networks showed that while Web and e-mail traffic returned at reduced levels after the "outage," Adobe Flash streaming video traffic did not.[40]

Monitoring of Internet traffic from Iran showed a near complete outage for several hours on June 13. While Web and e-mail traffic returned at reduced levels after the "outage," Adobe Flash streaming video traffic did not.

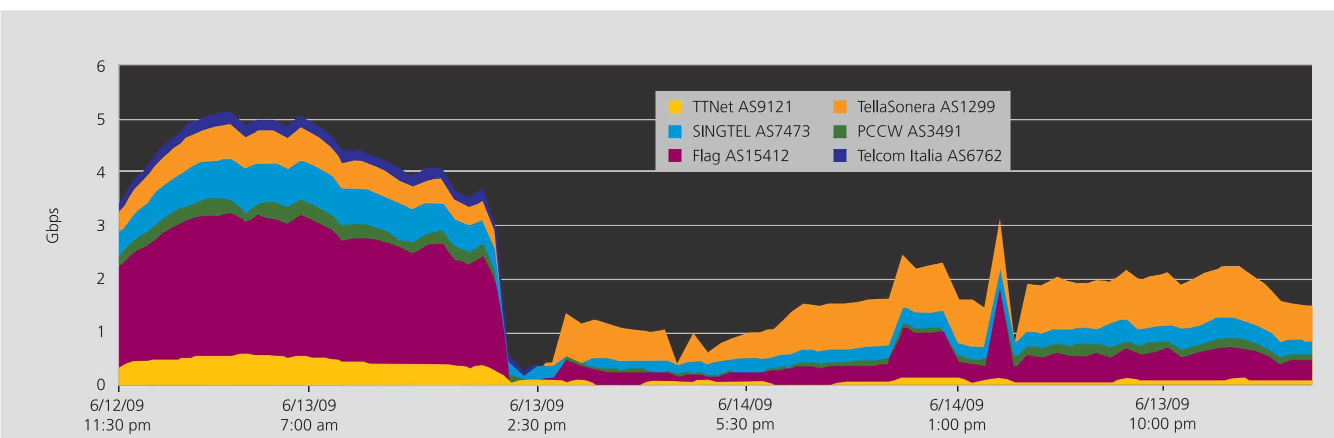


Figure 4: Iranian Internet Traffic Through Iran's Six Upstream Providers (Source: Arbor Networks)

3.2 Routing Issues

The *1st Quarter, 2009 State of the Internet* report discussed a routing issue caused by a Czech network provider that triggered a bug in older Cisco routers, as well as routers from Latvian vendor MikroTik. In May, a routing update from the African Network Operators Group (AfNOG) triggered a buffer overflow problem in older versions of free routing software called Quagga. According to network monitoring firm Renesys,[41] multiple prepends of a 4-byte ASN (autonomous system number) on an announced routing path caused routers running pre-October 2008 versions of Quagga to drop the associated BGP sessions, resulting in network outages and instabilities in Indonesia, Bulgaria, Germany, Romania, Brazil, Russia, the United States and many other places, as shown in Figure 5. The United States was impacted the worst, with 224 networks experiencing issues, according to Renesys' data, while Bulgaria, Russia, and the Ukraine all saw just over 200 networks with problems.

In addition, the Quagga bug also disabled several "Route Servers" at key Internet Exchange (IX) points around the world, though it did not cause direct outages at these IXs. These Route Servers trade prefixes between peer networks at the IXs. When these Route Servers crashed, network traffic had to be diverted to transit links (off of peering connections), which caused short outages as traffic was re-routed, and also caused congestion as transit links became full. The Renesys data does not show these networks as being unreachable (having outages) because the transit path still existed.

3.3 Web Site Outages

A number of Google services experienced outages in the second quarter, according to published reports. On April 16, a problem with Google Mail (Gmail) affected a "small subset" of users for approximately six hours,[43] and another outage occurred on May 8.[44] Just a week later, on May 14, a significant Google Apps service outage occurred. The company reported that the outage, which started a little before 11 a.m. EDT, caused about 14% of Google users to face slow service or interruptions. The problem affected all Google products, including Google Search, Google News, Gmail, Google Maps and Google Reader.[45] A Google vice president claimed that the problems occurred due to a system error that directed some of their traffic through Asia. According to Arbor Networks, Google's traffic constitutes up to 5% of all Internet traffic, and the company provided an interesting visualization of the impact of this Google service outage.[46] Figure 6 illustrates that during the approximately two-hour period of the outage, the average traffic levels across ten Tier1/2 ISPs in North America to Google's network dropped significantly. Additional problems with Google News were reported on May 18 and 19,[47] and YouTube users reported service outages and delays on June 3.[48]

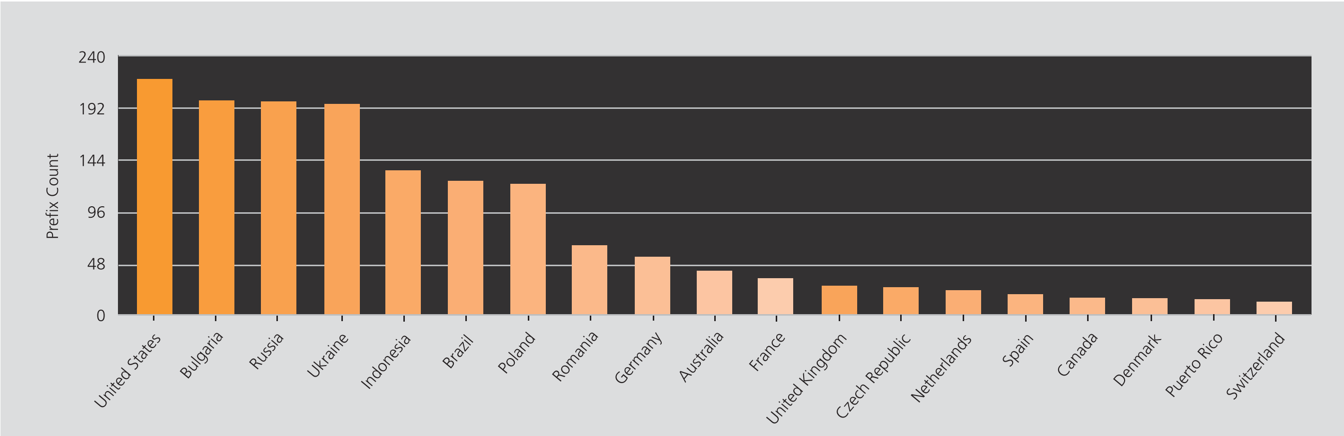


Figure 5: Network Outages By Country (Source: Renesys)

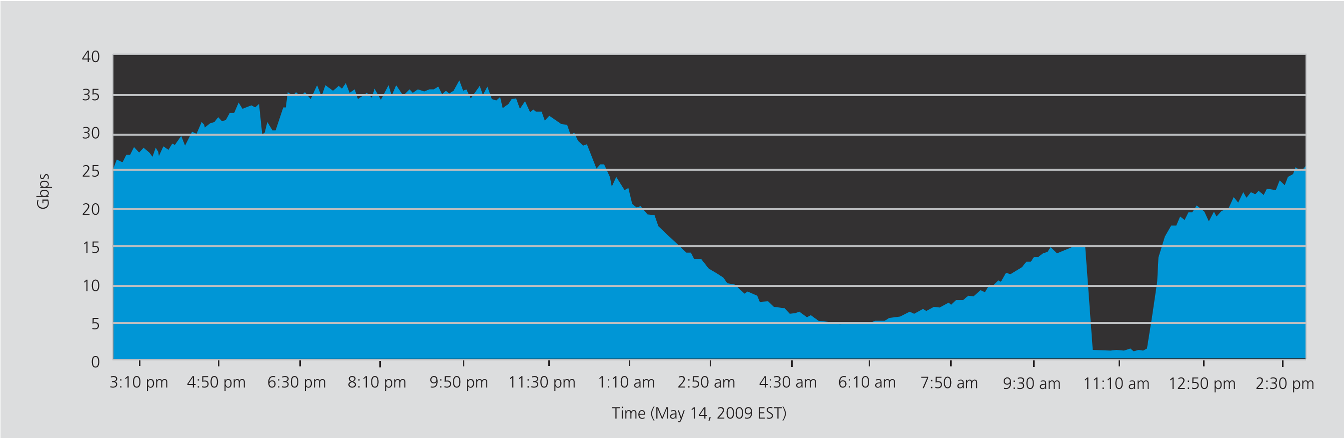


Figure 6: Average Traffic Across Ten Tier 1/2 ISPs in North America to Google's Network (Source: Arbor Networks)

Grid hosting provider Media Temple experienced problems on May 4 that took more than 16,000 customer Web sites offline. About 14,000 of the sites came back online after 10 hours of downtime, while the remaining 2,000 were down for more than a day. According to Media Temple, the problems occurred within a storage system, and were similar to those that caused a 38-hour outage in early March.[49] The company said that it would issue one-year service credits to affected customers.[50]

Outages at Web hosting providers impacted the availability of thousands of Web sites in the second quarter.

Just a week later, hosting provider The Planet experienced network problems that resulted in several half-hour periods of downtime on May 12 and 13. The downtime impacted not only hosting customers of The Planet, but also customers of HostGator and Site5, hosting companies that lease servers from The Planet. According to the company, the outage on May 12 was a result of human error, and the May 13 outage was likely caused by a software failure in several routers in Houston.[51]

June proved to be no better for hosting providers, as 100,000 customer Web sites hosted at VAserv.com were wiped out when intruders gained root access to the systems, apparently through a zero-day exploit in virtualization management software.[52] On June 10, a lightning strike caused a multi-hour outage for a number of server instances hosted on Amazon's EC2 service.[53] Closing out the quarter, a 45-minute power outage to hosting provider Rackspace's Grapevine, Texas data center on June 29 caused site outages for an unspecified number of hosting customers, and also impacted Rackspace's own Web site.[54] Customers of Akamai's site delivery services can, in many cases, leverage site failover capabilities to maintain Web site availability in the event that their origin becomes unavailable due to an outage at their hosting provider (or any other reason).

Telecommunications companies plan to lay 16 new undersea cables in 2009.

3.4 Significant New Connectivity — Undersea Cables

According to data published[55] in May by network research firm TeleGeography, telecommunications companies plan to lay 16 new undersea cables in 2009, which exceeds the number of cables laid in 2001, at the peak of the submarine cable investment bubble. TeleGeography notes that total projected spending on submarine cable construction in 2009 will reach USD$2.6 billion, which is a fraction of the USD$13.5 billion spent during the 2001 peak. This difference in spend is likely due to the newer cables covering shorter distances, as well employing simpler designs than earlier cable systems — many are intended to provide redundancy on popular existing cable routes, where outages have caused connectivity disruptions in the past.

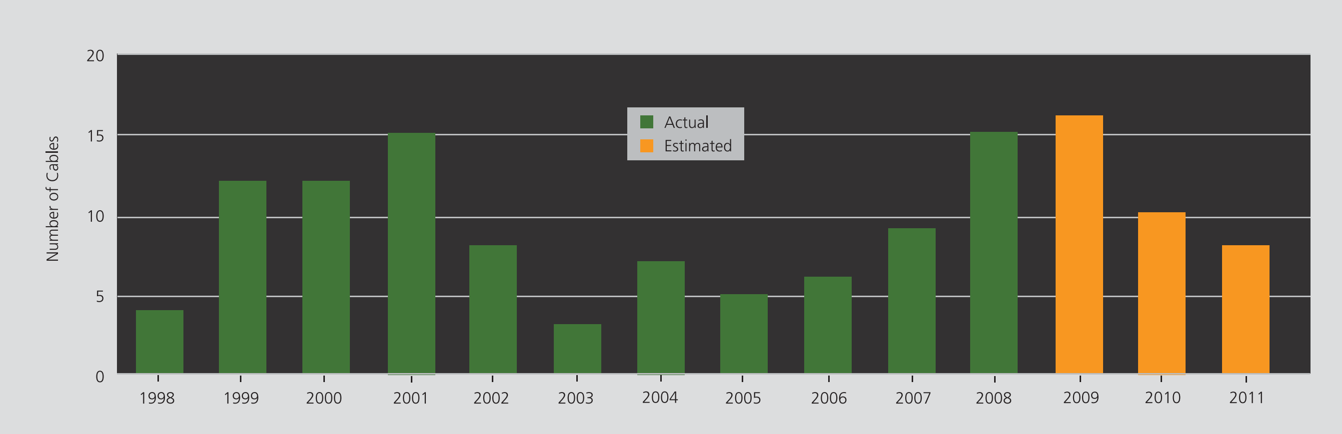


Figure 7: Submarine Cable Buildout, 1998-2011 (Source: TeleGeography)

The *1st Quarter, 2009 State of the Internet* report noted that Hibernia Atlantic had been selected to deploy a new cable network as part of Project Kelvin, intended to connect Ireland to the United States, Canada, and Europe. In June, Hibernia Atlantic announced that they had completed the first phase of the deployment, directly connecting North America to Northern Ireland through a cable landing at Portrush.[56]

Africa continued to see a significant amount of activity in the second quarter as well, with The East African Marine System (TEAMS) entering construction in April,[57] Namibian mobile operator Mobile Telecommunications joining the West Africa Cable System (WACS) consortium and pledging funding towards it,[58] and the planned extension of the ACE cable system to South Africa, connecting all countries along the West coast of Africa.[59] Completion of the SEACOM cable was delayed approximately a month, from June 27 to July 23. According to a post on the SEACOM Blog,[60] "The increase in pirate activity during April and May 2009, both in terms of intensity and geographical coverage, necessitated a change in SEACOM's cable installation plans…The planned route required the ship to transit an area of increased pirate activity where other ships had been attacked or seized."

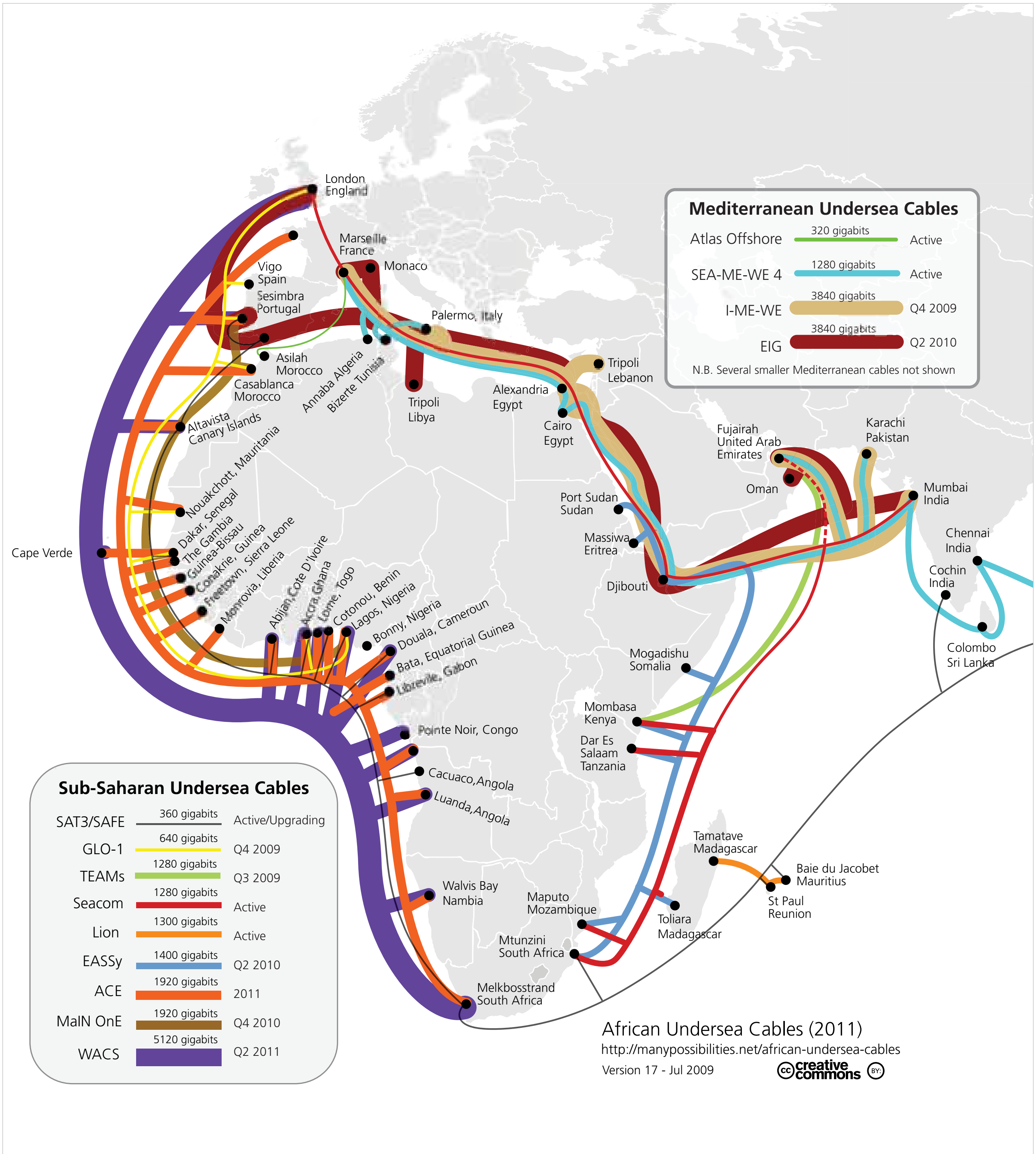


Figure 8: African Undersea Cables, 2011 (Source: http://manypossibilities.net/african-undersea-cables)

Two new cables were announced in the Asia-Pacific region during the second quarter. In May, nine Asia-Pacific telecommunications companies announced[61] the formation of a new consortium for the construction of a new regional undersea cable system dubbed the Asia Pacific Gateway (APG). Consortium participants include NTT Com (Japan), Chunghwa Telecom (Taiwan), China Telecom (China), China Unicom (China), KT Corp (South Korea), PLDT (Philippines), TOT (Thailand), Telekom Malaysia (Malaysia) and VNPT (Vietnam). This planned 8,000 km cable will connect Taiwan, China, South Korea, Japan, Hong Kong, Philippines, Vietnam, Thailand, Malaysia and Singapore. The APG cable will have a minimum capacity of 4 Tbps, and is expected to be ready for service in 2011. In June, Chunghwa Telecom and China Telecom announced plans to lay a 50-60 km submarine cable across the Taiwan Strait, between Kinmen and Xiamen.[62]

In addition to investments being made in new submarine cables, investments are also being made in capacity upgrades to existing systems. In June, Global Crossing announced[63] that they would be adding capacity to three of their fiber routes:

- The Mid-Atlantic Crossing (MAC) cable, which connects New York to Florida and the Virgin Islands.
- The Pan-American Crossing (PAC) cable, which cuts through Panama and connects Central America and the Caribbean to the west coast of the United States and to various transpacific cables.
- The South American Crossing (SAC) cable, which connects to both MAC and PAC and encircles most of South America.

3.5 Significant New Connectivity — Wireless

In April, satellite operator Eutelsat Communications launched its new Tooway consumer broadband service in the UK and Ireland, aiming to offer download speeds of up to 2 Mbps.[64] In June, Eutelsat announced that they would be raising the Tooway download speeds to 3.6 Mbps, with a planned increase to 10 Mbps after the launch of their KA-SAT satellite in 2010.[65] Satellite broadband provider WildBlue Communications demonstrated download speeds of 18 Mbps in April, although their high-end offerings will likely only offer speeds of 10 Mbps, and may not do so for at least another three years.[66]

Weather balloons acting as satellite substitutes may bring affordable broadband Internet access to Africa in the future.[67] Two entrepreneurs have secured exclusive rights to market technology developed by American telecommunications company Space Data throughout the African continent, and will operate through a formative consortium called Spaceloon. As individual users contact the balloons via modem, the balloons bridge them to a nearby Earth-bound network operations center (NOC), and the NOC in turn connects to various Internet gateways. Spaceloon will focus on four countries initially -- Sierra Leone, Liberia, Ghana, and Nigeria. The company is seeking subsidies from the governments to prove the concept, followed by plans for rollout as soon as possible. Spaceloon claims that transmission speed will depend on the customer's line of sight and the amount of bandwidth purchased, but that download speeds should match or exceed those of satellite Internet solutions, such as 10 Mbps for corporate customers.

In addition to Internet connectivity via satellite and weather balloon, the second quarter saw yet more announcements of planned WiMAX deployments and activations of new deployments around the world. While submarine cables will help to connect Africa to other countries, more WiMAX deployments on the continent will bring Internet connectivity to people living there.

Orange Cameroun expanded its WiMAX network to three new cities in May,[68] while in June, the Nigerian Communications Commission announced a partnership with Nigerian WiMAX operator ipNX to bring broadband access to all 36 states in the country through the 'State Accelerated Bandwidth Initiative' (SABI).[69] Saudi provider Mobily announced in June that it would be extending WiMAX coverage within the country from four cities to twenty by the end of 2009.[70]

A number of WiMAX announcements were made across Europe during the quarter as well. Users in the Athens and Thessaloniki regions of Greece will gain access to WiMAX service through Greek ISP Net One, the company announced in April.[71] May brought the announcement of WiMAX services in Catalonia, Spain;[72] seven cities in Montenegro;[73] and Kaunas, Lithuania.[74] In June, Maltese telecom operator GO,[75] Telecom Italia,[76] and Norway utility company Hafslund[77] all announced the deployment of WiMAX services across their respective countries.

In Asia, commercial WiMAX services were launched in April in Malaysia[78] and Taiwan.[79] In May, Comstar United TeleSystems announced that it would launch its WiMAX service in Moscow,[80] and a consortium of ISPs in Indonesia announced plans to invest in WiMAX services if they successfully secured a license in the country's July auction.[81]

As mentioned in the *1st Quarter, 2009 State of the Internet* report, Clearwire's WiMAX service continued to expand its footprint, and was officially launched in Atlanta in June.[82] Reports in the second quarter also indicated that Clearwire unofficially began offering service in Las Vegas in June, ahead of the planned commercial launch later in the summer.[83] Clearwire also announced that it would be launching what it called a "WiMAX innovation network" in California's Silicon Valley, with the aim of facilitating the development of new WiMAX applications.[84] Not to be left out, Verizon Wireless said that the new 4G network that the company is building will blanket the entire continental United States, including the far corners of rural America.[85] Verizon's 4G network will leverage Long Term Evolution (LTE) technology, and is targeted to reach 20-30 markets by the end of 2010. In addition, AT&T announced in late May that it planned to double the speed of its wireless broadband network by 2011, moving first to High Speed Packet Access (HSPA) technology, and eventually to LTE.[86]

June 2009 statistics published by the FTTH Council Europe found that FTTH adoption in Europe grew 18% during the first two quarters of 2009.

3.6 Significant New Connectivity — Fixed Broadband

Fiber-to-the-home/premises (FTTH/FTTP) initiatives continued to gain momentum in the second quarter, with some telecommunications companies announcing plans for new FTTx initiatives, while others announced the availability of new FTTx services. The June 2009 statistics published by the FTTH Council Europe found that FTTH adoption in Europe grew 18% during the first two quarters of 2009, and that Sweden leads the region in FTTH adoption, with nearly 11% of broadband connections leveraging the technology.[87]

In April, the i3 Group announced the availability of the first "Fibrezone" in South Ayrshire (UK), which will provide customers with connections at speeds up to 100 Mbps.[88] i3 Group also called on the UK government to commit to 100 Mbps FTTH broadband services, or "risk the country being left behind in the wake of a worldwide digital revolution."[89] German network operator Arcor launched a FTTH pilot in Hanau, connecting 'Coloneo', a rural housing project with 300 homes, at speeds of up to 100 Mbps.[90] Lyse Tele, a Norwegian provider, described its unique FTTH model — bring the fiber to the edge of a customer's lawn, and then provide the customer with instructions on how to bury their own fiber cable to the house.[91] At the end of the month, in Ellettsville, Indiana, local telecommunications company Smithville announced the completion of the first segment of a $90 million FTTH project to bring residential customers in the south-central and southern part of the state connectivity at speeds up to 100 Mbps.[92]

In Germany, in May, broadband provider HanseNet completed the first phase of a fiber-to-the-building (FTTB) network in Hamburg.[93] UTOPIA (Utah Telecommunications Open Infrastructure Agency), Utah`s municipal fiber-to-the-premise network, announced that it had connected its first customer to a 100 Mbps broadband service.[94] In addition, in May, Spain's telecom regulator, Comisión del Mercado de las Telecomunicaciones (CMT), issued a report noting that almost half of Spain's 14 million households could have FTTH connections by 2023.[95]

In June, the Electric Power Board of Chattanooga, Tennessee announced that it would soon begin offering FTTH connectivity to selected neighborhoods at speeds of 10-50 Mbps, and would reach its entire service area in 2010.[96] In the Philippines, telecommunications company Globe Telecom announced plans to launch a FTTH service in Makati's Forbes Park village in mid-June, with coverage expanding to three other villages in July.[97]

Cable companies also continued to upgrade their networks to support DOCSIS 3.0 during the second quarter. In Europe, Swiss provider Cablecom announced that a million households on its network had been upgraded to DOCSIS 3.0, capable of offering download speeds of up to 100 Mbps,[98] UPC Austria launched DOCSIS 3.0 services in Vienna,[99] and Germany's Kabel BW announced plans to begin rolling out new DOCSIS 3.0 broadband services in three regions this summer.[100] In the United States, cable provider Comcast launched DOCSIS 3.0 services in Pennsylvania,[101] West Virginia, Ohio, Maryland,[102] the Bay Area,[103] and Washington, DC.[104] Competitor Cox Communications expanded its DOCSIS 3.0 service availability to customers in Arizona[105] and Northern Virginia.[106]

DSL is still the dominant access technology, according to The Broadband Forum.

Interestingly, even with all of the deployment initiatives surrounding FTTH, DOCSIS 3.0, WiMAX, satellite, and other connectivity technologies, DSL is still the dominant access technology, according to data for the second quarter of 2009 published by The Broadband Forum. As shown in Figure 9, DSL connections account for nearly two-thirds of the market, with cable a distant second at 21%, and fiber in third place at 13%. Wireless and satellite each account for approximately 1%.[107]

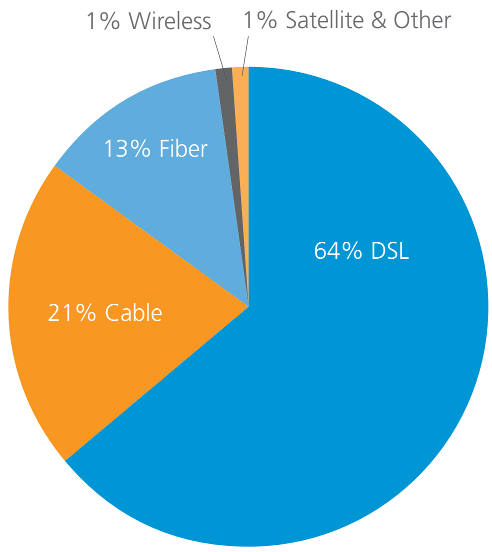


Figure 9: Global access technology market share, Q2 2009 (Source: The Broadband Forum)

3.7 IPv6

Reinforcing concern over the impending depletion of available IPv4 addresses, in April, the American Registry for Internet Numbers (ARIN) sent letters to owners of blocks of IPv4 address space, encouraging them to adopt IPv6, and outlining new requirements governing applications for additional IPv4 address space.[108]

Also in April, network monitoring site BGPmon.net published an analysis of IPv6 adoption, as determined by how many autonomous systems (ASNs) within a country were announcing an IPv6 prefix alongside their IPv4 prefixes. The results showed that Europe, East Asia, and parts of Africa scored high, and that Japan, New Zealand, the Czech Republic, and the Netherlands were among the leaders. However, it also noted that the United States average of 2% (316 of 13280 ASNs) was below the global average of 4%.[109]

April also saw the Canadian Federal Government present a three-phase IPv6 transition plan during the Plenary meeting of the ICT Standards Advisory Council of Canada. Building on the pioneering work that Canada has done with IPv6 since 1998, the full transition is targeted to complete by the end of 2015.[110] The United States Office of Management and Budget (OMB) announced the release in May of the "Planning Guide/Roadmap toward IPv6 Adoption within the US Government," which defines the Federal Government's IPv6 direction.[111] The purpose of the document is to provide United States government agency leaders with practical and actionable guidance on how to successfully integrate IPv6 throughout the enterprise, including transition milestones, a discussion of the impact on federal initiatives, and the need for support within governance and procurement programs.

In June, Comcast announced that it would be making IPv6 transit services available to wholesale customers, offering them at the same price as existing IPv4 services.[112] In addition, a Comcast Senior Vice President noted that residential tests could start in late 2009 or in 2010, although a full deployment would likely not occur for several years.[113] Forward-looking planning by Verizon Wireless was also uncovered in June, as several published articles in the industry press noted that device requirements published by Verizon earlier in 2009 stated that any device that connects to the LTE network currently being built [by Verizon Wireless] "shall support IPv6" and further states that "the device shall be assigned an IPv6 address whenever it attaches to the LTE network."[114]

The American Registry for Internet Numbers sent letters to owners of blocks of IPv4 address space, encouraging them to adopt IPv6.

3.8 DNS

Over the last several years, so-called "wildcard" redirection of DNS queries for inactive or nonexistent domains to Web pages operated by ISPs has created no small amount of controversy, for a variety of reasons. At the ICANN meeting that took place in Sydney in June, the Security and Stability Advisory Committee (SSAC) issued a report that recommended that ICANN should prohibit such use when introducing new top level domains (TLDs) and that existing TLD registries should also be stopped from exercising this practice.[115]

As noted in the *1st Quarter, 2009 State of the Internet* report, ICANN was developing plans to introduce additional generic TLDs, and had solicited feedback on the plans. Throughout the second quarter, additional concerns were raised about the potential introduction of these gTLDs and the processes through which they would be allocated, including potential favoritism for incumbent registrars,[116] trademark infringement issues,[117] the timetable for implementation,[118] and the perceived lack of need for additional gTLDs.[119, 120] In addition, technical concerns were raised relating to the introduction of new gTLDs and their impact on existing software tools that may operate from a hard-coded list of TLDs, that do not support TLDs with 4 or more characters, or that cannot handle double-byte strings for internationalized domain names.[121]

Since its founding in 1998, ICANN has operated under a "Joint Partnership Agreement" with the United States Department of Commerce. The current extension of this agreement is set to expire on September 30 of this year. In light of this impending expiration, the second quarter saw a call for ICANN's independence from the United States by Viviane Reding, European Union Commissioner for Information Society and Media.[122] Reding called for "a fully private and accountable ICANN, accompanied by an independent judicial body, as well as a 'G12 for Internet Governance' — a multilateral forum for governments to discuss general Internet governance policy and security issues." Along these lines, the United States Department of Commerce published a Notice of Inquiry[123] in April, seeking comments on how it should proceed. As expected, these moves generated debate on whether leaving "control of the Internet" with the United States[124] or providing ICANN with "independence"[125] were good things. The *3rd Quarter, 2009 State of the Internet* report will include information on the resolution of this issue, whatever it may be.

3.9 International Broadband Funding

Broadband initiatives are being funded by national governments in Australia, Estonia, the United Kingdom, Scotland, and New Zeland.

In early April, the Australian government announced that it had rejected the bids of all of the parties that had been involved in the tender process for the country's National Broadband Network (NBN), and that it would instead create a new public-private company to oversee and build the network.[126] The cost of the network could reportedly be as much as USD$31 billion, and it is expected to bring connectivity at speeds up to 100 Mbps to 90% of homes through FTTH services, with the remaining homes seeing speeds of up to 12 Mbps through a combination of ADSL broadband, wireless, and satellite connectivity. It is estimated that building the network would take 7-8 years.

Also in April, Estonia's government and the telecommunications companies operating there announced a €283 million (USD$374 million) project to provide access to broadband Internet for all by 2015. Known as the EstWin project, it calls for the development of a 100 Mbps network with access for all households and businesses across Estonia by 2015, in an effort to aid the development of the country, especially its rural areas.[127] The United Kingdom government also announced in April that it would back the creation of a "broadband-for-all" program in the country with initial funding of £250 million (USD $367.5 million). This funding pledge followed Lord Carter's Digital Britain report, which recommended the creation of a universal service obligation delivering a 2 Mbps broadband connection to every home in the country by 2012.[128] However, in June it was announced that the government would be levying a £0.50 tax on every fixed line voice and/or broadband connection, in order to help fund the rollout of services in rural regions.[129] The tax will be paid into a Next Generation Fund (NGF), and it is estimated that this extra fee will raise between £150-175 million per year.

In May, it was noted that in addition to the £250 million spent by the Scottish government to bring affordable 0.5 Mbps connectivity to virtually 100% of the populace, they would be spending another £102 million to bring broadband connectivity to more than 1,250 public buildings in remote areas.[130] Late in the month, the government of New Zealand announced that it would invest NZD $290 million (USD $180 million) in their national broadband network in 2009. This funding represents the first stage of a larger NZD $1.5 billion plan.[131]

3.10 United States National Broadband Plan

On April 8, the United States Federal Communications Commission (FCC) adopted a Notice of Inquiry,[132] formally beginning the proceedings to create the national broadband plan that Congress charged the Commission with developing in the American Recovery and Reinvestment Act of 2009. According to the Notice of Inquiry, the Recovery Act requires the plan to explore several key elements of broadband deployment and use, and the FCC now seeks comment on these elements, including:

- The most effective and efficient ways to ensure broadband access for all Americans
- Strategies for achieving affordability and maximum utilization of broadband infrastructure and services
- Evaluation of the status of broadband deployment, including the progress of related grant programs
- How to use broadband to advance consumer welfare, civic participation, public safety and homeland security, community development, health care delivery, energy independence and efficiency, education, worker training, private sector investment, entrepreneurial activity, job creation, and economic growth, and other national purposes.

Throughout the second quarter, much of the online coverage of the FCC's efforts to gather input on key elements of the national broadband plan focused on the need to not leave rural areas behind — $2.5 billion of the broadband stimulus funds are being administered by the Rural Utilities Service, intended to expand broadband access in so-called unserved and underserved areas. In May, acting FCC Chairman Michael Copps issued a report on broadband strategy for rural America.[133] Within the report, Copps identified a number of issues that must be overcome in order to deploy broadband in rural areas, including technological challenges, lack of data about where broadband is available and who is accessing it, and high network costs. In addition, net neutrality provisions associated with broadband stimulus funding were the subject of significant debate, and the FCC's *Bringing Broadband to Rural America* report noted that net neutrality rules are particularly important for rural broadband subscribers who may only have a single provider.[134]

SECTION 4: Internet Penetration

4.1 Unique IP Addresses Seen By Akamai

Through a globally-deployed server network, and by virtue of the billions of requests for Web content that it services on a daily basis, Akamai has unique visibility into the levels of Internet penetration around the world. In the second quarter of 2009, nearly 425 million unique IP addresses connected to the Akamai network — one and a quarter percent more than in the first quarter of 2009, and nearly 23 percent more than the same quarter a year ago. For the fifth consecutive quarter, the United States and China continued to account for nearly 40% of the observed IP addresses. The top 10 countries continued to remain the same quarter-over-quarter.

	Country	Q2 09 Unique IPs	Q1–Q2 Change	YoY Change
-	Global	424,808,918	+1.2%	+22.7%
1	United States	115,323,620	-0.7%	+13.1%
2	China	46,132,899	+3.5%	+35.7%
3	Japan	30,453,662	+3.5%	+19.6%
4	Germany	29,501,565	+3.3%	+23.8%
5	France	20,071,871	+2.5%	+18.7%
6	United Kingdom	18,549,665	-1.3%	+12.1%
7	South Korea	14,573,291	+1.2%	+10.0%
8	Canada	10,717,995	-4.2%	+5.70%
9	Spain	10,111,614	+2.0%	+19.3%
10	Brazil	10,077,917	+8.7%	+46.0%

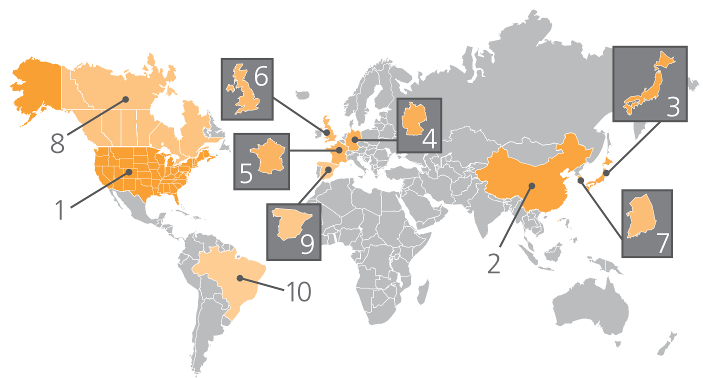


Figure 10: Unique IP Addresses Seen By Akamai

In the second quarter of 2009, nearly 425 million unique IP addresses connected to the Akamai network.

As shown in Figure 10, the quarterly growth in the number of unique IP addresses seen by Akamai was relatively muted, with Brazil showing the greatest gain, at 8.7% growth, among the top 10 countries. Interestingly, the United States, the United Kingdom, and Canada all had a lower number of unique IP addresses connecting to Akamai in the second quarter. Globally, more than 90 countries saw unique IP counts decline in the second quarter.

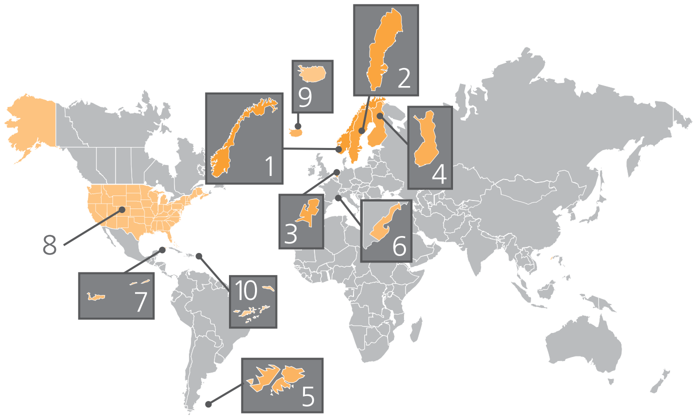
Looking at the "long tail," there were 183 countries with fewer than one million unique IP addresses connecting to Akamai in the second quarter of 2009, 143 with fewer than 100,000 unique IP addresses, and 35 with fewer than 1,000 unique IP addresses. All three counts remained fairly consistent with the prior quarter.

4.2 Global Internet Penetration

How does the number of unique IP addresses seen by Akamai compare to the population of each of those countries? Asked another way, what is the level of Internet penetration in each of those countries? Using the most recent global population data from the United States Census Web site[135] as a baseline, levels of Internet penetration for each country around the world were calculated based on Akamai's view into Internet traffic. These per capita figures should be considered as an approximation, as the population figures used to calculate them are static estimates — obviously, they will change over time, and it would be nearly impossible to obtain exact numbers on a quarterly basis. In addition, individual users can have multiple IP addresses (handheld, personal/home system, business laptop, etc.). Furthermore, in some cases, 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 one billion users per day, though we see only approximately 425 million unique IP addresses.

Akamai believes that it sees approximately one billion users per day.

In comparing the unique IP per capita figures for the second quarter of 2009, as shown in Figure 11, to those from the first quarter of 2009, we see some movement within the list, with the Falkland Islands and Monaco moving up higher among the top ten, while the United States and Iceland moved lower. Four countries (Falkland Islands, Monaco, Cayman Islands, and British Virgin Islands) experienced gains, four countries (Norway, Sweden, Finland, and Iceland) experienced losses, and the levels in the remaining two countries (Netherlands and the United States) in the top 10 remained static.



	Country	Unique IPs Per Capita
-	Global	0.08
1	Norway	0.46
2	Sweden	0.42
3	Netherlands	0.40
4	Finland	0.39
5	Falkland Islands	0.39
6	Monaco	0.38
7	Cayman Islands	0.36
8	United States	0.36
9	Iceland	0.35
10	British Virgin Islands	0.34

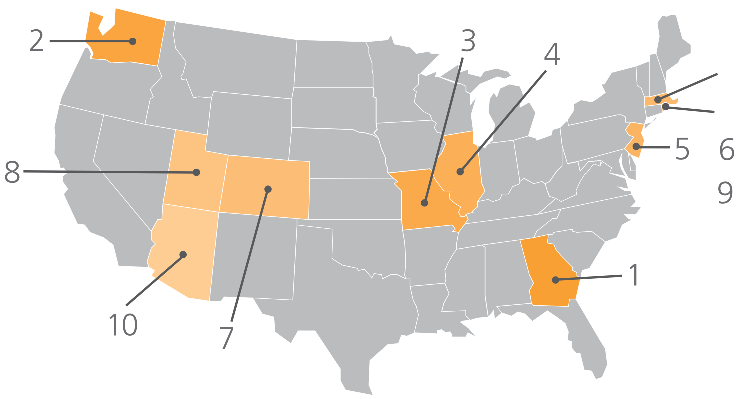
Figure 11: Global Internet Penetration

4.3 United States Internet Penetration

Internet penetration levels were mixed quarter-over-quarter.

Using state population estimates available from the United States Census Web site,[136] and the number of unique IP addresses from each state that Akamai saw in the second quarter of 2009, we calculated the levels of Internet penetration on a state-by-state basis — the top 10 states are shown in Figure 12. The same caveats noted above in Section 4.2, regarding per capita figures as an approximation, apply here as well.

Georgia saw the greatest quarter-over quarter increase, jumping from 0.62 to 0.70. Four other states (Missouri, New Jersey, Colorado, and Arizona) also saw increases, while Washington and Illinois saw no change quarter-over-quarter, and four states (Massachusetts, Maryland, Rhode Island, and Utah) saw declines, with Maryland dropping out of the top 10 list entirely (replaced by Arizona). In general, the levels of increase/decrease were fairly minor, and in line with the range of changes seen in previous quarters.



	State	Unique IPs Per Capita
1	Georgia	0.62
2	Washington	0.62
3	Missouri	0.57
4	Illinois	0.54
5	New Jersey	0.53
6	Massachusetts	0.51
7	Colorado	0.48
8	Utah	0.47
9	Rhode Island	0.46
10	Arizona	0.43

Figure 12: Internet Penetration in the United States

SECTION 5: Geography

Through its globally deployed server network and by virtue of the billions of requests for Web content that it services on a daily basis, Akamai has a unique level of visibility into the connection speeds of the systems issu-ing 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.[137]

The data presented below was collected during the second quarter of 2009 through Akamai's globally-deployed server network and includes all countries and U.S. states that had more than 1,000 average monthly unique IP addresses make requests to Akamai's network during the second quarter. For purposes of classification in this report, the "broadband" data included below is for connections greater than 2 Mbps, and "high broadband" is for connections of 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 Q1 value of 50% and a Q2 value of 51% would be reflected here as a +2% change.) A quarter-over-quarter change is shown within the tables in several sections below in an effort to highlight general trends. A year-over-year change is also shown in some tables in an effort to highlight longer-term trends.

Akamai's distributed network model, with servers deployed in 70 countries, can deliver content more reliably at broadband speeds.

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.[138] As we did in the first quarter, in order to provide additional insight into where users have connection speeds that would allow them to be able to effectively consume this higher quality media, we will continue to examine how the "high broadband" connections are distributed across speed groupings ranging from 5 to >25 Mbps.

On a global basis, the average connection speed declined by approximately 11%, and 125 countries had average connection speeds under 1 Mbps.

5.1 Global Average Connection Speeds

Examining the data for the third consecutive quarter, the overall trend in the second quarter of 2009 was not towards generally higher average connection speeds, as had been seen in prior quarters. Current highlights and historical trends for average connection speeds on a global basis can be found in Akamai's "Broadband Adoption Trends" data visualization tool, available at http://www.akamai.com/dv5.

As highlighted in Figure 13, a number of countries within the top 10 saw average connection speeds decline on a quarter-over-quarter basis. Globally, the average connection speed declined 11%, dropping back down to 1.5 Mbps — the same level as in the fourth quarter of 2008. Among the top 10 countries, seven of them saw lower average connection speeds in the second quarter, with Switzerland seeing the largest decline, at 13%. South Korea began to reverse the loss seen in the first quarter, increasing 3.2% to 11.3 Mbps.

During the second quarter, 125 countries had average connection speeds below 1 Mbps, up slightly from 120 countries in the prior quarter. The lowest average speed was seen in Eritrea, at 42 Kbps. Surprisingly, 14 countries globally had average connection speeds below 100 Kbps. In both cases, it is worth noting that many of these are small countries that have comparatively few connections to Akamai, and that many of them saw significant speed declines quarter-over-quarter.

	Country	Q2 09 Mbps	Q1–Q2 Change	YoY Change
-	Global	1.7	-11%	+8%
1	South Korea	11	+3.2%	-19%
2	Japan	8.0	-8.4%	-1.6%
3	Hong Kong	7.6	-8.8%	+4.0%
4	Romania	6.9	+5.8%	+49%
5	Sweden	5.8	-12%	+19%
6	Netherlands	5.7	-4.4%	+19%
7	Latvia	5.4	+8.5%	+33%
8	Switzerland	5.1	-13%	+5.4%
9	Czech Republic	5.0	-1.8%	+25%
10	Denmark	4.9	-7.4%	+19%
…				
18	United States	4.2	-8.4%	+1.6%

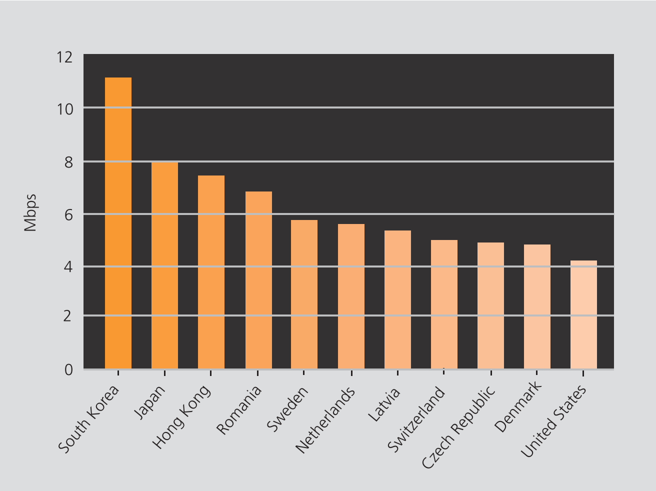


Figure 13: Average Internet Connection Speed by Country

5.2 United States Average Connection Speeds

Similar to trends seen in the global data for the second quarter of 2009, many U.S. states saw lower average connection speeds as well. While all states maintained average speeds above 2 Mbps, New Hampshire's average speed of 6.4 Mbps moved them into the top spot as the fastest state, as shown in Figure 14. Delaware fell to second place at 6.3 Mbps, down from 7.2 Mbps in the first quarter.

While all states maintained average speeds above 2 Mbps, New Hampshire's average speed of 6.4 Mbps moved them into the top spot as the fastest state.

	State	Q2 09 Mbps
1	New Hampshire	6.4
2	Delaware	6.3
3	New York	5.6
4	Vermont	5.4
5	Rhode Island	5.4
6	Connecticut	5.2
7	Maine	5.2
8	Nevada	5.2
9	Indiana	5.1
10	Oklahoma	4.9

Figure 14: Average Measured Connection Speed by State

Overall, 40 states plus the District of Columbia saw average connection speeds decline in the second quarter — Arizona shed 27%, while Vermont dropped just 0.2% The increases seen by the remaining 10 states were relatively modest, with Florida gaining 1.2%, and Maryland increasing 16%. Comparing average connection speeds year-over year, ten states saw speeds decline, from Georgia's 21% loss to Wyoming's 0.7% drop, while seven states (Maine, Vermont, New Mexico, Iowa, New Hampshire, Virginia, Hawaii) saw average speeds increase in excess of 25%.

Nearly one-fifth of the Internet connections around the world were at speeds greater than 5 Mbps.

5.3 Global High Broadband Connectivity

In the second quarter of 2009, 19% of the Internet connections around the world were at speeds greater than 5 Mbps. This represents a 5% decline from the prior quarter (bringing it back to the level seen in the fourth quarter of 2008), and only a 0.2% year-over-year increase.

South Korea reversed the decline seen in the first quarter of 2009, and is once again the country with the largest percentage of connections to Akamai at speeds over 5 Mbps, gaining 33% quarter-over-quarter to 69%. As shown in Figure 15, six countries in the top 10 saw lower levels of high broadband penetration in the second quarter, as did the United States. However, all countries in the top 10 saw yearly growth; in contrast, the United States declined year-over-year.

	Country	% above 5 Mbps	Q1–Q2 Change	YoY Change
-	Global	19%	-4.8%	+0.2%
1	South Korea	69%	+33%	+7.8%
2	Japan	56%	-1.6%	+6.7%
3	Romania	44%	+10%	+99%
4	Sweden	43%	-13%	+35%
5	Hong Kong	39%	-0.7%	+3.6%
6	Netherlands	34%	-4.6%	+55%
7	Czech Republic	33%	+0.9%	+126%
8	Denmark	32%	-11%	+77%
9	Belgium	31%	-8.8%	+17%
10	Canada	27%	+19%	+50%
…				
12	United States	24%	-7.1%	-8.0%

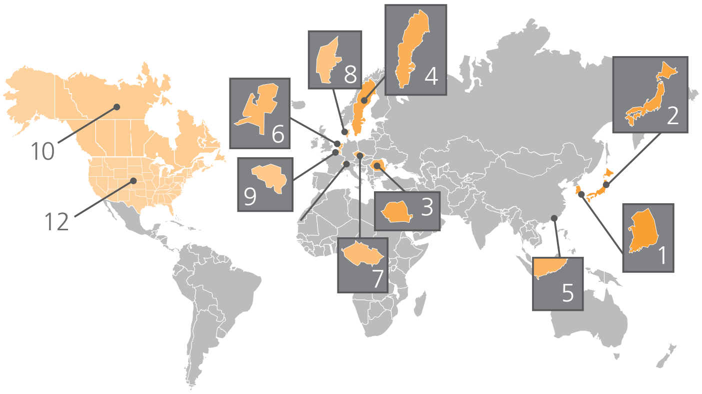


Figure 15: High Broadband Connectivity, Fastest Countries

With the exception of the Czech Republic, it appears that all of the other countries (Sweden, Netherlands, Denmark, and Switzerland) called out in the *1st Quarter, 2009 State of the Internet* report for having FTTH efforts that were bearing fruit saw quarterly declines in high broadband connectivity percentages — perhaps it was too early to declare those initiatives a success. Overall, however, 44 countries around the world saw increased quarterly levels of high broadband connectivity, and 74 countries saw yearly growth. In contrast, slightly more than 10 countries saw yearly declines, while just over 40 saw quarterly declines.

Given the quarterly growth in the level of high broadband connectivity seen in South Korea in the second quarter, it is not surprising to see the rate of high broadband penetration in the country, as shown in Figure 16, return to the level seen in the fourth quarter of 2008, after dropping to 0.15 in the first quarter of 2009. The global level of high broadband penetration remains consistent, and low, at 0.01 — that is, one high broadband IP per 100 people. Overall, only 30 countries globally had high broadband penetration rates higher than the global level.

Nearly a tenth of South Korea's connections to Akamai are at speeds greater than 25 Mbps.

	Country	High Broadband IPs Per Capita
-	Global	0.01
1	South Korea	0.21
2	Sweden	0.17
3	Netherlands	0.13
4	Japan	0.13
5	Denmark	0.11
6	Hong Kong	0.11
7	Norway	0.09
8	United States	0.09
9	Belgium	0.09
10	Finland	0.06

Figure 16: Global High Broadband Penetration

5.4 Global High Broadband Connectivity: Speed Distribution

As we examined the levels of high broadband connectivity around the world, questions frequently came up about the distribution of connections at speeds above 5 Mbps. In an effort to answer these questions, Akamai has done more detailed analysis on connections above 5 Mbps in order to publish more detailed data on the distribution of connection speeds, aggregated into 5 Mbps 'buckets.'

	Country	% above 5 Mbps	5-10 Mbps	10-15 Mbps	15-20 Mbps	20-25 Mbps	>25 Mbps
1	South Korea	69%	35%	14%	6.7%	3.9%	9.2%
2	Japan	56%	36%	13%	4.1%	1.6%	1.9%
3	Romania	44%	31%	7.3%	2.3%	1.1%	1.9%
4	Sweden	43%	31%	6.5%	2.5%	1.2%	2.2%
5	Hong Kong	39%	31%	6.4%	3.5%	2.1%	3.6%
6	Netherlands	34%	23%	2.8%	0.7%	0.4%	1.6%
7	Czech Republic	33%	29%	3.7%	0.9%	0.5%	1.3%
8	Denmark	32%	27%	2.8%	0.6%	0.3%	0.5%
9	Belgium	31%	28%	2.0%	0.2%	0.1%	0.4%
10	Canada	27%	23%	2.6%	0.7%	0.3%	0.7%
…							
12	United States	24%	20%	2.5%	0.7%	0.4%	1.0%

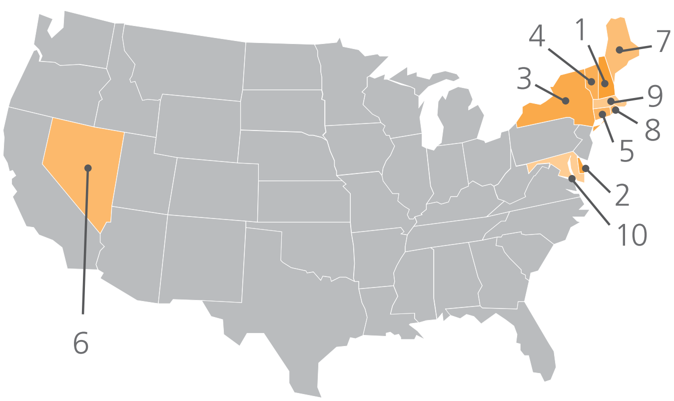
Figure 17: High Broadband Connectivity, Distribution of Speeds

As noted previously in Section 5.3, South Korea once again has the largest percentage of connections to Akamai (69%) at speeds above 5 Mbps. In looking at the distribution of these speeds in Figure 17, we find that while the percentage of connections in the 5-10 Mbps and 10-15 Mbps buckets map rather closely to second-place Japan, South Korea has significantly higher percentages of their connections in the higher speed buckets — most notably, for connections at speeds greater than 25 Mbps. Both South Korea and Japan saw the percentage of 5-10 Mbps connections grow quarter-over-quarter. In general, the highest percentages of connection speeds were once again in the 5-10 Mbps range, tailing off across the higher speed buckets.

We expect that, on a global basis, as the adoption and rollout of DOCSIS 3.0 technology by cable Internet providers, as well as other FTTH initiatives by telecom providers, become more widespread that the percentage of connections in the higher speed 'bucket' will grow over time. (Of course, this assumes that these providers are pricing the highest speed tiers of service at a level that subscribers find affordable.)

5.5 United States High Broadband Connectivity

The East Coast continues to be firmly established in leading the country with the greatest levels of high broadband connectivity, with nine of the top 10 slots as a result of Maryland displacing Oklahoma in the list. With a 20% quarterly increase, as shown in Figure 18, Maryland moved into the top 10, and was the only state within the top 10 to record a quarterly increase in the percentage of connections to Akamai at speeds over 5 Mbps.



	State	% above 5 Mbps	Q1–Q2 Change	YoY Change
1	New Hampshire	56%	-4.5%	+75%
2	Delaware	46%	-26%	-30%
3	New York	46%	-6.1%	+14%
4	Vermont	43%	-1.6%	+83%
5	Connecticut	39%	-5.2%	+12%
6	Nevada	37%	-19%	+11%
7	Maine	36%	-5.4%	+151%
8	Rhode Island	36%	-14%	-16%
9	Massachusetts	36%	-4.5%	+16%
10	Maryland	34%	+20%	+21%

Figure 18: High Broadband Connectivity, Fastest U.S. States

For the second quarter, 14 states saw quarter-over-quarter increases, with Hawaii jumping an impressive 65%. Hawaii also turned in the largest year-over-year increase, growing 773%, leading 38 other states and the District of Columbia that improved year-over-year. However, the District of Columbia and 36 additional states saw quarterly decreases, from South Dakota's 0.9% loss, to Arizona's significant 40% decline. Year-over-year, 12 states saw percentages decline, from Oklahoma's 0.4% loss to Delaware's 30% drop.

For the second quarter, 14 states saw quarter-over-quarter increases in levels of high broadband connectivity, with Hawaii jumping an impressive 65%

	State	High Broadband IPs Per Capita
1	Massachusetts	0.18
2	New York	0.17
3	New Jersey	0.16
4	Rhode Island	0.16
5	Washington	0.15
6	Maryland	0.14
7	New Hampshire	0.14
8	Oregon	0.12
9	Nevada	0.11
10	Connecticut	0.11

Figure 19: High Broadband Penetration in the United States

Looking at the levels of high broadband penetration across the United States as calculated for the second quarter, shown in Figure 19, we see that the penetration rates declined across the board, as compared to the first quarter. This decrease is likely due to the fact that many states had fewer unique IP addresses connecting to Akamai in the second quarter, and subsequently, fewer IPs connecting at speeds above 5 Mbps. While it doesn't account directly for the decline, published data from Leichtman Research Group indicated that net broadband subscriber additions in the second quarter across the nineteen largest cable and telephone providers in the United States, which represent 93% of the market, according to Leichtman, were the lowest in the eight years that they have been tracking the industry.[139]

Published data from Leichtman Research Group indicated that net broadband subscriber additions in the second quarter across the nineteen largest cable and telephone providers in the United States were the lowest in eight years.

The majority of the high broadband connections measure between 5-10 Mbps, with the next largest grouping between 10-15 Mbps.

5.6 United States High Broadband Connectivity: Speed Distribution

In looking at the ten states with the highest levels of high broadband connectivity, we find that the distribution of connection speeds above 5 Mbps generally follows a similar pattern. Unsurprisingly, the majority of the high broadband connections measure between 5-10 Mbps, with the next largest grouping between 10-15 Mbps. After that, the faster 'buckets' struggle to achieve even 2% of connections, as shown in Figure 20. This distribution of speeds is largely expected, as most residential broadband options offer connections in the 5-15 Mbps downstream range, with higher speed options available only in limited areas or at significantly higher prices. We expect that as the adoption and rollout of DOCSIS 3.0 technology by cable Internet providers, as well as other FTTH initiatives by telecom providers, become more widespread that the percentage of connections in the highest 'bucket' will grow over time, and that competitive market pressures will drive providers to price the highest speed tiers of service at a level that subscribers find affordable. In addition, as broadband stimulus funding is awarded and put to use, we expect that these numbers will likely grow commensurately in 2010 and beyond.

	State	% above 5 Mbps	5-10 Mbps	10-15 Mbps	15-20 Mbps	20-25 Mbps	>25 Mbps
1	New Hampshire	56%	47%	6.3%	1.3%	0.7%	1.4%
2	Delaware	46%	38%	4.2%	1.5%	0.9%	1.7%
3	New York	46%	37%	5.6%	1.2%	0.5%	1.2%
4	Vermont	43%	35%	5.1%	1.6%	0.6%	0.9%
5	Connecticut	39%	32%	4.7%	1.0%	0.6%	1.0%
6	Nevada	37%	28%	5.7%	1.1%	0.4%	0.9%
7	Maine	36%	32%	2.0%	0.8%	0.4%	1.4%
8	Rhode Island	36%	30%	2.9%	0.8%	0.4%	1.5%
9	Massachusetts	36%	28%	4.9%	1.1%	0.5%	1.3%
10	Maryland	34%	28%	3.8%	0.9%	0.4%	1.1%

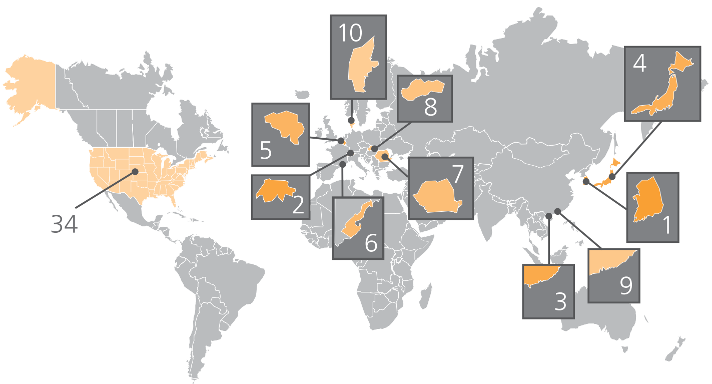
Figure 20: High Broadband Connectivity, Distribution of Speeds

5.7 Global Broadband Connectivity

As shown in Figure 21, a nearly six percent decline in broadband-level connections was seen globally in the second quarter, although more than half of all connections to Akamai are still at speeds above 2 Mbps. However, similar to the quarterly changes observed for global high broadband connectivity, quarterly changes for the top 10 countries with the highest levels of broadband connectivity were mixed as well for the second quarter of 2009. Six countries saw nominal increases; four countries saw slight declines as did the United States, dropping it to 34th place globally.

Three countries had 90% or more of their connections to Akamai at speeds over 2 Mbps.

South Korea, Switzerland, and Hong Kong were among the fastest countries in the world, with 90% or more of their connections to Akamai at broadband levels. In addition, all three countries saw modest levels of yearly growth as well. In total, more than 80 countries increased their levels of broadband connectivity year-over-year, while 50 did so from the first quarter.



	Country	% above 2 Mbps	Q1–Q2 Change	YoY Change
–	Global	53%	-5.8%	-9.5%
1	South Korea	93%	+13%	+3.7%
2	Switzerland	91%	-0.7%	+6.5%
3	Hong Kong	90%	+3.0%	+4.3%
4	Japan	89%	-0.6%	+2.0%
5	Belgium	89%	-1.5%	-1.1%
6	Monaco	88%	+2.9%	+50%
7	Romania	86%	+1.7%	+19%
8	Slovakia	84%	+2.0%	+1.8%
9	Macau	84%	+24%	+27%
10	Denmark	83%	-2.9%	+4.3%
	…			
34	United States	57%	-10%	-20%

Figure 21: Broadband Connectivity, Fast Countries

Looking at the levels of broadband penetration around the world, shown in Figure 22, we see that while the global average remained constant from the first quarter, levels in individual countries generally declined quarter-over-quarter, in some cases as much as 25-30%. While the United States saw a 12% decline, it climbed 12 places to #14 globally, up from #26 in the prior quarter. It isn't clear what drove the generally declining levels of broadband penetration in so many countries during the second quarter — seasonality, impact of the global economic recession on Internet usage, or some other reason.

	Country	Broadband IPs Per Capita
-	Global	0.02
1	Monaco	0.34
2	Norway	0.32
3	Sweden	0.30
4	Denmark	0.30
5	Netherlands	0.30
6	Switzerland	0.29
7	South Korea	0.28
8	Germany	0.28
9	Iceland	0.27
10	Belgium	0.26
...		
14	United States	0.21

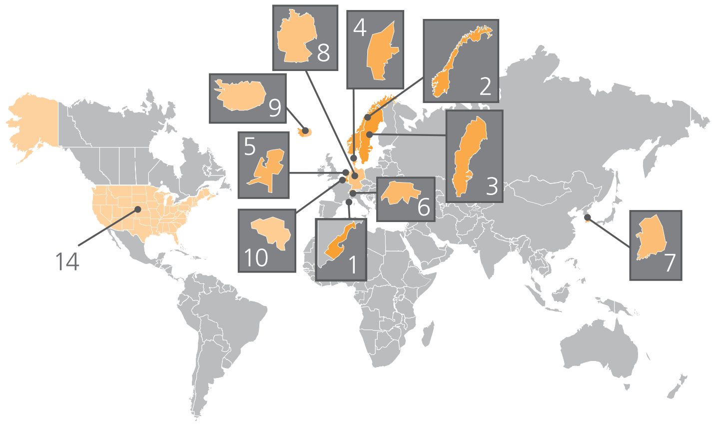


Figure 22: Global Broadband Penetration

5.8 United States Broadband Connectivity

The decline in the percentage of connections at high broadband speeds carried through to connections at broadband speeds as well. As shown in Figure 23, in the second quarter of 2009, all of the top 10 states saw a quarterly decline in their percentage of connections to Akamai at speeds over 2 Mbps. Delaware remained the top state, with 96% of their connections at broadband levels, though it was down approximately one percent from the prior quarter. While quarterly changes have been mixed in the past, it is somewhat surprising that all of the top 10 states saw percentages decline in the second quarter. However, they were not alone, as across the country, 46 states and the District of Columbia saw quarterly losses, from Alaska's miniscule 0.1% loss to Arizona's significant 31% loss. Only Maryland, Virginia, South Dakota, and New Jersey saw percentages increase from the first to second quarters. Yearly changes were more evenly split, with 25 states seeing yearly increases, including six of the top 10.

State	% above 2 Mbps	Q1–Q2 Change	YoY Change
1 Delaware	96%	-0.9%	+2.6%
2 New Hampshire	88%	-1.3%	+18%
3 Rhode Island	85%	-0.9%	+0.0%
4 Connecticut	82%	-3.3%	+3.3%
5 Maine	82%	-4.4%	+11%
6 Vermont	81%	-1.6%	+33%
7 Hawaii	79%	-5.3%	+12%
8 Nevada	78%	-8.5%	-5.8%
9 New York	78%	-3.4%	-0.3%
10 Oklahoma	74%	-7.4%	-4.4%

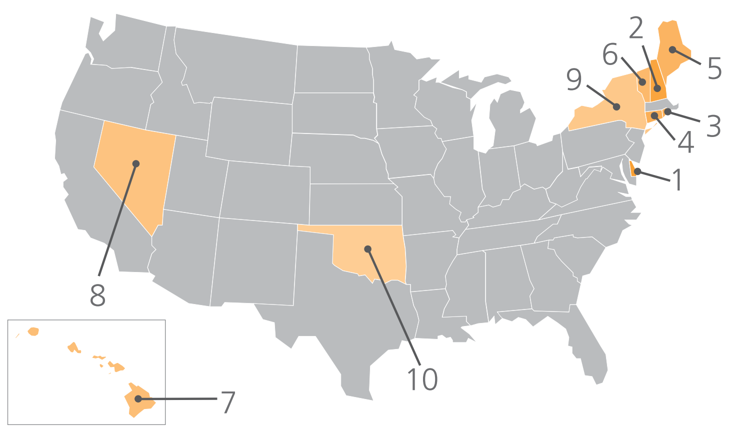


Figure 23: Broadband Connectivity, Fast U.S. States

Looking at the levels of broadband penetration across the United States as calculated for the second quarter, shown in Figure 24, we note that the penetration rates declined across the board, as compared to the first quarter, similar to what was seen globally, as well as within the United States for high broadband penetration. This decrease is likely due to the fact that many states had fewer unique IP addresses connecting to Akamai in the second quarter, and subsequently, fewer IPs connecting at speeds above 2 Mbps. In addition, as noted above in Section 5.5, the slow growth in new United States broadband subscriber counts during the second quarter, as highlighted in published data from Leichtman Research Group, may have contributed to this, though it is likely not the sole root cause. In contrast, however, a report published in June by market intelligence firm Strategy Analytics predicted that United States broadband service providers would add five million new subscribers during the course of 2009, and that broadband adoption levels in the United States should reach 80% in the next five years.[140]

	State	Broadband IPs Per Capita
1	Rhode Island	0.37
2	Massachusetts	0.32
3	New York	0.28
4	Washington	0.27
5	Colorado	0.26
6	South Dakota	0.26
7	New Jersey	0.26
8	Georgia	0.25
9	Nebraska	0.24
10	Illinois	0.24

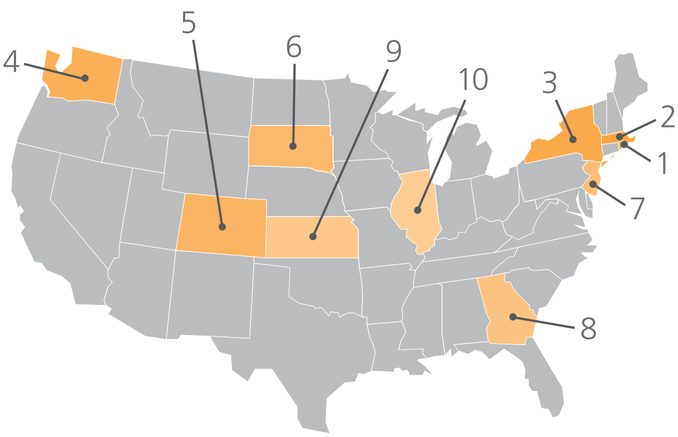


Figure 24: United States Broadband Penetration

A report published in June by market intelligence firm Strategy Analytics predicted that United States broadband service providers would add five million new subscribers during the course of 2009, and that broadband adoption levels in the United States should reach 80% in the next five years.

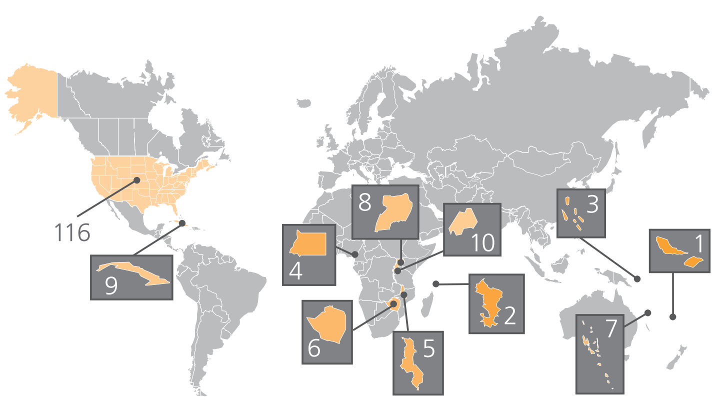
5.9 Global Narrowband Connectivity

14 countries saw declining quarterly levels of broadband connectivity, and 85 saw declining levels year-over-year.

In looking at narrowband connectivity, in contrast to the high broadband and broadband rankings, quarterly and yearly declines are considered to be a positive trend, as it likely indicates that higher speed connectivity is becoming more generally available, and more widely adopted. However, 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.

Interestingly, in the second quarter of 2009, many countries actually saw significant quarterly increases in their percentages of narrowband connections to Akamai. While this is not entirely unexpected, given the quarterly trends in broadband and high broadband connections described above, the size of the changes is somewhat surprising, with increases of 20% or more seen among the countries in the top 10, as shown in Figure 25. Even the global figure saw a significant quarterly increase, as did the United States, although both percentages continue to trend downward on a year-over-year basis. On a more positive note, 14 countries did see declining quarterly levels of broadband connectivity, and 85 saw declining levels year-over-year.

Consistent with prior 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. In addition, Akamai sees comparatively few unique IP addresses from these countries, so their high percentage of narrowband connections is not entirely unexpected.

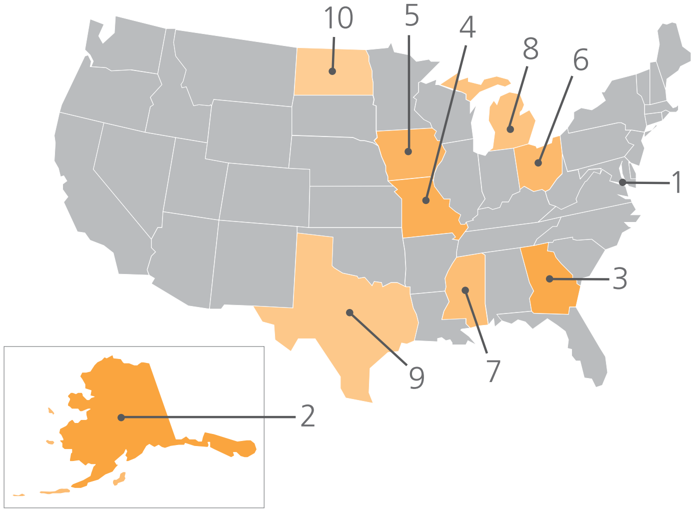


	Country	% below 256 Kbps	Q1–Q2 Change	YoY Change
–	Global	5.6%	+19%	-24%
1	Wallis And Futana	99.6%	+40%	+14%
2	Mayotte	99%	+21%	+10%
3	Solomon Islands	98%	+25%	+4.9%
4	Equatorial Guinea	98%	+32%	+12%
5	Malawi	97%	+25%	+23%
6	Zimbabwe	96%	+20%	+26%
7	Vanatu	96%	+28%	+9.5%
8	Uganda	95%	+22%	+11%
9	Cuba	95%	+30%	+8.5%
10	Rwanda	94%	+26%	+0.2%
	…			
116	United States	4.9%	+27%	-41%

Figure 25: Narrowband Connectivity, Slowest Countries

5.10 United States Narrowband Connectivity

The District of Columbia once again had the highest percentage of narrowband connections in the second quarter as observed by Akamai. It saw a significant quarterly increase in the level of narrowband connections, as did all of the states in the top 10, as shown in Figure 26. Only seven states saw the expected quarterly decrease in narrowband connection levels, from Nebraska's 31% loss to Illinois' 0.8% loss.



State	% below 256 Kbps	Q1–Q2 Change	YoY Change
1 District of Columbia	10%	+28%	-39%
2 Alaska	10%	+35%	+3.9%
3 Georgia	8.7%	+39%	-45%
4 Missouri	8.6%	+33%	+16%
5 Iowa	7.3%	+25%	-22%
6 Ohio	6.5%	+30%	+3.4%
7 Mississippi	6.2%	+25%	-11%
8 Michigan	6.0%	+25%	+10%
9 Texas	5.9%	+32%	-54%
10 North Dakota	5.8%	+57%	-10%

Figure 26: Narrowband Connectivity, Slowest U.S. States

While year-over-year changes among the top 10 states were mixed (six declined, four increased), across the whole United States, forty states and the District of Columbia had lower percentages of connections to Akamai at speeds below 256 Kbps than they did a year ago. Virginia and Washington State have made the greatest strides there, dropping 88% and 80% to 1.5% and 4.3% respectively.

Across the whole United States, forty states and the District of Columbia had lower percentages of connections to Akamai at speeds below 256 Kbps than they did a year ago.

SECTION 7: Appendix

REGION	% ATTACK TRAFFIC	UNIQUE IP ADDRESSES	UNIQUE IPs PER CAPITA	AVG SPEED (KBPS)	% ABOVE 5 MBPS	HIGH BB IPs PER CAPITA	% ABOVE 2 MBPS	BB IPs PER CAPITA	% BELOW 256 KBPS
Europe									
Austria	0.1%	1,830,259	0.22	3650	18%	0.04	65%	0.14	2.1%
Belgium	0.2%	2,992,197	0.29	4582	31%	0.09	89%	0.26	0.6%
Czech Republic	1.2%	1,465,727	0.14	4909	51%	0.05	76%	0.11	2.2%
Denmark	0.2%	1,980,139	0.36	4688	32%	0.05	83%	0.30	1.1%
Finland	0.1%	2,039,628	0.39	3313	17%	0.06	45%	0.17	1.6%
France	1.8%	20,071,871	0.31	3202	8.4%	0.03	70%	0.22	0.7%
Germany	1.9%	29,501,565	0.36	3677	15%	0.05	78%	0.28	1.6%
Greece	1.8%	1,710,771	0.16	2973	8.2%	0.01	60%	0.10	3.0%
Iceland	<0.1%	112,922	0.37	3878	15%	0.06	74%	0.27	–
Ireland	<0.1%	987,178	0.24	4210	9.0%	0.02	48%	0.11	3.7%
Italy	1.2%	9,104,612	0.16	2733	4.1%	0.01	68%	0.11	2.6%
Luxembourg	0.4%	153,817	0.32	2420	4.0%	0.01	49%	0.15	2.4%
Netherlands	2.1%	6,515,239	0.39	5126	34%	0.13	76%	0.30	1.9%
Norway	0.1%	2,092,867	0.45	4172	20%	0.09	70%	0.32	2.1%
Portugal	0.1%	1,803,445	0.17	3597	18%	0.03	77%	0.13	1.1%
Spain	1.3%	10,111,614	0.25	2654	4.3%	0.01	60%	0.15	1.7%
Sweden	1.5%	3,565,044	0.39	6037	43%	0.17	77%	0.30	2.2%
Switzerland	0.4%	2,375,230	0.31	4955	20%	0.06	91%	0.29	0.9%
United Kingdom	1.0%	18,549,665	0.30	3362	10%	0.03	72%	0.22	1.4%
Asia/Pacific									
Australia	0.3%	7,208,137	0.34	2698	18%	0.04	46%	0.16	7.4%
China	31%	46,132,899	0.03	813	0.5%	<0.01	4.0%	<0.01	12%
Hong Kong	1.0%	1,960,164	0.28	6915	39%	0.11	90%	0.25	0.7%
India	3.9%	3,317,873	0.00	895	1.1%	<0.01	5.0%	<0.01	27%
Japan	2.0%	30,453,662	0.24	7321	56%	0.13	89%	0.21	1.7%
Malaysia	0.2%	1,006,697	0.04	803	0.8%	<0.01	3.0%	<0.01	15%
New Zealand	<0.1%	1,161,504	0.28	2542	5.3%	0.01	54%	0.15	7.8%
Singapore	0.2%	1,359,585	0.30	3161	19%	0.06	55%	0.16	8.4%
South Korea	6.8%	14,573,291	0.30	11305	69%	0.21	93%	0.28	0.2%
Taiwan	2.3%	5,435,345	0.24	4128	20%	0.05	56%	0.13	2.0%
Middle East									
Egypt	0.3%	789,210	0.01	507	0.2%	<0.01	1.0%	<0.01	25%
Israel	1.3%	1,720,396	0.24	2720	3.9%	0.01	51%	0.12	0.6%
Kuwait	<0.1%	185,265	0.07	1929	5.8%	<0.01	31%	0.02	12%
Saudi Arabia	<0.1%	1,029,935	0.04	2089	4.1%	<0.01	36%	0.01	1.2%
Sudan	<0.1%	23,412	<0.01	354	–	<0.01	–	<0.01	43%
Syria	<0.1%	27,147	<0.01	339	–	<0.01	–	<0.01	66%
United Arab Emirates (UAE)	0.1%	390,676	0.08	2182	12%	0.01	21%	0.02	16%
Latin & South America									
Argentina	0.8%	3,170,536	0.08	1095	0.9%	<0.01	6.0%	<0.01	11%
Brazil	2.3%	10,077,917	0.05	1098	1.2%	<0.01	11%	0.01	21%
Chile	1.4%	1,693,502	0.10	1940	1.4%	<0.01	39%	0.04	6.8%
Colombia	1.0%	1,852,672	0.04	1429	0.8%	<0.01	18%	0.01	4.9%
Mexico	2.0%	6,631,706	0.06	991	0.6%	<0.01	5.0%	<0.01	3.5%
Peru	0.1%	580,050	0.02	850	0.4%	<0.01	3.0%	<0.01	8.1%
Venezuela	0.4%	1,608,511	0.06	762	0.3%	<0.01	1.0%	<0.01	12%
North America									
Canada	1.8%	10,717,995	0.32	3983	27%	0.07	75%	0.24	2.9%
United States	15%	115,323,620	0.38	3814	24%	0.09	57%	0.21	4.9%

SECTION 8: Endnotes

[1] http://www.microsoft.com/technet/security/bulletin/ms09-apr.mspx
[2] http://www.microsoft.com/technet/security/bulletin/ms09-may.mspx
[3] http://www.computerworld.com/s/article/9134156/Microsoft_sets_record_with_monster_Windows_IE_Office_update
[4] http://i.gizmodo.com/5197148/how-the-conficker-problem-just-got-much-worse
[5] http://news.cnet.com/8301-1009_3-10215678-83.html?part=rss&subj=news&tag=2547-1009_3-0-20
[6] http://news.cnet.com/conficker-also-installs-fake-antivirus-software/?part=rss&subj=news&tag=2547-1_3-0-20
[7] http://www.computerworld.com/s/article/9131139/Conficker_copycat_prowls_for_victims_says_Microsoft
[8] http://voices.washingtonpost.com/securityfix/2009/04/web_sites_disrupted_by_attack.html
[9] http://blogs.gartner.com/lydia_leong/2009/04/13/ddos-season/
[10] http://blogs.zdnet.com/security/?p=3157
[11] http://www.pcworld.com/businesscenter/article/165319/dns_attack_downs_internet_in_parts_of_china.html
[12] http://blogs.zdnet.com/security/?p=3613
[13] http://asert.arbornetworks.com/2009/05/60-days-of-attack-scale-duration/
[14] http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=217500479
[15] http://status.twitter.com/post/95332007/update-on-stalkdaily-com-worm
[16] http://news.cnet.com/8301-1009_3-10217681-83.html?part=rss&subj=news&tag=2547-1_3-0-20
[17] http://news.cnet.com/8301-1009_3-10217684-83.html?part=rss&subj=news&tag=2547-1_3-0-20
[18] http://blog.twitter.com/2009/04/wily-weekend-worms.html
[19] http://news.cnet.com/8301-1009_3-10210376-83.html?part=rss&subj=news&tag=2547-1_3-0-20
[20] http://securitylabs.websense.com/content/Alerts/3403.aspx
[21] http://www.reuters.com/article/pressRelease/idUS137513+06-Jul-2009+MW20090706
[22] http://www.xssed.com/archive
[23] http://blogs.zdnet.com/security/?p=3654
[24] http://news.cnet.com/8301-1009_3-10244529-83.html?part=rss&subj=news&tag=2547-1_3-0-20
[25] http://www.siliconrepublic.com/news/article/13025/cio/new-worm-to-rival-conficker
[26] http://news.cnet.com/8301-1009_3-10255226-83.html?part=rss&subj=news&tag=2547-1_3-0-20
[27] http://securitylabs.websense.com/content/Alerts/3421.aspx
[28] http://news.cnet.com/8301-1009_3-10228436-83.html?part=rss&subj=news&tag=2547-1009_3-0-20
[29] http://www.infoworld.com/print/75722
[30] http://www.nist.gov/public_affairs/releases/dnssec_060309.html
[31] http://icann.org/en/announcements/announcement-2-03jun09-en.htm
[32] http://assets.pir.org/PDFs/DNSSECSymposium_June11-12.pdf
[33] http://www.circleid.com/posts/20090602_org_first_open_top_level_domain_dnssec/
[34] http://www.internetnews.com/security/article.php/3823286
[35] http://www.enisa.europa.eu/doc/pdf/resilience_tech_report.pdf
[36] http://www.nytimes.com/2009/04/07/opinion/07crocker.html
[37] http://www.networkworld.com/news/2009/040909-att-outage-vandalism.html
[38] http://blogs.zdnet.com/BTL/?p=16106
[39] http://asert.arbornetworks.com/2009/06/iranian-traffic-engineering/
[40] http://asert.arbornetworks.com/2009/06/a-deeper-look-at-the-iranian-firewall/
[41] http://www.renesys.com/blog/2009/05/byte-me.shtml
[43] http://news.cnet.com/8301-17939_109-10221616-2.html?part=rss&subj=news&tag=2547-1_3-0-20
[44] http://royal.pingdom.com/2009/05/08/crowdsourced-error-detection-and-the-gmail-outage/
[45] http://www.networkworld.com/news/2009/051409-google-blames-outage-on-system.html
[46] http://asert.arbornetworks.com/2009/05/the-great-googlelapse/
[47] http://www.networkworld.com/news/2009/051909-google-news-stutters-for-second.html
[48] http://www.networkworld.com/news/2009/060309-youtube-hit-with-service.html
[49] http://www.datacenterknowledge.com/archives/2009/05/05/another-lengthy-outage-for-media-temple/

[50] http://www.datacenterknowledge.com/archives/2009/05/07/media-temple-issues-1-year-outage-credit/
[51] http://www.datacenterknowledge.com/archives/2009/05/13/ripples-felt-from-outage-at-the-planet/
[52] http://www.datacenterknowledge.com/archives/2009/06/09/web-host-hacked-via-virtualization-tool/
[53] http://news.cnet.com/8301-1001_3-10263425-92.html?part=rss&subj=news&tag=2547-1_3-0-20
[54] http://www.datacenterknowledge.com/archives/2009/06/29/outage-for-rackspace-customers/
[55] http://www.telegeography.com/cu/article.php?article_id=28286
[56] http://www.telegeography.com/cu/article.php?article_id=28984
[57] http://www.telegeography.com/cu/article.php?article_id=28058
[58] http://www.telegeography.com/cu/article.php?article_id=28079
[59] http://www.telegeography.com/cu/article.php?article_id=28811
[60] http://www.seacomblog.com/team-seacom/2009/06/pirates-delay-seacom-launch
[61] http://www.telegeography.com/cu/article.php?article_id=28624
[62] http://www.telegeography.com/cu/article.php?article_id=28755
[63] http://www.globalcrossing.com/news/2009/june/03.aspx
[64] http://www.eutelsat.com/news/compress/en/2009/pdf/CP2309UK-Tooway.pdf
[65] http://www.reuters.com/article/pressRelease/idUS77267+08-Jun-2009+PRN20090608
[66] http://gigaom.com/2009/04/29/wildblue-launches-bid-for-stimulus-funds/
[67] http://www.internetevolution.com/author.asp?section_id=694&doc_id=178131
[68] http://www.telegeography.com/cu/article.php?article_id=28400
[69] http://www.telegeography.com/cu/article.php?article_id=28729
[70] http://www.telegeography.com/cu/article.php?article_id=28825
[71] http://www.telegeography.com/cu/article.php?article_id=27995
[72] http://www.telegeography.com/cu/article.php?article_id=28640
[73] http://www.telegeography.com/cu/article.php?article_id=28662
[74] http://www.telegeography.com/cu/article.php?article_id=28673
[75] http://www.telegeography.com/cu/article.php?article_id=28865
[76] http://www.telegeography.com/cu/article.php?article_id=28803
[77] http://www.telegeography.com/cu/article.php?article_id=28727
[78] http://www.telegeography.com/cu/article.php?article_id=27934
[79] http://www.telegeography.com/cu/article.php?article_id=28201
[80] http://www.telegeography.com/cu/article.php?article_id=28225
[81] http://www.telegeography.com/cu/article.php?article_id=28583
[82] http://www.dslreports.com/shownews/Clearwire-Network-Officially-Live-In-Atlanta-102974
[83] http://www.telegeography.com/cu/article.php?article_id=28734
[84] http://www.telegeography.com/cu/article.php?article_id=27953
[85] http://reviews.cnet.com/8301-12261_7-10209933-51.html
[86] http://news.cnet.com/8301-17938_105-10250185-1.html?part=rss&subj=news&tag=2547-1_3-0-20
[87] http://www.ispreview.co.uk/story/2009/09/08/european-fibre-optic-ftth-broadband-grows-fast-but-not-in-the-uk.html
[88] http://www.ispreview.co.uk/story/2009/04/01/i3-group-preps-100mbps-fibre-optic-broadband-for-south-ayrshire.html
[89] http://www.ispreview.co.uk/story/2009/04/23/i3-group-uk-government-must-commit-to-100mbps-ftth-broadband.html
[90] http://www.telegeography.com/cu/article.php?article_id=27942
[91] http://telephonyonline.com/residential_services/news/lyse-tele-burying-fiber-cable-0421/
[92] http://www.smithville.net/press
[93] http://www.telegeography.com/cu/article.php?article_id=28295
[94] http://www.reuters.com/article/pressRelease/idUS258167+06-May-2009+BW20090506
[95] http://www.lightreading.com/document.asp?doc_id=177079&f_src=lightreading_sitedefault
[96] http://www.newschannel9.com/news/epb-978994-fiber-network.html
[97] http://www.telegeography.com/cu/article.php?article_id=28838

[98] http://www.telegeography.com/cu/article.php?article_id=28946
[99] http://www.telegeography.com/cu/article.php?article_id=28845
[100] http://www.telegeography.com/cu/article.php?article_id=28196
[101] http://www.broadbandreports.com/shownews/102375
[102] http://www.dslreports.com/shownews/102474
[103] http://www.dslreports.com/shownews/102029
[104] http://www.dslreports.com/shownews/102834
[105] http://www.dslreports.com/shownews/102791
[106] http://gigaom.com/2009/05/05/cox-offers-50-mbps-broadband-it-aint-cheap/
[107] http://www.thinkbroadband.com/news/4048-global-broadband-connections-reach-445-million.html
[108] https://www.arin.net/knowledge/about_resources/ceo_letter.pdf
[109] http://bgpmon.net/blog/?p=166
[110] http://www.circleid.com/posts/20090430_ipv6_canada_about_to_score/
[111] http://www.circleid.com/pdf/planning_guide_roadmap_toward_ipv6_adoption_in_usg_may2009_final.pdf
[112] http://www.internetnews.com/infra/article.php/3825696
[113] http://www.lightreading.com/document.asp?doc_id=178275&site=cdn&print=yes
[114] http://www.networkworld.com/news/2009/061009-verizon-lte-ipv6.html
[115] http://www.h-online.com/security/ICANN-security-experts-criticise-DNS-redirections--/news/113584
[116] http://www.circleid.com/posts/20090402_comments_icann_studies_new_proposed_tlds/
[117] http://www.internetevolution.com/author.asp?section_id=544&doc_id=175392
[118] http://www.circleid.com/posts/20090508_icanns_new_gtld_timetable_good_bad_ugly/
[119] http://www.circleid.com/posts/20090701_who_needs_more_tlds/
[120] http://www.circleid.com/posts/20090703_what_are_tlds_good_for/
[121] http://www.circleid.com/posts/20090625_new_top_level_domains_software_implications/
[122] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/696
[123] http://edocket.access.gpo.gov/2009/E9-9409.htm
[124] http://www.weeklystandard.com/Content/Public/Articles/000/000/016/515zoozk.asp
[125] http://www.circleid.com/posts/20090622_careful_what_you_wish_icann_independence_bad_idea/
[126] http://www.telegeography.com/cu/article.php?article_id=27955
[127] http://www.google.com/hostednews/afp/article/ALeqM5hIQGJsq0bYNb7c1f6An929x1LFXw
[128] http://www.pcpro.co.uk/news/broadband/251718/universal-broadband-pledge-gets-budget-boost
[129] http://www.telegeography.com/cu/article.php?article_id=28915
[130] http://www.ispreview.co.uk/story/2009/05/19/overview-scotlands-25m-gbp-universal-broadband-coverage.html
[131] http://www.telegeography.com/cu/article.php?article_id=28670
[132] http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-289900A1.pdf
[133] http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-291012A1.pdf
[134] http://www.pcworld.com/printable/article/id,165601/printable.html
[135] http://www.census.gov/ipc/www/idb/tables.html, http://www.census.gov/ipc/www/popclockworld.html (12/15/08 estimate)
[136] Ibid.
[137] http://www.akamai.com/dl/whitepapers/How_will_the_internet_scale.pdf
[138] http://www.blu-ray.com/faq/
[139] http://www.leichtmanresearch.com/press/081709release.html
[140] http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20090602006376&newsLang=en

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

Follow @akamai_soti on twitter

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

Akamai Technologies, Inc.

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)
www.akamai.com

International Offices
Unterfoehring, Germany
Paris, France
Milan, Italy
London, England
Madrid, Spain
Stockholm, Sweden
Bangalore, India
Sydney, Australia
Beijing, China
Tokyo, Japan
Seoul, Korea
Singapore

Akamai
Powering a Better Internet