Akamai

1st Quarter, 2008

The State of the Internet

REPORT

Executive Summary

Starting with the January to March (1st quarter) 2008 time period, Akamai will be publishing a quarterly "State of the Internet" report. This report will include data gathered across Akamai's global server network about attack traffic and broadband adoption, as well as trends seen in this data over time. It will also aggregate publicly available news and information about notable events seen throughout the quarter, including Denial of Service attacks, Web site hacks, and network events.

During the first quarter, Akamai observed attack traffic originating from 125 unique countries around the world. China and the United States were the two largest attack traffic sources, accounting for some 30% of this traffic in total. Akamai observed attack traffic targeted at 23 unique network ports. Many of the ports that saw the highest levels of attack traffic were targeted by worms, viruses, and bots that spread across the Internet several years ago.

A number of major network "events" occurred during the first quarter that impacted millions of Internet users. Cable cuts in the Mediterranean Sea severed Internet connectivity between the Middle East and Europe, drastically slowing communications. Cogent's de-peering of Telia impacted Internet communications for selected Internet users in the United States and Europe for a two-week period. A routing change by Pakistan Telecom that spread across the Internet essentially took YouTube, a popular Internet video sharing site, offline for several hours.

Akamai observed that from a global perspective, South Korea had the highest measured levels of "high broadband" (>5 Mbps) connectivity. In the United States, Delaware topped the list, with over 60% of connections to Akamai occurring at 5 Mbps or greater. At the other end of the bandwidth spectrum, Rwanda and the Solomon Islands topped the list of slowest countries, with 95% or more of the connections to Akamai from both countries occurring at below 256 Kbps. In the United States, Washington State and Virginia turned in the highest percentages of sub-256 Kbps connections. However, in contrast to the international measurements, these states only saw 21% and 18% of connections below 256 Kbps respectively.

Table of Contents

Introduction

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

Starting in the first quarter of 2008, Akamai will be aggregating and analyzing this data in conjunction with other publicly available information to publish a quarterly "State of the Internet" report. This first report includes baseline data on distributed denial of service (DDoS) attack traffic and global broadband connectivity and penetration rates as observed by Akamai. Future reports will explore trends in this data. In addition, each report will highlight significant Internet events, including attacks, outages, and Web site traffic peaks.

DDoS attack traffic in the first quarter of 2008 continued to target exploits that were identified years ago, suggesting that there is still a significant population of insufficiently patched systems connected to the Internet. During the quarter, there were several high-profile Internet outages, de-peering events, and route hijackings. These problems impacted millions of users across multiple networks, significantly degrading network performance and availability. On the bright side, however, broadband adoption statistics were encouraging, with Akamai observing a large percentage of connections at speeds over 2 Mbps for many countries and U.S. states.
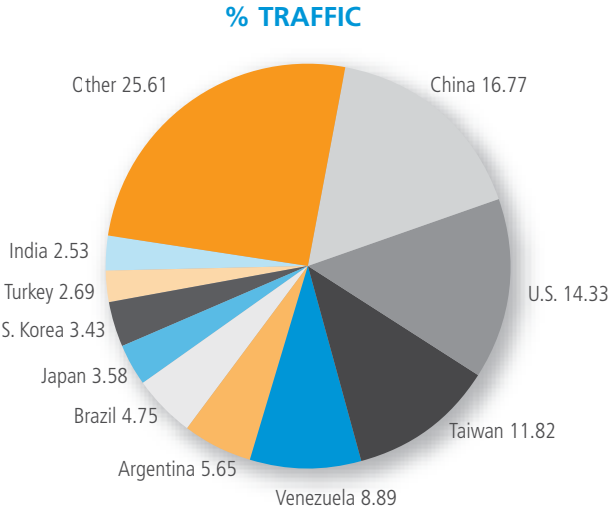
Section 2: Security

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 that attack traffic originates from, 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 first quarter of 2008.

In addition, published reports indicated that distributed denial of service (DDoS) attacks and Web site hacking attempts continued unabated in the first quarter, impacting thousands of Web sites. This section also includes information on selected DDoS attacks and Web site hacking attempts as published in the media during the first quarter of 2008. Note that Akamai does not release information on attacks on specific customer sites, and that selected published reports are simply compiled here.

2.1 Attack Traffic, Top Originating Countries

During the first quarter of 2008, Akamai observed attack traffic originating from 125 unique countries around the world. China and the United States were the two largest traffic sources, accounting for some 30% of traffic in total. The top 10 countries were the source of approximately three quarters (75%) of the attacks measured.

Country	% Traffic
China	16.77
United States	14.33
Taiwan	11.82
Venezuela	8.89
Argentina	5.65
Brazil	4.75
Japan	3.56
South Korea	3.43
Turkey	2.69
India	2.53
Other	25.61

% TRAFFIC

Other 25.61
China 16.77
India 2.53
Turkey 2.69
S. Korea 3.43
Japan 3.58
Brazil 4.75
Argentina 5.65
Venezuela 8.89
Taiwan 11.82
U.S. 14.33

2.2 Attack Traffic, Top Target Ports

During the first quarter of 2008, Akamai observed attack traffic targeted at 23 unique ports – some well known services, and others appearing to be more arbitrarily selected. The most attacked port, Port 135, was the target of nearly 30% of the attacks observed throughout Q1 2008. This port is used for remote procedure calls on Microsoft operating systems, and was used by the Blaster worm back in 2003 to facilitate propagation.[1]

% TRAFFIC

(other) 15.31
VNC Server 1.65
Remote Administrator 1.79
Symantec System Center Agent 2.93
MS SQL Server 6.12
WWW 6.19
Microsoft-DS 11.02
SSH 12.08
NETBIOS 13.27
Microsoft RPC 29.66

Destination Port	Port Use	% Traffic
135	Microsoft RPC	29.66
139	NETBIOS	13.27
22	SSH	12.08
445	Microsoft-DS	11.02
80	WWW	6.19
1433	MS SQL Server	6.12
2967	Symantec System Center Agents	2.93
4899	Remote Administrator	1.79
5900	VNC server	1.65
Various	(other)	15.31

OTHER PORTS OF INTEREST IN THE TOP 10 INCLUDE:

- Port 139, generally used for Windows network shares, enabling users to share files or folders across a network. This port was used by the Klez Family worm, Sircam virus, and Nimda worm back in 2001 to spread rapidly across networks, as they replicated themselves onto unprotected network shares.[2]

- Port 22, generally used for SSH (secure shell), enabling users to log in to remote machines in a secure fashion. Many attacks targeting this port are employing brute force methods in an effort to gain access to an account with a weak password.

- Port 2967, generally used by the Symantec System Center. In 2006, this port was targeted by an IRC Bot that exploited a buffer overflow problem in specific versions of the Symantec Anti-virus software.[3]

One interesting observation about the ports that see the highest levels of attack traffic is that they were targeted by worms, viruses, and bots that spread across the Internet several years ago. While that's not to say that there are not any current pieces of malware that attack these ports, it may point to a large pool of Microsoft Windows-based systems that are insufficiently maintained, and remain unpatched years after these attacks "peaked" and were initially mitigated with updated software.

Distributed Denial of Service (DDoS) Attacks

In late March, Arbor Networks[4] observed that approximately 2% of all inter-domain Internet traffic was DDoS traffic. The author of a post to the Arbor Weblog noted "Again, this is raw attack traffic, simply meant to exhaust connection state or fill links, nowhere in this mix is spam, phishing, scans, or other malicious or similarly annoying traffic." The Weblog post also noted that DDoS traffic has peaked above 5% of aggregated traffic.

In January 2008, an online group known as "Anonymous" targeted the Church of Scientology's Web site with a DDoS attack, in an effort to protest the Church's policies. The attack generated up to 220 Mbps of attack traffic at times, according to an article published in *PC World*.[5] Comparatively, it was a small attack — a single server can easily generate in excess of 220 Mbps of traffic. Given that there were likely thousands of larger attacks that occurred in the first quarter, this attack is somewhat noteworthy for the attention that it received in the mainstream and industry press, while other attacks received little to no press.

A number of gambling Web sites fell victim to DDoS attacks in February 2008,[6] according to the ShadowServer Foundation, a group comprised of volunteer security professionals from around the world. These Web sites were overwhelmed with a large number of HTTP GET requests, causing them to become unavailable for hours or days at a time.

Popular broadband Web site DSL Reports was also targeted by a DDoS attack in March 2008. According to an article in *The Register,*[7] the attack traffic was primarily comprised of open-connection requests from a distributed set of IP addresses – at least 1,100 systems were believed to have taken part in the attack.

While not likely to put a significant dent in the amount of DDoS traffic that floods the Internet, law enforcement officials continue to pursue those responsible for generating such traffic. In January, an Estonian man was fined the equivalent of a year's salary for his participation in DDoS attacks that targeted infrastructure within Estonia, knocking government Web sites, banks, and the local media off the Internet.[8] In February 2008, police in Quebec arrested 17 suspects that allegedly were participants in a 'hacker ring', each controlling approximately 5,000 computers that were used to generate Denial of Service attacks, send spam, and steal data.[9]

[4] http://asert.arbornetworks.com/2008/03/2-of-internet-traffic-raw-sewage/

[5] http://www.pcworld.com/article/id,141839-c,hackers/article.html

[6] http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080218

[7] http://www.theregister.co.uk/2008/03/19/dslreports_under_ddos_attack/

[8] http://www.securityfocus.com/news/11503

[9] http://www.nationalpost.com/news/story.html?id=322372

[10] http://www.msnbc.msn.com/id/22509653/

[11] http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=16&articleId=9055858&intsrc=hm_topic

[12] http://www.theregister.co.uk/2008/01/08/malicious_website_redirectors/

[13] http://www.darkreading.com/document.asp?doc_id=145665

[14] http://www.computerworld.com.au/index.php/id;257178610

Web Site Hacks

To no one's surprise, Web sites continued to be hacked in Q1 2008 – some hacking attempts targeted specific high-profile sites and may have caused minimal damage, while others wreaked havoc on thousands of sites by exploiting automated attack vectors. In addition to the hacking attempts reported on in the industry press, many more are never publicized – the hacking attempts described below are simply intended to be representative.

In January 2008, the Pennsylvania State Web site was targeted by hackers allegedly located in China.[10] According to State officials, the targeted Web pages were taken down for several hours as a precaution; they believe that no damage occurred and that no personal information was stolen.

Also in January 2008, tens of thousands of Web sites were targeted by an automated SQL injection attack – it is believed that up to 70,000 sites fell victim to the attack.[11] According to the Internet Storm Center (ISC), sites impacted by the attack included educational (.edu) and government (.gov) domains, as well as sites belonging to Fortune 500 companies.[12]

In February 2008, an Indian anti-virus firm was the target of a hack that exploited an iFrame vulnerability to install the Virut virus onto insufficiently patched Windows systems that visited the hacked pages.[13] Such exploits have come to be known as "drive-by" downloads, as a user's system can become infected by simply visiting a hacked Web page.

In March 2008, more than 10,000 Web pages on hundreds of Web sites were infected by hackers looking to steal passwords used in popular online games.[14] When an insufficiently-patched system visits one of these hacked pages, a JavaScript-based exploit installs a password-stealing program on the user's computer, which the hackers can then use to gain access to popular online games, where they can steal in-game resources to re-sell for cash.

Section 3: Networks

While network "events" such as outages, de-peering, and routing issues occur multiple times a day, every day, the first quarter of 2008 saw some rather significant events that were covered in both the industry and mainstream press. Errant ship anchors knocked an entire region of the globe offline in late January and early February, while a routing misconfiguration created a "black hole" for requests to one of the Web's most popular video-sharing sites in late February. In mid-March, a dispute between two leading backbone/transit providers impacted traffic exchange between the United States and countries in Northern Europe.

3.1 Outages

Perhaps the most noteworthy Internet outage in the first quarter of 2008 resulted from several undersea cables in the Mediterranean Sea being severed. Two cables were severed in late January, and two more went out of service in early February. These cable cuts significantly impacted Internet connectivity into and out of countries in the Middle East. The two cables account for the majority of international communications capacity between Europe and the Middle East, and the cuts reduced bandwidth between the region and Europe by 75%, according to TeleGeography.[15]

According to data collected by Renesys,[16] Egypt, Pakistan, Kuwait, and India had the most networks impacted by the cable cut. Data posted to the Renesys blog showed that over 1,000 customer networks in Egypt were impacted, with over 900 customer networks in Pakistan seeing problems; nearly 500 in India and almost 300 in Kuwait.

Data collected by Akamai's measurement systems showed the impact of these cable cuts on network latency in the region. A visualization available at http://www.akamai.com/mideast-outage shows the degradation in network latency between measurement points to 1.5x, 2x, and 3x or more beyond normal average latency. Data collected by in-region measurement agents showed that delivery of content for Akamai customers was not impacted by the cable cuts. Akamai's dynamic mapping system ensured that end-user requests were routed to available edge servers, which could deliver content from cache, and Akamai's optimized routing technology ensured that those Akamai servers chose the fastest, most available path when it was necessary for them to retrieve content from a customer's origin server. These technologies enable Akamai to provide superior availability for customer content in the face of Internet outages caused by man-made problems, or natural disasters, such as an earthquake.[17]

[15] http://www.telegeography.com/cu/article.php?article_id=21528

[16] http://www.renesys.com/blog/2008/01/mediterranean_cable_break.shtml

[17] http://www.akamai.com/html/about/press/releases/2007/press_013107.html

[18] http://www.datacenterknowledge.com/archives/2008/Apr/13/ships_impounded_in_middle_east_cable_cuts.html

[19] http://www.renesys.com/blog/2008/03/you_cant_get_there_from_here_1.shtml

[20] http://www.renesys.com/blog/2008/03/he_said_she_said_cogent_vs_tel.shtml

[21] http://blog.wired.com/27bstroke6/2008/03/isp-quarrel-par.html

[22] http://www.news.com/8301-10784_3-9878655-7.html

In April 2008, Reliance Globalcom used satellite imagery to identify two ships that were in the area of the original cable cuts, and that had improperly dropped anchor in the area.[18] The owners of one of the ships paid $60,000 in damages to compensate for repairs, while the second ship was impounded in Dubai.

3.2 De-Peering Events

On March 13, the network link between Cogent and Telia disappeared, from a routing perspective – the two network providers de-peered. As a result, customers of Cogent lost access to networks connected to Telia, and vice-versa. This effectively partitioned the Internet, as the alternate routes that Telia customers had been able to take to reach Cogent customers after the de-peering occurred were no longer available.[19,20] According to published reports,[21] the peering dispute was apparently sourced in capacity issues, where Cogent believed that Telia was not providing sufficient levels of capacity at some peering locations. In addition, the location of peering points is believed to have been an issue – specifically, the lack of peering points between the two networks in Europe. (This would result in packets having to cross the Atlantic Ocean twice if a Cogent user in Europe wanted to communicate with a Telia user in Europe.) Customers using Akamai to accelerate the delivery of their Web sites and Web & IP-based applications were unaffected by this de-peering – the sites and applications remained available to all Internet users.

On March 28, the link between Cogent and Telia was re-established, including new locations in London and Los Angeles, and traffic began flowing directly between the two networks once again.

3.3 Routing Issues

While routing issues occur regularly, few if any are as visible as the problem that YouTube experienced on February 24. In an effort to control access to YouTube for users within Pakistan, Pakistan Telecom began to filter requests bound for addresses in a subset of YouTube's address space. The intent of this filter was to prevent traffic from Pakistan Telecom users from reaching YouTube. However, a misconfiguration of the filter apparently caused Pakistan Telecom to announce a prefix owned by YouTube to Pakistan Telecom's upstream, PCCW. Because PCCW accepted this "hijacked" route, and because it was more specific than the route announced by YouTube, many other networks on the Internet sent their YouTube traffic to Pakistan Telecom. BGP-based routing on the Internet always prefers the most specific route, and the result of Pakistan Telecom's action was that within a few minutes, YouTube-bound traffic from networks around the world started flowing to the wrong place – Pakistan Telecom instead of YouTube.[22] A timeline published on the Renesys

Blog shows that within approximately two minutes, nearly 100 networks (autonomous systems) were carrying this hijacked route to YouTube, and Renesys estimates that it was seen by just over two-thirds of the Internet.[23]

YouTube quickly began to take countermeasures against this route hijacking, and PCCW began to filter the route announcement from Pakistan Telecom. Ultimately, just over two hours after the initial route broadcast by Pakistan Telecom, packets destined for YouTube's network were correctly sent to YouTube instead of Pakistan Telecom. During the period of time that the routes to YouTube were hijacked, traffic destined for YouTube's servers in the affected address block were sent to Pakistan Telecom and never reached YouTube, effectively black holing those requests.

Customers delivering Web site and media content through Akamai would not be impacted by such a route hijack, as Akamai does not rely on a single network address space. By locating content servers within nearly one thousand networks, the hijack of network address space from any one of them would not serve to completely remove Akamai customer sites from the World Wide Web – each network accounts for only a tiny percentage of customer traffic. Akamai's dynamic mapping system would detect problems in reaching Akamai servers within the network address space that had been hijacked, and would route end user requests for content to alternate Akamai edge servers.

3.4 Significant New Connectivity
New Internet connections are generally less than newsworthy, but two significant international Trans-Pacific cable projects were announced during the first quarter of 2008.

The "Trans-Pacific Express" United States. to China cable, announced in January 2008, is being built by a consortium comprised of Verizon Business, China Telecom, China Netcom, China Unicom, Korea Telecom and Chunghwa Telecom. The cable will initially provide capacity of up to 1.28 terabits per second, and is designed to eventually provide capacity of up to 5.12 Tbps.[24] In March 2008, AT&T and Japan's NTT announced that they would be joining the Trans-Pacific Express consortium. A United States to China route is expected to be operational by August 2008, and a Japan to China route by March 2009.[25]

In February 2008, a consortium of six companies announced a Japan to United States link that is slated to be completed in early 2010. Partners in the consortium include Google, Bharti Airtel, Global Transit, KDDI, Pacnet, and Singapore Telecommunications.[26]

[23] http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml

[24] http://www.chinatechnews.com/2008/01/15/6293-trans-pacific-express-approved-to-land-in-us/

[25] http://www.news.com/8301-10784_3-9902706-7.html

[26] http://www.news.com/8301-10784_3-9881578-7.html

4.1 Unique IP Addresses Seen By Akamai

Through our globally deployed server network, and by virtue of the billions of requests for Web content that we service on a daily basis, Akamai has a unique level of visibility into the levels of Internet penetration around the world. In the first quarter of 2008, over 329 million unique IP addresses connected to the Akamai network. Nearly 30% of those IP addresses came from the United States and just under 10% from China.

Country	Q1 08 Unique IP's	Q4 07 Change
- Global	329,059,516	+5.3%
1 United States	96,825,697	+5.5%
2 China	32,443,941	+7.6%
3 Japan	24,766,285	+2.1%
4 Germany	22,667,701	+13%
5 France	16,431,925	+3.3%
6 United Kingdom	15,889,511	+6.4%
7 South Korea	13,547,675	+2.6%
8 Canada	9,873,214	+4.2%
9 Spain	8,171,924	+4.0%
10 Italy	6,629,277	+7.1%

Looking at the "long tail", there were over 200 countries with under 1 million unique IP addresses connecting to Akamai in the first quarter of 2008, over 160 with under 100,000 unique IP addresses, and over 50 with under 1,000 unique IP addresses.

4.2 Internet Penetration

How does the number of unique IP addresses seen by Akamai compare to the population of each of those countries? Asked another way, what is the level of Internet penetration in each of those countries? Using 2008 global population data from the United States Census Web site[27] as a baseline, levels of Internet penetration for each country around the world were calculated. These levels were lower than expected, with no country exceeding 0.40 unique IP addresses seen per capita in the first quarter of 2008.

Country	Unique IP's Per Capita
- Global	0.05
1 Sweden	0.40
2 Norway	0.37
3 Iceland	0.37
4 Finland	0.35
5 Netherlands	0.35
6 Cayman Islands	0.34
7 Denmark	0.32
8 United States	0.32
9 British Virgin Islands	0.30
10 Canada	0.30

Section 5: Geography

These per capita figures should be considered as an approximation, as the population figures used to calculate them are static yearly estimates – obviously, they will change over time, and it would be nearly impossible to obtain exact numbers on a quarterly basis. In addition, individual users can have multiple IP addresses (handheld, personal/home system, business laptop, etc.). Furthermore, in some cases, many individuals are represented by a single IP address (or small number of IP addresses), as they access the World Wide Web through a proxy server. Akamai believes that we see approximately 1 billion users per day, though we see only see approximately 300 million unique IP addresses.
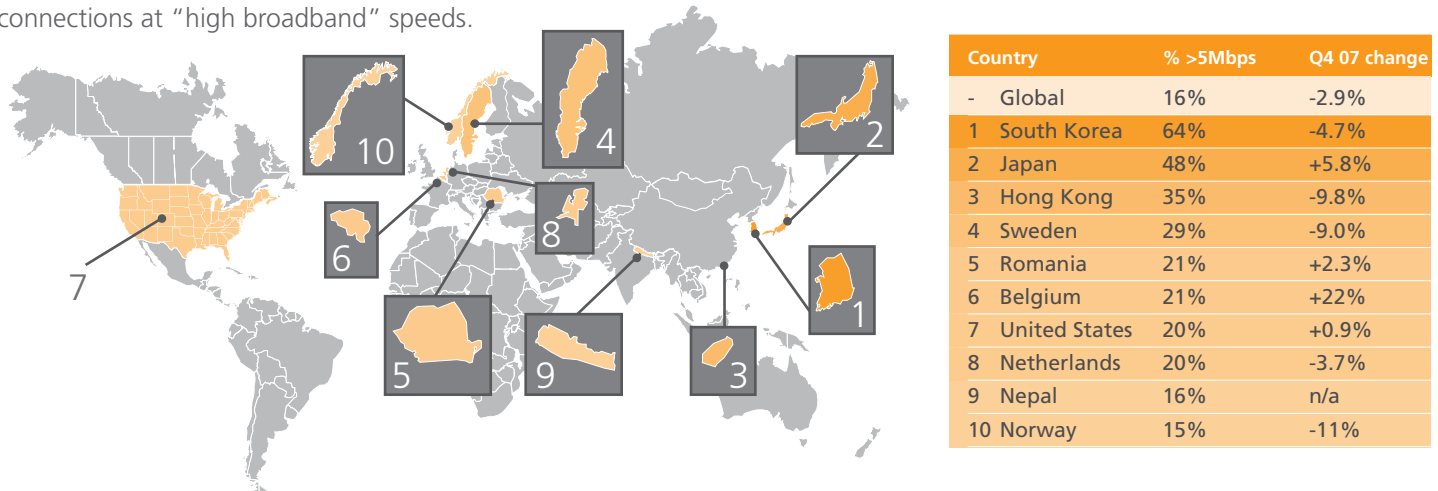
Through our globally deployed server network and by virtue of the billions of requests for Web content that we service on a daily basis, Akamai has a unique level of visibility into the connection speeds of those systems issuing the requests, and as such, of broadband adoption around the globe. Because Akamai has implemented a "distributed" network model, deploying servers within "edge" networks, we 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[28].

The data presented at right was collected during the first quarter of 2008, 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 first quarter. Updates to this report to be published for subsequent quarters will document trends in the growth of high-speed connectivity, both globally and in the United States, as observed by Akamai. For the purposes of classification in this report, the "broadband" data included below is for connections greater than 2 Mbps, and "high broadband" is for connections 5 Mbps or greater. In contrast, the "narrowband" data included below is for connections slower than 256 Kbps. Note that the percentage changes reflected below are not additive - they are relative to the fourth quarter 2007. (That is, a Q4 value of 50%, and a Q1 value of 51%,would be reflected here as a +2% change.)

As the quantity of HD-quality media increases over time, and the consumption of that media increases, end users will require ever-increasing amounts of bandwidth. A connection speed of 2 Mbps is arguably sufficient for standard-definition TV-quality video content, and 5 Mpbs 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.[29]

[28] http://www.akamai.com/dl/whitepapers/How_will_the_internet_scale.pdf
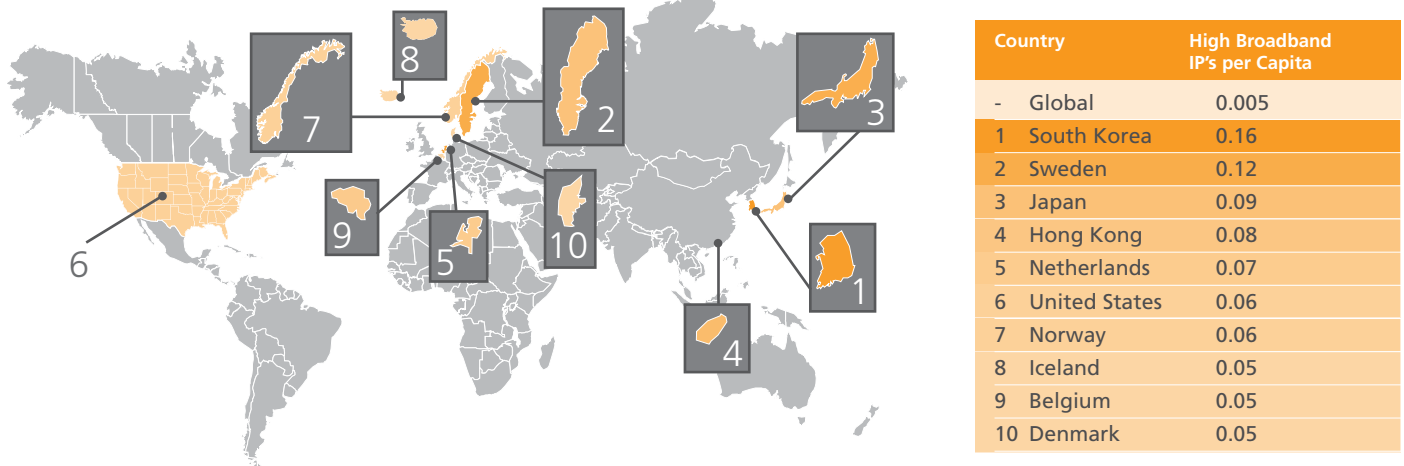
[29] http://www.blu-ray.com/faq

5.1 High Broadband Connectivity: Fastest International Countries

It comes as no surprise that South Korea tops the list of countries with the greatest levels of high broadband (>5 Mbps) connectivity, as it is widely regarded as one of the best-connected countries in the world, with average home broadband speeds in the tens of Mbps. With nearly 64% of connections to Akamai occurring at over 5 Mbps, they are far ahead of the second-most well connected country, which is Japan, with 48% of connections at "high broadband" speeds. The percentages drop off rapidly, and the United States comes in 7th, with just over 20% of the connections at "high broadband" speeds.

	Country	% >5Mbps	Q4 07 change
-	Global	16%	-2.9%
1	South Korea	64%	-4.7%
2	Japan	48%	+5.8%
3	Hong Kong	35%	-9.8%
4	Sweden	29%	-9.0%
5	Romania	21%	+2.3%
6	Belgium	21%	+22%
7	United States	20%	+0.9%
8	Netherlands	20%	-3.7%
9	Nepal	16%	n/a
10	Norway	15%	-11%

The quarter-to-quarter changes varied across countries in the top 10, with Belgium showing the greatest increase, and Norway showing the greatest decline. The United States showed a slight gain quarter-over-quarter, likely as a result of increased adoption of fiber-to-the-home services.

From an Internet Penetration perspective (unique IPs per capita), a number of the same countries can also be found in the High Broadband Top 10, as would be expected.

|	Country	High Broadband IP's per Capita
-	Global	0.005
1	South Korea	0.16
2	Sweden	0.12
3	Japan	0.09
4	Hong Kong	0.08
5	Netherlands	0.07
6	United States	0.06
7	Norway	0.06
8	Iceland	0.05
9	Belgium	0.05
10	Denmark	0.05

South Korea, Sweden, Japan, and Hong Kong once again round out the four top slots. However, such high-speed connections appear to be the exception, rather than the rule, as Akamai's data shows that over 200 countries have less than 1% penetration (0.01 IPs per capita) of high broadband connectivity.

5.2 High Broadband Connectivity: Fastest U.S. States

In the United States, the East Coast was very well represented in the Top 10 list of US states with the greatest levels of High Broadband (>5 Mbps) connectivity, taking eight out of the top 10 slots. Delaware holds a commanding lead, with 60% of connections from the state connecting to the Akamai network at speeds over 5 Mbps. Rhode Island comes in second, with 42% of the connections from that state occurring at speeds over 5 Mbps. Given the relative size and population density of both states, as well as their proximity to major East Coast cities, it is not entirely surprising that they show such high levels of broadband connectivity.
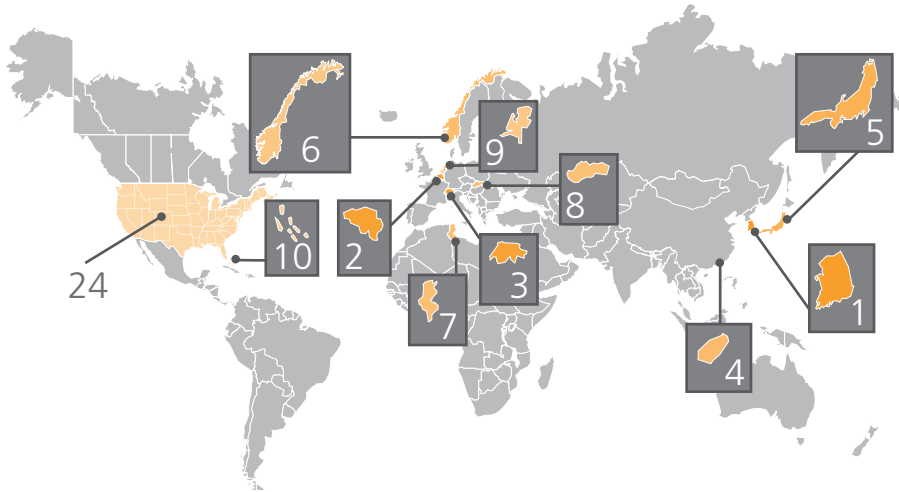
	State	% >5 Mbps	Q4 07 Change
1	Delaware	60%	+2.1%
2	Rhode Island	42%	-5.5%
3	New York	36%	-1.6%
4	Nevada	34%	-1.1%
5	Oklahoma	33%	+1.5%
6	Connecticut	32%	-3.9%
7	New Hampshire	30%	-0.6%
8	Massachusetts	29%	-5.4%
9	Maryland	27%	-6.5%
10	Dist. Of Columbia	27%	-3.2%
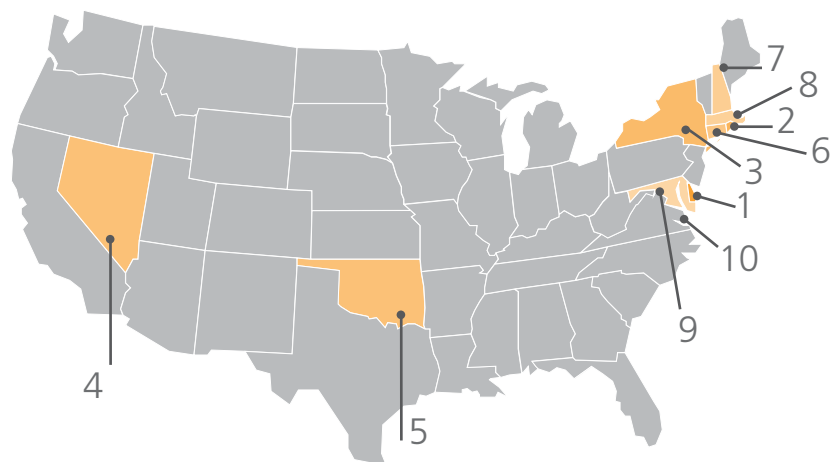
The quarter-to-quarter changes were fairly varied, with some states seeing nominal increases from the prior quarter, while others saw some significant decreases. Seven states had less than 10% of their connections to Akamai occur at speeds greater than 5 Mbps, with Hawaii at the bottom of the list, with 2.4%

## 5.3 Broadband Connectivity: Fast International Countries

Internationally, the percentage of connections to Akamai at bandwidth speeds exceeding 2 Mbps is significantly more clustered than the "high broadband" data, with just under 20% separating #1 South Korea (93%) and #10 Bahamas (74%). The United States comes in #24 on the list, with 62% of connections to the Akamai network occurring at speeds in excess of 2 Mbps. Half (five) of the countries in the Broadband Top 10 also appear in the High Broadband Top 10 for the first quarter of 2008, including South Korea, Belgium, Hong Kong, Norway, and the Netherlands.

Country	% >2Mbps	Q4 07 Change
- Global	55%	-2.0%
1 South Korea	93%	-1.5%
2 Belgium	90%	+1.5%
3 Switzerland	89%	+0.5%
4 Hong Kong	87%	-1.5%
5 Japan	87%	+1.0%
6 Norway	83%	-2.3%
7 Tunisia	82%	+29%
8 Slovakia	81%	+0.5%
9 Netherlands	78%	-2.6%
10 Bahamas	74%	-3.0%
... ...	...	...
24 United States	62%	-2.8%

The quarter-to-quarter changes again varied across countries in the Top 10, with Tunisia showing the greatest increase, with others showing nominal increases or declines. (The cause for Tunisia's significant increase is unknown, though the number of unique IPs from Tunisia connecting to Akamai increased 50% quarter-over-quarter.) The United States also showed a nominal decline quarter-to-quarter.

From an Internet Penetration perspective (unique IPs vs. population), Europe is very well represented, capturing all of the top 10 spots for broadband penetration.
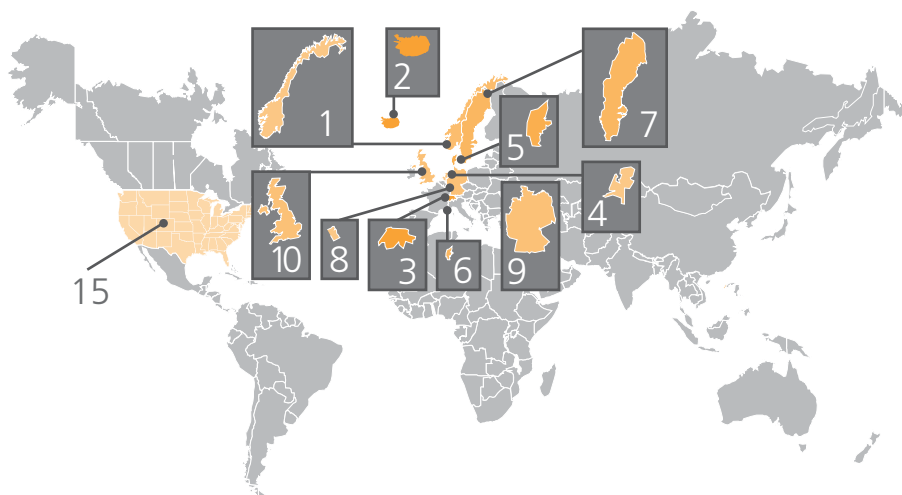
| Country	Broadband IP's per Capita
- Global	0.01
1 Norway	0.25
2 Iceland	0.21
3 Netherlands	0.20
4 Switzerland	0.19
5 Denmark	0.19
6 Monaco	0.18
7 Sweden	0.18
8 Luxembourg	0.17
9 Germany	0.17
10 United Kingdom	0.17
... ...	...
15 United States	0.13

The United States fared reasonably well, coming in 15th, and all of the top 20 countries showed broadband penetration in excess of 10% (0.10 IPs per capita).

5.4 Broadband Connectivity: Fast U.S. States

Similar to the High Broadband Top 10 list, Delaware leads the pack, again significantly ahead of #2 Rhode Island. Seven of the states in the Broadband Top 10 also appear in the High Broadband Top 10 for the first quarter of 2008, including Delaware, Rhode Island, Nevada, Connecticut, New York, Oklahoma, and New Hampshire.

|	State	%>2 Mbps	Q4 07 Change
1	Delaware	96%	+0.1%
2	Rhode Island	85%	+0.6%
3	Nevada	84%	-0.9%
4	Connecticut	80%	-2.6%
5	New York	78%	+1.8%
6	Oklahoma	78%	-1.6%
7	Michigan	75%	-3.8%
8	Tennessee	75%	+0.2%
9	New Hampshire	74%	+2.0%
10	South Carolina	73%	+1.1%
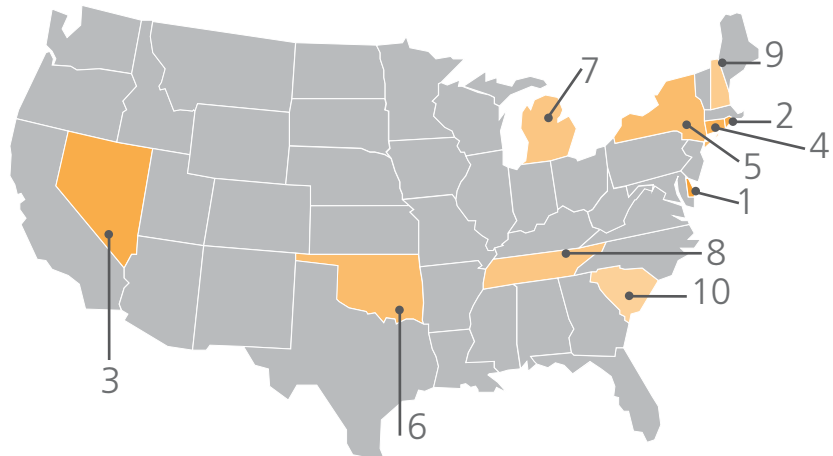
In terms of quarter-over-quarter changes, gainers outnumbered losers, as six states saw their broadband connectivity percentage increase, while the other four saw their percentages decline. New York saw the largest increase, at 1.8%, and Michigan saw the greatest decrease, losing 3.8%.

5.5 Narrowband Connectivity: Slowest International Countries

While broadband adoption races ahead around the world, many countries are stuck in the slow lane, with the vast majority of their connections occurring at speeds below 256 Kbps. (And presumably, for the most remote countries, at speeds significantly below that.)

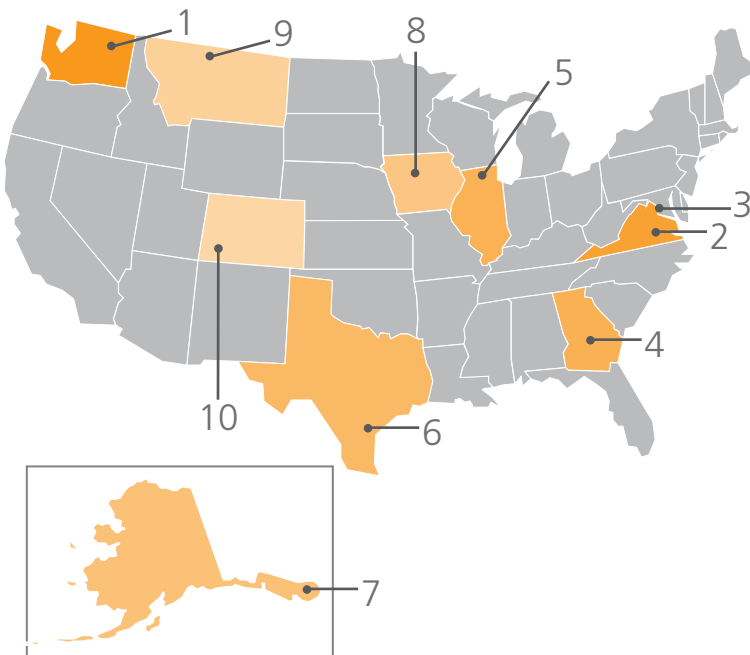|	Country	% <256 Kbps	Q4 07 Change
-	Global	7.9%	-8.1%
1	Rwanda	97%	-0.7%
2	Solomon Islands	95%	-0.7%
3	Ethiopia	94%	-1.0%
4	Cuba	94%	+1.0%
5	Uganda	92%	-0.2%
6	New Caledonia	91%	-1.3%
7	Malawi	90%	-2.6%
8	Bhutan	90%	-4.3%
9	Zambia	89%	+0.4%
10	Seychelles	88%	+9.5%
...	...	...	...
104	United States	7.8%	+3.8%
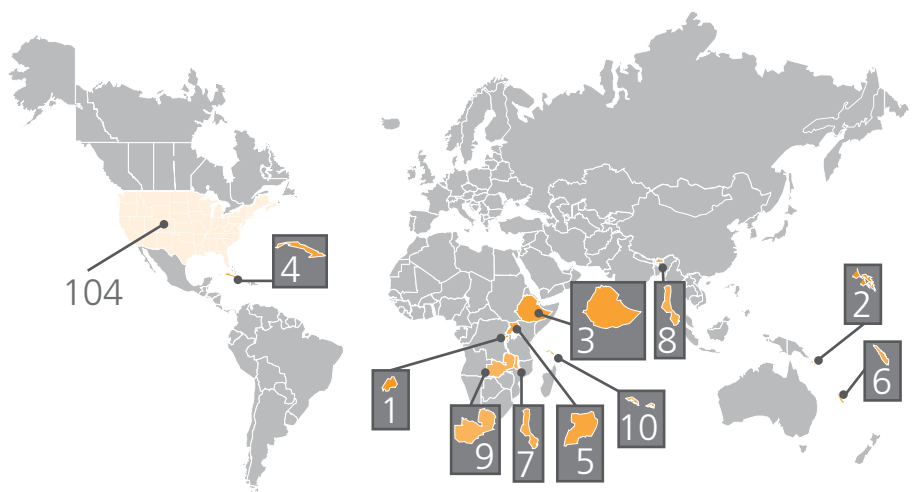
The data presented in the table below shows that many of the countries with the highest percentage of connections to Akamai occurring at below 256 Kbps are smaller, more remote Pacific islands, or on the African continent. Rwanda had the highest percentage of narrowband connections, with nearly 97% of connections at speeds under 256 Kbps. The narrowband connectivity percentages are also fairly clustered, with only 10% separating #1 and #10 (Seychelles). The United States comes in significantly lower on this list (as would be expected), at #104, with only 7.8% of connections at narrowband speeds.

The quarter-to-quarter changes were not as widely varied as we saw with broadband and high broadband connectivity. Seven of the top 10 saw narrowband connectivity percentages decrease, even if just slightly, while Seychelles saw the greatest increase.

5.6 Narrowband Connectivity: Slowest U.S. States

Washington State and Virginia top the list of US states with the largest percentage of connections observed at 256 Kbps or below. However, in contrast to the International list, only 21% of Washington's connections are "slow". The connection percentage quickly drops below 20%, as Virginia has the next largest percentage of narrowband connections, with 18%.

State	% <256 Kbps	Q4 07 Change
1 Washington	21%	+151%
2 Virginia	18%	-0.4%
3 District Of Columbia	17%	+4.5%
4 Georgia	15%	+9.2%
5 Illinois	15%	+9.5%
6 Texas	13%	+6.3%
7 Alaska	11%	-8.9%
8 Iowa	10%	-2.9%
9 Montana	8.6%	-6.3%
10 Colorado	8.2%	-4.1%

While most states in this top 10 list showed nominal increases or decreases in connection percentages, Washington State showed a significant increase in the percentage of connections to Akamai's network at narrowband speeds. It is not clear what the underlying reason was for the increase.

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

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

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

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

www.akamai.com