



BANDWIDTH BANDITS

**INTERNET BANDWIDTH IS A FINITE AND EXPENSIVE RESOURCE;
PROTECT IT FROM SPAMMERS, CRIMINALS, HACKERS, TIME-WASTERS
AND EMPLOYEE MISUSE.**

A SYMANTEC HOSTED SERVICES WHITEPAPER

INTRODUCTION: BANDWIDTH BANDITS

Internet bandwidth is a finite and expensive resource; protect it from spammers, criminals, hackers, time-wasters and employee misuse.

Your company's internet link is precious. Not only is it expensive and limited but it is a vital business tool. Yet our analysis shows that companies can lose around a quarter of their internet bandwidth to employee web misuse, streaming media and spam. Imagine if you had to give up a quarter of your office space for non-work activities; it's inconceivable. But when it comes to internet bandwidth, most companies don't even know about the loss, let alone take steps to prevent it.

The problem is about to get a lot worse. With the World Cup and Olympics coming up, employees will want to watch real-time TV feeds from their desks. This may trigger internet brown-outs in companies that are unprepared.

Part of the problem is that the internet is designed to continue operating even if links are busy or damaged; indeed that's the whole point of it. This means that you probably don't notice if your emails take longer to deliver, web pages take longer to load and internet phone and video conferences are lower quality. It all sort of works and you expect the occasional hiccup.

That doesn't mean that bandwidth loss is irrelevant. In fact, there are serious consequences:

- You buy more expensive connectivity than you need
- Business-critical internet connections, such as remote users' VPN (virtual private network) connections or business-related web use, are slower than they should be, wasting people's time
- In some circumstances, such as spam spikes or when everyone in the office is watching the same World Cup match, you may experience service outages or serious delays
- Internet communications such as desktop video conferencing, VOIP (voice over IP or internet telephony) have lower quality
- As internet-delivered applications and services become more widespread, important business functions such as customer relationship management will depend on a fast, high-quality internet connection

BITS, BYTES AND MEGABYTES

Employees are used to having fast internet connections at home and have come to expect that they can chat with their friends, browse photos, listen to music and watch TV over the internet. So when they come to work, they do the same there. If you have a hundred employees, the majority of them will have their own fast broadband connections at home. In the office, all of them have to share just one connection. So expectations are going up and the available bandwidth stays the same.

To make matters worse, the size of files and streams delivered over the internet has increased. When the internet first took off in the early 90s, most web pages were text-only. Today, it's perfectly normal to stream high-definition video over the internet. But a minute of HD video uses up massively more bandwidth than a page of text.

To understand the difference, consider that a King James Bible takes just 1.34 megabytes in text format¹. If it were scanned in as a series of 1,200 black and white pictures², it would require 58 megabytes³ – a huge increase. An unabridged voice recording of the same book runs to over 79 hours⁴. In MP3 format, this would require 4.3 gigabytes⁵ – yet another huge increase. This is about the same as a single DVD's worth⁶ of video information – say, for example, Monty Python's Life of Brian. In other words, each step from text to pictures to audio to video requires a huge increase in bandwidth.

¹King James Bible text: <http://www.gutenberg.org/etext/10>

²The Bible on my shelf is about 1,300 pages

³TIFF B&W file size at 300 DPI = 50 kB. See: http://en.wikipedia.org/wiki/Tagged_Image_File_Format

⁴Unabridged Bible recording 79 hours and 42 minutes: http://www.audible.co.uk/aduk/site/product.jsp?BV_SessionID=@@@@2120171133.1268672006@@@@&BV_EngineID=ccccadejldkglcefecekjdfkdfg.0&source_code=OGCS0001SH122309UK&p=BK_JODA_000001UK&source_code=OGCS0001SH122309UK

⁵Typical MP3 recorded at 128 kilobits per second

⁶<http://en.wikipedia.org/wiki/DVD>

WHO ATE ALL THE BANDWIDTH?

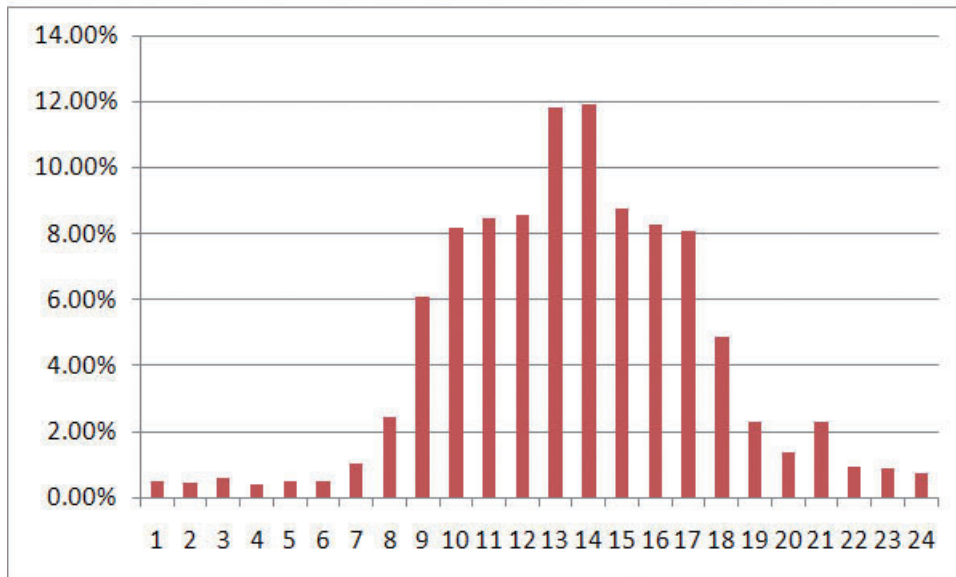
The MessageLabs Intelligence team sees billions of web and email connections every day⁷. As the market leader for hosted email and web security, they have a unique insight into the real state of the internet as a whole. In particular, they can see exactly what people do online.

The top ten most-blocked website categories are:

RANK	CATEGORY	% OF BLOCKS
1	Advertisements & popups	59.5%
2	Streaming media	12.5%
3	Games	8.6%
4	Chat	3.4%
5	Downloads	2.7%
6	Personal & dating	1.9%
7	Blogs & forums	1.8%
8	Adult/sexually explicit	1.4%
9	Photo searches	0.8%
10	Computing & internet	0.7%

The majority of these blocked sites use lots of bandwidth. For example, video and audio streams, photo searches, games and adverts all use lots of multimedia content which uses much more bandwidth than plain text or emails. Streaming media is the worst culprit because video and audio need the most bandwidth. That 12.5 percent represents a very large drain on companies' internet connectivity.

The majority (87 percent) of non-work internet usage occurs between 8am and 6pm. The busiest time is over lunch but personal internet use is pretty constant during working hours.



Websites blocked by MessageLabs services over a 24-hour period

⁷http://www.messagelabs.com/technology/data_centers.aspx

When it comes to bandwidth-intensive streaming media, the story is very similar; except that streaming media is more popular in the afternoon than the morning and there is another mini-peak around 5pm when people are getting ready to go home.

These peaks – at lunchtime and at 5pm – could affect a US business with interests in the US because the times coincide with the start of the business day on the East Coast and West Coast respectively.

SPAM SPIKES AND BLOWBACK

Streaming media and web browsing represent a constant drain on your bandwidth but email poses a different kind of risk. It is less bandwidth-intensive because individual emails are relatively small in size. However, the sheer volume of spam and the constant stream of unwanted messages represent a constant drain.

It is completely possible, on a bad day, for a company with a hundred employees to receive 1,000 legitimate emails and 200,000 spam messages. Around 90 percent of all emails processed by MessageLabs services are spam messages⁸.

The problem is made worse by spammers' use of random name generation to send emails to people at a given address even if they don't work there. For example, you might be joe@bloggs.com but spammers are also sending email to brian@, jane@, phil@ and uncle-tom-cobbley@bloggs.com too. It costs them nothing to send these messages because they use malware to turn thousands of unprotected PCs into spam factories.

Spam spikes and bounceback (also known as blowback or backscatter) spam can cause huge, short-term bandwidth problems. Spikes occur when spammers try new tactics, new botnets come online or when spammers use attachments in their spam messages. Spikes can produce a 25-fold increase in spam in a short period. Bounceback spam occurs when spammers use your email address as the 'reply-to' address in their messages. You end up dealing with all the 'message not delivered' and 'out of office' responses from recipients. This can produce another temporary burst in traffic and some companies see more than half of their spam load resulting from bounceback⁹.

Dealing with spam is a burden on companies with in-house spam filtering software. Every message has to be downloaded, whether it is wanted or not. It must then be processed to check if it is spam or if it contains malware. With nine spams for every real message, the result is that many companies have email systems that are ten times more capable (and expensive) than they actually need to be to process legitimate emails. When a spam tsunami hits, everything slows down. As a result, expensive bandwidth is wasted and legitimate business emails must wait their turn for processing, causing unnecessary delays.

A new trend, tracked by analysts in MessageLabs Intelligence, is that spammers are increasingly using the TLS protocol to send spam messages. TLS is an encryption system that ensures that messages sent from one mail server to another cannot be read by third parties. It's like putting post cards in envelopes. Spammers are using this protocol because it increases the chances of spam messages getting through defences, but it is also a bandwidth problem because each email now requires an extra two-way exchange of information to set up the encrypted link.

Rustock, one of the largest spamming botnets, sends 70 percent of its spam using TLS. Because Rustock spam accounts for a large proportion of global spam, this means that overall 20 percent of global spam is sent using TLS. This could increase rapidly if other botnets decide to follow Rustock's lead. If this trend becomes widespread, it could significantly increase the bandwidth drain caused by spam.

PROTECTING ROAMING USERS

Roaming and home-based workers present another bandwidth challenge. Mobile users typically have a slow wireless broadband connection via the mobile phone network. These links have a fraction of the capacity of landline connections. They can also be very expensive, with monthly costs per user running up to \$186.34¹⁰ and significant penalties for exceeding download limits.

Similarly, home workers with consumer broadband connections have limited bandwidth but may need most of it simply to maintain a VPN, VOIP or remote desktop link back to the company. If they start browsing the internet intensively or streaming video over a company-provided internet connection, it could affect their ability to do their job by slowing down their office links.

Both limitations – on mobile and home workers – mean that companies need to pay more attention to what they allow their employees to do online.

CALCULATING THE COST

What is the cost of all this waste? Taking a typical small to medium-sized firm as an example, with a leased line internet connection and around 100 employees, web misuse and email spam could waste around 23 percent of their internet bandwidth and cost thousands of dollars a year. Of course, your mileage may differ but our calculations and the research behind them may be a good starting point for estimating your own costs.

Let's take the direct costs first; that is the immediate cost of the bandwidth. A company might have a one megabit/second leased line that costs \$645.00 a month¹¹ that provides a maximum capacity of 10,800 megabytes per day. With a hundred employees spending, on average, an hour a day browsing the web at 40 pages an hour¹² and an average page weight of 312 kilobytes¹³, that would account for 1,218 megabytes a day or approximately 10 percent of the available bandwidth.

MessageLabs Intelligence reveals that 12.5 percent of all blocked websites are multimedia streaming sites, so let's assume that they spend 12.5 percent of that hour a day (i.e. 7.5 minutes) online browsing video sites. One hour of low-resolution internet video is 128 megabytes of data¹⁴ so 7.5 minutes requires 16 megabytes per employee per day – another 1,280 megabytes or 10 percent of the available bandwidth.

However, if they decide to leave a window open to watch a football match or listen to music while they work, the amount of downloaded data could increase dramatically. Also, higher-resolution or HD video requires significantly more bandwidth than standard resolution.

Email is a smaller burden, providing there are no spikes. If you assume 1,000 spam messages a day per employee at five kilobytes per message¹⁵, that equates to 488 megabytes a day. However, if the majority of those spam messages arrive in the course of an hour, it could squeeze out legitimate traffic and overwhelm email servers.

All told, even with relatively modest levels of personal web use and plausible levels of spam, your company could be wasting 2,985 megabytes a day or 27 percent of its download bandwidth. That costs the company \$2,090 a year.

¹⁰Typical data plans on Vodafone run from \$17.20 - \$186.34 per month depending on the cap: <http://online.vodafone.co.uk/business/s/price-plans/mobilebroadband>

The easiest way to do these calculations is to use Google calculator. For example, simply enter '7.5 minutes x 128 megabytes an hour' or '24 hours x 1 megabit per second' into the search box and press enter. Wikipedia has more information about the bandwidth required for different types of media: http://en.wikipedia.org/wiki/Bit_rate.

Beyond the raw cost of the connection, wasted bandwidth has a tremendous opportunity cost. It squeezes capacity for legitimate traffic, slowing down business web use and email. Dealing with spam in-house requires expensive servers and software. Employee time wasting has a real cost in terms of salary and missed opportunities. Even the disruption caused by one person watching a football game and disturbing his colleagues has a cost.

¹¹<http://www.zen.co.uk/LeasedLines/Products/ethernet.aspx>

¹²Typical time per page: <http://www.useit.com/alertbox/percent-text-read.html>

¹³Top 1000 websites home pages: <http://www.websiteoptimization.com/speed/tweak/average-top-100-weblog/>

¹⁴http://en.wikipedia.org/wiki/Streaming_media

¹⁵MessageLabs Intelligence estimate of average email size in Jan and Feb 2010

RECLAIM YOUR BANDWIDTH

There are several measures you can take to reclaim your bandwidth:

	WHY DO IT?	HOW SYMANTEC HOSTED SERVICES CAN HELP
Analyze your own usage	Use existing tools to get some insight into how your existing bandwidth is being used. For example, some firewalls have the ability to report on the types of traffic passing through them, and anti-spam software or services can give you an idea of the volume of spam reaching your systems.	The MessageLabs Security SafeGuard dashboard provides flexible reports via a web browser that include web usage volumes, percentage of web requests blocked by AntiVirus, AntiSpyware and URL Filtering services, the top sites. You can also get information about bandwidth used and time spent on websites by individuals.
Quality of service	Some firewalls and routers allow you to give priority to certain types of traffic. For example, you can give a higher priority to email traffic than web or make sure that VPN and VOIP traffic has the highest priority. This won't reduce the wastage but it will help reduce the impact.	You can use MessageLabs Security SafeGuard to restrict access to non-essential sites, freeing up bandwidth for business critical services. For example, you can restrict access to media streaming sites outside lunchtime.
Stop spam in the cloud	If you can stop unwanted email before it starts its journey through your internet connection to your servers, you free up all the bandwidth it uses and you don't need so much server capacity to process it. Cloud-based security and spam filtering services also block emails sent to non-existent addresses at your domain, further cutting the amount of spurious traffic you get.	MessageLabs Security SafeGuard blocks 99 percent of spam before it ever reaches your network or your internet connection. With a false positive rate of 0.0003% and an easy-to-use quarantine system, you can be sure to get all the emails you do want and avoid nearly all the ones you don't.
Block inappropriate web use	Supported by acceptable use policies, employee awareness, training and enforcement, website filtering and blocking can be very effective at ensuring that business traffic gets through and non-essential usage is kept to a minimum.	MessageLabs Security SafeGuard gives you control over who can access what online. You can set policies for the whole company, departments, types of employee or even on an individual basis. You can differentiate between websites that are absolutely off-limits, such as porn sites, and sites that you want to control but not ban altogether. For this reason, MessageLabs Security SafeGuard lets you set time limits on people's use of non-work websites.
Control remote users	Mobile and home workers have very limited and expensive bandwidth. If you can control the sites and services they use, you can keep costs down and ensure that their bandwidth is available for work purposes, such as internet phone systems and VPN connections to the office.	MessageLabs Security SafeGuard extends web protection and filtering to remote users, including policy enforcement. It also ensures that remote users' online activities are tracked by the service's reporting tools.

MESSAGELABS SECURITY SAFEGUARD

Every week, MessageLabs Security SafeGuard blocks millions of malicious, inappropriate or non-approved website requests for thousands of companies and billions of dangerous and unwanted emails. Whether it is email, websites or instant messaging, MessageLabs Security Safeguard will protect companies from more than malware and spam; it will help enforce acceptable use of IT systems to protect productivity, competitiveness and profitability.

To understand more about MessageLabs Security Safeguard, visit our website or request a free trial at www.messagelabs.com

ABOUT SYMANTEC HOSTED SERVICES

Symantec Hosted Services is a leading provider of hosted messaging and web security services, with over 30,000 clients ranging from small businesses to the Fortune 500, located in 102 countries. Symantec Hosted Services protects, controls, encrypts and archives communications across email, web and instant messaging. These services are delivered by a globally distributed infrastructure and supported 24/7 by our security experts. This gives a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information. For more information or to request a free trial of our services, visit www.messagelabs.com.

>EUROPE

>HEADQUARTERS

1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733
Support: +44 (0) 1452 627 766

>LONDON

3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

>NETHERLANDS

WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801
Support +44 (0) 1452 627 766

>BELGIUM/LUXEMBOURG

Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

>DACH

Humboldtstrasse 6
Gewerbegebiet Dornach
85609 Aschheim
Deutschland
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

>AMERICAS

>UNITED STATES

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

>CANADA

170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

>ASIA PACIFIC

>HONG KONG

Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

>AUSTRALIA

Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

>SINGAPORE

6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

>JAPAN

Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130



Confidence in a connected world.