The Application Usage and Risk Report

End User Application Trends in the Enterprise - Country Specific Findings

7th Edition, May 2011

Palo Alto Networks
3300 Olcott Street
Santa Clara, CA 95054
www.paloaltonetworks.com

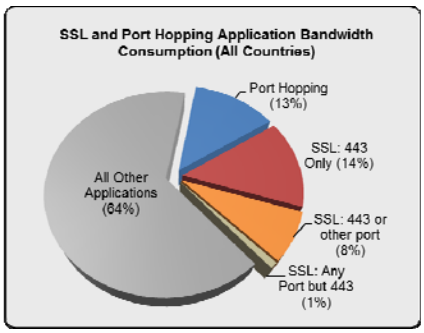
Table of Contents

Executive Summary

The *Application Usage and Risk Report (7th Edition, May 2011)* from Palo Alto Networks provides a global view into enterprise application usage by summarizing 1,253 application traffic assessments conducted between October 2010 and April 2011. The key findings and observations both globally and by specific countries are outlined below. To view additional details around the global findings, please download the *Application Usage and Risk Report (7th Edition, May 2011)* here.

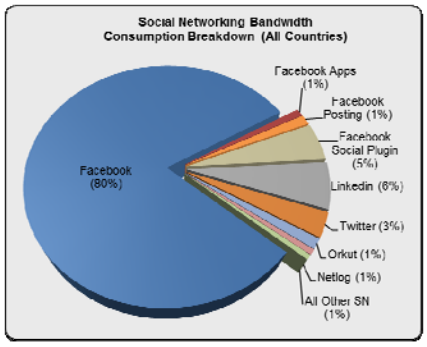
Global findings:

Hidden application traffic: more than 40% of the applications found can use SSL or hop ports; consuming roughly 36% of the overall bandwidth observed.



- Applications using SSL in some way, shape or form represent 25% (262) of the applications found and 23% of the overall bandwidth used. This segment of applications will continue to grow as more applications follow Twitter, Facebook and Gmail, who all have enabled SSL either as a standard setting or as a user-selectable option.
- Applications that can hop ports represent 16% (171) of the applications found and 13% of the bandwidth consumed. In general, the types of applications that hop ports are consumer oriented and include instant messaging, P2P, and photo video. There is no reason to expect the use of port-hopping as an accessibility feature by application developers to decrease.

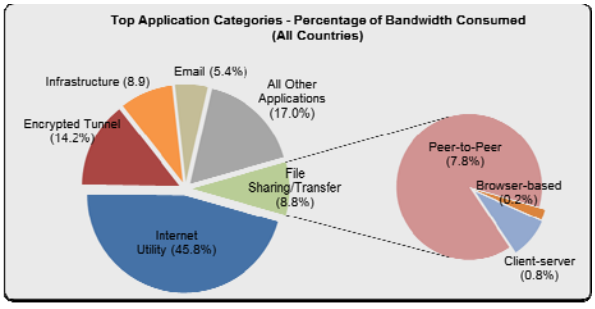
The work place has become more social.



- Contrary to popular opinion, social networking has not meant the death of instant messaging (IM) and webmail. Compared with 12 months ago, IM traffic, as a percentage of overall traffic has more than doubled; webmail and social networking increased nearly 5 fold.

File transfer applications: will history repeat itself?

- The progression from FTP, to P2P, to browser-based file sharing all show strikingly similar risk and reward characteristics. These applications, found with 92%, 82%, and 91% frequency respectively, each provide business value, but represent security and business risks that may include exploits, malware vectors, and data loss (intentional or otherwise).
- As browser-based filesharing applications leverage peer-based technology and add clients as a "premium offering", the question arises: will the business and security risks introduced by browser-based filesharing follow the same path as those that were introduced by P2P.



Country Specific Findings – Europe

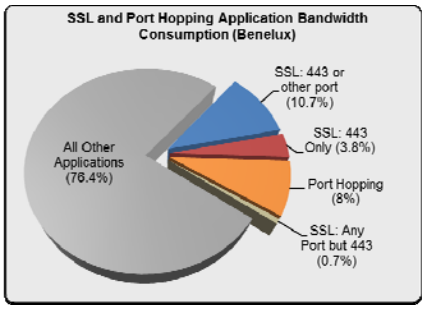
Benelux (Belgium, Luxembourg, Netherlands)

The Benelux sample encompassed 64 organizations with 664 applications detected that consumed 124 terabytes of bandwidth.

Key Benelux findings:

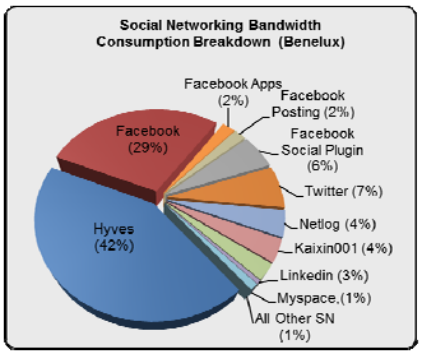
Hidden application traffic: 42% of the applications found can use SSL or hop ports; consuming roughly 24% of the overall bandwidth observed.

- SSL: 182 applications can use SSL in some way, shape or form. Compared with the global view, the bandwidth consumed by applications using SSL on port 443 is significantly lower by approximately 66% (3.8% vs. 14%). The remaining SSL segments, on average, are consuming bandwidth at roughly the same rate.
- Port-hopping applications: 96 applications that can hop ports are consuming 8% of the overall bandwidth observed, an amount that is slightly lower than the 13% consumed globally.



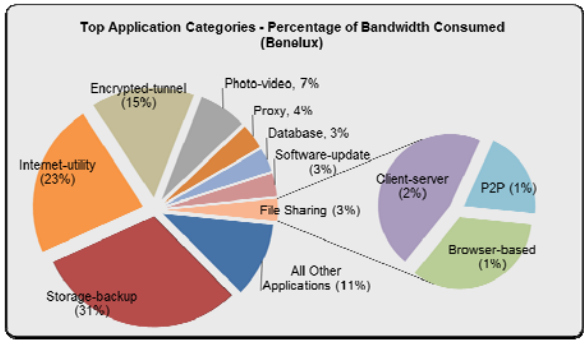
The work place has become more social.

- Benelux socializing traffic patterns showed that webmail and social networking consumed 4X and 9X more bandwidth than IM.
- Relative to social networking, Benelux was one of the few countries where local applications (Hyves) was used more heavily, based on bandwidth, than Facebook.



File transfer applications: will history repeat itself?

- The progression from FTP, to P2P, to browser-based file sharing all show strikingly similar risk and reward characteristics. These applications, found in Benelux with 92%, 67%, and 92% frequency respectively, each provide business value, but represent security and business risks that may include exploits, malware vectors, and data loss (intentional or otherwise).
- In Benelux, filesharing in general represented a smaller amount of bandwidth (3%) when compared to global view. Within that 3%, client-server file transfer (FTP, etc) was used most heavily, indicating a stronger propensity for work-related use.



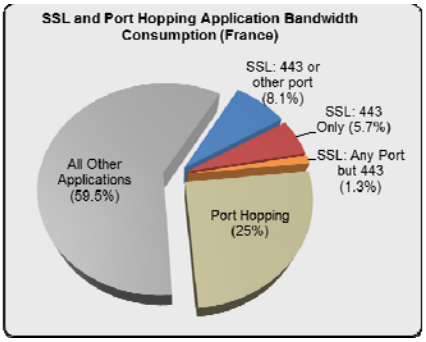
France

The French sample encompassed 79 organizations with 686 applications detected that consumed 88 terabytes of bandwidth.

Key findings in France:

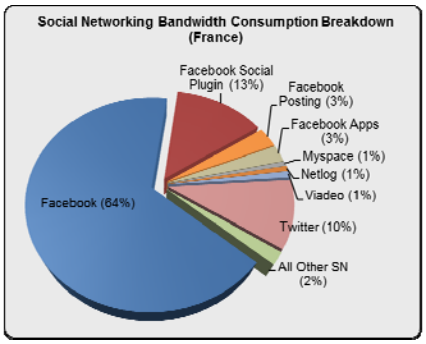
Hidden application traffic: 43% of the applications found can use SSL or hop ports; consuming roughly 40% of the overall bandwidth observed.

- SSL: 196 applications can use SSL in some way, shape or form. Applications using SSL specifically on port 443 are consuming significantly less bandwidth when compared to the global view (5.7% vs. 14%). The remaining SSL segments, on average, are consuming bandwidth at roughly the same rate.
- Port-hopping applications: 98 applications that can hop ports are consuming 25% of the bandwidth observed, nearly double that when compared to the global view (13%).



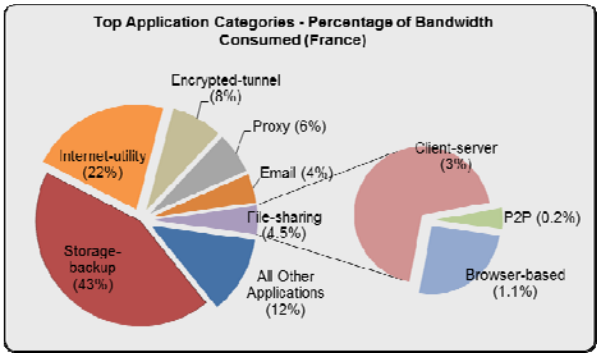
The work place has become more social.

- French socializing traffic patterns showed that webmail and social networking were used 5X and 4X more heavily than IM.
- Relative to social networking, Facebook was the dominant application. Facebook social plugins was used more than twice as heavily while Twitter use, at 10% was more than 3X greater than the 3% that was observed globally.



File transfer applications: will history repeat itself?

- The progression from FTP, to P2P, to browser-based file sharing all show strikingly similar risk and reward characteristics. These applications, found in France with 96%, 77%, and 96% frequency respectively, each provide business value, but represent security and business risks that may include exploits, malware vectors, and data loss (intentional or otherwise).
- In France, filesharing in general represented a smaller amount of bandwidth (4.5%) when compared to the global view at 8.8% of overall bandwidth consumed. Client-server file transfer (FTP, etc) was used most heavily at 3%, while P2P was nearly non-existent.



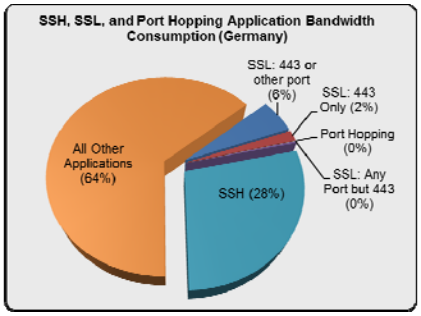
Germany

The sample in Germany encompassed 22 organizations with 527 applications detected that consumed 35 terabytes of bandwidth.

Key German findings:

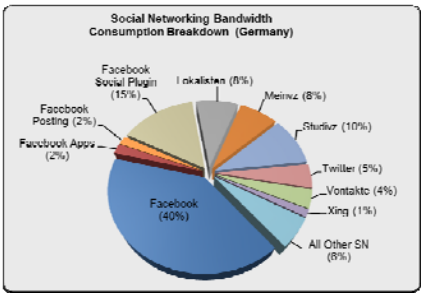
Hidden application traffic: 42% of the applications found can use SSL or hop ports; consuming roughly 8% of the overall bandwidth observed.

- SSL: 143 applications can use SSL in some way, shape or form. Applications that can use SSL represent only 8% of the overall German bandwidth observed, a relatively small amount when compared to the 23% consumed globally.
- Surprisingly, SSH consumed 28% of the bandwidth, an amount that, when compared to the global view, 14X greater. No other country showed SSH usage that was this significant.
- Port-hopping applications: 79 applications that can hop ports are consuming an almost immeasurable amount of bandwidth when compared to the global view (0.03% vs. 13%).



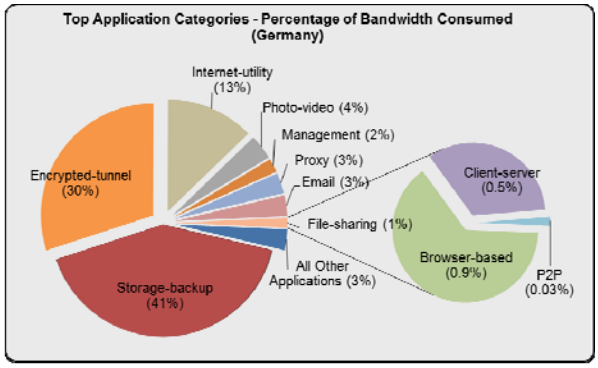
The work place has become more social.

- German socializing traffic patterns showed that IM and webmail represented a nearly immeasurable amount of overall bandwidth when compared with the global view.
- Social networking was used twice as heavily as webmail and 7X more heavily than IM. Facebook is heavily the most heavily used application, however, Germany exhibited the most evenly distributed local social networking usage patterns.



File transfer applications: will history repeat itself?

- In Germany, FTP, P2P and browser-based filesharing were found with 100%, 59%, and 77% frequency respectively.
- Collectively, filesharing represents only 1% of overall bandwidth, an amount that is nearly immeasurable when compared to the global view (1% vs. 8.8%). Browser-based filesharing is in use, although the volume is small, yet the business and security risks described in the Application Usage and Risk Report, May 2011 exist for those users.

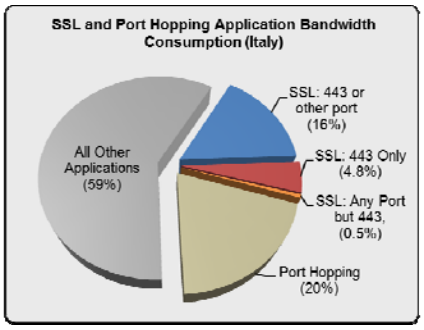


Italy

The Italian sample encompassed 49 organizations with 647 applications detected that consumed 46 terabytes of bandwidth.

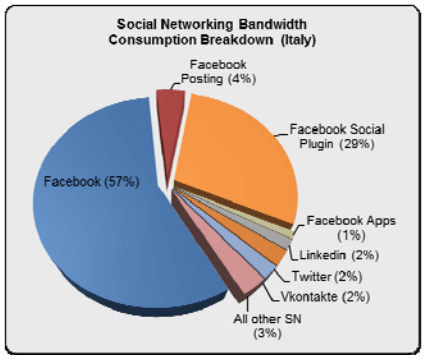
Key findings in Italy:

Hidden application traffic: 44% of the applications found can use SSL or hop ports; consuming roughly 41% of the overall bandwidth observed.



- SSL: 182 applications can use SSL in some way, shape or form. Bandwidth consumed by applications that can use SSL on any port was double the amount that was consumed globally (16% vs. 8%).
- Port-hopping applications: 104 applications that can hop ports are consuming 20% of the bandwidth observed, roughly 1.5X the amount that was consumed globally (13%).

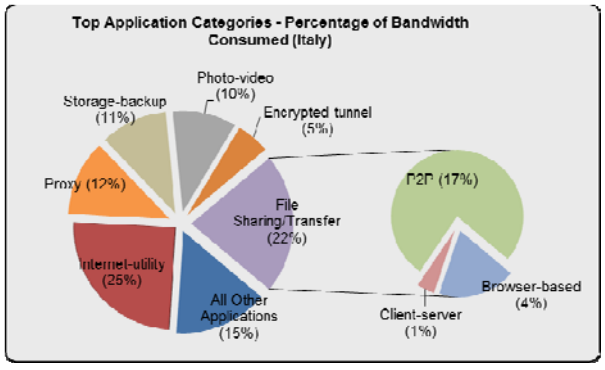
The work place has become more social.



- Socializing traffic patterns showed that webmail and social networking were used 2.5X and 5X more heavily than IM.
- Relative to social networking, Italy showed traffic patterns that were global in nature. Facebook was used most heavily, however, Facebook social plugins was used nearly 5X as heavily when compared to the global view (29% vs 3%).

File transfer applications: will history repeat itself?

- The progression from FTP, to P2P, to browser-based file sharing all show strikingly similar risk and reward characteristics. These applications, found in France with 98%, 90%, and 96% frequency respectively, each provide business value, but represent security and business risks that may include exploits, malware vectors, and data loss (intentional or otherwise).



- In Italy, filesharing in general consumed more than twice as much bandwidth as was consumed globally (22% vs 8.8%) P2P was most heavily used, while browser-based filesharing was also used heavily. This usage pattern exposes Italian users to a wider range of business and security risk when compared to the global view.

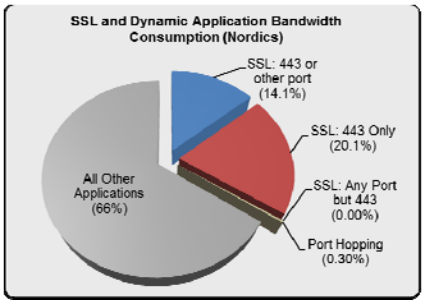
Nordics (Denmark, Finland, Norway, Sweden)

The Nordics sample encompassed 74 organizations with 693 applications detected that consumed 53 terabytes of bandwidth.

Key Nordics findings:

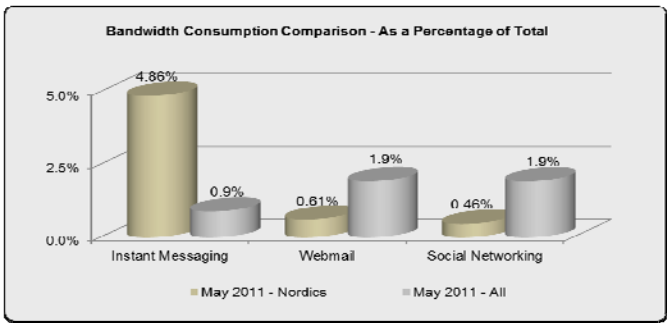
Hidden application traffic: 41% of the applications found can use SSL or hop ports; consuming roughly 33% of the overall bandwidth observed.

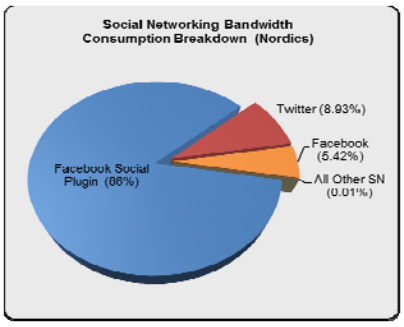
- SSL: 185 applications can use SSL in some way, shape or form. Applications that can use SSL only on port 443 consumed 1.5X more bandwidth when compared with the global view (20.1% vs. 14%). Conversely, those applications that can use SSL on ports other than 443 was nearly immeasurable.
- Port-hopping applications: 102 applications that can hop ports are consuming nearly an immeasurable amount of bandwidth when compared to the global view (13% vs. 0.03%).



The work place has become more social.

- Nordics socializing traffic patterns showed that IM consumed nearly 5% of the overall bandwidth, an amount that was nearly 5X that of Nordics webmail and social networking combined.

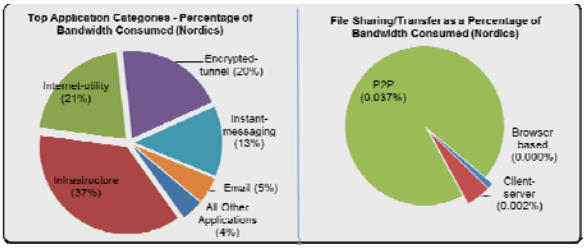




- Facebook social plugin consuming 86% of the overall Nordics social networking bandwidth. The heavy use of social plugins can be attributed, at least partially, to the popularity of Spotify, the streaming media application. No other country exhibited this type of application behavior.

File transfer applications: will history repeat itself?

- In the Nordics, FTP, P2P, and browser-based filesharing were found with 88% 74%, and 84% frequency respectively. However, their collective use was nearly immeasurable (less than 1%).



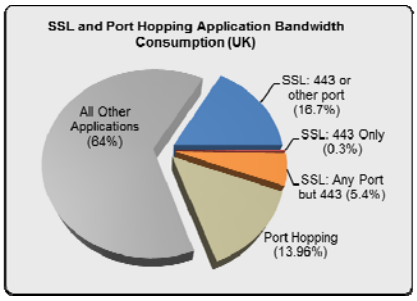
UK

The UK sample encompassed 59 organizations with 749 applications detected that consumed 106 terabytes of bandwidth.

Key UK findings:

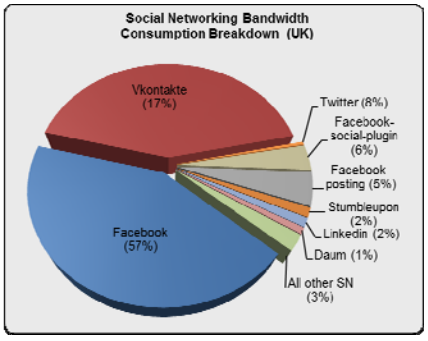
Hidden application traffic: 43% of the applications found can use SSL or hop ports; consuming roughly 36% of the overall bandwidth observed.

- SSL: 204 applications can use SSL in some way, shape or form. Applications that can use SSL on any port consumed more than twice as much bandwidth when compared to the global view (16.7% vs. 8%). Conversely, applications that can use SSL only on 443 consumed a fraction of the bandwidth when compared to the global view (0.3% vs. 14%)
- Port-hopping applications: 120 applications that can hop ports are consuming nearly the same amount of bandwidth when compared to the global view (13.96% vs. 13%).



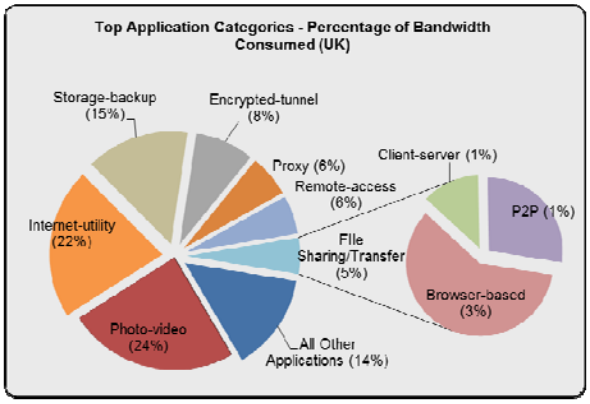
The work place has become more social.

- UK socializing traffic patterns showed that IM, webmail and social networking were used in equal proportions when compared to the global view.
- Social networking traffic patterns showed that Facebook was most heavily used, but Vkontakte also showed fairly heavy usage at 17% of overall social networking bandwidth.



File transfer applications: will history repeat itself?

- In the UK, FTP, P2P and browser-based filesharing were found with 95%, 78%, and 95% frequency respectively.
- The volume of usage showed that browser-based filesharing was more heavily used than both FTP and P2P. The heavier use of browser-based filesharing may expose UK organizations to unseen business and security risks as described in the recently published Application Usage and Risk Report, May 2011.



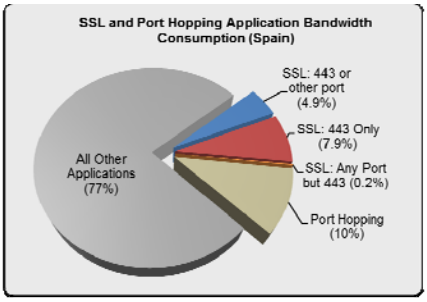
Spain

The sample in Spain encompassed 36 organizations with 648 applications detected that consumed 62 terabytes of bandwidth.

Key findings in Spain:

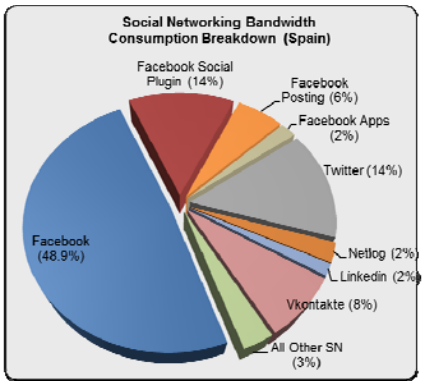
Hidden application traffic: 42% of the applications found can use SSL or hop ports; consuming roughly 23% of the overall bandwidth observed.

- SSL: 176 applications can use SSL in some way, shape or form. Compared with the global view, the traffic patterns shown in the SSL usage categories are similar to those shown in the global view.
- Port-hopping applications: 96 applications that can hop ports are consuming 10% of the overall bandwidth, an amount that is slightly less when compared to the global view (13%).



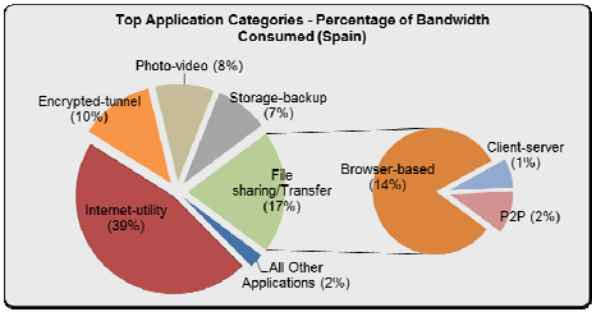
The work place has become more social.

- Spanish socializing traffic patterns showed that webmail was used more heavily than IM and social networking, when compared with the global view.
- The most surprising aspect of Spanish social networking traffic patterns was how little Tuenti, a very common local social networking application, was used. Tuenti is in use, however, the volume of traffic measured was less than 1% overall social networking bandwidth. The use of Facebook Posting and Apps indicates that the usage is more "active" than what was observed globally. Twitter was used more than 4X as heavily when compared to the global view (14% vs. 3%).



File transfer applications: will history repeat itself?

- In Spain, FTP, P2P, and browser-based filesharing were found with 86%, 67%, and 89% frequency respectively. The bandwidth consumed is nearly twice as much bandwidth when compared to the global view (17% vs. 8.8%).
- Much like the UK and other countries, the volume of usage showed that browser-based filesharing was more than 4X as heavily as both FTP and P2P combined. The heavier use of browser-based filesharing may expose organizations to unseen business and security risks as described in the recently published Application Usage and Risk Report, May 2011.



Country Specific Findings – APAC

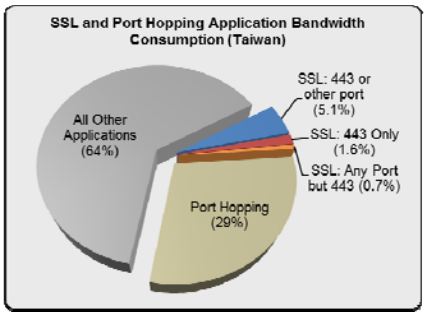
Taiwan

The Taiwan sample encompassed 147 organizations with 828 applications detected that consumed 338 terabytes of bandwidth.

Key Taiwan findings:

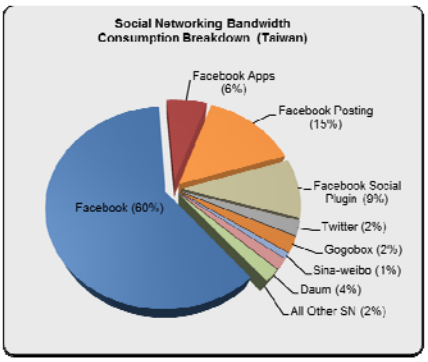
Hidden application traffic: 42% of the applications found can use SSL or hop ports; consuming roughly 36% of the overall bandwidth observed.

- SSL: 207 applications can use SSL in some way, shape or form. Compared with the global view, the use of SSL specifically on port 443 is significantly lower, based on the percentage of bandwidth consumed (1.6% vs. 14%). The remaining SSL segments, on average, are consuming bandwidth at roughly the same rate.
- Port-hopping applications: 137 applications that can hop ports are consuming 29% of the overall bandwidth, an amount that is more than double the amount consumed globally (29% vs. 13%).



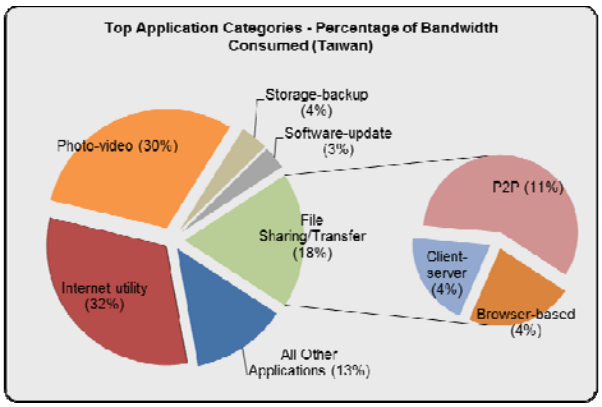
The work place has become more social.

- Taiwan socializing traffic patterns showed that IM, webmail and social networking were used at similar volumes.
- Relative to social networking, Facebook is very popular in Taiwan, however, several local social networking applications were also used fairly heavily. Facebook Posting and Apps consumed 15% and 6% of social networking bandwidth respectively, indicating that Facebook usage is more "active" when compared to the global view where both consumed 1% of the overall bandwidth.



File transfer applications: will history repeat itself?

- In Taiwan, FTP, P2P, and browser-based filesharing were found with 92%, 93%, and 67% frequency respectively.
- Collectively, filesharing consumed more than twice as much bandwidth when compared to the global view (18% vs. 8.8%). The volume of usage showed that P2P was nearly 3X as heavy as both FTP and browser-based filesharing. The heavier use of browser-based filesharing exposes organizations to known P2P related business and security risks.



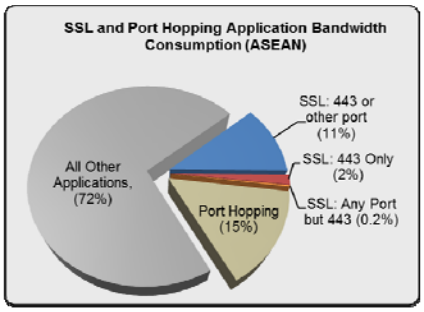
ASEAN

The ASEAN sample encompassed 95 organizations with 725 applications detected that consumed 225 terabytes of bandwidth.

Key ASEAN findings:

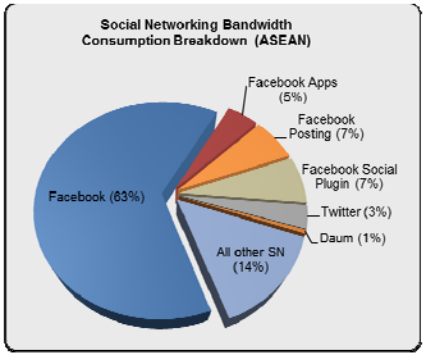
Hidden application traffic: 43% of the applications found can use SSL or hop ports; consuming roughly 28% of the overall bandwidth observed.

- SSL: 198 applications can use SSL in some way, shape or form. Compared with the global view, the use of SSL specifically on port 443 is significantly lower based on percentage of bandwidth consumed (2% vs. 14%). The remaining segments, on average, are consuming bandwidth at roughly the same rate.
- Port-hopping applications: 117 applications that can hop ports are consuming 15% of the overall bandwidth, an amount that is roughly the same as the amount consumed globally (15% vs. 13%).



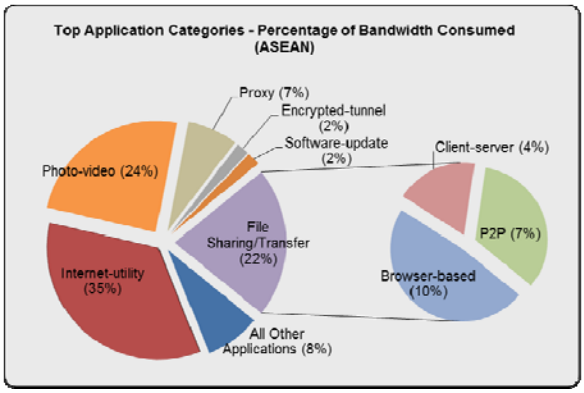
The work place has become more social.

- ASEAN socializing traffic patterns showed that IM, webmail and social networking were used at similar ratios.
- Relative to social networking, Facebook is very popular and can be viewed as more "active" with Facebook Posting and Apps consuming 5% and 7% of social networking bandwidth respectively. Globally, both of these Facebook applications consumed 1% of the overall bandwidth respectively.



File transfer applications: will history repeat itself?

- FTP, P2P, and browser-based filesharing were found with 84%, 91%, and 95% frequency respectively.
- Collectively, filesharing is consuming 22% of the overall bandwidth, a quantity that is more than double that of the global view (22% vs. 8.8%).
- The heavier use of browser-based filesharing and P2P exposes organizations to a combination of known (P2P) and unknown (browser-based filesharing) business and security risks.

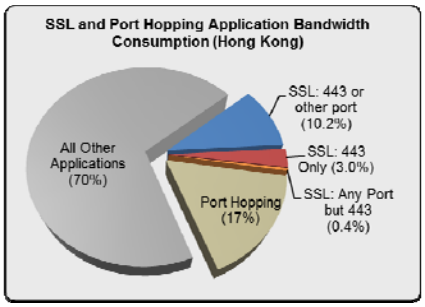


Hong Kong

The Hong Kong sample encompassed 37 organizations with 660 applications detected that consumed 65 terabytes of bandwidth.

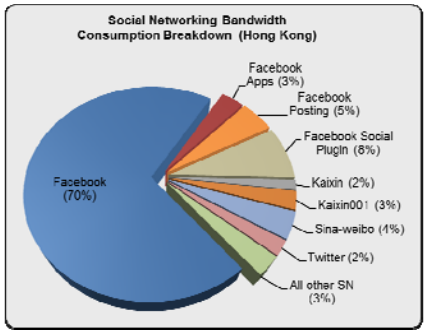
Key Hong Kong findings:

Hidden application traffic: 43% of the applications found can use SSL or hop ports; consuming roughly 30% of the overall bandwidth observed.



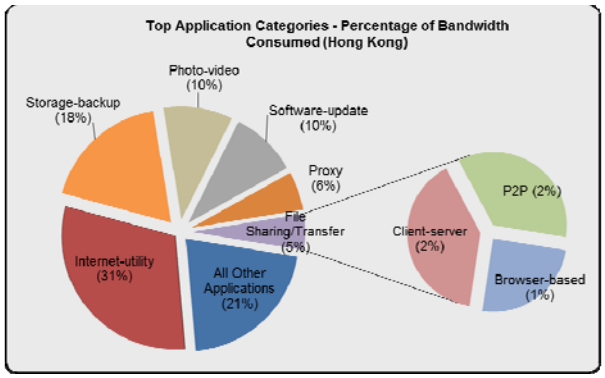
- SSL: 169 applications can use SSL in some way, shape or form. Compared with the global view, the use of SSL specifically on port 443 is significantly lower based on percentage of bandwidth consumed (3% vs. 14%). The remaining SSL segments, on average, are consuming bandwidth at roughly the same rates.
- Port-hopping applications: 115 applications that can hop ports are consuming 17% of the overall bandwidth, an amount that is slightly higher than the amount consumed globally (17% vs. 13%).

The work place has become more social.



- Hong Kong socializing traffic patterns showed that IM, webmail and social networking were used at rates that were similar to those observed globally when measured by bandwidth consumed.
- Relative to social networking, Facebook is very popular and can be viewed as more "active" with Facebook Posting and Apps consuming 3% and 5% of social networking bandwidth respectively. Globally, both of these Facebook applications consumed 1% of the overall bandwidth respectively. Several local social networking applications were also found to be consuming measurable bandwidth.

File transfer applications: will history repeat itself?



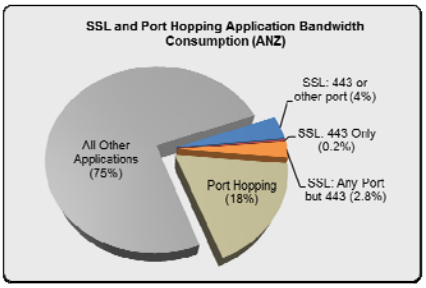
- FTP, P2P, and browser-based filesharing were found with 97%, 95%, and 97% frequency respectively. Collectively, filesharing activity is lower, when compared to the global view (5% vs. 8.8%).
- Within the 5% observed, client-server file transfer (FTP, etc) and P2P were used equally, indicating both work (FTP) and non-work (P2P) related use.

Australia and New Zealand

The Australia and New Zealand (ANZ) sample encompassed 9 organizations with 528 applications detected that consumed 27 terabytes of bandwidth.

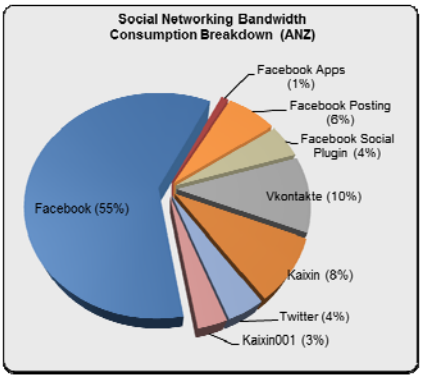
Key ANZ findings:

Hidden application traffic: 44% of the applications found can use SSL or hop ports; consuming roughly 25% of the overall bandwidth observed.



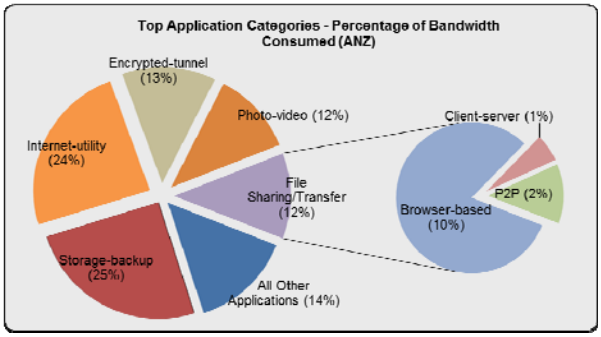
- SSL: 149 applications can use SSL in some way, shape or form. Bandwidth observed for applications that can use of SSL specifically on port 443 is nearly immeasurable when compared to the global view (0.2% vs. 14%). The remaining SSL segments, on average, are consuming bandwidth at roughly the same rates.
- Port-hopping applications: 80 applications that can hop ports are consuming 18% of the overall bandwidth, an amount that is slightly higher than the amount consumed globally (18% vs. 13%).

The work place has become more social.



- ANZ socializing traffic patterns showed that IM, webmail and social networking were used at similar ratios when measured by bandwidth consumed.
- Relative to social networking, Facebook is very popular and can be viewed as more "active" with Facebook Posting consuming 6% of social networking bandwidth. Globally, Facebook Posting 1% of the overall bandwidth. Several "international" social networking applications were also found to be consuming measurable bandwidth (Vkontakte, Kaixin, and Kaixin001).

File transfer applications: will history repeat itself?



- FTP, P2P, and browser-based filesharing were found with 100%, 78%, and 89% frequency respectively. ANZ filesharing activity is slightly higher, when compared to the global view (12% vs. 8.8%). Browser-based consumed 10% of the overall bandwidth, a quantity that is more than 3X that of P2P and FTP.
- The heavier use of browser-based filesharing may expose organizations to unseen business and security risks as described in the recently published Application Usage and Risk Report, May 2011.

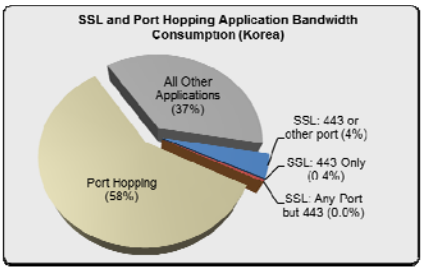
Korea

The Korean sample encompassed 6 organizations with 467 applications detected that consumed 39 terabytes of bandwidth.

Key Korean findings:

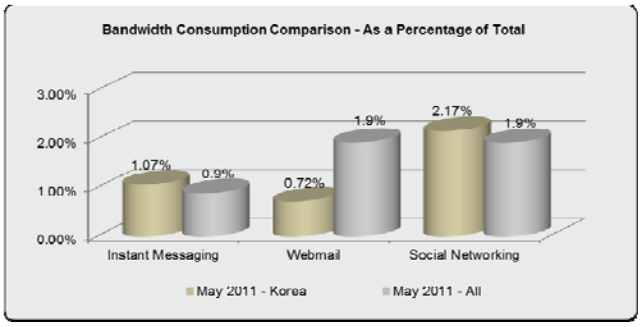
Hidden application traffic: 43% of the applications found can use SSL or hop ports; consuming roughly 63% of the overall bandwidth observed.

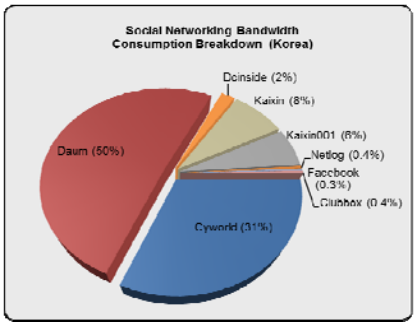
- SSL: 126 applications can use SSL in some way, shape or form. Applications that use of SSL specifically on port 443 is nearly immeasurable when compared to the global view (0.2% vs. 14%). The remaining SSL segments, on average, are consuming bandwidth at roughly the same rates.
- Port-hopping applications: 75 applications that can hop ports are consuming 58% of the overall bandwidth, an amount that is significantly greater than the amount consumed globally (58% vs. 13%). The high Port-hopping bandwidth can be attributed to the very high use of P2P filesharing, shown below.



The work place has become more social.

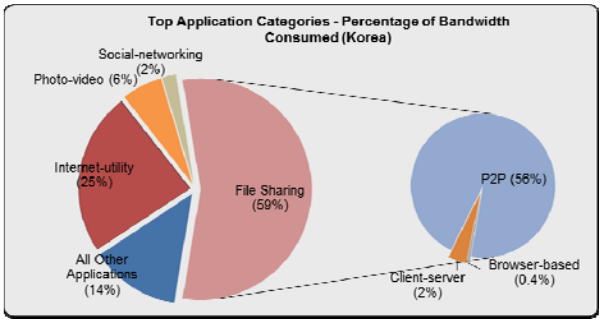
- Korean socializing traffic patterns showed that IM and social networking were used at higher ratios than the global view. Social networking in Korea is heavily skewed towards local applications such as Daum and Cyworld. Korea is the only location where Facebook is nearly immeasurable.





File transfer applications: will history repeat itself?

- FTP, P2P and browser-based filesharing were found with 83%, 100%, and 83% frequency respectively. Korean filesharing activity is more than half of the overall bandwidth, an amount that is 6X that of the global view(59% vs. 8.8%).
- P2P represents 56% of the overall bandwidth consumed, with client-server and browser-based both consuming a minute amount of bandwidth.



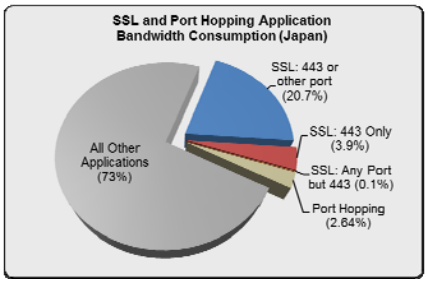
Country Specific Findings – Japan

The Japanese sample encompassed 6 organizations with 467 applications detected that consumed 39 terabytes of bandwidth.

Key findings in Japan:

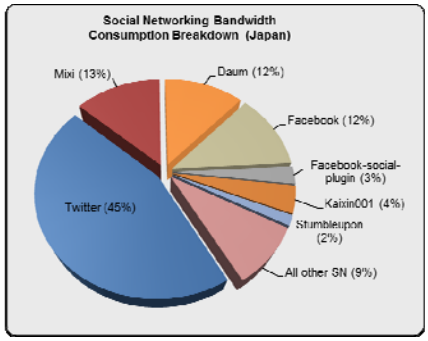
Hidden application traffic: 41% of the applications found can use SSL or hop ports; consuming roughly 27% of the overall bandwidth observed.

- SSL: 173 applications can use SSL in some way, shape or form. Compared with the global view, the use of SSL on any port is 2.5x more than the global view (20.7% vs. 14%). Conversely, SSL on 443 only is approximately half of the amount that is consumed globally (3.9% vs. 8%).
- Port-hopping applications: 173 applications that can hop ports are consuming a mere 2.64% of the overall bandwidth, an amount that is significantly less than the amount consumed globally (2.65 vs. 13%).



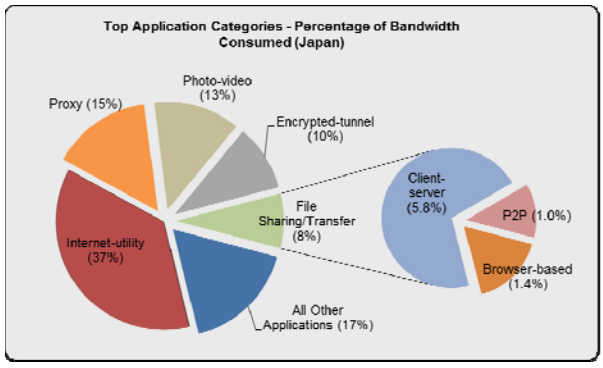
The work place has become more social.

- Social networking in Japan is dominated by Twitter at 45% of the overall social networking bandwidth measured.
- Japan is the only country where Twitter is the most heavily used social networking application. Mixi and Daum are also used frequently, pushing Facebook to a tie for 3rd most heavily used in terms of bandwidth consumed.



File transfer applications: will history repeat itself?

- FTP, P2P, and browser-based filesharing were found with 82%, 63%, and 83% frequency respectively.
- Filesharing activity in Japan is roughly the same amount as that of the global view, however, client-server filesharing (FTP) is the bulk of the usage (5.8%).



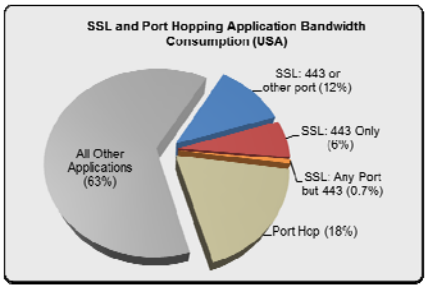
Country Specific Findings – North America

USA

The USA sample size encompassed 296 organizations with 928 applications detected that consumed 776 terabytes of bandwidth.

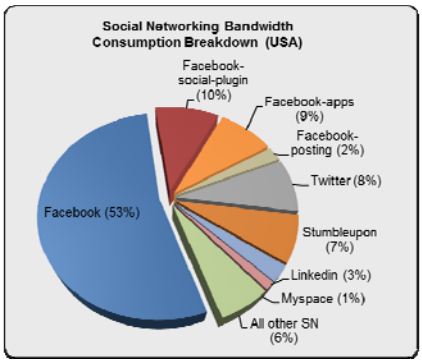
Key USA findings:

Hidden application traffic: 42% of the applications found can use SSL or hop ports; consuming roughly 37% of the overall bandwidth observed.



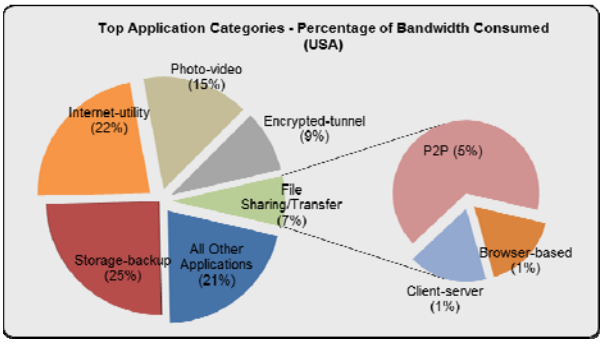
- SSL: 242 applications can use SSL in some way, shape or form. Applications that can use SSL on any port is 1.5X greater when compared to the global view (12% vs. 8%). SSL on 443 only is less than half of what is consumed globally (6% cs. 14%)
- Port-hopping applications: 152 applications that can hop ports are consuming 18% of the overall bandwidth, an amount that is slightly greater than the amount consumed globally (18% vs. 13%).

The work place has become more social.



- Webmail, IM and social networking usage in the USA are roughly the same rations as observed globally.
- Social networking traffic patterns in the USA mimic the global patterns

File transfer applications: will history repeat itself?



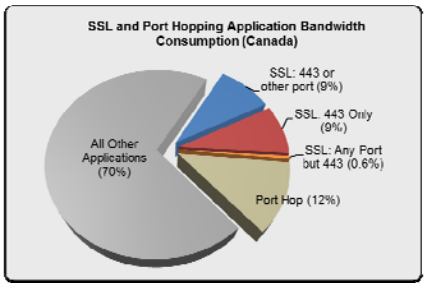
- FTP, P2P, and browser-based filesharing were found with 95%, 79%, and 93% frequency respectively.
- USA filesharing activity is roughly the same as the global view (7% vs. 8%) and the ratios are similar with P2P representing the highest amount. Heavy P2P use introduces known business and security risks related to P2P filesharing.

Canada

The Canadian sample encompassed 26 organizations with 731 applications detected that consumed 292 terabytes of bandwidth.

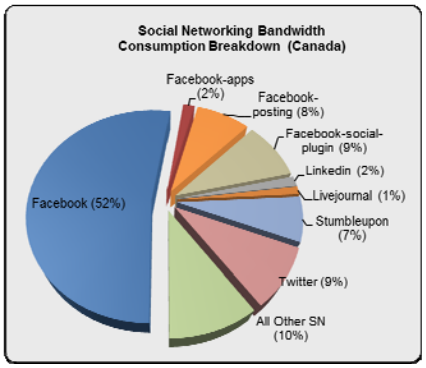
Key Canadian findings:

Hidden application traffic: 47% of the applications found can use SSL or hop ports; consuming roughly 30% of the overall bandwidth observed.



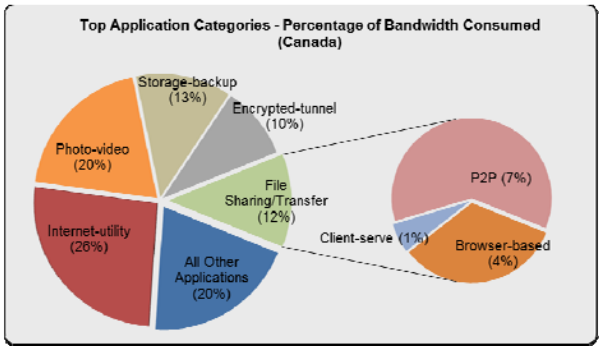
- SSL: 195 applications can use SSL in some way, shape or form. Compared with the global view, the use of SSL on any port is roughly the same as viewed globally (9% vs. 8%) while SSL on 443 only is slightly lower (9% vs. 14%).
- Port-hopping applications: 111 applications that can hop ports are consuming roughly the same amount that is being consumed globally (12% vs. 13%).

The work place has become more social.



- Canadian socializing traffic patterns showed that webmail, IM and social networking were used at roughly the same ratios as viewed globally.
- Social networking in Canada is more "active" than globally. Facebook Posting is consuming 8X more bandwidth while Facebook Apps is consuming 2X. Twitter use in Canada is 3X more than observed globally.

File transfer applications: will history repeat itself?



- FTP, P2P, and browser-based filesharing were found with 100%, 86%, and 92% frequency respectively.
- Collectively, filesharing activity is 1.5X greater than observed globally (12% vs. 8.8%) P2P represent the highest amount with browser-based filesharing consuming significantly more than globally, based on percentages (4% vs. 0.2%).
- Heavy P2P use introduces known business and security risks related to P2P filesharing. As browser-based filesharing applications leverage peer-based technology and add clients as a "premium offering", the question arises: will the business and security risks introduced by browser-based filesharing follow the same path as those that were introduced by P2P.