

Keeping an Eye on Recreational Traffic

Intelligent Lifecycle Series

Contents

- 2 Introduction
- 3 The Impact of Recreational Traffic
- 4 P2P
 - Social Networking
 - Video Sharing — YouTube
- 6 The Intelligent LifeCycle Approach
 - Assess: Determine the Right Tools for the Job
- 7 Provision: Find and Fix
- 8 Contain Recreational Traffic
 - Protect Business Critical Applications
 - Accelerate: Take it to the Next Level
- 9 Extend: Everyone, Everywhere,
 - Further Reference

Keeping an Eye on Recreational Traffic

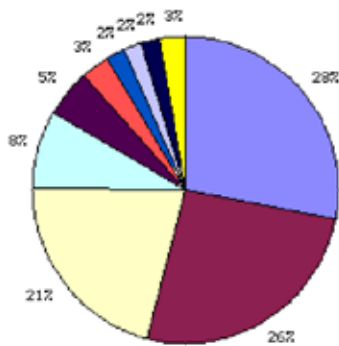
Introduction

The perennial problem of Peer to Peer (P2P) file sharing, the explosion of social networking sites like MySpace and Facebook, video sharing sites like YouTube, all conspire to have a significant impact on the volume of traffic on your networks.

The resulting bandwidth congestion causes poor performance of the applications that run your business. Many of these problems originate from competition between them and similar sanctioned applications (video conferencing, web-based applications or file management systems), that join your other business applications and collaboration traffic in an all-out battle for bandwidth with recreational traffic. P2P file sharing which is designed to be aggressive and evasive, and bandwidth-hogging social networking sites exacerbate the problem. The result? Unpredictable network traffic and unstable networks that cripple performance and threaten business processes. As an IT Manager, you are faced with the challenge of regaining control of the networking infrastructure, investment and resources that support your business.

Recreational traffic steals bandwidth that should otherwise be used for business applications. When bandwidth is consumed by recreational traffic, the business processes are tied directly to those critical applications are threatened or disrupted.

Top 10 Classes

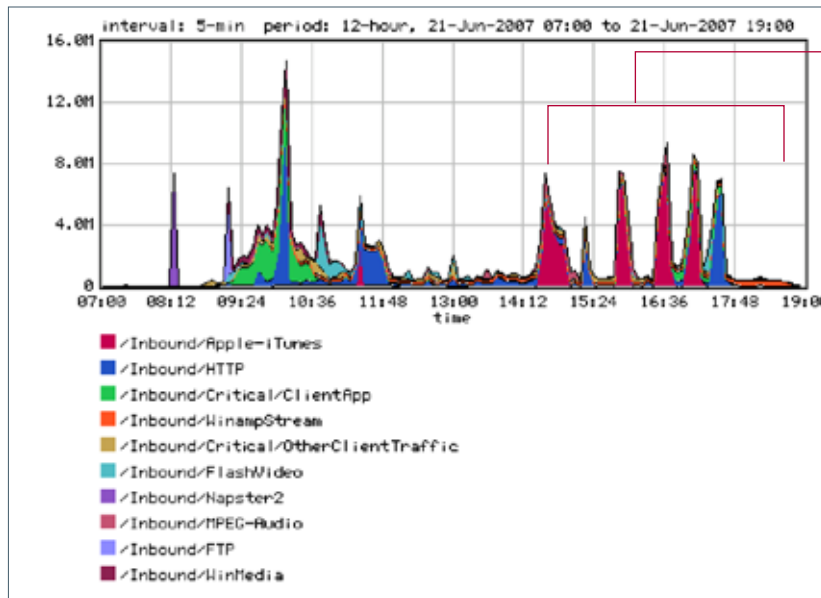


Class Name	Average Rate (bps)	(%)
1. /Inbound/Apple-iTunes	577k	28
2. /Inbound/HTTP	526k	26
3. /Inbound/Critical	420k	21
4. /Inbound/WinampStream	171k	8
5. /Inbound/FlashVideo	110k	5
6. /Inbound/Napster2	51k	3
7. /Inbound/MP3-Radio	43k	2
8. /Inbound/FTP	36k	2
9. /Inbound/Media	37k	2

period: 12-hour, 21-Jun-2007 07:00 to 21-Jun-2007 19:00

Recreational applications can consume very large portions of bandwidth, inhibiting critical applications from getting the bandwidth they need to perform efficiently and reliably.

A normal quality video, streamed from YouTube can consume 640kbps. Someone viewing a high quality movie trailer consumes 1.5Mbps while the video streams. Even innocent recreational traffic quickly adds up to a large problem.



Four iTunes purchases create havoc all afternoon by crowding a critical client application, compromising business processes. Almost 8 Mbps consumed for 20 minutes!

The Impact of Recreational Traffic

Although many IT managers may know that recreational applications are on their network, they are usually unaware of the impact. It's no wonder that many are surprised to learn that recreational applications can consume 60 to 70 percent of their WAN and Internet service links.

Recreational applications are very aggressive and burst to consume large amounts of WAN and Internet bandwidth. To download quickly, stream "live" video or swap files efficiently, recreational applications initiate a large number of connections and burst to consume large amounts of bandwidth for sustained periods of time. This presents a serious problem for less aggressive business applications running over those same WAN and Internet links.

Congestion from recreational traffic crowds out critical systems that are sensitive to delay. This affects performance and response times of transactional apps, the quality of Voice over IP (VoIP), or video conferencing. When latency-sensitive applications struggle to acquire their requisite shares of bandwidth, they perform slowly, or not at all. Even other bursty, less-sensitive applications (email, image transfers, database synchronization, and backup) are vulnerable to bandwidth contention.

Let's explore the characteristics of several popular recreational traffic types: P2P, MySpace, and YouTube.

P2P

P2P activity creates very heavy inbound traffic flows. As users download files, inbound traffic crosses over the WAN. Routers, firewalls, and queuing devices are powerless to manage the impact on your WAN because they only manage outbound traffic. This is true for many types of traffic that follow standard client-server models, where a client query returns large amounts of information from the server (asymmetric traffic flows).

Operation	Characteristics
Search for “peers”	<ul style="list-style-type: none"> • Large amounts of ping-like traffic indicate P2P applications searching for visible peers or content server nodes.
Search for files	<ul style="list-style-type: none"> • Large numbers (hundreds) of simultaneous connections widen search for files to download.
Upload and download	<ul style="list-style-type: none"> • Transfer large files across the WAN and Internet links. • Portions of files are loaded from different peer targets simultaneously. • Applications are efficiency-driven, bursting to consume as much bandwidth as possible in an effort to complete file transfers quickly. • Aggressive behavior — P2P pushes out other applications that are sharing and contending for that same bandwidth. • Behavior is multiplied for number of files transferred and bandwidth available from targets. • Traffic is bidirectional: Any node can download (receive) and upload (send) files to multiple peers.
Power servers and super-nodes	<ul style="list-style-type: none"> • Many P2P applications recognize “power servers” that have very high-speed connections. These power servers become popular destinations for the other millions of peers using the application. • More than 20,000 simultaneous connections can service uploads and downloads. • The more bandwidth you have, the more attractive your network is to P2P applications.

Users acting as “servers” generate large amounts of outbound traffic. P2P users act as content servers. Other users can continue to search and download files from peers, whether or not the user is aware of the activity. This “server” traffic leads to a lot of inbound (search) traffic, as well as heavy, bandwidth intensive outbound file transfer traffic that competes with other applications.

Social Networking

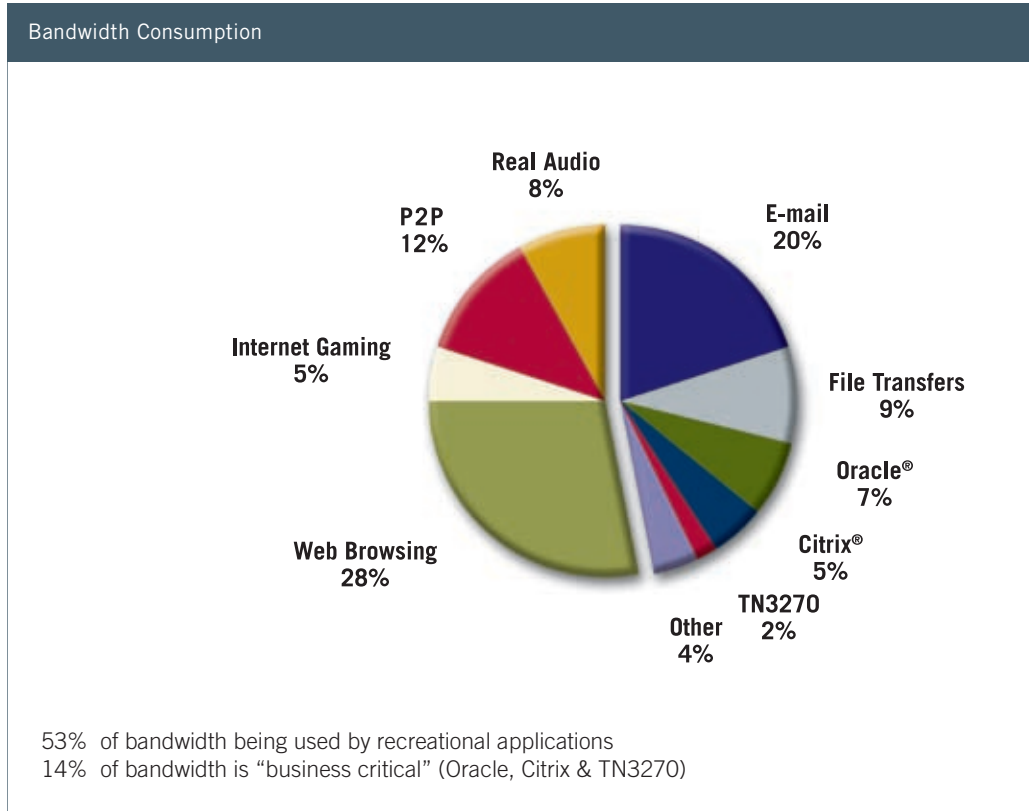
MySpace and FaceBook are popular social networking websites offering an interactive, user-submitted network of friends. MySpace has more pageviews per day than any site on the web except Yahoo. And it’s not just pageviews and it’s not just once: checking messages, posting comments and pictures, and getting comments bring people back to MySpace every day, multiple times a day.

In addition to personal information in text format, a profile on social networking sites normally contains embedded links to a plethora of multimedia content: photos, slideshows, graphic images (cartoons, icons), music, and videos. A single MySpace page, for example, can have 200-300 DNS lookups, as compared to an average news page that contains 10-15 DNS lookups. So, not only is bandwidth impacted, but they also give rise to an exponential increase in DNS traffic.

Video Sharing — YouTube

YouTube is a video sharing website where users can upload and view video clips. Other country-specific sites such as France’s DailyMotion share similar attributes and cause similar problems. YouTube accepts uploaded videos in .WMV, .AVI, .MOV, MPEG, and .MP4 formats, and then converts them into .FLV (Adobe Flash Video) format after uploading. According to Michael Dell of Dell Inc., YouTube traffic in 2007 consumes as much bandwidth as the entire Internet utilized just seven years ago. To give you an idea of YouTube bandwidth consumption, a single video uses around 100Kbps up to 1 Mbps of bandwidth, and Internet video uses 1000 times as much bandwidth as a single email.

Unlike P2P, all video files are served from the YouTube servers, not from peers. However, to handle the volume of video files, servers are located at multiple locations. YouTube videos are not streamed; they are downloaded and buffered so that the user can begin viewing the video before the file has finished downloading.

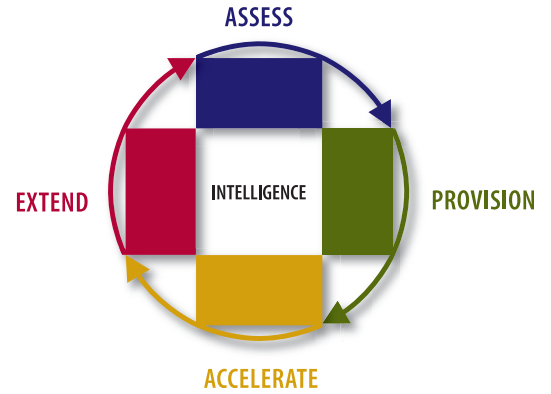


You may be surprised by just how much of your bandwidth budget is spent on recreation. These results from a Packeteer customer survey show more than 50% recreational traffic on average in the typical enterprise.

The Intelligent LifeCycle Approach

Packeteer's Intelligent LifeCycle describes a proven methodology for assessing, troubleshooting, and managing application performance across a wide variety of environments. This process calls for four distinct activities that help customers focus their efforts on providing fast, effective solutions rather than temporary fixes for application performance issues. The four steps are: Assess, Provision, Accelerate, and Extend.

Let's see how this methodology can help you keep an eye on — and eliminate the damaging effects of — recreational traffic.



Assess: Determine the Right Tools for the Job

Identify what applications are running on the network, what approaches to take to resolve issues, and continuously monitor performance

Many network managers and directors have an idea that P2P, YouTube, and other types of recreational applications are running on their network, but they usually do not have the tools to see them nor understand the impact on network performance.

See Clearly

The growing complexities associated with recreational traffic make sophisticated classification techniques a necessity. P2P applications in particular are very elusive — they hop ports and masquerade as other traffic. This inherent trait represents P2P's defense mechanism, enabling the applications to avoid detection by firewalls, routers, and filters. These devices typically work on Layer 2, 3, and 4 of the OSI model (for example, MAC or Ethernet address, IP address, and TCP/UDP port numbers). As a result, firewalls, routers, and filters lack the application-level awareness to track many forms of recreational traffic accurately. Their simple IP address or static port schemes simply fall short.

Encryption	Port Hopping
<p>Sometimes peer-to-peer traffic uses encryption to try to disguise itself and avoid detection. When applications, such as Ares, obscure their content through encryption, the traffic can circumvent security. Allowing encrypted P2P traffic exposes organizations to potential worms, viruses, spyware, and other unauthorized files. Because the Packeteer system is able to identify connection setup sessions for P2P applications that utilize encryption to obscure transferred content (such as Ares 1.8.1), you have the ability to block or discard the connections.</p>	<p>Port hopping is another technique developed for avoiding application detection. Many P2P protocols, such as AOL (America Online) and KaZaa, use port hopping so that they can bypass firewalls and router configurations that are designed to block or rate-limit them. When an application has port hopping capability, it will try to reach a remote host on a different port when it is unable to connect on the default port. For example, a P2P program might first try to connect on port 80. If this fails, it might try on port 3904. If port 3904 doesn't work, it might jump to port 4556. Because Packeteer visibility features understand protocols up to level 7 of the ISO model, it is able to recognize many port-hopping protocols no matter what port they are using.</p>

Packeteer's Layer 7 Plus classification and analysis capabilities provide the application-level intelligence necessary for identifying and tracking recreational traffic on your network. Packeteer discovers hundreds of applications automatically by leveraging special Layer 7 signature and behavioral techniques. After installing Packeteer system and providing basic IP configuration, simply enable Auto-Discovery to identify and analyze all traffic on the network.

Packeteer's classification detects dynamic and migrating port assignments, differentiates applications even when they are using the same port, and uses Layer 7 application indicators to identify applications. The Packeteer approach and technology allow you to verify that an application flow is what it's supposed to be.

To see a complete list of all the applications the Packeteer is able to classify, see Applications, Protocols, and Services:

<http://support.packeteer.com/documentation/packetguide/8.2/reference/services.htm>

Ongoing Monitoring

Any best practice involves continually monitoring your network to spot changes in behavior. Employ Packeteer's detailed performance and utilization statistics to benchmark and track critical applications. Use its in-depth diagnostic information to pinpoint causes of performance problems and leverage the adaptive response facility for updates when important applications or other traffic fall outside of configured performance envelopes. Report results to important stakeholders with onboard reporting.

In the following example, monitoring class utilization has profiled recreational traffic resulting from streaming video of the US March college basketball finals. Armed with this kind of detailed information, the Packeteer system can be used to rapidly respond to and set time or bandwidth limits to usage like this before it causes problems for business applications — and the processes they support.



1. Viewer #1 starts watching
2. Viewer #2 joins, high quality stream
3. Viewer #3 joins, normal
4. Fan #2 stops watching
5. Fan #3 stops watching

Monitoring for Class — Inbound/Real/CBSSportsLine.com

Provision: Find and Fix

Create network resource policies to align network resources with the business

When recreational applications or traffic hijack the network bandwidth, causing poor network performance of critical applications, one seemingly logical response is to increase the capacity of the link. But without other controls in place, throwing more bandwidth at the problem doesn't solve anything. The recreational traffic will just be happy to have more bandwidth available, and the critical applications will still suffer from poor response times.

Another possible tactic for controlling bandwidth is to set rate limits on certain traffic using policies in the router. But this approach is ineffective because the policies don't have Layer 7 visibility into the different application types. Plus, rate-limiting adds significant processing overhead to the router.

Packeteer offers more effective approaches.

Organizations' philosophies on how the network can be used, and, thus, how recreational traffic should be treated, vary. Regardless of your philosophy, Packeteer recommends two best practices:

- Communicate network usage policies clearly
- Devise a simple means to enforce network usage policies

It is IT and/or HR's job to communicate network usage policies to staff. Packeteer can help enforce these policies. Packeteer's network optimization solution and associated best practices help organizations gain visibility into and control over their network links.

Packeteer systems measure bandwidth utilization and its impact on critical applications. In doing so, it allows network managers to administer appropriate policy controls to contain unsanctioned traffic, protect mission-critical traffic, and pace bursty business applications. Through simple policy setting and patented technology, Packeteer provides visibility and control over traffic on an application, user, or session basis.

Packeteer Best Practices derived from real-world customer experiences are listed below. Which of the approaches you should adopt depends on your network management philosophy.

Contain Recreational Traffic

Packeteer automatically classifies most of the applications that people use for recreation. Doom, Quake, Tribes, and Microsoft Xbox are a few of the Internet game applications classified. The popular instant messaging services, including AIM, Lotus, and Yahoo, are also automatically discovered, as are YouTube, Google Video, Radio@Netscape, and Slingbox. For MySpace traffic, you create a web-based class with a www.myspace.com URL criterion. For more obscure recreational traffic types, you can easily create classes manually. Identifying and creating classes for the most popular P2P applications: BitTorrent, KaZaA, Warez, and Ares, is automatic.

Packeteer controls traffic bi-directionally, providing control over inbound traffic flows before they hit your router, so you can ensure that bandwidth is available to other important applications. To do this, set specific bandwidth maximums (called partitions) and choose to limit available bandwidth.

Although Packeteer application QoS can be used to block traffic from a particular application, user or source, for P2P traffic, it is almost always better to limit bandwidth — not block.

Blocking P2P often results in helpdesk calls because users perceive that the network is down. In addition, blocking policies can motivate P2P applications to develop erratic and advanced evasion techniques. The recommended approach involves squeezing P2P partitions gradually to modify user behavior. As P2P performance slows, users will eventually refrain from using the application because of the long, unproductive waiting periods. When this occurs, IT achieves its objective — and the users themselves have governed their own usage in the process.

By limiting the amount of bandwidth that P2P file sharing consumes, you eliminate P2P's impact on your critical applications. For unauthorized P2P traffic a very small partition will frustrate users and discourage P2P use. Users may even refrain from complaining — they may feel uncomfortable about complaining openly about poor performance of unauthorized traffic. Once P2P applications are identified and classified, create a folder for your P2P applications, and then move all the P2P-related classes into this folder.

For P2P, create a partition for the P2P folder, with a maximum of 20Kbps or 5–10 percent of your network bandwidth.

Protect Business Critical Applications

You can ensure bandwidth guarantees either on a per-application, per-connection, or per-user basis. This protects performance of critical applications by ensuring that adequate resources are available when needed. Those resources can be reallocated to other important applications when available.

Identify your critical applications and examine their bandwidth utilization, efficiency, and Response Time Measurement (RTM) statistics. Identify targeted service levels and set a bandwidth minimum for that class (for example, a minimum of 20 percent of the link, burstable to 50 percent). To guarantee bandwidth on a per-session basis, create policies to support those requirements. Track the service levels and amend your policies accordingly.

Accelerate: Take it to the Next Level

Apply technologies to enhance performance and capacity

The preceding steps of the Intelligent LifeCycle have told us exactly what recreational applications are responsible for network traffic, and allowed us to provision resources according to policies. We have determined which key applications to protect and we've efficiently and effectively allocated network resources to drive toward consistently meeting and exceeding application performance levels. Now we can turn our attention to optimizing application data as it flows across the network.

There are two primary ways of achieving this: compression and acceleration

Compression	Acceleration
Compressing application data removes redundant or unnecessary data as the traffic crosses the network. It effectively reduces the demand for bandwidth by applications.	Acceleration aims to increase usage of the network by sending more data across the network than can be done natively by the application.

But in isolation, without having followed and implemented the Assess and Provision steps, Compression and Acceleration are unlikely to achieve your objectives.

Adding bandwidth is often the default reaction to attempt to provide resources to improve performance of critical applications. It is a high cost, recurring operating expense that ends up funding better performance for P2P applications. Rewarding P2P with more bandwidth punishes critical apps and your budget. Adding bandwidth just makes networks more attractive to P2P applications, further punishing critical applications at a high cost. In fact, many P2P applications 'promote' higher bandwidth users to a higher status, attracting more peers to download from your users, consuming your new bandwidth, and making problems worse.

Packeteer provides protocol and application-specific acceleration and the ability to intelligently compress application traffic. Layer 7 Plus visibility allows us to identify the applications that should have the benefit of compression and acceleration and our patented control technologies allow us, if desired, to determine the level of acceleration and compression for a given application all while continuing to protect critical real-time convergence and encrypted applications.

Extend: Everyone, Everywhere

Create an intelligent overlay that extends and adapts current infrastructure to new and emerging issues

At this point we've put some powerful solutions into place to limit the impact of recreational applications and ensure that key business applications perform as expected. Having controlled traffic and managed the performance of key applications, we can now turn our attention to replicating this success for new and future applications — and protect from future phenomena like YouTube.

Keep on top of the problem

Understanding which applications are competing for the bandwidth and which users are taking more than their fair share will help you zero in on the trouble spots.

Continually monitor to spot changes in behavior. For example, Packeteer's traffic distribution and top conversation reports give early warning of the rise of new recreational pressures on the network.

Examine specific cross-sections of traffic on your network. Group information by geography, business unit, as well as by application or any other appropriate basis, and then analyze very specific information at an extremely detailed level by performing custom queries and filtering out irrelevant data.

Apply frequent updates

Just like new virus definitions, make sure you apply application discovery updates that enable identification of new P2P applications or other recreational technologies or behaviors that will impact your network and the performance of key applications.

Packeteer's plug-in architecture for application definitions allows us to quickly and easily implement solutions for new applications while continuing to enhance the performance of existing applications.

Further Reference

For more information, see:

- Packeteer 'The Intelligent LifeCycle for Networked Applications' Whitepaper — http://www.packeteer.com/resources/prod-sol/Intelligent_LifeCycle_Introduction.pdf
- Packeteer 'Best Practices for Application Traffic Management' Site — <http://www.packeteer.com/support/BestPractices>
- Recommendations for Real-World Situations: Procedures to Address Network and Application Issues — <http://support.packeteer.com/documentation/packetguide/8.0/solutions/app-control/prepare-for-next-napster.htm>
<http://support.packeteer.com/documentation/packetguide/8.0/solutions/app-control/control-p2p.htm>
<http://support.packeteer.com/documentation/packetguide/8.0/solutions/app-control/control-internet-radio.htm>



World Headquarters

Packeteer, Inc.
10201 N. De Anza Blvd.
Cupertino, CA 95014
USA
T +1.408.873.4400
+1.800.697.2253
F +1.408.873.4410
www.packeteer.com

Packeteer Europe

Packeteer Europe B.V.
Louis Braillelaan 80
2719 EK Zoetermeer
The Netherlands
T +31 88 7427377
F +31 88 7427300

Packeteer Japan

Packeteer Japan Inc KK
2-7-1, Nishi-Shinjuku
Shinjuku-ku Tokyo 163-0704
Japan
T +81 0 3 5339 7970
F +81 0 3 5339 7979

Packeteer Asia Pacific

Packeteer Asia Pacific Ltd.
Suite 1507, 15th Floor, Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing, Hong Kong
T +81 0 3 5339 7970
F +81 0 3 5339 7979