Best Practices -

Monitoring and Controlling Peer-to-Peer (P2P) Applications

White Paper

PACKETEER®

Fast WAN. Fast Apps. Fast Business.

APPLICATION

- Peer-to-Peer (P2P)

EXAMPLES

- AudioGalaxy, eDonkey, BitTorrent, KaZaA, etc.

USAGE

- Locate and exchange (swap) files. Often used to exchange copyrighted music and video files.

BEHAVIOR

- P2P applications are extremely aggressive. They consume large, inordinate amounts of bandwidth and can burst for long periods of time (hours/days) as multiple files are downloaded and uploaded.

IMPACT

- P2P's aggressive bandwidth consumption causes poor, unpredictable performance for business-critical applications and the business operations that depend on them.

COST

- How much bandwidth dollars are funding P2P? Do you really know?

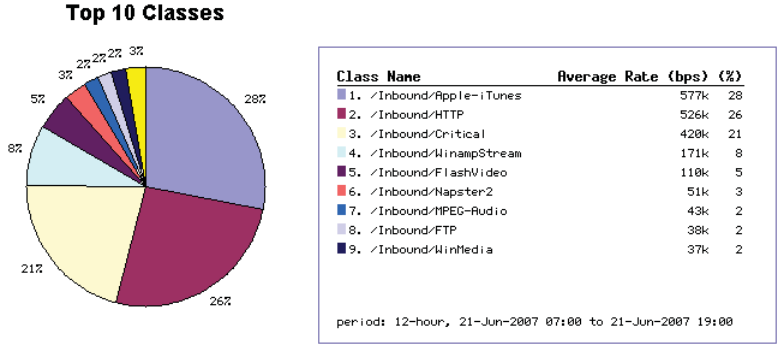
BEST PRACTICE

- Contain P2P's harmful impact on mission-critical applications with bi-directional bandwidth maximums (partitions) on P2P traffic using the Packeteer® PacketShaper® or iShaper™.

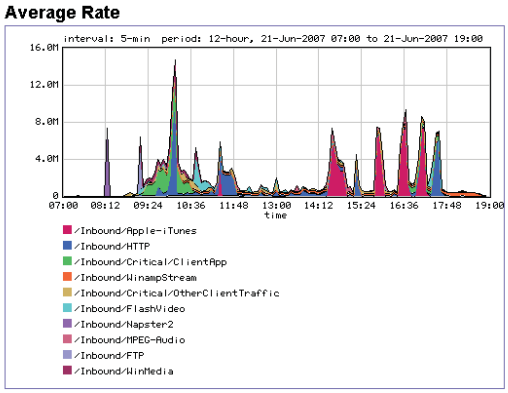
Best Practices –
Monitoring and Controlling Peer-to-Peer (P2P) Applications

The explosion of peer-to-peer (P2P) file sharing has had a significant impact on corporate networks and the business operations that they support. P2P applications provide a highly accessible outlet for downloading or sharing music, video, software, and photos. Because of P2P's accessibility and convenience, sharing large music and video files over high-speed corporate networks has become extremely popular. The resulting bandwidth congestion causes poor application performance. Many of these problems originate from competition among business applications (ERP, CRM), bulk data transfers (database synchs, e-mail, image transfer), and recreational applications (Internet radio, gaming) for bandwidth-constrained links. The addition of aggressive P2P file sharing exacerbates the problem and has led to unpredictable networks that threaten business performance.

Problem: P2P file sharing steals bandwidth that should otherwise be used for business-critical applications. When bandwidth is consumed by P2P applications, the business operations that are tied directly to those critical applications are threatened, or worse, disrupted.



Peer-to-peer applications can consume very large portions of bandwidth, inhibiting critical applications from getting the bandwidth they need to perform efficiently and reliably. Unfortunately, inefficient performance translates to business performance.



P2P Impact: P2P's traffic characteristics are redefining network engineering. Above, a single user consumes the entire inbound bandwidth of a T1 link for a sustained period of time (even while that user is away from their desk). This peak rate analysis is crucial in determining when critical applications perform poorly, or not at all.

File-Sharing Applications	
Operation	**Characteristics**
Search for "peers"	• Large amounts of ping-like traffic indicate P2P applications searching for visible peers or content server nodes.
Search for files	• Large numbers (hundreds) of simultaneous connections widen search for files to download.
Upload and download	• 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	• 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 an downloads. • The more bandwidth you have, the more attractive your network is to P2P applications.

P2P's Network Impact — Redefining the Rules of Traffic Engineering

Although many IT managers may know that P2P applications are on their network, they are usually unaware of the extent. It's no wonder that many are surprised to learn that P2P applications can consume 60 to 70 percent of their WAN and Internet service links. Because many organizations consolidate Internet access at a couple of main sites and provide access through their corporate WANs, P2P's disruptive impact extends throughout the network.

P2P applications are very aggressive and burst to consume large amounts of WAN and Internet bandwidth. To swap files efficiently, P2P 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. After all, P2P applications are not the only applications running on the network. Mission-critical applications run over those same WAN and Internet links.

Congestion from P2P crowds out business-critical systems that are sensitive to delay (latency) such as ERP applications, CRM systems, supply chain management (SCM), and thin-client technologies (Citrix®, Winterm). 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 (e-mail, image transfers, database synchronization, and backup) are vulnerable to bandwidth contention.

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).

P2P: Rethinking Traffic Engineering				
	P2P	**P2P Supernode**	**Web Surfing**	**Query to CRM Database**
Time	Constant. P2P searches find dozens of files and allow users to run downloads (and uploads) unattended over hours and days.	Constant. Unattended user downloads, plus extraordinary traffic of other peers loading files (uploading) from the supernode.	Periodic, user attended usage. Usually involves periods where many pages accessed, but limited by time of user.	Periodic, user attended query usage. Frequency and duration mirrors customer service workflow.
Number of Flows	Hundreds of simultaneous flows, searching for files to download.	Thousands of flows, as it searches and is searched for files.	One to several flows (1-4) for a typical Web page accessing different objects/components from different places.	One or a few, depending on data structures.
Bandwidth Usage	Intense bandwidth usage. Applications burst to consume large amounts of bandwidth. Aggressive behavior devours resources, often 60-80 percent of network link with multiple users.	Because of large amounts of download and upload traffic, even more bandwidth-intensive and aggressive than normal P2P client. Applications burst to consume bandwidth, in both directions.	Medium usage, very irregular. Page downloads are bursty, but last for a short duration. Heavy use of high content sites with numerous users becomes problematic.	Low to medium bandwidth usage, depending on amounts of data downloaded. Frequency and duration mirrors customer service workflow. Web-based applications require more bandwidth (sending of UI).
Latency Sensitivity	Not latency-sensitive. Bulk data transfers over time, allow for latency.	Not latency-sensitive. Bulk data transfers over time, allow for latency.	Medium sensitivity to delay. Users desire response times of a few seconds, but non-business nature makes delay more tolerable (to the business, maybe not the user).	High sensitivity to latency (packet delay measured in milliseconds). Responses to customers and productivity are tied to fast response.

Users acting as "servers" generate large amounts of outbound traffic — whether they realize it or not.

P2P users act as content servers. Other users can continue to search and download files from peers, whether the user is aware of the activity or not. 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.

The Challenge of Identifying P2P on the Network

Many network managers and directors have an idea that P2P applications are running on their network, but they usually do not have the tools to see them nor understand the impact on network performance. This is because P2P applications are very elusive – they hop ports and masquerade as other traffic (such as FTP, HTTP, and others). This inherent trait represents P2P's defense mechanism, enabling the applications to avoid detection by firewalls, routers, and filters.

Adding bandwidth: Reward P2P, Punish Critical Applications

- Ignorance is not a pretty word, nor is it a best practice. Companies often do not know that they have P2P traffic on their network; they just know that critical applications are slowing down or not performing at all. Their traditional monitoring tools are not intelligent enough to find P2P traffic (and certainly can't fix it).
- Adding bandwidth is often the default reaction to attempt to provide resources to improve performance of critical applications. It is a high cost, recurring operation 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. 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.

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 P2P traffic accurately.

How Can I Control P2P?

Packeteer Best Practices — Control P2P and Fix Performance of Important Applications

Organizations' philosophies on how the network can be used, and, thus, how P2P 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's job to communicate network usage policies to employees and other users. 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's Layer 7 Plus classification and analysis capabilities provide the application-level intelligence necessary for identifying and tracking P2P on your network. Packeteer measure bandwidth utilization and its impact on business-critical applications and 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.

Thousands of customers worldwide use Packeteer to protect the performance of their mission-critical applications and ensure that WAN and Internet usage is aligned with their business objectives. 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.

Approach	Best Practice Implementation
Discovery & Analysis	**Approach**: Find out if P2P is on the network and how it impacts the performance of business applications using a combination of signature and behavioral classification techniques. Discovery and Analysis is usually a "phase" in the adoption of additional traffic management techniques, rather than a sustained approach. Once P2P's impact is understood, organizations can advance quickly to a control-based approach. **Implementation**: Packeteer discovers hundreds of applications automatically by leveraging special Layer 7 signature and behavioral techniques. After installing PacketShaper or iShaper and providing basic IP configuration (both products operate as an inline bridge, transparent to the router and application infrastructure), simply enable AutoDiscovery to identify and analyze all traffic on the network.
P2P Containment	**Approach**: Limit bandwidth used by P2P. Set specific bandwidth maximums (i.e. partitions). By containing the amount of bandwidth that recreational file sharing consumes, you eliminate P2P's impact on your critical applications. For unauthorized P2P traffic a very Z small partition will frustrate users and discourage P2P traffic. Users will refrain from complaining — after all why would they complain openly about poor performance of unauthorized traffic? **Implementation**: Using PacketShaper or iShaper, create a P2P partition with a maximum of 20Kbps or 5-10 percent of your network bandwidth. Move your P2P traffic classes into that folder. **Note: PacketShaper and iShaper control traffic bi-directionally, providing control over inbound traffic flows before they hit your router, ensuring bandwidth is available to other applications. **Why not block?** Although PacketShaper or iShaper can be used to block P2P, it's not a suggested best practice. Blocking P2P often results in helpdesk calls because users perceive that the network is down. In addition, blockage 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.
Critical Application Protection	**Approach**: You can ensure bandwidth guarantees with a PacketShaper or iShaper 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). This also protects your network against unknown applications. **Implementation:** Using PacketShaper or iShaper, identify your critical applications and examine their bandwidth utilization, efficiency, and Response Time Management (RTM) statistics. Identify targeted service levels and set a bandwidth minimum for that class (i.e., 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.
Common to All Approaches: **Ongoing Monitoring**	Any best practice involves continually monitoring your network to spot changes in behavior. Employ the PacketShaper or iShaper'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 event configuration facility for updates when important applications or other traffic fall outside of configured performance envelopes. Report results to important stakeholders with onboard reporting.

PACKETEER®

Fast WAN. Fast Apps. Fast Business.

For More Information

If you'd like more information about Packeteer products, consult Packeteer's web site (www.packeteer.com) or call +1.408.873.4400 or +1.800.697.2253.

For detailed information guidance for this and other Best Practice information, see the Packeteer Support site http://www.packeteer.com/support/.

www.packeteer.com

10201 N. De Anza Blvd
Cupertino CA USA 95014
T +1 408.873.4400 F +1 408.873.4410

PACKETEER®