exinda

Controlling Peer-to-Peer and Recreational Internet Traffic

Reclaim Bandwidth for Business-Critical Applications exinda

Controlling Peer-to-Peer and Recreational Internet Traffic

Reclaim Bandwidth for Business-Critical Applications

"On average, 37% of network capacity has been occupied by traffic that is not business-critical."

Aberdeen Group,
"Application Performance Management: Getting IT on the C-Level Agenda",
March 2009

Executive Summary

Recreational use of the Internet at work has far reaching implications for employers in both the private and public sector. Recreational Internet traffic is defined as any type of traffic on the network that is neither directly nor indirectly related to line of business activities. Today's networks are inundated with ever-increasing volumes of recreational traffic generated by peer-to-peer (P2P) file downloads, access to broadband media via sites like YouTube, and repeated visits to popular social networking sites like Facebook®, MySpace and LinkedIn.

Beyond the cost of employees not doing their work, recreational Internet applications drive enormous volumes of traffic over organizations' Internet links. This high volume of traffic increases communication and network operating costs by forcing organizations to upgrade their bandwidth and invest in high capacity WAN. Recreational Internet traffic also increases congestion and competes with legitimate business applications for available bandwidth, creating delays, frustration and lost productivity when employees need to access business applications on the network.

Organizations' networks, already strained to the limit supporting business-critical Web-based applications, are increasingly vulnerable to the adverse effects of recreational traffic. A single bandwidth-hogging employee downloading illegal movies using a P2P application may result in the entire branch office workforce suffering from slow access to their CRM application. Recreational traffic is not merely an IT issue. When we talk about application performance, we're really talking about employee efficiency and overall business performance.

Aside from application delivery and cost issues, organizations may also face moral and legal imperatives to control recreational traffic due its questionable content. The network is an important asset that should not be used for delivering illegal or inappropriate content such as pornography or content that violates copyright laws.

This paper will discuss strategies for controlling a broad range of recreational Internet traffic such as instant messaging, P2P file downloads and social networking activities that can significantly slow business applications and impact employee productivity. By implementing a solution to effectively detect, classify and control recreational traffic, including encrypted P2P traffic designed to slip past corporate firewalls, organizations can improve employee productivity, accelerate application response times, reclaim bandwidth for business-critical applications and defer costly bandwidth upgrades.

Most Common Types of Recreational Internet Traffic

Today’s networks are besieged by a broad range of recreational Internet applications of different types that can siphon bandwidth from legitimate business applications, leading to slow response times and lost productivity. The most common types of recreational traffic passing over the network are outlined below.

Type of Recreational Internet Traffic	Occurrence of Recreational Internet Traffic
Streaming Video	75%
Internet Radio/ Streaming Radio	73%
Instant Messaging	73%
File Sharing (P2P)	63%
Online Gaming	58%

Ashton, Metzler & Associates, *Application Delivery Handbook*, January 2007

Peer-to-Peer File Sharing

The recreational use of peer-to-peer file sharing applications such as BitTorrent, eMule and Limewire to download large files including movies, television episodes, games and MP3 audio files has become a serious problem for businesses and service providers alike. By some accounts, BitTorrent alone is responsible for roughly 27-55% of all Internet traffic depending on geographical location. P2P applications have a way of making legitimate business applications run as if they were in slow motion. Because these greedy applications use as much bandwidth as is available, and because P2P traffic is bi-directional in nature, P2P has been known to cause network crashes that disrupt employees and critical business functions, as well as add to the expense of maintaining the network.

Security is another concern with P2P. Because P2P networks are installed on local client machines and link directly to the Internet, those client machines are vulnerable to abuse that is difficult to control using standard IT security measures. The protocols used by these applications are stealthy, often encrypting themselves or tunneling undetected through open ports. The security risks to businesses are very real. It is estimated that as many as 50% of all programs available for download via a popular file sharing network contained viruses or Trojans that could be used by a hacker to gain control of the user’s computer or network.

As much as network managers may wish to block access to P2P applications altogether, this is not a viable option for most organizations. There are many situations where encrypted peer-to-peer traffic is used for legitimate business purposes such as conference calls hosted on Skype. Because P2P can be put to good use as well as bad, network managers must be able to detect, classify and prioritize this Internet traffic rather than restrict it altogether.

Social Networking

In recent years, the growth in popularity of social networking sites has been phenomenal. Facebook recently announced that it has surpassed 200 million users worldwide, while Twitter, according to Nielson online, has grown 2,565 percent in the last year alone. Hardly a day goes by that we don’t receive several invitations to join LinkedIn or MySpace or get poked on Facebook.

As social networking applications are increasingly used for sharing text, photos, personal profiles, videos and more, their usage has become a serious concern for organizations. Not only do social networking applications distract employees from their tasks, they also negatively impact the performance of critical business applications. Many network managers also have security concerns about the leakage of sensitive data on social networking sites, as well as spam, phishing, viruses and malware attacks originating via these sites and spreading across the network.

Instant Messaging

Popular instant messaging application such as Microsoft Messenger and Skype also contribute to network congestion. Skype, free software that is used extensively for both business and recreational purposes, offering instant messaging, file transfer and video conferencing capabilities, is well known for its ability to circumvent corporate firewalls. Like BitTorrent, Skype is designed to use different network ports and file server IP addresses, making it difficult for firewalls to detect. Skype also employs encryption and a proprietary communication protocol. The fact that Skype is also used as a legitimate business application by many organizations makes it that much more difficult to control because network managers must have the ability to differentiate the good traffic from the bad.

Broadband Media

This class of recreational traffic includes bandwidth-intensive Internet radio, streaming audio and video content and videos accessed on YouTube, which is now the third most visited website in the world according to web monitor Alexa. It is projected that YouTube will attract over 375 million visitors in 2009. YouTube videos in Adobe Flash Video format are not streamed, but rather downloaded and buffered for faster viewing by users. A single YouTube video can consume from 100Kbps to 1 Mbps of bandwidth, causing significant issues for organizations with limited bandwidth. As with Skype, instant messaging and social networking, many companies use YouTube as a no-cost marketing and promotional vehicle. Its use for legitimate business reasons makes it that much more difficult for organizations to block access to YouTube altogether.

Recreational Internet Usage
By the Numbers

According to a survey conducted by America Online and Salary.com, employers spend $759 billion per year on salaries for which real work is expected, but not actually performed. Web surfing for recreational use was cited as the #1 time waster at work by 44.7 percent of more than 10,000 people polled.

Online Gaming

The popularity of online multiplayer video games has also had an impact on organizations' networks. You may have seen the episode of NBC's hit series "The Office" in which the entire branch office including its manager is engaged in an epic struggle for victory in the World War II game "Call of Duty." The new guy, Jim, explains that what began innocently enough as a team-building exercise has escalated into a deadly serious waste of time for all employees – not to mention a significant drain on network resources.

Deliberately Evasive Applications

The number of different recreational Internet applications that network managers must deal with is significant, and more applications appear on the scene every day. To make matters worse, a large number of these applications are designed specifically to evade detection and slip past corporate firewalls by port hopping or masquerading as legitimate business applications. If a port-hopping application is unable to connect to a remote host on the default port, it will jump to another port and keep trying until it finds an open port through which it can connect. Web proxies are one way that recreational traffic attempts to masquerade as harmless HTTP traffic. The techniques employed by these types of recreational applications to evade detection are growing more and more sophisticated – to the extent that they are rapidly outpacing the efforts of organizations to bring them under control.

Lack of Network Visibility: A Major Issue

As sobering as this picture of P2P and recreational traffic running out of control might seem, in reality, the problem is likely worse than we know. Many organizations have limited or no visibility into the types of applications running on the network.

In many cases, network managers only have insight into the traffic visible to network routers and firewalls. As we have seen above, recreational Internet applications are designed specifically to go undetected by most routers and firewalls. In most cases, routers and firewalls lack the ability to accurately distinguish between business-critical traffic – such as Web-based business applications, off-peak file backups and VoIP – and more trivial recreational Internet traffic.

According to Aberdeen's October 2007 benchmark report, *Optimizing WAN for Application Acceleration*, 47% of all organizations that increased their bandwidth capacity over the last two years did not experience any improvement in application performance.

Many organizations also lack the ability to measure application response times to proactively identify cases where recreational traffic is impeding application performance. According to a survey conducted by the Aberdeen Group in May 2009, 60% of respondents cited the inability to identify performance issues before end-users are impacted as a top application delivery challenge (Source: Aberdeen Group, Application Delivery over the WAN).

When it comes to the explosive growth of recreational traffic, what you can't see can hurt you. Lacking network visibility or the ability to measure application performance, IT departments are often left scrambling to deal with the issue of poorly performing applications as quickly as possible. Some organizations will attempt to solve the problem by simply adding more bandwidth. Unfortunately, throwing more bandwidth at the problem is a temporary, partial and expensive solution.

Another common approach is application acceleration. Organizations will invest in solutions that accelerate everything on the network including unwanted and unproductive recreational traffic. Just like adding more bandwidth, this approach is ultimately shortsighted. While accelerating all traffic, including the good and the bad, may appear to work for a time, eventually the link will be maxed out again and the organization will be back to square one. Greedy P2P applications, for example, will continue to consume all of the additional bandwidth that is made available, eventually squeezing out more important business applications. When an organization invests in an application acceleration solution that accelerates everything, they are, in a sense, spending money to improve the speed of recreational applications and enhance the user experience for those who are using the network for P2P file sharing and other unwanted recreational purposes.

To effectively manage P2P and recreational traffic and reclaim bandwidth for business-critical applications, network managers and administrators require a proven, long-term solution to detect and analyze network traffic and apply network policies to control unwanted traffic.

Recreational Traffic Detection and Control

Modern WAN optimization solutions provide the most effective way to detect and control recreational and P2P traffic on the network. As opposed to firewalls that allow the majority of recreational traffic to pass undetected, WAN optimization solutions use sophisticated Layer 7 application signatures, packet classification, behavior monitoring and advanced heuristics to detect traffic patterns and apply the proper network policies to control them.

The most advanced WAN optimization solutions are capable of accurately detecting, classifying and controlling 98% of encrypted peer-to-peer traffic before it can negatively impact business applications. By extending visibility across the network, a WAN optimization solution allows the network manager to identify thousands of applications. He or she can then set policies to prioritize critical business applications and allocate appropriate bandwidth to them, while blocking or slowing low-priority recreational and P2P traffic.

WAN Optimization Solutions Deliver Enhanced Visibility

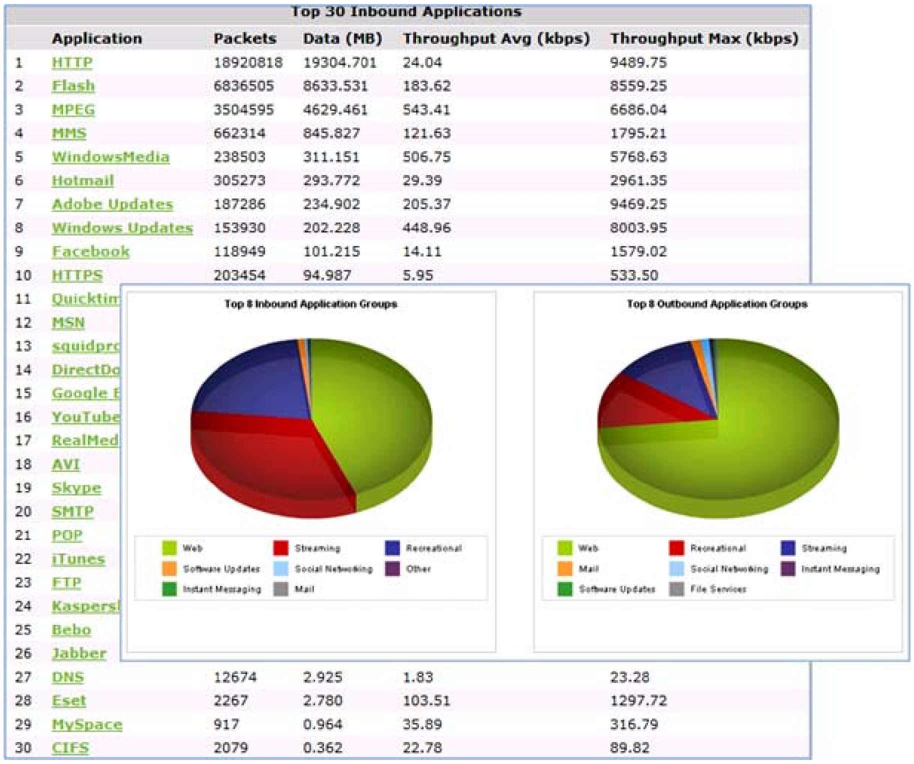
The first step toward effectively controlling recreational and P2P traffic is to understand exactly what is happening on the network. A WAN optimization solution provides deep visibility into network activity, usage and performance, giving network managers the intelligence, knowledge and foresight needed to keep the network and the applications that depend upon it operating at peak performance.

Application visibility allows IT staff to visualize all traffic on the network at the application layer (Layer 7). Using an advanced application classification engine, the WAN optimization solution can identify and classify all peer-to-peer traffic, URLs, applications, Sip call information and more. The Session Initiation Protocol, or SIP, is widely used for VoIP, video conferencing, streaming multimedia distribution, instant messaging and online gaming. At a glance, network managers and administrators can instantly see:

- Top applications for inbound and outbound traffic
- Traffic by user IP address, subnet and/or Microsoft® Active Directory name
- Percentage of bandwidth being used by traffic type
- Top URLs in and out of Internet link

IT staff can drill down to identify recreational traffic including evasive applications, and view bandwidth utilization down to the individual user level through integration with Microsoft Active Directory. Real-time monitoring and historical statistics help IT understand what applications are running on the network and how much bandwidth each application is consuming.

Sample Application Visibility Report



Top 30 Inbound Applications

	Application	Packets	Data (MB)	Throughput Avg (kbps)	Throughput Max (kbps)
1	HTTP	18920818	19304.701	24.04	9489.75
2	Flash	6836505	8633.531	183.62	8559.25
3	MPEG	3504595	4629.461	543.41	6686.04
4	MMS	662314	845.827	121.63	1795.21
5	WindowsMedia	238503	311.151	506.75	5768.63
6	Hotmail	305273	293.772	29.39	2961.35
7	Adobe Updates	187286	234.902	205.37	9469.25
8	Windows Updates	153930	202.228	448.96	8003.95
9	Facebook	118949	101.215	14.11	1579.02
10	HTTPS	203454	94.987	5.95	533.50
11	Quicktim				
12	MSN				
13	squidpro				
14	DirectDo				
15	Google E				
16	YouTube				
17	RealMed				
18	AVI				
19	Skype				
20	SMTP				
21	POP				
22	iTunes				
23	FTP				
24	Kaspersl				
25	Bebo				
26	Jabber				
27	DNS	12674	2.925	1.83	23.28
28	Eset	2267	2.780	103.51	1297.72
29	MySpace	917	0.964	35.89	316.79
30	CIFS	2079	0.362	22.78	89.82

Figure 1 – This graphic detail from a sample report lists out the top inbound and outbound applications on the network. Graphical reports can be automatically emailed in PDF format on a daily basis to key IT personnel or business executives.

Control

It's one thing to be able to see what's happening across the network, and another to be able to actually do something about it. With a modern WAN optimization solution, network managers not only gain visibility into why applications are performing slowly, but they also get advanced control capabilities that allow them to proactively address performance issues such as mis-configurations, congestion and bottlenecks.

Organizations should look for a WAN optimization solution that includes sophisticated controls that allow IT staff to create network polices to prioritize the most critical applications, fair-share network resources, throttle recreational traffic or block some types of unwanted traffic altogether.

Evasive Application Traffic Detection

Many P2P and file sharing applications are evasive. They may mask their behavior on the network or masquerade as other more legitimate applications. Using Layer 7 application signatures, behavior monitoring and advanced heuristics, WAN optimization solutions enable IT staff to detect and control all applications on the network including those that are designed to be evasive.

Policy-based Traffic Management

Organizations can develop policies to precisely control bandwidth availability by limiting or eliminating unwanted network traffic such as P2P or other recreational traffic. In such a way, organizations can prevent low-priority traffic from interfering with the performance of the WAN or impeding response times for critical applications.

Fair Sharing

With this tool, network administrators can easily allocate specific amounts or percentages of bandwidth to individual users, user groups or sub-nets to ensure that no single user or host can monopolize bandwidth.

Adaptive Response

This advanced control mechanism allows IT staff to set policies that allow the network to automatically adapt to changing traffic conditions without requiring manual intervention. This low-touch approach allows network administrators to set alerts, notifications and execute custom scripts that automatically change the behavior of the network based on user-defined events and triggers. If we look at the fair sharing example above, for instance, an adaptive response mechanism could be configured to meter an individual's network usage and automatically throttle his or her bandwidth once the consumption exceeds a set threshold or allotment.

Summing Up

Organizations rely heavily upon their network and applications to drive day-to-day operations and support employees and customers. When recreational traffic is allowed to congest the network and impede the performance of critical applications, productivity suffers and the entire organization may be put at risk. Organizations must find a way to manage recreational network usage so that application performance is preserved without imposing heavy-handed restrictions on users.

WAN optimization technology combined with the detection and suppression of recreational and P2P traffic has proven to be a highly effective solution. WAN optimization solutions allow organizations to see and understand exactly what is happening across the network so IT staff can detect recreational traffic, mis-configured or misbehaving services and users who are consuming more than a reasonable share of the bandwidth. With real-time visibility into network activity and rich historical reporting and trend analysis, network managers can make informed decisions about what traffic to control in order to ensure application performance. Visibility also supports effective capacity planning.

Equipped with a 360-degree view of the network, organizations can apply policies to control unwanted or aggressive recreational and traffic on the network, as well as prioritize bandwidth resources for important business applications. A wise investment in WAN optimization technology will pay large dividends for organizations by ensuring predictable application performance and containing recurring Internet communication costs.

Best Practices for Controlling Recreational Traffic

1. Develop a Network Usage Policy

Technology can only go so far in addressing recreational Internet usage. HR and senior management should work together to develop an Internet usage policy that clearly outlines proper and improper network usage. Clearly communicate this policy to all employees and new hires.

2. Measure Application Response

Put a solution in place to accurately measure application response times and regularly monitor whether application performance is degrading or improving. Measuring application response will allow you to better determine the root cause of poor performance and proactively address the issue before it impacts end users.

3. Limit Recreational Traffic Instead of Locking It Down

Blocking recreational traffic and access to sites like Facebook altogether may have a negative impact on employee morale and erode employee-employer trust. It is generally a better idea to limit recreational traffic in such a way that the needs of the business and the rights of employees are kept in balance.

About Exinda

Exinda is a global provider of WAN optimization and application acceleration products. Exinda has helped over 2,000 organizations worldwide reduce network operating costs and ensure consistent application performance over the WAN. The Exinda Unified Performance Management (UPM) solution encompasses application visibility, control, optimization and intelligent acceleration – all within a single network appliance that is affordable and easy to manage.

Founded in 2002, Exinda is headquartered in Boston, Massachusetts with regional offices in Canada and the United Kingdom. Research and Development is centralized in Melbourne, Australia.

To learn more about Exinda's award-winning solutions for enterprise, education and service provider clients, contact your local reseller or visit www.exinda.com.

exinda

North America
1 877 439 4632

EMEA
0 808 120 1996

Asia Pacific
1 877 439 4632

www.exinda.com