Coping with P2P Applications - Mitigating Bandwidth Consumption on Managed Networks View PDF

Jason Lackey, Riverstone Networks

In the Beginning

It started with Napster, the now defunct MP3 file sharing network. Network managers with various organizations around the world noticed that a large percentage of the traffic on their networks was from Napster, using precious bandwidth, slowing down network performance for everyone. In the wake of various legal issues, Napster went away but the root problem did not.

Enter the Hydra - Kill one Head and Two More Replace It

Kazaa and the various Gnutella clones (Limelight, BearShare et al) introduced the decentralized peer-to-peer (P2P) model. Unlike Napster, these decentralized peer-to-peer systems have a fully distributed network and directory. This makes for a very robust network in that the loss of any one node will not impact other nodes on the network. Unfortunately, it also makes for a very inefficient and chatty network.

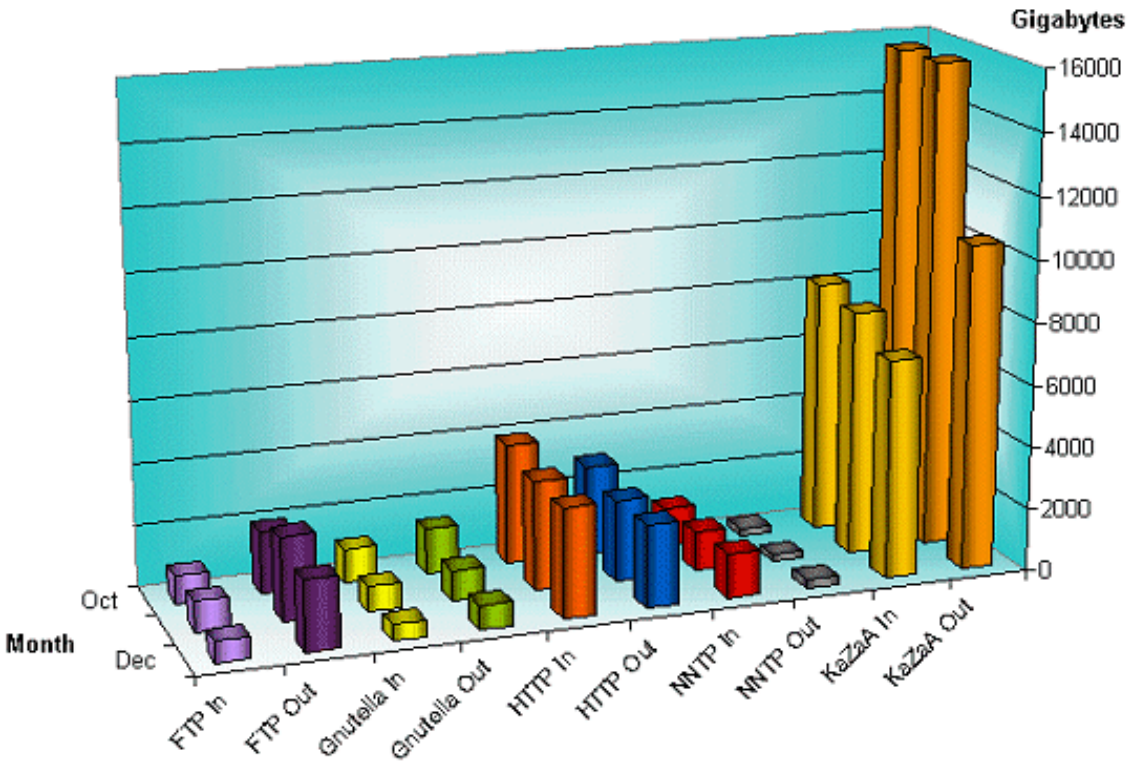

Figure 1: Cornell University Internet Usage by Protocol: Top 5 Protocols, Oct.-Dec. 2001 - Note that KaZaA accounts for more traffic than any other protocol

Analysis of P2P network traffic has shown that P2P overhead (the portion of traffic that is not active user file transfers) can be over 50 percent of the total P2P traffic (Matei Ripeanu, University of Chicago Computer Science Department, http://www.computer.org/proceedings/ p2p/1503/15030099.pdf). Even when not being used by the user these applications are often burning up to 150 kbps just sitting in the task bar.

It gets worse. According to Cornell University, for some organizations, more than 60 percent of total Internet traffic on their network is Kazaa. Other surveys have shown that as much as 30 percent of Internet2 traffic

consists of Kazaa applications (http://darkwing.uoregon.edu/ ~joe/kazaa.html). Reports from the field show that this is a common concern for operators of university and other educational networks. It is clear that these P2P applications are using significant amounts of bandwidth and that network administrators are clearly concerned.

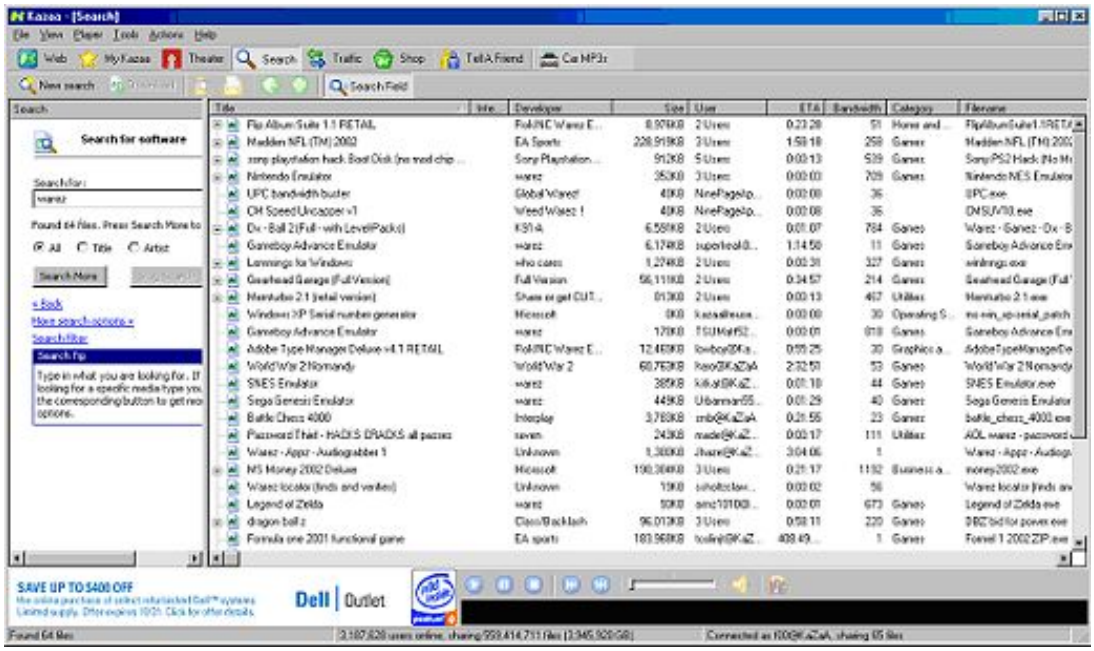

Figure 2: KaZaA Screenshot - This is a list of files available for download. Note that the available bandwidth of the users hosting the various files is visible, encouraging users to target those with fast connections for downloads.

Also, users will tend to connect not with nodes that are closest to them but rather to nodes that have the fastest connection. Kazaa and other P2P applications show the bandwidth of the users who are sharing files. When users download files, they naturally tend to select those files from other users that have fast connections. This means that a user in Norway would download a file from a user in Korea versus a user in Norway if the Korean user had a higher speed connection. Hence, increasing bandwidth in networks already clogged with P2P traffic is akin to trying to put out a fire with a bucket of gasoline, not necessarily a preferred solution.

Super Users and the Tragedy of the Commons - All for Me and None for Thee

Another problem associated with P2P is the Super User. As in most network applications, the top few percent of users often account for the majority of network traffic. In the case of P2P, the Super User phenomenon is amplified by the nature of P2P applications. Super Users have an unusually large number of files in the shared folders on their systems, which are available for other users to download. Users looking for files to download are often connected with these Super Users, who are rewarded increased "participation levels" and are awarded ranks such as "guru" and "deity" depending on how much data they allow their system to upload to the file sharing network.

Kazaa assigns these users with high "participation levels" a higher priority for downloading files, a particularly powerful incentive on crowded networks where downloads are difficult to complete. In essence, Kazaa is encouraging the user to increase bandwidth consumption, which can result in the application running and consuming bandwidth 24x7. In environments where bandwidth is either supplied for free or sold at a fixed monthly rate there is little to no incentive for the individual user to stop such behavior, and plenty of incentive to continue.

Kill the Hydra , Lock it Out or Put a Leash on It?

Now that we have taken a look at the nature of the problem, it is time to explore some solutions. As is the case with many things in life, the most obvious and seemingly easiest solutions are not necessarily the best or most cost effective.

Well Guarded Fortress with Anarchy Inside

The most obvious approach would be to purchase a traffic shaping appliance such as those offered by companies like Packeteer. This approach handles traffic to and from the Internet fairly well, but it does not address traffic on the LAN/MAN. On a large campus or facility it is possible to have significant levels of P2P and other unregulated traffic creating congestion between dorms, barracks or buildings.

Also, adding another device to a network increases costs associated with network management and staff training. Furthermore, installing additional devices into the data path of a network tends to increase latency,

particularly in cases where the device is doing deep packet analysis. There is also the issue of price, as these appliances are not cheap.

This is the well guarded fortress with anarchy inside. The gate between the network and the internet is well guarded, but there are no rules or limits inside. On a small 20-user LAN this is not likely to be a problem, but on a larger network unregulated traffic could create issues in the network backbone or elsewhere.

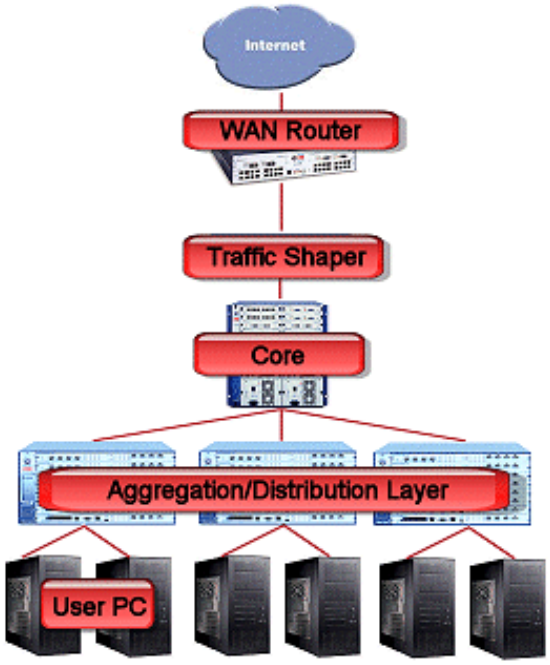

Figure 3: A Traffic Shaper in a Typical Network

Block all P2P Traffic

Riverstone ACLs allow you to grant or deny access to specific IP addresses for all types of traffic or specific traffic types such as FTP, HTTP and even traffic on high numbered ports such as P2P and yet undefined traffic types.

Theoretically, a network operator could set up an ACL (Access Control List) - a line in the router configuration that grants or denies access to or from certain destinations - that will block traffic on Port 1214 (Kazaa) and 6346-7 (Gnutella). This approach, though simple, is rarely effective. First, these P2P clients were built with the understanding that there will be people who will be interested blocking their use. With that in mind, these applications can be configured to work with firewalls or in many cases to use a common port for connections, such as port 80, which is used for web browsing. Second, these are also 3rd party software packages (Kazaahttp - http://www.iprisma.com/kazaahttp/) that enable Kazaa to operate over a standard HTTP proxy (it already supports socks5 proxies). If you are able to completely block such applications, the user community would not benefit from (or tolerate) the loss of this functionality.

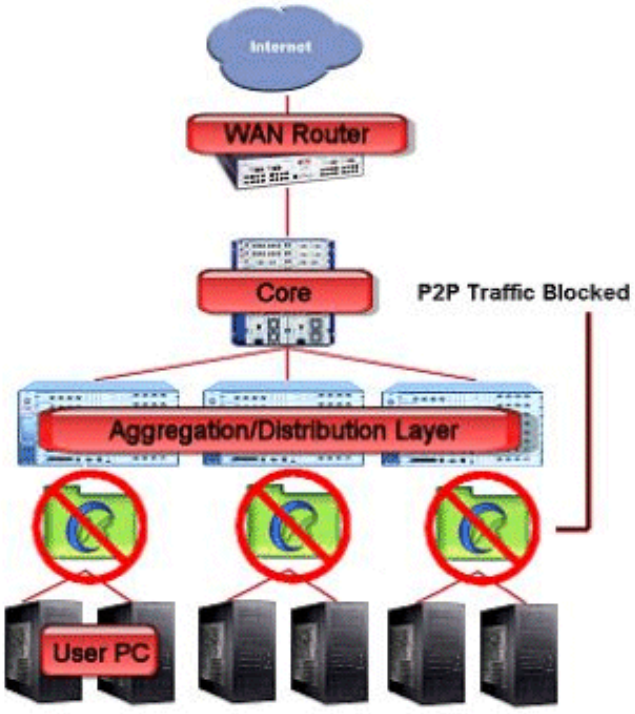

Figure 4: P2P Traffic Blocked by Routers

Rate Limit End User Internet Traffic
For a cost effective and easy-to-implement solution to the P2P problem, network operators can rate limit end-user Internet access. By capping, or rate limiting, both inbound and outbound traffic (these values need not be the same), network administrators can prevent the Super User, who may have a large number of outgoing file transfers, from consuming all available bandwidth while ensuring other network users have ample bandwidth.

This is an easily configurable solution that requires network operators to simply implement blanket rate limits on the customer edge router (the last router between the customer and the Internet). However, like the traffic shaping solutions, this approach does not address traffic within the LAN or campus MAN. It also has the unfortunate limitation of restricting legitimate use of the Internet as limits will remain in place even if nobody else is using the network.

Riverstone's solutions can rate limit and manage traffic with 1-kbps granularity that network operators can limit the bandwidth of problem users, departments, or buildings on both the LAN and WAN side. For more details on Riverstone's rate limiting functionality, please see http://www.riverstonenet.com/technology/rate.shtml.

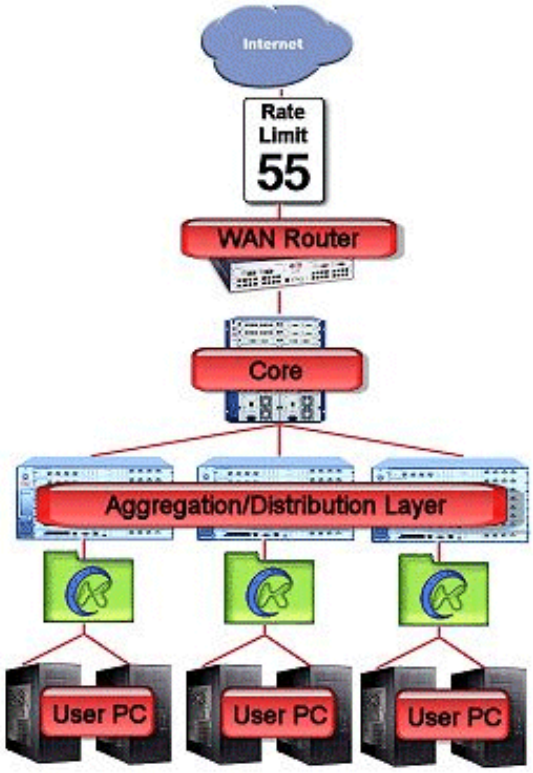

Figure 5: Traffic Controlled by Rate Limits Imposed at the Customer Edge Router

Rate Limit P2P Traffic - A Traffic Cop on Every Corner

The most efficient method for regulating network traffic is to rate limit the offending traffic. In this case, network operators apply rate limits to traffic from any IP address to any IP address on port 1214 and 6346-7 (in the case of Kazaa and Gnutella P2P applications, other applications will likely use other ports. For more details on which port numbers are assigned to which applications, please see the IANA website). Using the Riverstone CLI (Command Line Interface), it is relatively easy to apply this to all ports used to support end users.

Riverstone's GUI-based RapidOS Management Center makes it faster and easier to manage your network. Furthermore, Riverstone equipment interoperates with 3rd party SNMP-based network management systems such as Aprisma Spectrum and HP Openview

With this approach, these applications will still work on their default ports, allowing users to connect and download. The difference is that network operators will be able to control the amount of bandwidth used by these applications and thus minimize the negative impact on the network. To prevent unlimited P2P traffic from causing congestion in the network core, this is best done as close to the user edge of the network as possible.

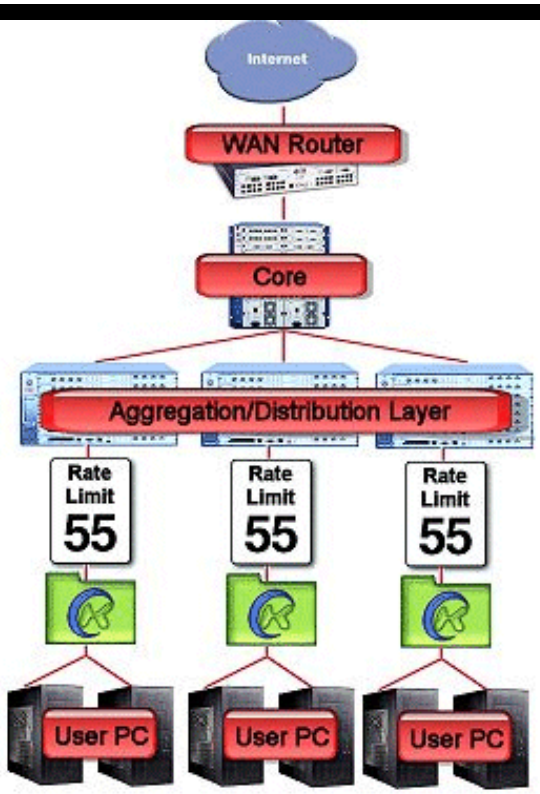

Figure 6: P2P Traffic Controlled by Rate Limits Imposed at the Aggregation/Distribution Layer

Conclusion

With the rise of the post-Napster file sharing systems, network operators are forced to deal with the problems created by P2P networking. The unreasonable demands these applications put on the bandwidth of an organization have a direct impact on both the efficiency and operational costs of managing a network.

Riverstone provides network operators with solutions that can provide many of the benefits of having a dedicated traffic shaping appliance without the additional costs (both capital and operational) associated with having another device in the network. These capabilities are a standard feature on all Riverstone routers and are easily implimented via the company's Command Line Interface. Riverstone's RapidOS Management Center, a comprehensive network management system that provides a full suite of configuration and monitoring tools, provides network operators with a powerful tool for easy activation and management of these features.