ROBERT HASKINS

ISPadmin: traffic shaping

Robert Haskins has been a UNIX system administrator since graduating from the University of Maine with a B.A. in computer science. Robert is employed by Shentel, a fast-growing network services provider based in Edinburg, Virginia. He is lead author of *Slamming Spam: A Guide for System Administrators* (Addison-Wesley, 2005).

rhaskins@usenix.org

IN THIS EDITION OF ISPADMIN, I LOOK at the area commonly referred to as "traffic shaping." Traffic shaping is the process by which network operators manage the somewhat random flow of packets to and from their networks to achieve the desired flow characteristics. Synonyms for "traffic shaping" include "packet shaping," "bandwidth limiting," "rate limiting," and "bandwidth management." These terms (among others) are commonly used in this article and elsewhere.

Some of the traffic flow characteristics a network operator might like to achieve would include the following:

- Adhering to customer service level agreements (SLAs)
- Ensuring fair use of egress bandwidth (commonly referred to as Internet traffic)
- Managing egress bandwidth links so as to not exceed committed and/or purchased data rates and (potentially) associated monetary charges
- Guaranteeing per application level minimum or maximum rates of use

In the enterprise space, traffic shaping is also used, though for different reasons. For example, bandwidth limiting (traffic shaping) can be used in conjunction with a corporate firewall to control access to time-sensitive applications such as Citrix and Remote Desktop. However, an enterprise is unlikely to be using traffic shaping to control peer-to-peer traffic such as BitTorrent, as those applications will normally be banned altogether.

Background

Bandwidth limiting is normally deployed on networks that don't have some other means OF controlLING them. For example, traffic shaping is not normally required on egress networks that are servicing dial-up networks, owing to the slow nature of analog modems. DSL, cable modem customer premises equipment, and/or provider-side equipment normally have a simpler form of traffic shaping built in. As a result, bandwidth limiting is normally only necessary on Ethernet and similar access technologies such as wireless.

Although some service-provider-class wireless equipment does have built-in policy control, most

if not all consumer-grade wireless access devices (which might be in use on university networks) do not. If consumer-grade wireless access devices are in use on the network, packet shaping can be very helpful in limiting abuse.

Wired Ethernet access is often utilized in what are often called MDUs, short for "Multiple Dwelling Units." MDU is telco-speak for apartment and condominium complexes, dormitories, and similar types of building structures.

The boundary between policy enforcement (see my June 2006 ISPadmin column) and bandwidth shaping is a little blurry. The biggest difference would be the level of flexibility bandwidth shaping allows when compared to policy enforcement mechanisms. Typical policy enforcement engines are used for provisioning user connections one by one, but bandwidth-shaping policies can be defined at an aggregate level for all connections. Bandwidth-shaping systems can be controlled by a global policy enforcement engine such as Broadhop. This integration gives the network operator the most flexibility, as IP and bandwidth policy can be set at multiple points on the network.

Although bandwidth shaping cannot help directly with denial-of-service attacks and malware activity, IT can be useful in helping to determine the perpetrator(s), either internal or external. Many solutions allow the network operator to sort connections via bandwidth, flows, and failed flows. In the case of a commercial appliance solution, a GUI facilitates quick access to this information.

What Can Be Shaped, Exactly?

First, we need a word or two about bandwidth limits. It's important to note that bandwidth limits can be "hard" or "soft." In the case of hard limits, the user is strictly limited when the hard limit is reached. With soft limits, so long as another higher priority request isn't outstanding, the user can exceed the preset limit. The types of bandwidth controls can be broken down into three categories:

- Per-user
- Per-application
- Priority-based

Per-application can also be thought of as per-port. For example, email (SMTP) is synonymous with TCP port 25.

PER-USER

It is often desirable to limit each user's bandwidth usage, by itself as well as in conjunction with other applications and/or ports. Also, it would be very useful to have a default per-user bandwidth profile that could be customized if and when necessary.

PER-APPLICATION

One of the biggest bandwidth hogs is peer-to-peer traffic such as BitTorrent or Kazaa. Many commercial bandwidth shapers can identify and limit such traffic based upon the protocol, port, and connection characteristics of the traffic in question. For example, Voice over Internet Protocol (VoIP) traffic can have dedicated bandwidth, so users don't experience voice dropouts and other annoying behavior because of lack of bandwidth.

PRIORITY-BASED

A very strict configuration employed by a university might be to allow peer-to-peer traffic *only* when there is idle bandwidth. In this way, the network operator can allow the "most important" traffic to pass, and the "less important" connections must fight for a smaller share of the connection.

Implementations

There are several ways bandwidth shaping can be implemented, including:

- Routers
- Open source solutions
- Commercial "appliance" devices

Each of these will be examined in the following sections.

ROUTERS

The simplest and potentially cheapest way to implement bandwidth shaping is to activate policy routing on existing routers. Policy routing enables changes to routing tables via general terms. For example, all SMTP traffic could be policy routed to a spam-washing device in your network via policy routing. Both Juniper [1] and Cisco [2] have this functionality built into the core software routing engines. However, the downsides to implementing bandwidth shaping via policy routing are rather significant:

- Routers are not designed or optimized to be packet shapers.
- Implementing packet shaping in routers will likely cause performance degradation.
- Routers will have less packet-shaping functionality than a dedicated bandwidth-limiting device.

One simple way routers could be used to shape traffic via policy routing would be to route "bandwidth hogs" to a slower egress connection. For example, assume a college has two separate egress links to the Internet, one being an DS3 (45 Mbps) and one a T1 (1.5 Mbps). All users and IPs would be initially routed out the DS3 connection and their usage tracked. If a particular user (or IP) exceeded a preset threshold, then that user or IP would be routed out the slower connection until such time as its usage dropped. At that point (or when the user called into the support center and was informed of the reason for the slower connection), the user could be routed back out the faster connection.

The bottom line is that routers are rarely used as bandwidth-management devices except in simple network designs and the most lightly loaded networks. However, they can be used to augment other bandwidth-control mechanisms.

OPEN SOURCE SOLUTIONS

Bandwidth management can be implemented by using one or more open source components. Among the approaches that can be used to achieve this are:

- Squid, iptables, and CBQ (class-based queuing) [3]
- Iproute2 plus iptables [4]
- Snort, iptables/ipchains, and CBQ

One benefit of any open source solution is that you have the ability to tailor it to exacting requirements. A build-it-yourself solution is not for the faint of heart, as it requires deep knowledge of firewalls and routing, as well as the interactions between the two. Also, home-grown solutions require time and testing to be successfully utilized. However, a do-it-yourself deployment may be preferable in certain cases.

COMMERCIAL APPLIANCES

Arguably the most well known commercial bandwidth-controlling device is the Packeteer PacketShaper [5]. According to the company's Web site, the device can control over 500 application types. Packeteer manufactures a number of models, ranging from a low end of 6,000 flows and 2 Mbps of traffic to a high end of 1,260,000 flows and 1 Gbps of traffic. Other manufacturers of commercial bandwidth shapers include XRoads Networks [6] and Cymphonics [7].

These devices are usually deployed at the egress points of MDU (and other Ethernet-based customer) networks, so that all customer traffic goes through the device. This enables the shaper device to control all traffic to and from the network in question.

Issues

One big issue with bandwidth-management devices is that an appliance device failure could cause the attached MDU network to fail completely. Packeteer has engineered their copper-based devices to automatically pass all traffic if the device should fail. With fiber-optic-media network connections, a fiber bypass device is required. This device would route the photons around the failed appliance automatically.

Another issue with bandwidth-shaping devices surrounds virusES and worms. It is difficult for the bandwidth-shaping device to discern between legitimate user traffic and malware traffic.

Summary

Bandwidth-limiting devices are common features of networks where shared access causes contention for limited Internet egress. IP routing policy systems can be used in conjunction with packet-shaping devices, though they aren't usually used in place of such systems. Bandwidth can be limited on a per-user, per-application, and priority basis and/or a combination of these methods. Some approaches used to shape bandwidth include routers via routing policy, collections of open-source components, and commercial appliances. Problems with bandwidth shaping include planning for device failure and the inability of the device to discern "real" traffic from virus and worm traffic.

I wish to thank Pete Carey and Rik Farrow for their help with this article.

REFERENCES AND FURTHER READING

[1] Juniper QoS chapter in JUNOSe 7.1 documentation:

http://www.juniper.net/techpubs/software/erx/junose71/swconfig-qos/download/parameters-config.pdf.

[2] Cisco Bandwidth Management and Queuing paper: http://www.cisco.com/en/US/tech/tk331/tk336/technologies_design_guide09186a0080237a48.shtml.

[3] Bandwidth Limiting HOWTO: http://www.tldp.org/HOWTO/Bandwidth-Limiting-HOWTO/index.html.

[4] Linux Advanced Routing & Traffic Control HOWTO: http://lartc.org/howto/.

[5] Packeteer Packetshaper: http://www.packeteer.com/products/packetshaper/.

[6] XRoads Networks traffic shaping products: http://www.xroadsnetworks.com/products/EdgeXL.xos.

[7] Cymphonix: http://www.cymphonix.com/.

Basics of traffic shaping: http://cc.uoregon.edu/cnews/winter2002/traffic.html.

SecurityFocus article on traffic shaping: http://www.securityfocus.com/infocus/1285.

Squid proxy home: http://www.squid-cache.org/.

Iptables home: http://www.netfilter.org/.

CBQ.init traffic-based queuing script implementation: https://sourceforge.net/projects/cbqinit.

Iproute2: http://www.policyrouting.org/iproute2.doc.html.

Ipchains: http://people.netfilter.org/~rusty/ipchains/.