

Bandwidth Managers: Going With The Flow

Edwin E. Mier, Vincent J. Battistelli and Alan R. Miner

Bandwidth managers address a common problem, but differ in some key respects, like the ways they control VOIP traffic.

Supply and demand. That's pretty much what bandwidth management is all about. And meeting your users' demands with the meager supply of bandwidth you have, especially your bottleneck WAN links, is what bandwidth managers—and this latest *BCR* Best-In-Test review—are all about.

A bandwidth manager is a specialty network appliance. It plugs into your LAN and keeps a watchful eye on everything coming from and going to the WAN. But it doesn't just watch: When conditions warrant, the device will take aggressive remedial action to ensure that bandwidth is made available to users, servers and traffic types in whatever manner the enterprise network manager specifies.

Our research turned up a half-dozen vendors with products advertised as being able to manage

bandwidth. MierLabs then devised a detailed test methodology, oriented towards managing the bandwidth of a DS3 capacity (44.736-Mbps) WAN link. The methodology was sent out along with an invitation to these vendors, asking them to submit their latest and greatest wares for an open, competitive review for *BCR*.

One vendor's product wasn't yet ready for public scrutiny. Another confided that our test bed's DS3 capacity (see "Testing Bandwidth Managers," p. 34) was applying more traffic and bandwidth than their unit could manage. And one lacked the people and resources to support the testing, which took place in February at MierLabs' main lab facility in central New Jersey.

Three vendors, whose products collectively account for the bulk of this burgeoning marketplace, accepted the challenge:

■ **Allot Communications**, which submitted its AC-302 NetEnforcer. This fixed-configuration model was engineered for tracking and manipulating the full bi-directional bandwidth of a DS3 WAN link.

■ **Packeteer**, which sent us its PacketShaper 4500. Like Allot's unit, the PacketShaper 4500 is also built for handling the full bandwidth of a DS3

Ed Mier is president, Vince Battistelli is VP of operations and Al Miner is VP of technology analysis at MierLabs Inc., a network research and product test center based in Hightstown, NJ, which specializes in IP telephony and network management technologies. They can be reached at 609/371-8100, or by email to: emier@mierlabs.com, vbatt@mierlabs.com or aminer@mierlabs.com

TABLE 1 Best-In-Test Scoring

Category—Weighting	Allot	BCR Best in Test	
		Packeteer	Sitara
Configuration—10% (1)	83	90	75
Traffic-Class/Policy Definition—20% (2)	85	85	85
Policing/Policy Enforcement—30% (3)	85	85	80
Traffic Monitoring, Administration, Reporting—20% (4)	88	85	80
Advanced Features—20% (5)	85	90	77
	85	87	80

(1) Includes: the availability of different price-performance models; scalability; modularity; management access options; redundant and multisite support; and supported interfaces and network topologies.

(2) Includes all the ways that traffic can be isolated for the purposes of bandwidth control (i.e., per IP destination, per IP subnet, by assigned priority, by TOS/DiffServ value, bandwidth guaranteed per-flow, by time-of-day, etc.)

(3) Reflects the system's actual tested ability to enforce the policies we defined and applied.

(4) Includes the effectiveness and efficiency of the user interface, clarity and layout of the management interface; real-time monitoring; and integral capabilities for generating reports.

(5) Unique or special features offered beyond the specific capabilities we evaluated and tested, relevant to bandwidth management and traffic control, whether integral or extra-priced.

TABLE 2 Bandwidth Managers Tested

	Allot	Packeteer	Sitara
Product and version tested	NetEnforcer AC-302, v4.2.4; standalone unit with 20 GB internal hard disk, inserted in-line in LAN; Linux-based	PacketShaper 4500, v6.0 build 39 beta; standalone unit with 40 GB internal hard disk, inserted in-line in LAN; proprietary operating system	QoSWorks Model QWX10000, v2.1.1; standalone unit with 16-GB internal hard disk; inserted in-line in LAN; BSD Unix-based
Price (U.S. List), as tested	\$12,000	\$16,650 per unit	\$25,000 per unit; tested with 2 units
Single unit, or deployed in pairs?	Single unit	Single unit	Max control requires 2 units, on either side of the WAN link
Redundant configuration support	Yes, hot-standby units can be deployed in line; connect via a separate cable, which signals failover; policy changes are distributed automatically	Yes, units can be deployed redundantly; a “master” unit maintains synchronization by distributing policy changes	Yes, hot-standby units can be deployed in line; policies are synchronized manually
Management access	In- or out-of-band (integral out-of-band port); via browser, Java-based; console; Telnet	In- or out-of-band (optional); via browser, Java script based; console, Telnet	In-band only; via browser, Java based (requires JRE 1.3.1 or later; installed automatically if not present); console; Telnet
Other models, scalability	6 models address WAN-link bandwidths from 128 kbps to 155 Mbps; license-key capacity upgrade for low-end models	5 models address WAN-link bandwidths from 128 kbps to 200 Mbps (\$32,000); expansion modules and some software-upgrade options	6 models address WAN-link bandwidths from 384 kbps (\$4,000) to 155 Mbps (\$32,000); units are not upgradable
Options not tested	NetAccountant for report generation, \$3,000; NetBalancer, for server load balancing, \$3,000; Cache-Enforcer, for traffic redirection to cache servers, \$3,000	Report Center v2.0, for centralized data collection and report generation, \$10,000; Policy Center v1.1, for central-site admin of many units, policy distribution and synchronization, \$6,000	QOSDirector v1.6, for central-site admin of many units, \$10,000 to \$75,000, depending on number of units; QOSArray, special high-availability configurations, \$45,000 to \$90,000

WAN connection. Unlike Allot, however, Packeteer’s device has two LAN-expansion module slots, which let it support more diverse topologies—involving, for example, fail-over and DMZ (demilitarized zone) connections.

■ **Sitara Networks**, which provided two of its QoSWorks QWX10000 units. This model is reportedly built for managing up to 100 Mbps of bandwidth, somewhat more than we needed, but the vendor said these were the only units they had available to send us.

Sitara recommends that two of its units, one at either end of a DS3 link, be deployed in cases where lots of Voice over IP (VOIP) traffic needs to be controlled. A single unit is normally adequate for handling Web and other TCP-based client/server traffic, the vendor says. Allot and Packeteer each said they needed just a single unit, and both were tested that way.

After nearly a month of exercising the products in every bandwidth-management scenario we could think of, Allot and Packeteer ended up virtually tied. When it all was over and with all results considered, we concluded Packeteer edged out Allot by a whisker (Table 1). Sitara’s units exhibited some troublesome problems in the testing, which is discussed later.

Table 2 summarizes the products tested. As shown, all three vendors offer a half-dozen other models, which handle WAN bandwidths from 128 kbps up to 155 Mbps—a very high-end WAN environment, typified by an OC-3 packet-over-SONET (POS) link.

Compared to Allot’s \$12,000 NetEnforcer AC-302 and Packeteer’s \$16,650 PacketShaper 4500, higher price, the \$25,000 for Sitara’s QoSWorks 10000 reflects the unit’s 100-Mbps bandwidth-managing capacity. Still, with two units required in many scenarios, versus just one for Allot and Packeteer, Sitara’s costs come out considerably higher.

A basic, but noteworthy, product difference has to do with units of measure employed by different vendors. Allot and Sitara measure, report and manipulate all bandwidth based on packets with LAN Layer-2, or MAC, overhead included. Packeteer, on the other hand, reports and manipulates all bandwidth from Layer-3 and up only. That means that Packeteer’s product sees and handles traffic just in terms of IP bandwidth, and without the additional MAC overhead.

This can make a sizable difference—with a lot of short packets, such as with VOIP, up to a 20 percent difference. We think Packeteer’s IP-level

**The products
were more alike
than different**

Testing Bandwidth Managers

The network environment we created for this test had to support multiple concurrent applications and a broad range of traffic characteristics. The test bed had to consistently re-create complex combinations of VOIP—of varying call duration, composition and protocols—and Web traffic—of varying load levels and between many different browser clients and Web servers.

Our IP infrastructure was built around Extreme Networks' Summit 48i L2/L3 switches. Through VLANs and routing on the Summits, we set-up three IP subnets, which were deployed as two LANs, interconnected by a high-speed IP WAN.

A Hurricane IP Network Emulator from PacketStorm Communications simulated our WAN environments. We defined various WAN link profiles which, once defined to the PacketStorm system, could be readily applied or deactivated via a single mouse click. For most of this testing, the PacketStorm throttled the bandwidth of our simulated IP WAN to appear and behave as a DS3 (44.736-Mbps) link.

A Hammer LoadBlaster 500, from Empirix, generated the bulk of our VOIP traffic. With automated scripts, the Hammer delivered calls of carefully timed frequency and duration, in different directions through our IP LAN/WAN. Other VOIP calls were placed between laptops running softphone applications.

Our HTTP/Web environment featured all real Web traffic, which came from two main tools: one from Ixia, the other from Microsoft.

An Ixia 1600T Traffic Generator/Performance Analyzer, equipped with an eight-port LM100TXS8 module, enabled us to apply high levels of genuine Web/HTTP traffic. The Web traffic module generated up to 12,000 concurrent HTTP connections, more than sufficient to flood the simulated DS3 WAN. We also utilized ports of the system's LM-100TX module to perform latency measurements and determine traffic delay through the three bandwidth managers.

High volumes of client-side Web requests were also generated using Microsoft's Web Application Stress Tool, v1.1, and delivered to a Microsoft IIS Web Server running on a Windows 2000 platform.

A T1-full of calls from the Hammer was processed using H.323-based VOIP gear from Avaya. Running Avaya's MultiVantage control software, an S8700 server handled H.323 call control between two Avaya G600 gateways, each linked via T1s to the Hammer, and headset-equipped, Windows XP-based laptops running Avaya's softphone.

Another T1 load of calls was processed using SIP-based VOIP gear. This was provided by Tangerine, which specializes in enterprise-class SIP call controllers. The SIP proxy server and softswitch, called Tangerine Connect, drove Mediant 2000 gateways from AudioCodes, as well as laptop-to-laptop VOIP calls, which used Microsoft's XP-based SIP stack and Messenger application□

—Edwin E. Mier

perspective is preferable, because LAN-based MAC overhead is in most cases stripped off packets before they are sent out over the WAN. And keeping all traffic in consistent terms of IP layer seems more appropriate for WAN bandwidth management.

There's another notable configuration difference: Allot comes equipped with a built-in LAN port for out-of-band management access. Packeteer requires an optional LAN-expansion module to support out-of-band management access. Sitara does not support out-of-band management access, but it says that it plans to add it soon in an upcoming release.

Out-of-band management lets you access the device via a LAN connection separate from the main traffic flow, which the bandwidth manager is busily analyzing. It's up to the network manager to determine how separate-path LAN connectivity to the out-of-band port is implemented, but we believe having out-of-band access available, whether you use it initially or not, is still a worthwhile plus.

Commonality

Pricing and some configuration differences aside, the products tested are, in general, more alike than different. For example:

■ All three need to be oriented with one end towards the "inside" of the network, where the LAN is, and the other towards the "outside," where the WAN is. The vendors all clearly label which of their devices' 10/100 LAN ports is which.

■ The vendors' products all insert directly "in-line" on a physical LAN link that carries all traffic between the LAN and the WAN. This typically is the LAN link between the WAN router and the nearest LAN switch.

■ If there's an IPSec-based VPN gateway "behind" the router, as many enterprises employ today, it's best to insert the bandwidth manager on the "inside" of the VPN gateway—between the gateway and the switch. That's because traffic on the "outside" of the VPN gateway (towards the WAN) is encrypted above the IP layer. The bandwidth managers we tested all support features for

working in and around VPN gateways, and even across encrypted VPN tunnels. But they do their job best by being able to observe traffic at all layers, unencrypted, which can be done only from the “inside” of the VPN gateway.

■ All the devices are adept at observing, analyzing and automatically categorizing user traffic by application. The vendors all claim their units automatically detect, and can isolate and separately control, the traffic of more than 1,000 known applications and protocols.

■ The bandwidth-managing capacity of these devices is set when they are configured, and is unrelated to their physical 100-Mbps LAN connections. These units “think” in terms of, and apply their bandwidth-management magic based on, the specified amount of WAN-link bandwidth that is further down the line. We had to tell each of them that it was to manage 45 Mbps of bi-directional WAN bandwidth, even though 100 Mbps of LAN traffic could be passing through the box in either direction. We could just as readily have set them to constrain WAN traffic to a maximum of 1.544-Mbps, if we had a T1 link instead of a DS3.

We observed that “specs-manship” and semantics are both out of control when it comes to the bandwidth-manager marketplace. This is most apparent in the capacities the vendors claim for their products, and in their accusations that competitors are not delivering what they claim.

Rather than propagate this noise, we note that all vendors claim their units support many thousands of concurrent “connections,” or many thousands of concurrent “policies” or “classes.” These generally are not valid metrics for selecting from among competing bandwidth managers. When these specs are quoted, we advise users to ask whether the performance claim applies to each direction, or if it is a total for both directions. And get the answer in writing.

How They Work

The job that bandwidth managers do is nothing short of mind-boggling. They can examine each passing packet’s full seven-layer information, and track the conversation that the packet belongs to, as well as calculate and monitor the conversation’s ongoing bandwidth consumption.

At the same time, the bandwidth manager has to determine whether all such conversations are operating within acceptable “class” bandwidth limits. And if not, it must then take seemingly drastic action, depending on its instructions, to bring the traffic flows into compliance.

Now a few words about words: There is little consistency in the bandwidth-manager marketplace in the use of terms. Take, for example, the chunk of virtual bandwidth that is allocated to a particular traffic type. Packeteer calls this a “partition.” Allot calls it a “pipe.” Similarly, the bandwidth that’s left over after all class allocations

have been made, is called “default” bandwidth by Packeteer, and “fallback” bandwidth by Allot.

And on it goes. The process of actively managing bandwidth allocation is called “shaping” by some, and “enforcement” or “policing” by others. We will call it bandwidth management.

Now what do you call a discrete conversation between two communicating network end-points? Vendors alternately call this a “flow,” a “connection,” a “stream” and/or a “session.” Indeed, with some protocols and applications, the terms might seem synonymous.

That’s not always the case, however. A “connection” can imply just the packets associated with establishing the initial logical link between end-points, like the three-step TCP connection that precedes a Web transaction. A “flow,” on the other hand, entails the packets that actually convey content between two end-points, but may not also entail the packets that set up and close the underlying “connection.”

Richard V. Ford, a product manager with Packeteer, maintains that a “flow” is appreciably different than a “session,” especially with regards to VOIP traffic. With Web traffic, a straightforward exchange moves Web pages and elements directly between a client browser and a Web server. But VOIP involves two or more third-party dialogues to first set up the actual VOIP connection. Then direct “flows,” in the form of RTP streams, carry the actual encoded voice content between the communicating VOIP end-points. All of this is a “session,” according to Ford.

For consistency, we will refer to all the traffic associated with a dynamic network conversation as a “session,” including all the underlying connection set-up as well as the actual information-transfer flow(s).


Gotta Have Class

Any particular traffic type that a bandwidth manager can identify and isolate is called a “class.” And the class is the basis for assigning and controlling bandwidth. This is one of the few terms the vendors generally agree on.

But a class can take many different forms. In our methodology, we considered many different ways of defining traffic types—one class, for example, containing all the Web traffic to and from a particular Web server, and another comprising all VOIP traffic using G.729 encoding.

Then we set out to see which and how many of these classes the bandwidth managers could “classify,” and then apply bandwidth control. Some of the traffic types and the products’ ability to successfully classify and separately bandwidth-manage them are shown in Table 3, p. 36.

We uncovered some differences, but they were fairly minor. For the most part, the products’ abilities to classify traffic types—by VLAN tag, by TOS/DiffServ value, by HTTP versus VOIP, by destination IP address, by IP subnet, by UDP port



Make sure to pin the vendor down on capacity claims

Managing the Web traffic is well understood

range, and so on—were fairly equivalent overall. And for this reason we rated all of them the same, 85 out of 100, in this category.

Controlling Web Traffic

For HTTP Web traffic, the products all did a consistently impressive job of implementing the various classes and then effectively applying bandwidth control. This is in large part because the Web protocols, HTTP and the underlying TCP, are straightforward, well understood and, from a connection and bandwidth-control perspective, readily controllable.

Traffic such as TCP-based Web traffic is readily controlled in several ways and the network manager selects which of these methods the bandwidth manager will use. If the prescribed amount of bandwidth for a Web-traffic class is exceeded, the bandwidth manager can:

- a.) Yank some packets out of the existing Web sessions (some clients will retransmit the dropped packets, others will timeout); or
- b.) Drop all packets for new Web requests (no new connections will be set up, but existing ones won't be bothered); or
- c.) Drop some existing connections. The bandwidth manager typically will send TCP reset commands to some clients, and their TCP connections will summarily drop; or
- d.) Consider new Web connection attempts as "burst-able." This means give the new connections a "best-effort" connection, tapping available bandwidth from elsewhere, such as unused but sharable bandwidth that is earmarked for other classes.

All the products tested support all these options for HTTP Web traffic, although their terminologies for the control processes varied widely. And for this portion of the testing, we would have

TABLE 3 Job Performance (1)

	Allot	Packeteer	Sitara
Traffic isolation/control by VLAN tag	✓	✓	✓
Traffic isolation/control by IP source/destination address, IP subnet, UDP/TCP ports and port ranges	✓	✓	✓
Traffic isolation/control by TOS/DiffServ values	✓	✓	✓
Traffic isolation/control by IP protocol/application	✓	✓	✓
Traffic isolation/control by Web URL	✓	✓	Limited
Traffic isolation/control by VOIP call control (H.323)	Limited	✓	No
Traffic isolation/control by VOIP RTP streams	✓	✓	✓
Traffic isolation/control by VOIP codec (H.323 G.729)	Limited	No	✓
Preserving maximum bandwidth by application: Web/HTTP and VOIP (H.323)	Limited	✓	Limited
Special facilities for VPN traffic handling	✓	✓	✓
Time-of-day, day-of-week policy application (scheduling)	Limited	Limited	✓
Guarantee bandwidth to/from a specific Web Server	✓	✓	✓
Constrain maximum number of concurrent connections to a Web server	✓	✓	No
Constrain VOIP traffic to a maximum of 10 concurrent SIP VOIP calls (employing silence suppression/VAD)	✓	No	No
Preserve maximum-bandwidth limits concurrently for different classes: Web and VOIP (H.323 and SIP)	✓	✓	✓
Issue alarm when VOIP latency exceeds threshold	No	No	No
Maximum latency added by bandwidth manager	Under 1 ms	Under 1 ms	Under 1 ms
Reject all Web connection attempts by a specific client	✓	✓	No
Preserve VOIP call integrity against heavy Web loads, using prioritization	✓	✓	✓
Effectively resolves multiple, overlapping policies	✓	Limited	Limited
Can monitor traffic by user, link, class, application in real-time	✓	✓	✓
Report number of currently active VOIP sessions	✓	Limited	No
Report VOIP call set-up time	No	Limited	No
Long-term trend monitoring and reports (specifically, report bandwidth by IP address for the last hour)	✓	✓	✓
Report latency and jitter for VOIP traffic	No	No	No
Alarm/event thresholding, logging; issue SNMP trap	✓	✓	✓

(1) A checkmark (✓) indicates the system successfully accomplished the task(s).

"Limited" indicates that one or more issues precluded the task from being fully and clearly accomplished. In most cases this was due to set-up complexity and/or incomplete, unclear or inaccurate results.

A "No" means the task could not be successfully accomplished.

awarded them similar scores. But VOIP control was different.

VOIP—More Than One Way

The products had all recently been upgraded to bolster their ability to classify and control VOIP traffic. We found Packeteer's and Allot's capabilities in this regard fairly equivalent, but Sitara exhibited some problems.

There are a number of ways the product can control VOIP traffic:

- If the bandwidth manager understands the high-level VOIP call-control protocol, it can readily—and elegantly—constrain calls and thereby regulate the bandwidth that VOIP uses. We employed both SIP and H.323 for control of the VOIP used in our test bed.

- To preserve VOIP traffic, and protect it from other traffic types, a higher priority value can be assigned to VOIP than all other traffic; theoretically, VOIP packets will be sent ahead of all other traffic types with a lower priority. Allot uses a 1 to 10 priority scale, with 10 as the highest; Packeteer uses 0 to 7, with 7 as the highest; Sitara avoids numbers completely and uses five levels: Very Low, Low, Medium, High and Very High.

- You can specify how much bandwidth each VOIP "session" is to get, on a guaranteed basis, and how much overall bandwidth the whole VOIP class gets. This means that, after all allowed guaranteed slots are filled, the bandwidth manager has to take action. If the bandwidth manager can't properly speak the VOIP call-control language, it must then apply one of the control measures previously listed for paring down Web/HTTP traffic. Again, it is up to the administrator which action is taken.

One mechanism that absolutely does not work for throttling VOIP is the first Web option, where packets are yanked out of the existing VOIP calls. If you are lucky this will only degrade the VOIP voice quality. In many cases, though, it will cause the VOIP calls to drop.

Several of our test tasks involved limiting the amount of bandwidth that VOIP uses. And the vendors' performance here was more varied. In today's networks, however, bandwidth managers are being asked more to preserve or protect VOIP traffic, in essence making sure that VOIP gets a higher QOS treatment than all other traffic.

Handling VOIP

Packeteer did a wonderful job of protecting and preserving VOIP traffic, and so did Allot.

The release of Sitara software we tested exhibited two problems with handling VOIP. The vendor recently added a high-level H.323 capability, but problems with this new code prevented it from

properly throttling H.323 traffic. Too many calls were dropped, and new calls, seeking to reuse the bandwidth of calls that closed or were dropped, did not set up properly. A second problem related to controlling traffic on a per-session basis. The system could constrain VOIP calls within a prescribed amount of bandwidth, but it could not properly assure guaranteed bandwidth on a per-call (per-session) basis.

Sitara informed us after the testing that its engineers had found and fixed both problems. The vendor says that it will be shipping a new release of its software, with the fixes, before this article is published.

Packeteer's software can spot H.323 and SIP call-control protocol traffic, and can treat these as separate traffic classes. But it cannot now use the SIP call-control protocol to elegantly close or control SIP calls.

Packeteer had a hard time regulating the number of concurrent SIP calls for another reason, too. Our SIP calls employed silence suppression (also called VAD, or voice activity detection), and that caused the per-call bandwidth to vary considerably,

from a high point when the call first sets up, to a much lower bandwidth level as packets carrying the inherent silence in the speech stream are eliminated. The Packet-Shaper sought to control the number of SIP calls by

applying and enforcing a constant and consistent per-flow bandwidth, which the administrator specifies. In this case, though, with the calls' varying and diminishing bandwidth, far too many SIP calls would be allowed.

Allot also had recently added H.323 protocol recognition to its software, and it was able to throttle H.323 calls by issuing reset commands to callers when there wasn't sufficient bandwidth for new H.323 calls. This is easier to do with H.323 than SIP, because H.323 call control runs over TCP, as does Web/HTTP traffic, while SIP call control usually runs over the connectionless UDP protocol.

Allot fared well in our test for controlling SIP traffic via its per-session "admission control." It is able to limit the maximum number of sessions in the class, but without having to fix the upper limit of bandwidth for each session. All things considered, Allot offered the best combination of controls for VOIP handling, and especially H.323, of the products tested.

In light of these and all the other results relating to bandwidth control and policy enforcement, we rated Allot's and Packeteer's actual policy-enforcement capabilities the same, 85 out of 100. While Allot has the edge in terms of constraining SIP traffic, Packeteer offers some better enforcement capabilities. For example, it cleanly and

Packeteer and Allot did best at handling VOIP traffic



Advanced features include reporting, security and Web-caching capabilities

accurately protects all VOIP traffic using just a “high-priority” designation—designating all VOIP a “6” and everything else a “3.” Sitara received an 80 in this category.

User Interface

While their functions and capabilities are fairly similar, the user interfaces for driving these products are quite different. We felt that Allot offers the most effective user interface of the products tested, with clear and clean displays, and a nearly intuitive organization and layout. We especially liked the consolidated, single-screen, Policy Editor display.

Sitara’s interface was also simplistic, but we felt that setting up a policy was more circuitous and tedious than it has to be. There are three disjointed processes—defining the class, building filters and then applying the policy. It’s easy to get lost, especially when you have to replicate the process to put the same policy on a second unit.

Packeteer’s interface also is fairly compact and consolidated. However, all classes and policies are replicated between one direction, at the top of the main screen, and the other direction, which you must always scroll down to find. Invariably, anything that you do or apply for a class in one direction you then have to scroll down and completely repeat for the other direction. It is a tedious process, prone to error.

Another lament with Packeteer’s interface is that a lot of what we needed to do could not be done via the regular user interface, and instead required using the vendor’s arcane command line. The problem was not just the cryptic command syntax, but the fact that the GUI showed no record of the processes we had invoked via the command line. These are easily forgotten, and their running quietly in background can affect the stability of the rest of the system.

With all other administrative issues considered, including real-time monitoring and reporting capabilities that are included with the system, we rated Allot 88, Packeteer 85 and Sitara 80 in this category.

Advanced Features

Our test methodology defined many specific tasks, which addressed many of the features and functionality involving bandwidth management. But each of the products also offers some special and unique capabilities and options, which enhance the value of the overall package.

Packeteer emerged ahead of its competitors in this regard. It has, for example, an integral feature for automatically collecting traffic-class information from routers via SNMP, about ATM and frame relay links, and incorporating these as traffic classes into the PacketShaper. It also offers an optional Report Center, which provides a centralized platform with database for collecting data in XML format from many PacketShapers, and pre-

senting the data in consolidated reports. The PacketShaper also supports full remote access to all traffic data via SNMP and its private MIB.

One of Allot’s most impressive advanced features is denial-of-service attack mitigation. The system incorporates a number of automated processes under the covers, which can significantly abate the effects of a denial-of-service attack. The user only really needs to set the maximum number of allowed concurrent connections and the maximum rate of new connections per second. Other notable advanced features of the Allot product package include optional Web-server load-balancing software, and optional cache-server redirection software.

Sitara offers a leaner set of advanced and optional features. A noteworthy one, however, is a native, integral Web-cache capability. Frequently accessed Web content is stored right on the QoS-Works 10000; users can then retrieve these pages much faster, while reducing the WAN bandwidth consumed. Like Packeteer, Sitara also offers full, private MIB-based SNMP access to its traffic classes and statistics.

Conclusion

Bandwidth management works. The ability—of all three products tested to automatically analyze, classify and then, in real-time, manipulate connections and bandwidth, is impressive.

Fully two-thirds to three-fourths of the tasks we defined and applied for this review were performed successfully, and to the same functional degree by all the products tested. The areas that distinguish the products are in their handling of VOIP traffic and advanced features.

Allot and Packeteer performed surprisingly well in their ability to safeguard and protect VOIP traffic, and nearly as well in controlling and constraining VOIP traffic. With the insertion of a single unit in the network, these boxes can virtually assure that VOIP call quality enjoys high end-to-end quality of service protection□

Companies Mentioned In This Article

- Allot (www.allot.com)
- AudioCodes (www.audiocodes.com)
- Avaya (www.avaya.com)
- Empirix (www.empirix.com)
- Extreme Networks’ (www.extremenetworks.com)
- Ixia (www.ixiacom.com)
- Microsoft (www.microsoft.com)
- Packeteer (www.packeteer.com)
- PacketStorm Communications (www.packetstorm.com)
- Sitara Networks (www.sitaranetworks.com)
- Tangerine (www.tangerineinc.com)