

## Flow-Oriented Management – The Next Level of Management

Net Forecasts – Peter J. Sevcik

BCR Volume 33, Number 5

May 2003

Every enterprise has at least one IT management system. It starts with buying management software for each major device, and then a management platform is needed to act as a common server for all the software. Eventually, the number of data elements in the database becomes unwieldy, and a manager-of-managers is brought in to integrate the various views. When the number of alarms becomes overwhelming, an event-correlation engine is needed to filter down to the few events that require immediate attention.

This evolution has led to a classic "stove pipe" approach to managing the IT infrastructure. The good news is that it has proven adaptable; tools are selected and deployed to match the organization chart of the company.

### **The Sum of the Parts is Flawed**

But the stovepipe approach has other byproducts as well. It assumes that if you can keep all the elements working well on their own, the result will be universal wellness of the whole. It's the network equivalent of "all boats are raised by the rising tide." It implies that the sum of the parts (subsystems) creates a properly operating total, and here is where it breaks down, particularly from a performance perspective.

To begin with, not all business applications are created equal; some generate revenue or save lives, others are merely "nice to have" or, at worse, waste resources. Without understanding the application flows and which devices the apps use, managers have no way to focus on the proper subset of devices. This result is often a "fire-drill" approach to problem solving; all the experts in the company are told to do *something*. And, following human nature, most experts usually report that it is not *their* problem, so it keeps recurring.

Second, real systems operate differently from the plan. All too often, management information about devices creates a sense that all's well, when that's far from the actual case. Consider the following real-world examples:

The sinking supply chain: A manufacturer's supply-chain management system worked well, but since SSL access to critical resources was being provided to more than 300 suppliers, security became a concern. The security group re-routed all connections through a new SSL proxy server and, to be extra secure, the TCP connections supporting SSL were terminated after each element transfer to avoid keeping any state information around. Introducing the proxy caused round-trip times across the Internet to mushroom five-fold, and users complained mightily. All the while, however, the device management systems were reporting proper operations, with no bottlenecks.

Waiting for Order Entry: A European company's key customers use a Web-based application to order parts and supplies via the Internet. The largest customer group, located in Asia, was experiencing terrible performance, even though all systems were reporting light loads and fast response. The culprit: Despite using three carriers for multihomed connections to the Internet, all traffic had to travel two-thirds of the way around the world through the U.S.

Missing the Forest for the Trees: A global financial services firm had a chronic performance problem between their New York and London offices. Months of finger pointing produced nothing, and the device management systems continued to report that the routers were healthy and operating normally. But the tools could only see individual hops; there was no way to correlate end-to-end performance of network flows with the physical routes. The finger pointing finally stopped – and performance improved – when they located a particular route-configuration anomaly

Name that Tune: A firm running a financial information portal believed business was great. The hosting company told them that traffic on the site was growing at 35 percent per month and it was time to upgrade bandwidth. It turned out that legitimate users of the site were setting up various information exchanges, and all the traffic growth was coming from a peer-to-peer music exchange.

When Old is New: A telemarketer came up with a new, better application for generating revenue. While the old application was much simpler and ran faster, it did not produce results. One day, for no apparent reason, the old application started up and was running concurrently with the new. Both operated from the same customer database, but the old app operated faster, and so it consumed most of the resources. Customers were inundated with solicitations but sales dropped. Since the network couldn't distinguish between the old and new flows, there were no problems to be found.

Permanent Back-Up: A cellular phone company had a T1 running to each of its 500 retail stores, and each T1 was backed-up with ISDN dial circuits. When the error rate on a T1 would climb past a threshold, the ISDN would take over and the router would operate with little interruption in service. The ISDN connections were slow and costly, but transferring back to the T1 required manual intervention. When the office managers would review their telecom bills, they'd find that the ISDN back-up mode was running most of the month. Reports from the data center, however, would show all the routers were highly available.

Light Load, Big Impact: A regional airline was having chronic problems with one circuit, but this wasn't considered serious, because the circuit was lightly loaded, and the routers dynamically found paths around it. But it turned out that one of airline's most critical, revenue-generating applications was producing the traffic, and whenever the circuit went down and transactions slowed, business and customer satisfaction dropped.

#### **Follow the Bits**

So, what's the lesson? There are several, but the first is that business applications create distinct flows of traffic, which must be discovered, measured, managed and diagnosed to maintain a proper service level.

In the examples described above, traffic was flowing over paths that were not planned or extra traffic was being generated. And even though all the system elements were operating "correctly," a flow change, however slight, created ripple effects that added burdens on the application – more traffic or longer network paths. This extra work – useless

application turns or slow transit devices – are extremely difficult to find, because they appear as legitimate traffic. Discovering these time sinks requires knowing a transaction's precise path, and how much time is spent at every station along that path. That's not what traditional device managers are designed to do.

To some extent, the industry is a prisoner of its own success. We know how to design around many of the "gotchas," so systems rarely experience a hard failure. But our management systems are somewhat analogous to our medical system: The focus is on treating people who are already ill, often seriously, instead of on recognizing the little things that indicate that a problem is either likely or building. If we either ignore or don't see chronically poor performance, we're exposed to major disaster down the road.

#### **Flow Management – The Next Generation**

The good news is that some firms are starting to supply tools that address this problem. Open Service and Fidelia gather data from devices, subsystems or their managers, and correlate the information into clear flows that are matched to business functions. Open Service also adds security analysis to the performance management picture.

ProactiveNet and Quantiva also gather a lot of information from devices, but add real-time measurements from the Internet. ProactiveNet can integrate live feeds from Keynote Systems or Gomez, while Quantiva operates its own measurement agents, including critical performance data from customer desktops. ProactiveNet automatically baselines performance to create "zones of proper performance," and then it correlates deviations from these zones. This approach is well suited to find true performance problems.

NetScout and Concord Communications are more traditional traffic and device-load measurement companies, but they've adapted their tools for flow management. They can generate data on flows that can help to diagnose performance issues at the application level.

Network Physics has developed a unique measurement system that gathers data on all packets as they traverse a system – from server

through switches and onto the Internet. Network Physics keeps track of all flows automatically discovered through tracking the pattern of TCP connections, and can determine performance behavior across the Internet for each flow. It is the leader in supplying precise flow details.

### **Conclusion**

These flow-based management tools are the next step in managing complex and robust systems. However, to really succeed, we need standards. The industry needs to converge on one definition of flow statistics from routers (currently there are three: Cisco, Extreme and Juniper). Then we need to support the Open Group's QOS Task Force initiative on application quality and resource management standards. Finally, the business function standards coming from the Business Process Management Initiative (BPMI) should be used as high-level definitions of traffic flows. It is time to move flow management out of the realm of an interesting conversation among vendors, and into a meaningful industry model that can take IT management to the next level of sophistication.

### Companies Mentioned

Business Process Management Initiative  
([www.bpmi.org](http://www.bpmi.org))  
Concord Communications ([www.concord.com](http://www.concord.com))  
Fidelia ([www.fidelia.com](http://www.fidelia.com))  
NetScout ([www.netscout.com](http://www.netscout.com))  
Network Physics ([www.networkphysics.com](http://www.networkphysics.com))  
Open Service ([www.open.com](http://www.open.com))  
ProactiveNet ([www.proactivenet.com](http://www.proactivenet.com))  
Quantiva ([www.quantiva.com](http://www.quantiva.com))  
The Open Group ([www.opengroup.org](http://www.opengroup.org))

*Peter Sevcik is president of NetForecast in Andover, MA, and is a leading authority on Internet traffic, performance and technology. Peter has contributed to the design of more than 100 networks, including the Internet, and holds the patent on application response-time prediction. He can be reached at [peter@netforecast.com](mailto:peter@netforecast.com).*

NetForecast Inc. is a network technology consulting firm based in Andover, Massachusetts. Our seasoned consultants draw on decades of experience to help clients worldwide choose new technologies, improve performance, and align infrastructure to business. We have helped leading enterprises, service providers, and vendors navigate the changing competitive landscape of the Internet economy. Please call us to discuss how we can help your information network succeed.

