Policy-based Management: Beyond The Hype

Michael Jude

Billed as the ultimate in IT infrastructure management, PBNM has yet to fulfill its promise. But new tools and capabilities are arriving.

When first conceived in the late 1990s, policy-based network management (PBNM) promised enterprise IT shops the ability to control the quality of service (QOS) experienced by networked applications and users. Accounting transaction data, for example, could be assured of high throughput, while email got best-effort delivery.

In fact, the hype went further than that: Vendors promised that CIOs or CEOs would soon be able to control policies through a simple graphical interface on their desk. Behind the scenes, those instructions would translate into specific traffic management adjustments, bypassing traditional network operations.

Reality, of course, is different. PBNM turned out to be difficult to put into practice. Early adopters have found that developing and deploying policies is not simple, cheap or quick. Instead, PBNM has been a time-intensive, complex, expensive process. Additionally, it has demanded that the enterprise organization mutate to match the technology—rather than the technology meeting the enterprise's management needs.

Finally, many PBNM solutions tend to be single-vendor approaches and, as such, are not readily employed in existing multivendor networks. Despite these setbacks, there are good reasons why the lofty goals of PBNM are still being pursued, and there are PBNM tools that can provide useful capabilities.

Using Policies To Achieve Control

Why PBNM in the first place? Few CIOs may want to directly manage computing priorities, but many would love to be able to allocate expensive computing resources, and ensure that mission-critical computing takes place, especially in an age where Web-surfing employees could be watching streamed *I Love Lucy* reruns on their desktops—or worse.

PBNM is a way to prioritize applications and users, by assigning and enforcing different QOS levels. Rather than implement PBNM, however, many IT managers simply add bandwidth, server capacity and so forth. The problem with this approach is that it is static and inefficient. While you may have enough capacity to meet peak loads, you are probably over-provisioned for most situations. And, during peak demand, even extra capacity may not be enough. PBNM, by allowing efficient resource utilization, can be thought of as flexible provisioning or, at the very least, as an alternative to overprovisioning.

PBNM, however, is much more than a provisioning alternative. Any capability that allows you to control QOS also lets you detect the nature of a particular packet flow and, if necessary, turn it off. This allows for a high degree of control over such things as unauthorized traffic. In fact, when Enterprise Management Associates (EMA) recently surveyed enterprises and service providers, we found security and application performance improvements at the top of their list of reasons for adopting PBMN.

As shown in Figure 1, controlling QOS and saving money came in only about midway down the list. The implication is that PBNM is seen more as a strategic enabler of existing and emerging applications than as a mechanism for saving money. In fact, PBNM should be viewed as the logical end-game for things such as service level management (SLM), performance management and other approaches to controlling QOS.

Unlike the monitoring and reporting functions of SLM and performance management, however, PBNM gives real control to the IT manager. Using PBNM, the network can be managed actively to compensate for service-affecting degradations. Ultimately, PBNM may prove more valuable for the control it provides to the NOC than for any capability it gives to the CIO.

Of course, it's expensive to set up committees and build organizational structure to manage policy. And it is a truism of management applications generally, and policy-based network management in particular, that the ongoing costs associated with their use can be considerable. For the policy-PBNM adopter, these costs may be hard to justify in the face of cheap bandwidth and hardware. Yet EMA's recent survey found 28 percent of respondents already using policy-based network man-

Michael Jude, Ph.D. is a senior analyst with Enterprise Management Associates, specializing in network management tools and technologies. He can be reached at 303/543-9500 ext. 122 or jude@enterprisemanagement.com

agement and another 50 percent planning to adopt it in the next two years. The point is to be sure the PBNM solution is being considered for reasons that can justify its costly setup and operation.

PBNM At A Glance

PBNM functions start with bandwidth management, i.e., prioritizing the applications or transactions that must share network resources. This can be as simple as the bandwidth of a particular transmission path or as complex as the bandwidth of a server. In any case, PBNM is dedicated to allocating scarce bandwidth resources.

In practice, PBNM manifests itself as a set of rules that define the relationships among:

- A set of network conditions.
- Potential responses to those conditions.
- The devices that will implement the responses.

For example, if a particular application is defined to have a high priority, then a condition that threatens its performance, such as server cycle over-utilization, might trigger a response that throttles back competing applications in that server. In this case, a rule has been generated that defines the policy that applies to this application under this condition.

Policies can be applied at any layer of the networked environment. They can be developed to restrict access to applications and network resources by time of day or other variables. Generally speaking, the more pervasive the policy, the more complicated it is to implement, as more devices must be able to participate in the rules, condition detection and responses.

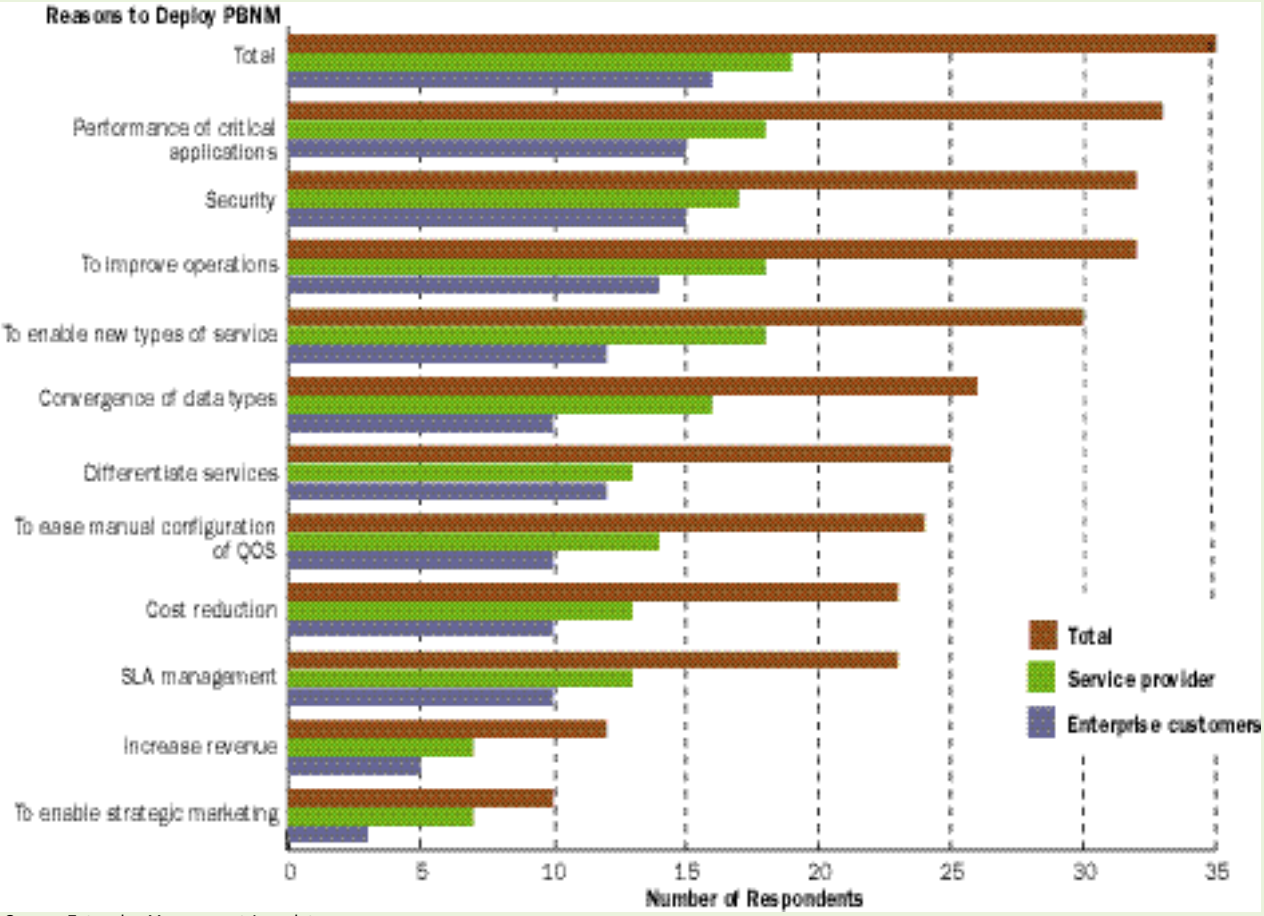
Defining a PBNM approach to managing QOS can be complex and time-consuming. Theoretically, rules must be developed for all the resources in the managed network. Practically, a few strategic links and/or applications are usually given high priority and everything else is kept at a "best effort" level. However, even this requires the IT department, in collaboration with other departments, to develop a set of priorities.

Usually this process escalates quickly to the CIO level. Rather than mandating policies, the CIO mediates competing demands for priority. Once these demands have been reconciled, the IT department can sit down and develop a set of absolute policies that can be translated into rules.

Then the policy infrastructure can be put in place. This involves deciding whether to manage policies at the edge or within the existing network

PBNM gives real control to the IT manager

FIGURE 1 Reasons For Deploying PBNM



Source: Enterprise Management Associates

Not all vendors use protocols and standards in the same way

TABLE 1 Policy-related Standards And Protocols

Standard/Protocol	Purpose
LDAP	**Lightweight Directory Access Protocol:** A client/server protocol that defines the ways in which directories can be accessed and shared.
COPS	**Common Open Policy Service:** A protocol that defines the way in which a policy server exchanges information with its clients.
DiffServ	**Differential Services:** A standard which redefines the IP type of service (TOS) field in the packet header to expand the number of possible services.
802.1Q	**A standard** that defines the header for an Ethernet frame, such that the header specifies the class of service for the information carried in the frame.
802.1p	**A standard** that defines the 8 possible classes of service for an Ethernet frame, if class of service is specified. These range from background to network critical.
IP TOS	**Internet Protocol Type of Service:** A standard that defines 8 classes of service in an IP WAN environment.
RSVP	**Resource Reservation Protocol:** A negotiation protocol for requesting a specific amount of bandwidth be allocated to a particular transaction across a number of devices.

switches, routers and other devices. Using a standalone product at the edge is generally less expensive, and appropriate if the focus is on bandwidth management. The edge device can also confer a certain degree of vendor independence, but the disadvantage is the same: it adds another device and vendor to the network.

On the other hand, implementing PBNM in the existing networked devices costs more but gives finer control—assuming a single-vendor network is in place. The down side is the additional complexity PBNM adds to the management of those devices. Also, bear in mind that the dedicated policy servers required as part of many PBNM solutions must be treated as critical network components with all the demands such components make: redundancy, security and fault tolerance.

The principal thing to remember is that all PBNM solutions are based on the rules that must be defined and implemented. These rules are implemented by manipulating protocols inherent in the managed devices (Table 1). So the user intent on implementing PBNM should understand how the selected solution and the devices to be managed use these protocols. Also, since different vendors comply with these standards to varying degrees, users should anticipate much greater complexity when applying PBNM in multivendor networks than in single-vendor networks.

Single-vendor And Multi-vendor Architectures

Regardless of the network infrastructure, the policy development process alone can take months to refine and implement. While this can be daunting, most of the vendors who offer PBNM software and systems, including those listed in Table 2, also provide comprehensive professional services to assist the implementation.

Choosing a PBNM product exposes another significant issue: Most of the solutions offered by network hardware vendors are (understandably) optimized by the vendor for use with its own hardware product line. For example, while Avaya's CajunRules solution can manage policies for certain classes of Cisco equipment, its full range of functionality is reserved for Avaya gear. Likewise, Cisco's CiscoWorks QOS solution set does not really manage other vendors' hardware.

Having said this, it is important to note that most PBNM vendors do provide basic policy-driven capabilities, such as traffic prioritization, for competing products. For example, Extreme can manage traffic priority for Cisco routers.

The fact remains that a single-vendor network will allow the fullest range of policy management capabilities, although some software vendors, such as Orchestream and IPHighway, are working toward hardware-independence. In the meantime, the network may have to be adjusted to implement the policies. For example, an end-to-end DiffServ-based traffic prioritization approach may require single-vendor devices in the wide area, with no need to replace local multivendor equipment.

The prospective PBNM implementer can now choose from a significant list of vendors and solution types. Hardware vendors such as Extreme, Nortel, Cisco, Intel and Avaya have all embraced policy management in a large way. Avaya, for example, has built a policy solution on its Definity platform, not only extending its PBX functionality into the IP world, but also providing bandwidth management functionality.

Edge devices, such as those from Allot, Packeteer and Sitara do nothing but bandwidth management at the edge of the network, and have become all but plug and play. And software-based solutions from companies like Orchestream and HP now provide links to traditional network management systems, enabling integrated management and control over the networked space. Of course, such solutions are complex, but for some networked situations they can be worth it.

Vendors optimize PBNM products to work with their own hardware

TABLE 2 Policy-Based Network Management Vendors To Watch

Vendor	Solution	Purpose
Nortel (www.nortel.com)	Optivity Policy Services	Policy management software that allows end-to-end QOS and security management.
Orchestream (www.orchestream.com)	Version 2.1	Automated provisioning solution that defines services in terms of policies.
Avaya (www.avaya.com)	CajunView	Policy management software that enables rules development and deployment, to manage Avaya switches and routers.
Cisco Systems (www.cisco.com)	Works	A suite of tools, including QOS Policy Manager, that can reserve or prioritize bandwidth using centralized policy control and policy deployment.
Allot Communications (www.allot.com)	Net Policy	Policy management software, used in conjunction with Allot's NetEnforcer policy enforcement hardware, which enables QOS and bandwidth management.
IP Highway (www.iphighway.com)	Performance Pro	Provisioning solution that enables policy-defined prioritization of bandwidth and applications.
Intel (www.intel.com)	NetStructure Policy Manager v 1.0	Policy management application which provides traffic prioritization, bandwidth management and security management.
HP (www.hp.com)	Policy Xpert	Policy management solution built on popular Openview platform that manages QOS and bandwidth in multi-vendor networks.
Extreme Networks (www.extremenetworks.com)	ExtremeWare Enterprise Manager	Policy and QOS management for Extreme switches and selected Cisco equipment.

The selection of a PBNM solution, of course, depends upon multiple variables. The principal consideration is whether a particular solution will work with your infrastructure. If your network is homogeneous, then the best bet is to look to your vendor for PBNM. If that vendor's solutions provide less functionality than you require, or if your network is a mix of vendors' equipment, then you must look at cross-vendor solutions or edge devices.

Vendors, by and large, have moved beyond hype to delivering PBNM products that work as advertised. While many still claim more functionality than they can deliver out of the box, in homogeneous environments many deliver a great deal of control over such things as bandwidth and application-specific QOS. For enterprises that have made significant investments in management infrastructure, many PBNM solutions will integrate with and extend that functionality.

Conclusion

The PBNM picture is a lot brighter than it was even a year ago. Vendors are bringing out better solutions, and implementation is not quite the harrowing experience it once was. Most major vendors also offer professional consulting and implementation support.

However, buyers still need to swallow a healthy dose of "caveat emptor," and prepare for a barrage of techno-babble. Be sure that prospective PBNM solutions will work with your existing infrastructure and grow with your needs. The best way to do this is to test-drive the application or establish a test network to work out the bugs. A solution that works for only a subset of your network equipment will only increase management overhead, even if it provides greater control for that subset. Cross-vendor solutions may be so superficial that they provide little in the way of real benefit.

PBNM is not a quick fix. It is, however, a logical extension to service level management (SLM), as well as an effective way to optimize the use of networked resources and to ensure that mission-critical computing is given priority and security. For those willing to spend the time, effort and money to implement a policy-based approach to network management, the rewards can be great□

Companies Mentioned In This Article

Allot Communications (www.allot.com)
Avaya (www.avaya.com)
Cisco Systems (www.cisco.com)
Extreme Networks (www.extremenetworks.com)
HP (www.hp.com)
Intel (www.intel.com)
IP Highway (www.iphighway.com)
Nortel (www.nortel.com)
Orchestream (www.orchestream.com)
Packeteer, Inc. (www.packeteer.com)
Sitara Networks (www.sitaranetworks.com)