An Internet Paradigm Approach to Policy-based Network Management of Legacy Kit for VoIP Services in Next Generation Networks

V.D. Naidoo and W.D. Tucker
Broadband Applications and Networks Group
Department of Computer Science
www.whipper.uwc.ac.za

Abstract

With QoS available on IP-dominant NGNs, Policy-based Network Management (PBNM) is an effective mechanism for managing services as opposed to actual devices. IP is ubiquitous, and any NGN must contend with legacy devices that do not support emerging PBNM protocols. This Work in Progress uses the common Internet notion of a proxy to enforce policies on legacy equipment. We use VoIP as a mechanism to test the validity of our intended solution.

1 Quality of Service on Next Generation Networks

There are currently three communication network paradigms: packet switched data, circuit switched telecommunications and converged multiservice. The introduction of Voice over IP (VoIP) into two of these paradigms is leading us to the Next Generation Network (NGN), where the Internet Protocol (IP) is likely to dominate and the Public Switched Telephone System (PSTN) may indeed evolve in or out of the picture.

Quality of Service (QoS) cannot be guaranteed over IP because of its best effort paradigm. [4] QoS is best defined as a collective measure of the level of service delivered to an application (or service) user that can be characterized by packet delay, jitter and loss [11]. Dedicated IP networks can provide end-to-end QoS with protocols such as Resource ReSerVation Protocol (RSVP), Differentiated Services (DiffServ) and eventually Multi-Protocol Label Switching (MPLS) [11]. Armed with proper QoS, we can now develop broadband IP applications and services that will cause the perception of broadband applications to change.

All of the new services, technologies and applications that will appear on the NGN must adhere to the 99.999% standard currently offered by the telcos for voice, fax, and other forms of information that have traditionally been carried over the dedicated circuit-switched connections of the PSTN [10]. In order to manage these services, the focus has changed from managing Network Elements (NEs) to managing network services. The most dominant approach is Policy-based Network Management (PBNM), a solution that essentially defines and enforces policies to provision QoS for specific services.

2 Policy-based Network Management

PBNM allows management of a network so that various kinds of traffic - data, voice, and video - get priority of availability and bandwidth needed to serve a network's users effectively. For example (see Figure 1), with policy statements, network administrators can specify that a particular service gets priority, at a given time of day, on certain a network. A policy contains rules that govern how a resource or service in the network can be used. A PBNM system transforms policies into configuration changes and applies those changes to the network(s). These policies, then, abstract away from the physical NE specifics to simplify and enhance the management of QoS.

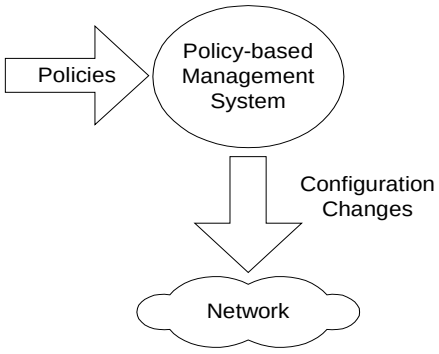

Figure 1: PBNM overview

A PBNM system consists of the following components (see Figure 2): Policy consoles, Policy Decision Points (PDP), Policy Enforcement Points (PEP), Policy repositories and Policy communication protocols. A policy console is a user interface to construct policies, deploy policies, and monitor the status of the policy-managed environment. A PDP is a process that makes decisions based on policy rules and the state of the services those policies manage. A PEP is an agent that

runs on or within a resource that enforces a policy decision and/or makes a configuration change. A PDP enforces policy decisions on the PEP. A policy repository is a directory and/or storage service for policy-related information. Policy communication protocols are the protocols used to read/write data from/to a policy repository. These protocols are also used to communicate between PDPs and PEPs [7].

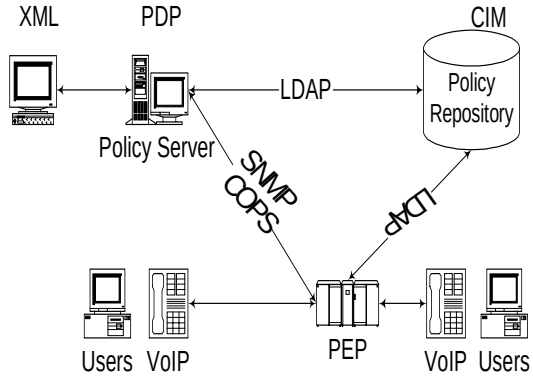

Figure 2: PBNM system

PBNM has two models: outsourcing and provisioning. The outsourcing model assumes there is a signaled event in the PEP that needs to be resolved based on policy rules. Signaling events are typically associated with end-to-end network control protocol such as RSVP. Interestingly enough, the provisioning model is almost the reverse of the outsourcing model in that the PDP typically predicts future configuration needs, and configures policies for them ahead of time. The PDP prepares and pushes configuration information to the PEP, as a result of an external non-PEP event, such as a change of applicable policy, time of day, or a result of third party (non PEP) signaling [8].

Multiple policy systems may need to interoperate within a single domain, and share the same policy information due to networks containing a variety of vendor equipment. A central repository can be used to store, distribute and coordinate policy information among these systems. Lightweight Directory Access Protocol (LDAP) is the current dominant protocol for accessing online directory services. Interoperability is gained by using the Distributed Management Task Force (DMTF) information model schemas to store policy information. The information is stored using the Common Information Model (CIM). [5]

Common Open Policy Service (COPS), an International Engineering Task Force (IETF) creation [2], was developed as a standard protocol for exchanging network policy information between a PDP and its associated PEPs. This TCP/IP based protocol was created because traditional network management protocols such as the Simple Network Management Protocol (SNMP) [3] cannot efficiently support PBNM systems.

3 VoIP PBNM with Legacy IP Equipment

While COPS does not use SNMP, most legacy IP equipment does talk SNMP, and that equipment must be integrated into IP-based NGNs. The "holy grail" is to provide carrier grade services on NGN networks by guaranteeing QoS of IP services using PBNM. In the meantime, the problem is to retain links to legacy IP-based equipment and guarantee QoS to services and applications as much as possible. Thus there is a need for interoperability between the legacy, contemporary and future equipment (see Figure 3).

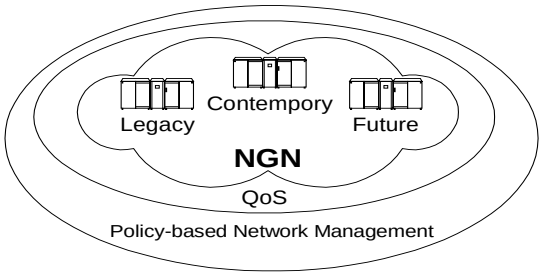

Figure 3: Providing Interoperable QoS with PBMN

Contemporary and future devices will contain the protocols necessary for QoS and PBNM. For our purposes, devices that do not explicitly support voice, COPS and QoS are now termed legacy with respect to NGN. Legacy IP equipment may not be able to provide QoS (see Figure 4), but they can still push IP packets, and they could communicate with PBNM systems with SNMP. The legacy equipment, if left in the network topology, will still be able to support the type and volume of traffic on the network, but will not be able to reserve bandwidth or give priority to certain types of packets, a service that is needed for PBNM to function. Current PBNM systems however do not support legacy equipment. The goal is to extend PBNM of QoS in an NGN to include legacy equipment with IP-oriented "best effort".

4 Proxy Policy Enforcement

A solution (see Figure 5) entails incorporating the SNMP management protocol into a Proxy PEP (P-PEP). The network policy information carried by the COPS protocol, sent by the PDP, should be interpreted by the P-PEP proxy and enforced with SNMP on legacy kit.

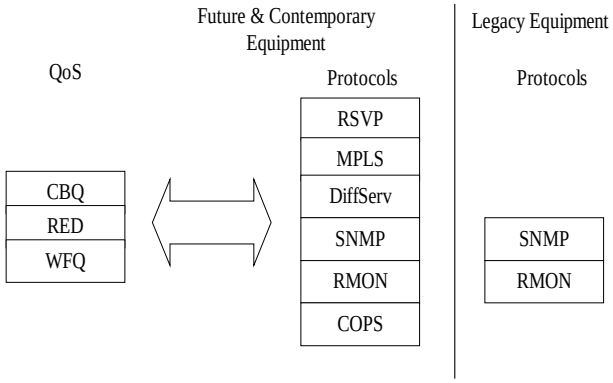

Figure 4: Equipment Protocol Comparison

In other words, the P-PEP is a policy translation mechanism. The enforcement functionality of COPS can be emulated by the P-PEP, as enforcement is a critical component of PBNM systems to ensure QoS.

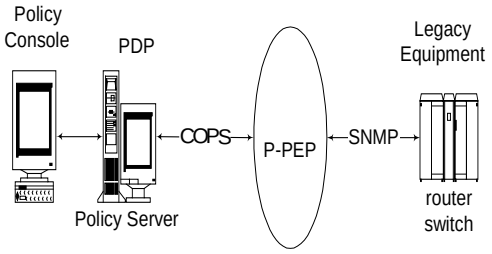

Figure 5: The solution

The P-PEP will interpret the PDP's instructions , determine and appropriate form of action, and then use SNMP to direct the legacy IP equipment to make some form of configuration change. The PBNM outsourcing model can be implemented using SNMP sets and traps to send signals to and from the P-PEP and the legacy gear. SNMP traps from the legacy kit can be translated and passed up to the PDP with COPS. The P-PEP can also use SNMP sets to enact configuration settings. This mechanism can also be used to support COPS provisioning model with SNMP sets.

This approach has several limitations. First, SNMP is unreliable due to it being based on UDP. Second, the P-PEP may not be able to enforce a policy due to the limitations of the legacy kit's configuration abilities. SNMP also does not have an automatic fail-over and Policy Information Base (PIB), and this fail-over must be provided by the P-PEP [8]. We expect more limitations to reveal themselves as the research progresses.

There is a possibility that these limitations can be overcome by building PEP-type functionality into a firewall. In fact, a P-PEP (see Figure 5) can be thought of as a firewall, and deployed as such. A firewall solution could incorporate traffic shaping QoS techniques such as Class-based Queuing (CBQ), Random Early Discard (RED) and or Weighted Far Queuing (WFQ) [11] (see Figure 4), where a P-PEP would dynamically block specific types of traffic, at certain times of the day, in legacy equipment or at aggregation points.

5 VoIP Network Test Scenario

We intend to use VoIP traffic to test out the P-PEP concept. We will create a network of COPS-enabled and COPS-lacking equipment and use the Smartbits frame thrower to generate VoIP traffic (see Figure 6). The network itself can consist of a variety of LAN and WAN configurations. We are especially interested in multi-vendor environments to prove the robustness of our solution.

We feel there are two significant advantages of using the SmartBits system to drive our network in order to prove the concept. First, we have a QoS analysis package on the SmartBits engine. Second, the SmartBits API should allow us to regulate (or shape) the traffic on the network(s) depending on how the network reacts to policies defined to the PDP. This means we must either wrap the PDP with an API to the SmartBits engine to change the traffic generation based on the policies, or somehow intercept the policy directives to the PEPs in order to accomplish the same task. Traffic generation for the network will test the PBNM system's ability to dynamically change policies, when the network goes "live".

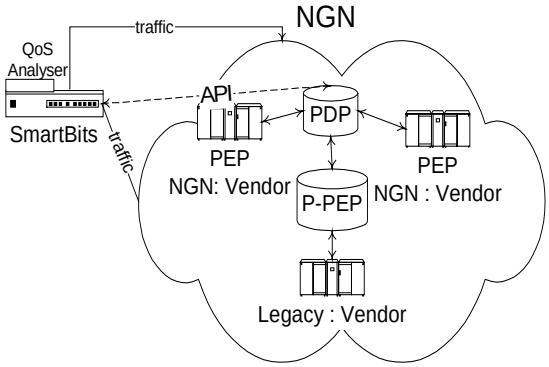

Figure 6: Test scenario

The main goal, however, is to try and effect the policies on the legacy equipment. Applications and services given priority through policies should still receive priority, even when stressed tested by the Smartbits device,

even if it means that the PDP stalls less important services or applications. The PBNM should dynamically change its policies to cater for mission critical applications or services, even if it means that other applications and services cease or fall over. This is especially true for the legacy kit, where we either block traffic with a firewalling P-PEP, or shut down a route with an SNMP call.

6 The Big Picture

The Centre of Excellence in ATM and Broadbroad Networks and their Applications (CoE) at the University of the Western Cape (UWC) is developing scalable broadband distance education environments to anyone connected to the Internet, but especially targeted toward previously-disadvantaged peoples in all areas of South Africa. There is a severe lack of educational facilities and infrastructure in South Africa that we perceive as an opportunity to deploy cutting and bleeding edge NGN technologies, and the applications that require them. With the integration of the PSTN and dedicated IP networks, distance learning courses can reach formerly unreachable areas through on-line Internet services with guaranteed QoS, either land-based or wireless.

Enhancing PBNM with hooks to manage legacy equipment will allow disadvantaged communities to still partake in a distance learning environment even when the equipment becomes outdated, and co-exists with NGN-type kit.

References

[1] Cisco Systems, ,“COPS for RSVP”, 2000, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/copsrsvp.htm, Last visited August 2000.

[2] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, Network Working Group : Request for Comments: 2748, The COPS (Common Open Policy Service) Protocol, Januaury 2000, www.ietf.org/rfc/rfc2748.txt Last visited August 2000.

[3] D. Perkins and E. McGinnis, “Understanding SNMP MIBs”, Prentice Hall, 1997, ISBN: 0-13-437708-7.

[4] D.H. Lorenz and A. Orda, “QoS Routing in Networks with Uncertain Parameters”, May 1998, ACM S 1063-6692(98)09580-6.

[5] DMTF ,“CIM Specificationhttp and Schema”, 2000, www.dmtf.org/spec/cims.html, Last visited August 2000.

[6] E.R. Harold, “The XML Bible” IDG Books Worldwide, Inc, 1999, ISBN 0-7645-3236-7.

[7] IPHighway, Inc. and IPHighway,Ltd, “Introduction to policy-based networking and quality of service”, 2000, www.stardust.com/qos/whitepapers/IPHighway_Vol2paper/polstandardsIETFterm_02.htm Last visited August 2000.

[8] IPHighway, Inc. and IPHighway,Ltd, “Policy-based networking products, design and architecture”, 2000, http://www.stardust.com/qos/whitepapers/IPHighway_Vol3/polbasednetworkproduct_01.htm Last visited August 2000.

[9] J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, J. Perry, S. Herzog, A. Huynh, M. Carlson, “Policy Framework Working Group Internet Draft : Policy Terminology”, IETF, July 2000, www.ietf.org/internet-drafts/draft-ietf-policy-terminology-00.txt. Last visited August 2000.

[10] Nortel Networks , “Voice Fundamentals”, 1999, GD505-3406EC-A.

[11] P. Ferguson and G. Huston, “Quality of Service: Delivering QoS on the Internet and in Computer Networks”, John Wiley and sons, Inc, 1998, ISBN: 0-471-24358-2

[12] R. Caruso and M. Kean, “POWER PROGRAMMING IN HP OPENVIEW” , Prentice Hall, 1997, ISBN 0-13-443011-5.

[13] S.T. Joyce and J.Q. Walker, “Policy-Based Management White Paper by Ganymede”, Ganymede,1999,www.ganymede.com/download/whitepapers/pbmwhite.pdf. Last visited August 2000.

[14] The International Engineering Consortium ,“Internet Telephony Tutorial “,, 2000, http://www.webproforum.com/int_tele/index.html, Last visited August 2000.

[15] The International Engineering Consortium ,“Voice Quality (VQ) in Converging Telephony and Internet Protocol (IP) Networks Tutorial”, 2000, http://www.webproforum.com/voice_qual/index.htm , Last visited August 2000.

[16] Y. Snir, Y. Ramberg, J. Strassner, R.Cohen, “Policy Framework Internet Draft, QoS Policy Schema”, IETF, February 2000, www.ietf.org/internet-drafts/draft-ietf-policy-qos-schema-01.txt Last visited August 2000.