Policy-based Network Management of
Legacy Equipment in
Next Generation Networks

VD Naidoo and WD Tucker

Broadband Applications and Networking Group
Department of Computer Science, University of the Western Cape
http://www.whipper.uwc.ac.za/

ABSTRACT

Next Generation Networks use policy-based network management and QoS protocols to provide voice services on IP networks. Large numbers of older equipment still push IP packets. We present several solutions that include legacy equipment into a PBNM and QoS system. A static design uses traffic shaping at the legacy edge. A dynamic solution uses a Quasi-PEP implemented over RSVP and COPS. Preliminary test results are presented for the static solution. Collected data shows that the solution decreases packet loss on the legacy side.

1 INTRODUCTION

Contemporary Network Elements (NEs) such as routers and switches support QoS protocols such as ReSource reserVation Protocol (RSVP), MultiProtocol Labeled Switching (MPLS) and Differentiated Services (DiffServ). These protocols have resolved many QoS issues. Future devices will automatically have support for these QoS protocols. Legacy NEs, defined as NEs that do not have these protocols to support voice adequately, are regarded as unsuitable for voice communications. Legacy NEs not only lack QoS functionality but also lack the protocols and mechanisms necessary for Policy Based Network Management (PBNM) systems such as the Common Open Policy Service Protocol (COPS) [6]. The management commonality between Legacy and contemporary NEs is the Simple Network Management Protocol (SNMP).

One could surmise that in order to provide voice services on an existing network, one must buy voice enabled equipment that supports the necessary QoS protocols (RSVP, MPLS, DiffServ) and management protocols (COPS, SNMP)[5]. Yet legacy NEs do predominate. They have the same abilities to push packets through their ports, but lack the intelligence to provide QoS. This is certainly not a basic hardware problem but a configuration limitation. The ideal situation is to leave as much legacy kit as possible in a network while introducing voice-enabled kit on an as-need basis. It is the authors' opinion that there exists a possibility to bridge the gaps between the two types of kit in order to provide enough QoS to deliver voice.

The aim of this research is to show that voice services can be provided on Legacy NEs when congestion occurs using PBNM together with Traffic Shaping methods. If Legacy NEs are to be included in contemporary networks, they should not in any way lower the QoS provided by increasing network congestion or decreasing the saturation point. The research will be proven a success if, within mixed legacy and contemporary networks, better QoS is provided and/or the period to reach network saturation prolonged.

2 TOWARDS A QUASI-PEP

QoS requirements are fundamentally either provisioned or signaled. With provisioned QoS, network resources are statically configured in anticipation of traffic that will flow through them. With signaled QoS, applications dynamically signal network devices in an attempt to reserve resources on them. The signal contains information describing the specific QoS necessary for the application to function. The RSVP protocol is an IETF standard for signaled QoS [10] that is supported in PBNM.

We consider two possible approaches: implementing PBNM using SNMP on the entire network enforcing traffic shaping methods (see Figure 1) and implementing PBNM with COPS and enforcing traffic shaping methods on the Legacy NEs. Both solutions provide QoS using traffic shaping at Layer 4 of the Open Systems Interconnect (OSI) model i.e. using port numbers to identify traffic types and deploy traffic management/shaping.

Traffic shaping is of great importance in today's packet networks. Sophisticated queuing can improve network performance with respect to bandwidth utilization, delay, jitter, and packet loss. Thus, queuing can help to meet the requirements of real-time services [7]. Queuing is also vital to best-effort services to avoid congestion and to provide fairness and protection. This leads to more stable and predictable network behaviour. We make use of two queuing utilities here: Linux advanced routing and ALTQ. Each solution affects the structure of how QoS can be applied to a network, thus resulting in the solution being two tailed; static and dynamic.

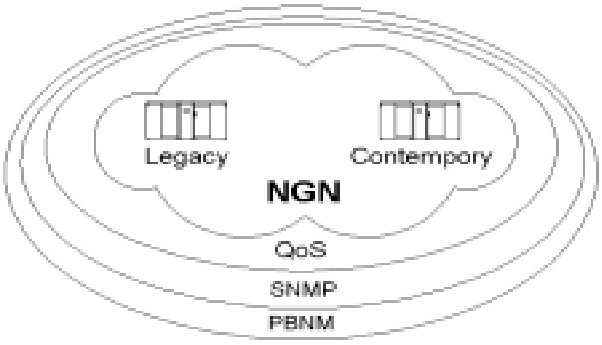

Figure 1. PBNM using SMNP

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices which enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Managed devices are monitored and controlled using four basic SNMP commands: read, write, trap, and traversal operations [2]. QoS would be provided by using traffic shaping methods, statically and dynamically rejecting or allowing certain types of traffic to transgress a NE thus giving various kinds of traffic – data, voice, and video – various priorities of availability and bandwidth.

The static implementation for provisioned QoS requires background information of the network under scrutiny as too what traffic types cause network congestion and saturation. These traffic types would then be either denied if necessary or allowed and given a percentage of the bandwidth. This information would then be statically deployed on all NEs on the network using SNMP set commands.

The dynamic implementation for signalled QoS provision requires no background network information. This approach needs detailed policy statements defined as to what traffic types to give priority when certain conditions occurred. SNMP traps, designed for real time error reporting, would be configured on the NEs to identify certain traffic types. These traps would then signal the SNMP Policy Decision Point (PDP) when certain predefined traffic types are identified on the ingress ports. The SNMP PDP would then enforce a decision based on the policies configured on the PDP on the requesting NE/Policy Enforcement Point (PEP). This approach was soon abandoned due to SNMP's inherent problems.

Earlier versions of SNMP lacked authentication capabilities, which resulted in vulnerability to security threats. SNMP also sits on top of UDP and is therefore unreliable. But more importantly, SNMPv2 is incompatible with SNMPv1 in two key areas: message formats and protocol operations. Traps were designed for real time error reporting, but due to SNMP's security problems, it is usually reduced to a network-monitoring tool and not for making configuration changes to devices remotely. COPS uses TCP as its transport protocol for reliable exchange of messages between policy clients and a server. COPS provides message level security for authentication, replay protection and message integrity and is thus the preferred protocol for PBNM [6].

A second solution replaces SNMP with COPS and uses traffic shaping. QoS is provided using Class-based Queuing (CBQ), a technique that classifies the packets according to classes and allocates bandwidth to the different traffic types within these groups as to provide differential treatment for each traffic class on the Legacy infested Network. The packets were divided into a hierarchy of classes based on a port numbers. Specific port numbers were assigned to a set of bandwidth priorities and given a percentage of the total bandwidth. The traffic shaping was implemented using ALTQ [3] and IPRoute [8] on the Legacy NE part of the network

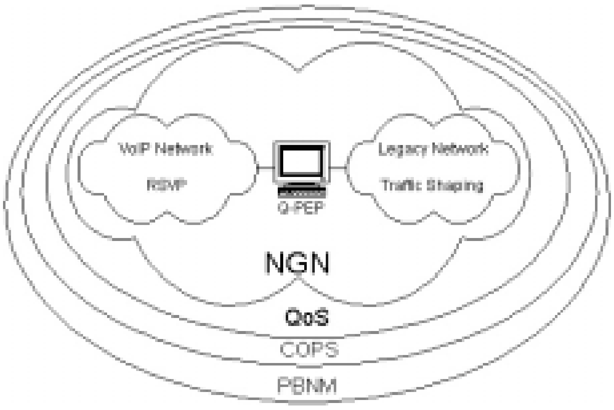

Figure 2: PBNM using COPS

The static implementation only required a detailed understanding of how traffic flows across the Legacy infested network, the major bandwidth hogs and then applying the QoS using ALTQ.

3 STATIC SOLUTION RESULTS

The results depicted in the paper are preliminary results that was obtain using a packet generator. The packet generator was used to test the static software solution but not only generated packets to test whether the solution was scalable and robust, but also collected various QoS statistics to check whether the solution is viable. Table 1 lists the amounts and types of packets generated. The traffic generated was set up like this to show what effect other traffic types have on voice. This explains the huge amount FTP, HTTP and Telnet packets.

Table 1. Packets Generate

Packet Type	Number of packets/min
FTP	98298
HTTP	32766
Telnet	32766
Voice	11997

QoS requires strict guidelines for thresholds for delay, jitter and packet loss. These values indicate whether or not VoIP will be acceptable to users or is being deployed at a suitable level of QoS [9]. These can be seen in Table 2.

Table 2: Qos Threshold values

Factor	Value
Delay	less than 50ms
Jitter	less than 50ms
Packet Loss	less than 0.2%

Traffic shaping was configured to give certain traffic types of traffic a percentage of the bandwidth and thus giving them priority. ALTQ was configured to fit the structure displayed in Figure 3.

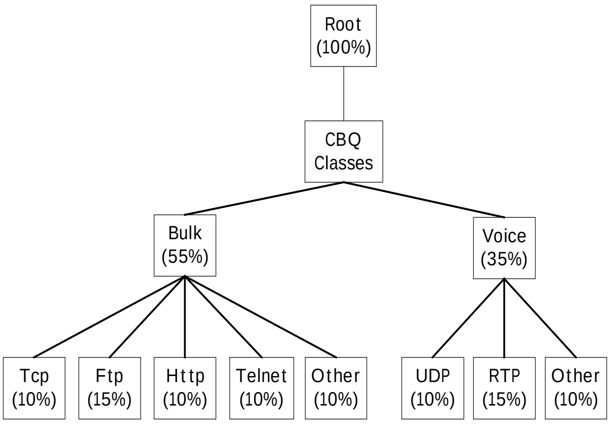

Figure 3: CBQ Bandwidth allocations

The results are shown in Table 3 and Table 4, using CBQ in Figure 3, and the traffic in Table1.

Table 3: Total number of packets dropped per minute.

Packet Type	No Traffic Shaping	Traffic Shaping
Ftp	268	273
Telnet	52	34
Http	34	36
Voice	25	12

Table 4: Voice specific QoS metric results.

QoS Metric	No Traffic Shaping	Traffic Shaping
PSQM	1	1
Jitter	0.1 ms	0.1 ms
Latency	1.9 ms	1.9 ms

4 CONCLUSIONS

There are several measures to evaluate voice quality. Telephone companies assembled people in a room to listen to voice. The average opinion of all people was referred to as the Mean Opinion Score (MOS). Perceptual Speech Quality Measurement (PSQM) is a voice quality scoring system endorsed by the ITU. PSQM attempts to “listen” to voice as a human being would listen, and rates the received voice sounds accordingly. It does this by measuring how much noise has been added to the originally transmitted voice signal. PSQM ratings range from 0 to 6.5, with 0 noise being the most desirable [4]. The PSQM rating should not be affected by traffic shaping as it is software based and causes no extra noise on the wire. The PSQM value was found to be 1, which meant that a minimal amount of noise was added to the voice packets. An interesting comparison would be test a circuit switched network and compare the results.

Latency, defined as the time between the arrival of a frame and the frame been sent [9], was given a rating of 1.9 microseconds for both situations (Traffic shaping and no Traffic Shaping). This result was surprising. The authors' view was that due to packets being put into queues and others given priority, i.e. more available bandwidth, one would have expected the Latency for traffic shaping to be less. However, this value met the QoS threshold value for both situations, (see Table 2).

Jitter, defined as the variability of arrival time of a packet [9], followed a similar pattern to latency. They were also equal in value (see Table 4). This value however met the QoS threshold value for both situations (see Table 2).

The evidence that traffic shaping provided some QoS was in the packet loss test results (refer Table 3). Traffic shaping lost fewer packets, it may only be a difference of 15, but one must remember that losing voice packets is unacceptable and even the slightest improvement is greatly welcomed. The packet loss value on the non-Traffic shaped network was 0.208%, which is just outside the accepted value, however, the Traffic shaped network had no problems.

Also proven from the results are once bandwidth capacities are reached e.g. ftp, shaping falls. A possible cause for this that packets go into queues, and their Time To Live (TTL) expires and are dropped. This can be catered for in a real environment, not as the one tested by using Random Early Discard (RED) [7]. This congestion avoidance algorithm, works well with TCP traffic, by dropping packets in anticipation of congestion causing the window size to become smaller causing the data to be sent more slowly. This will not work with the packet generator, as it will not regenerate the packet as other applications would if affected.

Correctly designing the network can improve QoS delivered. The newest of new NEs, if deployed incorrectly, can provide lower QoS than Legacy NEs. Thus toggling CBQ allocations by increasing or decreasing bandwidth allocated percentages to certain traffic types could cause an increase in QoS provided.

5 FUTURE WORK

A dynamic implementation requires building a Quasi-PEP (Q-PEP) (see Figure 2) that acts as an enforcement point for the traffic shaping. The Q-PEP listens on a predefined port and relays all RSVP messages to the COPS client on another port and to the local Traffic shaper, which will map them to CBQ traffic shaping.

The static implementation should provide better QoS than the dynamic solution. The dynamic solution maps RSVP decision messages to traffic shaping methods which should result in configuration changes in allocating/de-allocating bandwidth which in the authors' opinion could have a negative effect on the QoS provided. The dynamic solution thus would inherent latency problems caused by these mappings. Another possible reason for the decrease in QoS could be packets inserted into queues and not processed due to unpredictable configuration changes and settings.

REFERENCES

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

[2] Case, Fedor, Davin, and Schoffstall, “Standard 15 : A Simple Network Management Protocol”, May 1990, http://www.sri.ucl.ac.be/normes/std.html

[3] K. Cho, “Managing Traffic with ALTQ”, *USENIX 1998 Annual Technical Conference*, June 1999.

[4] Communication Standards Information Service IEEE , “Voice over IP Technology”, June 1999, http://www.comsoc.org.mx/standard/voip.html

[5] P. Ferguson, 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

[6] OpenView Network Management Division Hewlett-Packard Company, “A primer on Policy-based Network Management”, September 1999.

[7] David McDysan, QoS & Traffic Management in IP & ATM Networks, McGraw-Hill,2000, ISBN: 0-07-134959-6

[8] BV Netherlabs, G. Maxwell, R. van Mook, M. van Oosterhout and P.B. Schroeder, “Linux 2.4 Advanced Routing HOWTO”, September 2001, http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html_single/Adv-Routing-HOWTO.html

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

[10] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, “Network Working Group: Request for Comments: 2749, COPS Usage for RSVP”, Januaury 2000, ww.ietf.org/rfc/rfc2749.txt