Dynamic network reconfiguration based on application measurements with the goal of network traffic optimization

Martin Tkačik, Katarína Kleinová, Peter Feciľak
Dept. of Computers and Informatics, Faculty of Electrical Engineering and Informatics
Technical University of Košice
Letná 9, 04001 Košice, Slovakia
Email: ¶Martin.Tkacik,Katarina.Kleinova,Peter.Fecilak♢@cnl.sk

***Abstract*—Problems of quality management of various types of communications in the IP network is becoming important increasingly, because of a growing amount of transferring data. This paper explains the basic operation of VoIP technology, problems concerning the reduction of transmitted voice quality caused by network load factor, and ways of solving these problems. This work also deals with methods for detection of network topology and automatic reconfiguration of network devices. The aim of this work is an automatic network reconfiguration in the interest of optimize VoIP traffic.**

***Keywords*—optimization, management, measuring, VoIP, IP network, detection, load balance, QoS, IP SLA, LDAP, CDP, SNMP**

I. INTRODUCTION

IP network is used for transferring messages demanding for low latency and for messages requiring error-free transmissions. Transmissions such as voice and video have significantly different requirements for transfering like computer data in the form of files, photos or documents [1]. To ensure the quality of the transmission, the Quality of Services (QoS) methods are being used. Individual communication links are not constant and it is necessary to dynamically adjust the rules governing the routing of data in the network.

In this paper the methods used for detection of network topology on the 3rd layer of the OSI model are analyzed. The search of alternative routes between routers, the valuation of lines, application optimization commands for routers and ongoing exporting of current information to an external server is also part of our solution.

The aim of this work is to develop a tool which will help network administrators to prevent poor quality on real-time communication and thus the poor clarity of human speech which is transmitted by VoIP technology assuming that the reduced quality is caused by overloaded communication links in the network.

II. GOALS

The goal of this work is to develop a fully autonomous software running on the background of operating system, where it can manage the quality of transmitted voice over IP network which is being monitored. With the goal of obtaining VoIP network parameters we have developed a VoIP analyzer. To communicate with the VoIP analyzer an own communication protocol has been developed.

III. ANALYSIS

A. Quality of VoIP Communication

For the purposes of achieving a certain quality of voice applications over the Internet, certain criteria for value of transmission parameters are required. Whereas calling is a real-time communication, the first place in requirements have low delay and jitter [1]. Those requirements are followed by low error rate, which may be delivery of damaged packets, delivery in a wrong order, or in the worst case packet loss rates. A list of basic network parameters and their requirements for the use of VoIP communication is seen in Table I.

TABLE I.
TYPE SIZES FOR CAMERA-READY PAPERS

Quality of sound	Excellent	Fair	Bad
bitrate [kbps]	2 – 64 (depending on the audiocodec)		
packetloss [%]	0-0,5	0,5-1,5	Above 1,5
delay [ms]	0-150	150-400	Above 300
jitter [ms]	0-20	20-50	Above 50

With the goal of achieving the required quality of a particular VoIP connection, increased priority for the network transition or distribution of data sent via multiple parallel paths can be configured.

Changing priority is a part of QoS techniques, which consists of the sign of each packet under its competence to transmission, which we want to influence. Identification is carried out on the basis of data (IP, port) about sender and recipient. For the marked packets the rules can be assigned for prioritized processing at routers [2].

Distribution of traffic on several routes leads to a reduction of bandwidth that is used for the current route. This method is called loadbalancing. Its implementation in this particular case was by using configuration of static routes (static routing has increased priority over the dynamic routing protocols) and load-sharing. This makes it possible to have rules on the network with an even

978-1-4577-0052-1/11/$26.00 ©2011 IEEE

higher priority for routing, for example policy based routing.

B. IP network topology discovery

CDP and SNMP protocols can be used with the goal of topology discovery [3]. For their utilization it is necessary to be active on each router to which it is necessary to communicate. The router's SNMP MIB database can be used to obtain any information about the router. The list of neighboring routers of active router is possible to obtain, when protocols SNMP and CDP are cooperating.

C. Valuation of lines quality

IP SLA service is the most suitable method to gather network parameters with the goal of analyzing qualitative parameters of network environment [5]. IP SLA is an intrusive method simulating a particular type of traffic on the network and the transmission parameters measured on this traffic provides a numerical rating. This result defines the current state of the line, which may be obtained from each router by SNMP.

D. Analysis of a VoIP connection

VoIP analyzer, which was developed as a part of this work, allows us to list ongoing active VoIP connections. This tool, based on sniffing SIP [4] and RTP packets, determines which call is currently active and also detects packet loss rates and delay variations of this communication. The resulting information is periodically sent by its own protocol to the newly - developed tool for managing network traffic ability.

E. Remote control of routers

SSH or telnet are protocols which are mainly used for remote administration of systems via interactive command line tool. This method also appears as the most appropriate method for automated control of routers using the software. Responses to the expected answers of devices during ssh connection is possible to solve by an external tool "expect" [6]. It processes in advance generated script that contain expected questions and responses to them.

F. Export of informations

All information gathered about the structure of the network and current ongoing calls should be exported to a standalone server for the possibility of usage in additional applications. Given the expected utilization of developed tool in place of Computer Networks Laboratory at the Technical University in Kosice, technology of directory services by LDAP server was selected [7]. This technology enables the creation of tree structure of objects and each object keeps certain information about itself.

IV. Solution and Results

A. Developed tool and testing environment

The final result of this work is the application environment called "Network Topology Tool"(NTT). This tool was programmed in C language and compiled out by gcc compiler. It is distributed in the form of a single deb package. After installing and restarting the PC, NTT starts during Linux boot process. After an automatic start, NTT is running in the background of OS in the form of a daemon. Setting up all necessary parameters can be done by a configuration file, which is always loaded when applications is launching. While program is running, the processing of procedures is possible to manage only by telnet connection. It is possible through telnet server compiled in NTT. This interface offers the ability to enter execution instructions for reconfiguration, restoring data to an LDAP server, display current information concerning the structure of IP networks, display information about current VoIP communications, etc. Detailed reports of actually performed actions can be observed in statements in the console, in which NTT is running.

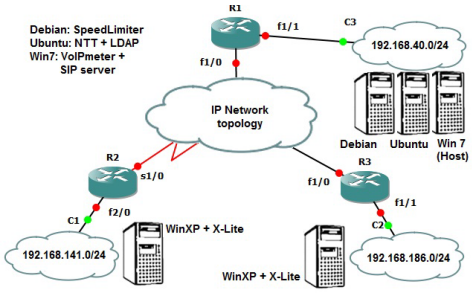

Figure 1. Software tools schematic layout

Figure 1 shows a schematic representation of a test environment. In this environment there were 3 final subnets. On subnet 192.168.40.0/24 was ran 3 PCs with different operating systems, as shown. Application Speedlimiter on Debian was used to generate synthetic traffic. Application VoIPmeter on Win 7 was used as a VoIP analyzer and sending out all the information of ongoing calls to the NTT via custom protocol named "Information Protocol VoIP"(VIP). SIP server has served as a registration server for SIP phones. On the Ubuntu system there was running the test application "Network Topology Tool" and LDAP server. Each of the remaining two subnets includes one Win XP with installed software SIP phone "X-Lite". All communication between subnets 192.168.141.0/24 and 192.168.186.0/24 has been redirected so that it passes through the network card in the system Win 7. With this modification it is possible to detect phone connection between the X-Lite phones using the VoIPmeter.

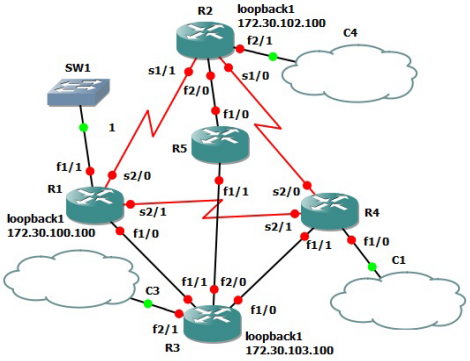

Figure 2. One of the test environment

Figure 2 shows one of the tested IP networks. These networks were used for testing the detection of structure, finding alternative routes between routers, as well as for automated reconfiguration of routers. In Figure 3 there is a segment of statement from telnet interface of NTT tool, which contains a text description of monitored network topology. Concrete, information of router R4 can be seen.

```
ROUTER: R4.GNS UNIQUE_SERIAL: ca-3-c-24-0-0
        IF NAME: FastEthernet1/0
        IF IP: 192 168 40 130
        IF IP_MASK: 255 255 255 0
        IF MAC: ca 3 c 24 0 1c
                VoIP Info:
                # Calls 0
                Link Icpif: 0
        -----------------------------------
        IF NAME: FastEthernet1/1
        IF IP: 172 20 0 43
        IF IP_MASK: 255 255 255 0
        IF MAC: ca 3 c 24 0 1d
                VoIP Info:
                # Calls 0
                Link Icpif:  1
        Neighbor: R3.GNS
        -----------------------------------
        IF NAME: Serial2/0
        IF IP: 172 20 103 45
        IF IP_MASK: 255 255 255 0
        IF MAC: 0 0 0 0 0 0
                VoIP Info:
                # Calls 0
```

Figure 3. An extract of the detected IP network by "Network Topology Tool"

B. *Progress and results of testing*

Testing optimization process based to the loadblanacing and QoS is the same, except the point where the mention of that specific method was used and in results of testing. The sequence of events during the testing of Automatic QoS reconfiguration of network topology to optimize VoIP communication was as follows:

1. Manual start NTT application environment and application VoIPmeter. NTT perform the whole initialization process (detect network topology, etc.).
2. Start a phone call between the X-Lite phones. VoIPmeter captures start of VoIP communication and detects communication ports for RTP transmission. This event is sent to NTT.
3. Transmission of RTP data with voice data in progress. VoIPmeter monitors the transfer and calculate transmission parameters, which are then sent to NTT.
4. Launch an application "Speedlimiter" for generating synthetic data to simulate network traffic.
5. NTT tool according to data from VoIPmeter detects that the packet loss and jitter rates increases. In excess of the threshold, automatic reconfiguration takes place. This is done by expect scripts with dynamicallygenerated instructions for setting Assured Forwarding and Expedited Forwarding, as part of QoS optimization.
6. After completion of optimization process, the transmission parameters of the phone connection return to normal.
7. Termination of VoIP connection. VoIPmeter detects this event and communicates it to NTT. The "Network Topology Tool" setup all reconfigured routers to its original form on the basis of information about completion of call connection.

The main difference in testing loadbalance optimization versus QoS optimization was, that sending packets through different routes, although the same qualitative valuation (such routes are the preferred by NTT tool), may cause delivery of packets in wrong order.

V. CONCLUSION

The aim of this work was to create applications, that will run on the background of linux operating system, where they will autonomously manage network traffic, focusing on optimization of VoIP communications.

With the tool "Network Topology Tool" is automatic detection of IP network structure available. With the information obtained directly from the network and with information of ongoing calls it is possible to automatically reconfigure a group of routers. This reconfiguration may be accomplished by distribution load or by increasing the priority of critical communications. QoS optimization provides the necessary effect of increasing the quality of transmitted voice. Method of loadbalance, in case of absence of buffer on the recipient side, could adversely affect quality of communication. For this reason it would be appropriate to replace the distribution of communications for redirect communication. Redirection would be undertaken through a less busy Path.

Suitable continuation of this work would extend its support for IPv6, or addition program based on updated data on LDAP server for drawing the entire network topology and displaying parameters of elements.

VI. ACKNOWLEDGEMENT

This work was supported by The Slovak Cultural and Educational Grant Agency of Ministry of Education of Sslovak Republic (KEGA) under the contract no. 3/7245/09(60%). This work is also the result of the project implementation: Development of The Center of Information and Communication Technologies for Knowledge Systems (Project number: 26220120030) Supported by The Research & Development Operational Program funded by The ERDF (40%).

VII. REFERENCES

[1] WALLACE, K. VoIP bez pedchozch znalost. translated by J.Gregor. $1st$ ed. Brno: ComputerPress a.s., 2007. 231 p. ISBN 978-80-251-1458-2

[2] WANG, Z. 2001. Internet QoS : architectures and mechanisms for Quality of Service. San Francisco: Morgan Kaufmann Publishers, 2001, 239 p. ISBN 1-55860-608-4

[3] MAURO, D., SCHMIDT, K. Essential SNMP. $2nd$ ed. Sebastopol: O'Reilly Media, 2005. 460 p. ISBN 0-596-00840-6

[4] RUSSELL, T. 2008. Session Initiation Protocol (SIP): Controlling Convergent Networks. New York: McGraw-Hill Companies, 2008. 264 p. ISBN 0-07-148852-9

[5] CISCO SYSTEMS, Inc. Cisco IOS IP SLAs Configuration Guide: Release 12.4. San Jose: Cisco Systems, Inc., 2008. 271 p.

[6] LIBES, D. Exploring Expect. Sebastopol: O'Reilly Media, 1994. 608 p. ISBN 978-1-56592-090-3

[7] VOGLMAIER, R. 2004. The ABCs of LDAP: How to Install, Run, and Administer LDAP Services. Boca Raton:Auerbach Publications CRC Press Company, 2004. 440 p. ISBN 0-8493-1346-5