Bandwidth Management Application in Directory Service Environment

Marius C. BREABAN, Adrian GRAUR, Alin D. POTORAC, Doru G. BALAN
Computers, Electronics and Automation Department, Integrated Center for Research, Development and Innovation in Advanced Materials, Nanotechnologies, and Distributed Systems for Fabrication and Control (MANSiD)
Stefan cel Mare University of Suceava, Romania
marius.breaban@gmail.com, adrian.graur@usv.ro, alinp@eed.usv.ro, dorub@usv.ro

***Abstract*-In the current context of developing real-time applications and actual data networks access dynamic, organizations (public institutions, companies, etc.) there are turned into account by using important resources so that to provide data traffic with a manageable bandwidth for all users. Security policies and Quality of Service (QoS) on current networks need to be manually configured or transmitted as configuration scripts on hundreds or even thousands of network devices. This generates changes for extremely complicated trafficking policies. Considering the above, in this paper we are aiming to present a new type of bandwidth management application, targeted for particular users' group, depending on the prerogatives given by a Directory Service type server. The bandwidth control solution is shown using a JAVA developed application. Bandwidth limiting process is conducted by replacating and automatically run a java file, followed by the user's authenticating process on an Active Directory server. This paper presents the involved elements used to perform network bandwidth limitations, bandwidth tests and also the results obtained while testing the developed bandwidth control application**

Keywords—bandwidth management; computer network directory service; quality of services; user level java environment;

I. INTRODUCTION

The large organizations development needs a variety of activities, constructively conducting to the fast evolution of network infrastructure and IT services. According to the complexity and specificity of different types of transmitted information, this infrastructure needs to be efficient, malleable and controllable while accomplishing the expectations.

Available solutions fulfill these demands, but they are always connected to different necessary changes as hardware and software upgrades, as the extension of the number of users with an exponential increase of related services, as communication management centralization and flexibility to several important reconfiguration needs.

A different specific goal to providing the access to network facilities based on the particular needs of accessing clear information or applications.

Nevertheless, in handling a private network by limiting the traffic rate, network administrators can manage the incoming and outgoing traffic data rate so that no user or application should exceed the maximum allocated transmission rate or monopolize the channel bandwidth. Network administrators can setup policies to confer bandwidth to specific users, user groups, or applications.

For real-time applications, there is needed to be found a path satisfying the requirements in terms of bandwidth, delay buffer, etc. needs to be found. As conventional IP routing is based only on hop counts, it is not suitable for multimedia applications. It is clear that, to route requests that have QoS requirements, existing routers should have QoS awareness and the packet forwarding should be based on QoS parameters.[1]

Bandwidth limitation can help streamline activity by controlling how much and when a specific amount of bandwidth is available as alternative for purchasing additional WAN capacity, unless the situation requires it.

Traffic limitation policy imply network policy that allows the network administrator to manage the traffic flows by applying defined rules to the entire traffic, from or to a particular network interface.

Bandwidth management is a major requirement when it comes to data traffic demands for operations of corporations or institutions with a large number of users, from the point of view concerning the quality of data services, regard of the physical zone of activity.

In this paper, we propose a new approach and a developed application for bandwidth management that relies on the idea of moving the control from the network equipment to the network interface of the computing system. Using this application we provide to the user a certain amount of bandwidth depending on the type of application that he uses at a particular time. Basically, this new approach is a solution for configuring QoS parameters by running the necessary procedures on the local communication interface with externally provided data traffic limitation parameters.

This application provides the limitation parameters, as data rate, for every user interface while for other users a guaranteed bandwidth naturally appears. The bandwidth availability depends on the user's appurtenance to a specific user group in a Windows Domain Controller (AD) service and is not involving the active networking devices into the scenario.

978-1-5386-1495-2/18/$31.00 ©2018 IEEE

II. BANDWIDTH MANAGEMENT APPLICATION

A. Bandwidth management-actual pattern

Today, there are a multitude of software and hardware solutions for data traffic management over the networks. Among the most important we can nominate the following ones:

- Sophos [2]- provides solutions to limit data traffic through firewall equipments, for each user using, an integrated software management platform on an Active Directory server;

- Fiddler [3]- Provides solutions for limiting local data traffic, on the workstations, over TCP / IP (8080 and 21 ports);

- SolarWinds [4] - is a network configuration manager that allows heterogeneous configuration management, providing a single point of management for routers, switches, firewalls.

- Nomadix [5] - Provides bandwidth control through dedicated access gateway equipment for wireless or wired networks. This solution, offer wireless connectivity solutions across networks and public access enterprises, providing easiness in data network management. The equipment's ensures user's authentication and bandwidth control.

The analysis of each solution has shown that bandwidth management requires resources so that to acquire dedicated network equipment or dedicated software programs. The software solutions offer Layer 2 and Layer 3 data traffic limitation and they are developed on C++ platforms or C++ and Java combined platforms.

Additionally, traffic-limiting software solutions provide limitation of traffic only locally and not in a client's-server configuration, moreover, only filter data traffic in the public Internet network.

The proposed solution can limit the traffic of data as well both in the public Internet network and in private networks.

B. The new bandwidth management application

The conducted researches investigate the problem and identify as a viable solution the possibility to manage and shape the data flow on the user's side interface instead of doing that on the data concentrator node. The goal is to distribute and to move the processing effort related to traffic shaping computations in to the local user reducing the data load starting with the first communication area.

As described in other papers as "New Approach to Traffic Management on Local Networks" [6] and "Endorsement of a User-level Bandwidth Management Application in a Directory Service Environment" [7], the new approach is a solution based on a Java application that allows data traffic to be limited to the user, taking into account his appurtenance of a group of users in Active Directory server. [8]

This application allows traffic limitation management directly on the workstation, running automatically and with no needed traffic management on network data switches.

It should be noted that the proposed application can be a solution for small and medium-sized enterprises where these traffic restrictions are necessary so that to avoid network congestion. User's control is performed through an Active Directory server, which was interrogated for authentication. This process provides individual variable bandwidth depending on the users' group membership.

The new solution, proposed here, allows a data traffic management feature, usually configured on active devices available in network nodes, being replaced by a data traffic limitation application that works on the local workstation, where the users are logged in, making available the remaining bandwidth for other users.

Here, we propose a new solution for TCP/IP communication between the systems belonging to the same domain server.

As presented in the article "Local Management for QoS parameters" [9], to provide filtering of data traffic through the system network interface for TCP/IP protocol, all at various bandwidth, there was chosen the Fiddler web debugger.

This software solution, provide a local proxy for data traffic, thus ensuring data traffic filtering, being data traffic monitoring tool on the network interface of host system.

It simulates some network tests, using some traffic rules established by the administrative user which are defined in the Java type files.

Unfortunately, as is mentioned above, this local proxy software, perform bandwidth limitation only for two logical ports": 21, meaning File Transfer Protocol (FTP) and 80, HyperText Transfer Protocol (HTTP). [3]

Practical, the new solution proposed in this article, provides network data limiting, for all TCP/IP data traffic, generated by any computer system joining the Active Directory server.

Being given the software and hardware requirements that are necessary to run files limiting traffic, this new solution offers the advantage of running on all computer systems, regardless of the configuration provided to support Java utility installation.

C. The testing of new solution

As test bench, the used available hardware was based on one HP Probook 640 series computer having an Intel i5 processor, 4GB RAM and a Gigabit Ethernet interface (WS3) and two Fujitsu Lifebook series computer with Intel i5 processor, 4GB RAM and a Gigabit Ethernet interface (WS1, respectively WS2). Presentation of topology is in fig. 1.

We mention that, the setting of the Cisco Catalyst 3750 switch had QoS services disabled, during which all frames/packets passing through the switch are unaltered and all traffic is transmitted on a "best-effort".

On WS3 workstation, we accommodated Windows 2003 Server as a virtual machine that ran the "*bandwidth.test*" domain server and host "*Active Directory*" server.

Fig. 1. Client-server topology

In the "*Active Directory*" server, there were aroused groups and users. Each user was inserted into a user's group as presented in figure no. 2.

We have to mention that users and user groups have been created to reflect the imposed traffic restrictions.

Thus user100M, belonging to the group "admin100M", has a bandwidth of 100 Mbps, user70M, belonging to the group "admin70M" has a bandwidth of 70 Mbps, user50M belonging to the "admin50M" group has a bandwidth of 50 Mbps and so on.

In order to run automatically, on WS1 workstation we copied a "*banda.bat*" file that contains the command to copy and respectively to launch the developed java traffic limiting file transferred from the "Active Directory" server to the workstation memory. [11]

The effectively run of "*banda.bat*" file consists in a few steps starting with copying the "*banda.bat*" file, after logon, as presented in fig. 3 and in fig. 4 and run the "*banda.bat*" file. The "*banda.bat*" file implies the following commands:

- compare if "*Banda*" directory exists on "C:\" drive, if not, the need to be aroused is flagged;

- copy the "*ClientTCPIP8080.jar*" or "*ClientTCPIP21.jar"* file from the server to the workstation in the new "*C:\ Banda*" directory;

- run the "*ClientTCPIP8080.jar*" or "*ClientTCPIP21.jar"* file.

All these operations with their syntaxes are detailed in Fig. 5 and 6. [8]

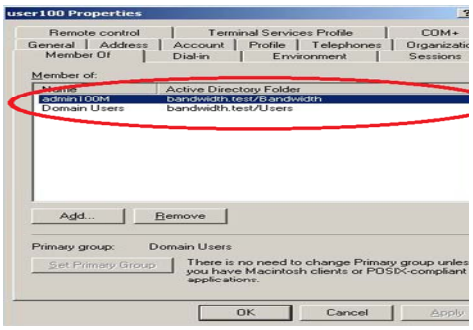

Fig. 2. Groups and users in Active Directory server

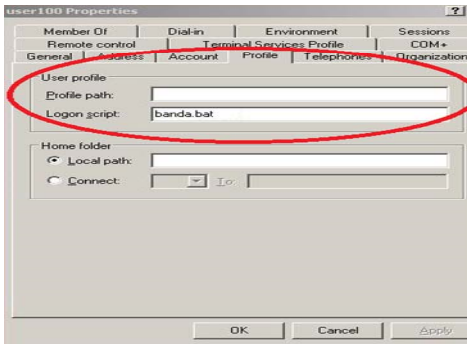

Fig. 3. Set profile user's logon copy "*banda.bat*" file at user's logon

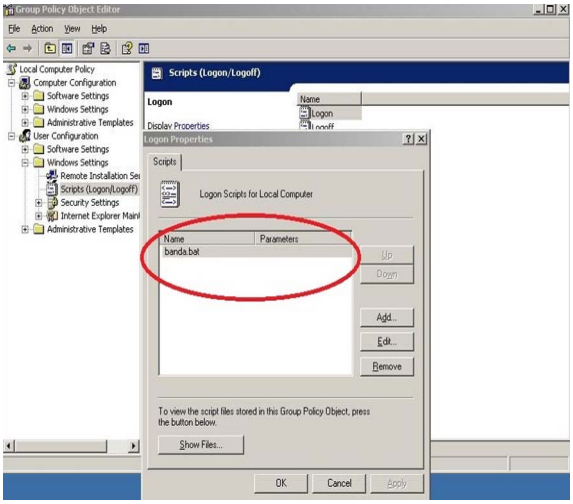

Fig. 4. Set profile user's logon to run "*banda.bat*" file at user's logon

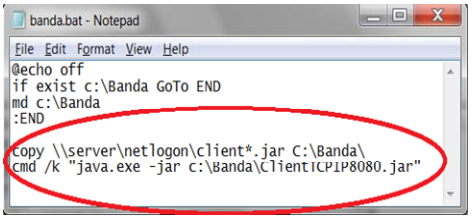

Fig. 5. "*Banda.bat*" file content for 80 TCP/IP port

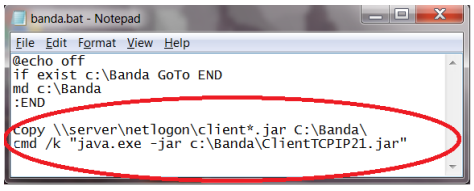

Fig. 6. "*Banda.bat*" file content for 21 TCP/IP port

A Java project may contain, depending on the complexity, one or more classes (files that contain program routines), and one class being defined as the primary class.

In such a project, the main class is automatically run and the other classes are called according to its content.

Reported to the Java TCP/IP application, the project "*ClientTCPIP8080.jar*" contains the main class (file) "*BandwidthUser.java"* and "*ClientTCPIP1.java"*.

”*BandwidthUser.java”* file contains the following operations:

- Extract the user’s rights, using the Microsoft Windows command "*gpresult*" and spotting the user in the user’s group as named on the domain controller;

- Define and provide a variable bandwidth, depending on the users group from the Active Directory server. We have to note that the bandwidth provided for each user was defined by setting a buffer length for each user group as follows: 2535 bytes for user100M, belonging to the group "admin100M" - 100 Mbps bandwidth, 1750 bytes for User70M, belonging to the group "admin70M" - 70Mbps bandwidth, 1210 bytes for the user50M belonging to the "admin50M" group - 50Mbps bandwidth, 690 bytes for user30M, belonging to the "admin30M" bandwidth 30 Mbps, 215 bytes for user10M, belonging to the "admin10M" group - 10 Mbps bandwidth;

- Call the "*ClientTCPIP1.java*" file.

The "*ClientTCPIP1.java*" file contains the following commands:

- takes the value of the bandwidth allocated to the user from the "*BandwidthUser.java*" file;

- establishes connections to the server on port 80 or 21;

- establishes input and output communication channels on the network board;

- transmit to server the information about bandwidth allocated to the user;

- reads and displays the data received from the server.

On the workstation WS2, defined as server station, we run the ”*server.bat*” file that contains the command to launch the ”*ServerTCPIP.jar*”, as presented in fig.7.

”*ServerTCPIP.jar*” file contains the main class (file) ”*ServerTCPIP1.java*”.

”*ServerTCPIP1.java*” file contains the following operations:

- establishes connections to the WS1 workstation on port 80 or 21;

- attends for traffic on the network interface entry;

- establishes input and output communication channels on the of the network interface;

- reads the user bandwidth value;

- sends a data stream at the bandwidth set by the user and displays information about the transmitted data.

The above steps are shown in fig. 8.

The WS1 workstation transmits the data packets with limited bandwidth, depending on the bandwidth transmitted by the WS2 workstation, allocated after the user’s authentication.

The WS2 workstation receives the data packets at the bandwidth transmitted by the WS1 workstation, as can be seen from the traffic analysis in Fig. 9, 10, 11 and 12.

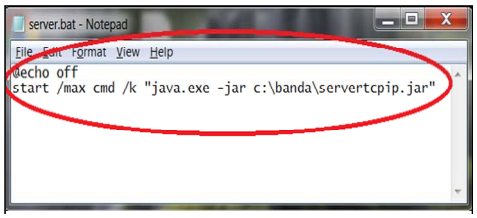

Fig. 7. “*Server.bat*” file content

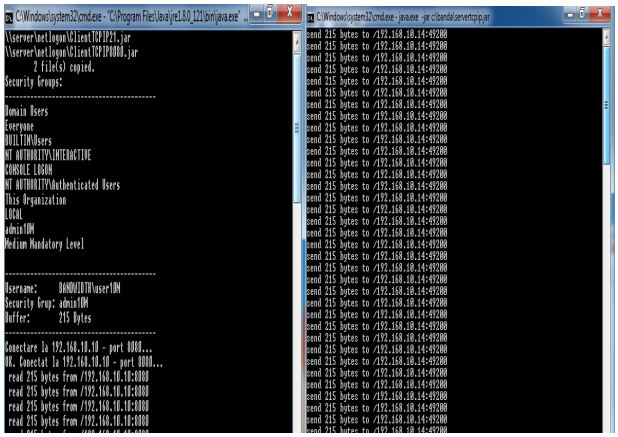

Fig. 8. User10M from admin10M group authentication and server transmission

We have to mention that, for graphical traffic analyze we used mrtg free software.[11]

The *Multi Router Traffic Grapher* or MRTG is an opened source tool, that creates graphs analyzing SNMP information collected from network equipment and servers.

Almost any SNMP-capable device can be managed with MRTG utility and all information generated by MRTG is displayed through a web browser.

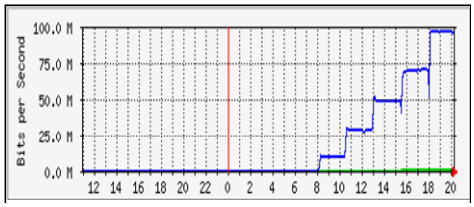

Fig. 9. Traffic analysis for WS1-port 80

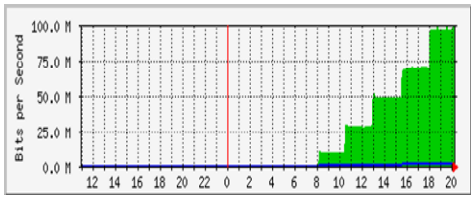

Fig. 10. Traffic analysis for WS2-port 80

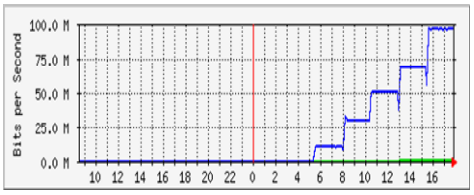

Fig. 11. Traffic analysis for WS1-port 21

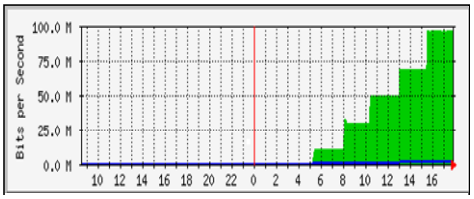

Fig. 12. Traffic analysis for WS2-port 21

Analyzing the graphs generated by the transmission/reception of data flow on network ports, can be specified that there are no significant variations between the bandwidths limitations applied for port 80 and port 21, except a bandwidth with an upward trend (approximately 0.5 Mbps) for the limitation applied to the transmission on port 21, due to the way the packet is made.

The explanation for this enhancement should be the fact that data transfer using HTTP, includes in the header, at the moment of transmission, a set of information regarding last change data, character encoding, server name and version while FTP transfers do not send such a header.

For smaller files, the header can be a significant part belonging to the amount of actual data transferred.

We mention that, after consulting the published papers, no such simulations have been identified.

III. Conclusion

The traffic limitation management application is actually a system, providing a solution to successfully replace the bandwidth control on switches and router devices.

The novelty is that, this application allows managing the output data traffic limitation directly on the client is workstation, automatically running without the need to configure or reconfigure the active network equipments (router, switch).

The above-mentioned developed application provides the ability to shape the traffic in a unitary mode, centralized and a dynamically way at the user's application level. The method is based on facile configuration steps and does not need advanced knowledge in information technologies and data flow management.

Moreover, the only interaction with the server is when the user logs in, the traffic limitation being performed independently from the workstation.

The advantage such a solution is the facility and minimal use the resources of the computing system.

Another advantage is represented by the user's security insurance meaning that, by copying the HTML "gpreport" file and taking by comparison, the user is framed in a certain group having allocated a certain bandwidth, independent of the connection to the AD server.

The next development direction of this solution is to integrate into a single software packet the data traffic limitation files for UDP and TCP / IP protocols for all logical ports so that, depending on the protocol used, the application performs, automatically limiting the traffic for a particular user.

Acknowledgment

Thanks to the Integrated Center for Research, Development and Innovation in Advanced Materials, Nanotechnologies and Distributed Systems Manufacturing and Control, developed under the Contract No. 671/04.09.2015, the Sectorial Operational Program Increase of Economic Competitiveness, co-financed by the European Regional Development Fund for research infrastructure made available and used in the thesis.

References

[1] D. Ghosh, V. Sarangan, R. Acharya, "Quality-of-service routing in IP networks", IEEE Transactions on Multimedia (Volume: 3, Issue: 2, Jun 2001)

[2] Sophos XG Firewall, https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophos-xg-series-appliances-brna.pdf?la=en, [available at February 22, 2018]

[3] Fiddler-The free web debugging proxy for any browser, system or platform, https://www.telerik.com/ download/fiddler/fiddler2 [available at February 22, 2018]

[4] Network Configuration Manager-Administrator guide, version 7.7, https://www.solarwinds.com/ [available at February 22, 2018]

[5] Bandwidth Management Access Gateways, http://www.nomadix.com/access-gateway [available at February 22, 2018]

[6] Marius C. Breabăn, Adrian Graur, Alin D. Potorac, Doru Bălan "New approach of traffic limitation management on local networks" 2017 16th Optimization of Electrical&Electronic Equimpment, Aegean Conference on Electrical Machime and Power Electronics(OPTIM), Braşov, 2017

[7] Marius C. Breabăn, Adrian Graur, Alin D. Potorac, Doru Bălan "Endorsement of a User-level Bandwidth Management Application in a Directory Service Environment" 21st International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, *2017*

[8] Microsoft Official Course, "2279B:Planning, Implementing and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure", Microsoft Corporation, 2003

[9] Marius C Breabăn, Adrian Graur, Alin D. Potorac, Doru Bălan "Local management for QoS parameters", 15th RoEduNet Conference: Networking in Education and Research, 2016

[10] Java SE, http://www.oracle.com/technetwork/java/javase/downloads/index-jsp-138363.html#close [available at April 20, 2018]

[11] Elliot Rusty Harold, "Java Network Programming-fourth edition", O'Reilly Media, pp 28-30, 2014

[12] The Multi Router Traffic Grapher, http://oss.oetiker.ch/mrtg/doc/mrtg-nt-guide.en.html [available at April 20, 2018]