A NOVEL SOLUTION FOR QOS IMPLEMENTATION IN DATA NETWORKS

Marius C. Breabăn,¹ Adrian Graur,² Alin D. Potorac,³ Doru G. Bălan⁴

Abstract: Current data networks carry a multitude of data types. These include high-definition video streams and other data sensitive to network delays as well as real-time voice transmissions.

Active network node equipment fulfills requests, while providing network management without affecting the data availability. Starting out from this model, a new idea is based on moving the network bandwidth control at the user's communication interface. This paper presents a new approach to setting up QoS parameters based on local upstream traffic limitation management. This approach is quite useful in providing a certain guaranteed bandwidth for the users. So, this software ensures a specific network bandwidth according to with the rights coming up from their association with a certain "Active Directory" group of users. The necessary active network equipment in terms of basic QoS management can be replaced by a local application for data traffic limitation, while for the involved participants the remaining bandwidth for other communications has a higher degree of availability. An efficient bandwidth control can be implemented when extracting specific AD fields and transferring pre-calculated user related parameters to a local running limiter.

UDC Classification: 004.77 **DOI:** <http://dx.doi.org/10.12955/cbup.v5.1070>

Keywords: QoS, bandwidth limitation.

Introduction

The continued development of organizations, as well as the diversification of activity has also implicitly led to the rapid development of network infrastructure. Due to the complexity of the types of information conveyed, this infrastructure must be efficient, flexible and manageable. Unfortunately, the existing solutions partially meet these requirements, being susceptible to changes such as hardware and software upgrades, exponential growth in organizational development, centralized management, and efficiency improvements to major reconfiguration changes.

Another major issue is providing access to network resources based on the need to access certain information or applications.

Thus, in managing a private network by limiting the traffic rate, network administrators can control the input and output traffic rate, ensuring that no user or application exceeds the maximum transmission rate or monopolizes the band.

Network administrators can set policies to allocate bandwidth to specific users, user groups, or applications.

A traffic limitation policy is a network policy that allows the network administrator to evaluate traffic flows by allowing the policy to apply to all traffic from or to a particular network interface.

Bandwidth management is a requirement of data traffic, necessary for the efficient operation of data network corporations or institutions with many users, while ensuring the quality of data services regardless of the area of activity.

The solution for data traffic limitation

Current traffic patterns allow setting QoS rules on a distributed model at the traffic source using proper equipment.

According to the new approach of traffic limitation management, we propose a java application solution, which would provide traffic limitation options for a specific user, depending on his affiliation with a certain group of users.

This application can provide traffic limitation management avoiding the use of a layer three data switch and setting specific bandwidth availability for other client workstations.

The novelty of this implementation consists in the fact that, by applying upstream data traffic limitation at the network interface level, it provides, data upload traffic limitation at each user's level. (Breabăn, 2016)

¹ Ștefan cel Mare - University of Suceava, Romania, marius.breaban@gmail.com

² Ștefan cel Mare - University of Suceava, Romania, adrian.graur@usv.ro

³ Ștefan cel Mare - University of Suceava, Romania, alinp@eed.usv.ro

⁴ Ștefan cel Mare - University of Suceava, Romania, dorub@usv.ro

We focused on the following research directions:

- transferring the traffic limiting java file, after the user authentication on the workstation; (Microsoft, 2003)
- file transformation, which use commands to launch the java application as a Windows service and run it automatically when the operating system starts up;
- reading user's rights and account proprieties, using a Microsoft Windows tool, *gpresult* command ([https://technet.microsoft.com/en-us/library/cc733160\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc733160(v=ws.11).aspx), 2017), and then placing the user in the user's group membership, as it is defined in the *Active Directory* server; (Microsoft, 2003)
- providing a specific bandwidth limit for the outgoing traffic through the network interface of the workstation;

For the tests, there were two HP Probook 640 series computers used, with Intel i5 processors, 4 GB RAM, Gigabit Ethernet network cards and a switch Cisco Catalyst without the QoS settings (Cisco, 2010). The topology is presented in Figure 1.

Figure 1: Client-server topology

Source: Author

On the HP Probook 640 series computer having the IP address 192.168.10.15, we installed a Virtual Machine Windows 2003 Server, with a running Active Directory and DNS (Domain Name Server) (Microsoft, 2003) server while at the other end the host workstation is engaged.

On the "Active Directory" server, we created groups, respectively users, as presented in Figure. 2.

Figure 2: Groups and users in Active Directory server

Source: Authors

For the automatic run, we proceeded in copying a "bandwidth.bat" file from the Active Directory server to the workstation, and converting it as a Windows service able to automatically run after the user login. The "bandwidth.bat" file contains the following elements:

- compare if the directory named “Bandwidth” exists on “C:\”drive, if not it will be created;
- copy the “*bandwidthUser.jar*” file from the server to the workstation in “C:\ Bandwidth” directory already created;
- run the “*bandwidthUser.jar*” file.

All those operations are presented in Figure 3. We mention that Java(TM) SE Runtime Environment (build 1.8.0_112-b15) (Java SE, 2017) was used, both for the server and for the workstation.

Figure 3: BandwidthUser.jar file contains

The conversion as Windows Service was made using “NSSM” (<http://www.nssm.cc>) freeware software, as presented in Figure 4.

Figure 4: NSSM launch service install

For the automatic run after the user’s logon, we setup the “bandwidth” service to run automatically, as presented in Figure 5.

The “*bandwidthUser.jar*” file has the following functions:

- reading the user’s rights, using Microsoft Windows “*gpresult*” command and placing the user in the user’s group membership, as it is defined on the *Active Directory* server,
- creating a string buffer in which information from the “*gpreport*” file are stored, (<https://technet.microsoft.com/en-us/library/cc733160>, 2017) from the “*Active Directory*” server;
- selecting from the string buffer only the lines with the information regarding the security group;
- building a security groups list by ordering decreasingly using an associated UDP buffer value for the maximum outgoing data bandwidth to be tied with the workstation network interface. An UDP

datagram has a 1470 byte length. So, for a 100 Mbps bandwidth we have an UDP buffer size of 1470 bytes. From this point, we calculate the buffer size for respectively 70 Mbps, 50, Mbps, 30 Mbps and 10 Mbps;

- going along the list of the assigned security groups and check if the user is in one of the listed security groups. The loop stops at the first security group found in the list, and the amount of bytes that can be transferred in a time unit by each group member is extracted.
- the last step consists in displaying the user information;

Figure 5: Bandwidth Window service run automatically

Source: Author

We should mention that, the last step - user's information display, represent a necessary option, so that to show the java file execution. Normally, the application runs automatically, without displaying a message.

Thus, after running the "*bandwidthUser.jar*" file, the workstation displays the user's information, according to the security group membership.

So after logging the user belonging to a certain user group, a buffer size value is allocated representing bandwidth, as presented in table 1.

Table 1: User buffer allocation

User	Group	Buffer (byte)	Bandwidth (Mbps)
user10	admin10	109	10
user30	admin30	424	30
user50	admin50	728	50
user70	admin70	1038	70
user100	admin100	1470	100

Source: Authors

Figure 6 shows the displayed message for a user belonging to a group having the associated bandwidth of 30 Mbps. This message is displayed after logging in into AD domain. For user10, user50, user70, user 100 included in specific security groups the messages are similar except for the transferred traffic parameter numerical value which is a specific one for each individual group.

Figure 6: User30 from admin30M authentication

Conclusions

As presented above, this is a new approach as a software solution, in granting access to a larger or smaller traffic bandwidth to a group of users according to the user's position in the hierarchy and to the specificity of their activity among an organization.

The application for data traffic limitation is actually a system comprising of combined and distributed elements that offer an integrated solution to successfully replace the hardware data switch types of equipment for the implementations of local one-way data flow limitation but based on a centralized management.

As a further developing direction, the use in intensive data traffic conditions is about to be tested, based on the *iperf* (<https://iperf.fr>, 2107) tool, with an UDP (Postel, 2017) data transport between the two systems, continuously, at a 100 Mbps constant speed.

After the authentication, based on the predefined user's rights, the provided bandwidth should automatically be allocated in a group personalized manner, offering the necessary bandwidth allocation as part of QoS policy implementation.

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, to the Sectorial Operational Programme Increase of Economic Competitiveness, co-financed by the European Regional Development Fund for research infrastructure. All nominates, made available and used in the thesis.

References

- Aurrecoechea, Campbell, C., Hauw, A.T. and L. (May 1998). "A survey of QoS Architectures". Springer Verlag Multimedia Systems Journal, 138–151. <https://link.springer.com/article/10.1007/s005300050083>
- Breabăn, M.C., Graur, A., Potorac, A.D., Bălan, D.G., (2016). "Contribution for limiting and testing network policies". 2016 4th International Symposium on Environmental Friendly Energies and Applications (EFEA), Belgrade, 1-4. DOI: 10.1109/EFEA.2016.7748782
- Breabăn, M.C., Graur, A., Potorac, A.D., Bălan, D.G., (2016). "Local management for QoS parameters". 15th RoEduNet Conference: Networking in Education and Research, 1-4. DOI: 10.1109/RoEduNet.2016.7753218
- Breabăn, M.C., Graur, A., Potorac, A.D., Bălan, D.G., (2017). "New approach of traffic limitation management on local networks". 16th Joint International Conference OPTIM-ACEMP 2017: Optimization of Electrical & Electronic Equipment, 941-946.-to be published
- Cisco 4700 (2010). Cisco 4700 Series Application Control Engine Appliance Administration Guide. Retrieved from http://www.cisco.com/c/en/us/td/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA4_1_0/configuration/administration/guide/admgd.pdf
- iPerf (2017). The ultimate speed test tool for TCP, UDP and SCTP. Retrieved from <https://iperf.fr>

- Java (2017). Java SE. Retrieved from <http://www.oracle.com/technetwork/java/javase/downloads/index-jsp-138363.html#close>
- Kreutz, D., Fernando, M. V. Ramos, Verissimo, P, Rothenberg, C.E., Azodolmolky, S., Steve, U.(Oct 2014). "Software-Defined Networking: A Comprehensive Survey". Proceedings of the IEEE, 14 – 76. DOI: 10.1109/JPROC.2014.2371999
- Microsoft (2017). Gpresult. Retrieved from [https://technet.microsoft.com/en-us/library/cc733160\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc733160(v=ws.11).aspx)
- Microsoft Official Course (2003). "2279B:Planning, Implementing and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure". Microsoft Corporation
- Microsoft Official Course (2005). "2273B:Managing and maintaining a Microsoft Windows server 2003 Environment". Microsoft Corporation
- Patterson, I., (2017). NSSM - the Non-Sucking Service Manager. Retrieved from <http://www.nssm.cc>
- Postel, J., (1980). User Data Protocol, IETF. RFC 768. Retrieved from <https://tools.ietf.org/html/rfc768>
- Tadrous, J., Eryilmaz A., Gamal H.E., (2015). "Proactive Content Download and User Demand Shaping for Data Networks" IEEE/ACM Transactions on Networking , 1917-1930. DOI: 10.1109/TNET.2014.2346694