Transactions. Georgian Technical University. AUTOMATED CONTROL SYSTEMS - No 2(3), 2007

RESEARCH OF SERVICE DISTRIBUTION IN EDUCATIONAL NETWORK

Kartvelishvili Mikheil, Kartvelishvili Otar
Georgian Technical University

Summary

This article presents the service distribution analysis in network flows of the external traffic of the Georgian Research and Educational network and its application to the detection of typical and anomalous traffic patterns. As a result of this analysis the most used services were identified for different parts of the network. Network statistics collection was performed by the software system, that was constructed by optimal interconnection of different Netflow and SNMP protocol components, which gave the opportunity to acquire much more detailed statistical information.

Key words: Network. Research. Education. Application. Statistics. Software system. Protocol. Information.

1. Introduction

Collection of statistical data about individual network flows in computer networks creates the opportunity to perform an investigation of the link load levels, which will allow identification of overloaded segments and problematic areas. It is also possible to provide accounting of the traffic volume consumed by each user based on statistical data in order to charge him appropriately.

As SNMP protocol, which is currently widely used for collection of network statistics, does not give possibility to retrieve detailed information about separate flows, we constructed software system, which uses components of the new protocol created by Cisco Systems – Netflow. In order to make collected information more understandable, we intergrated into the system visualization software component – Cacti, which was originally built for SNMP protocol backend. Methodics of configuration of each component were developed, which allowed to perform interconnection of different building blocks. As a result of operation of the above mentioned system it became possible to obtain and visualize more detailed statistical information, than it was possible with previously used similar systems.

2. Discussion

The research of proportions of different network services – either inbound and outbound in relation to Georgian Research and Educational Networking Association (GRENA) network and its customer organizations, was performed. The analysis period was chosen to be equial to 24 hours during peak usage days. The obtained service distributions for inbound and outbound network traffic is shown on Fig. 1 a) and b) correspondingly.

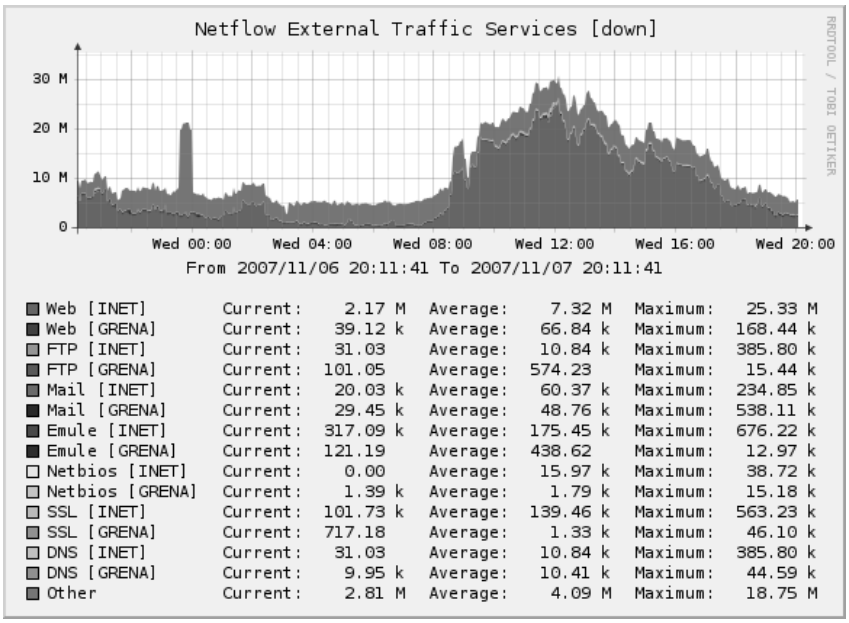

Fig.1- a)

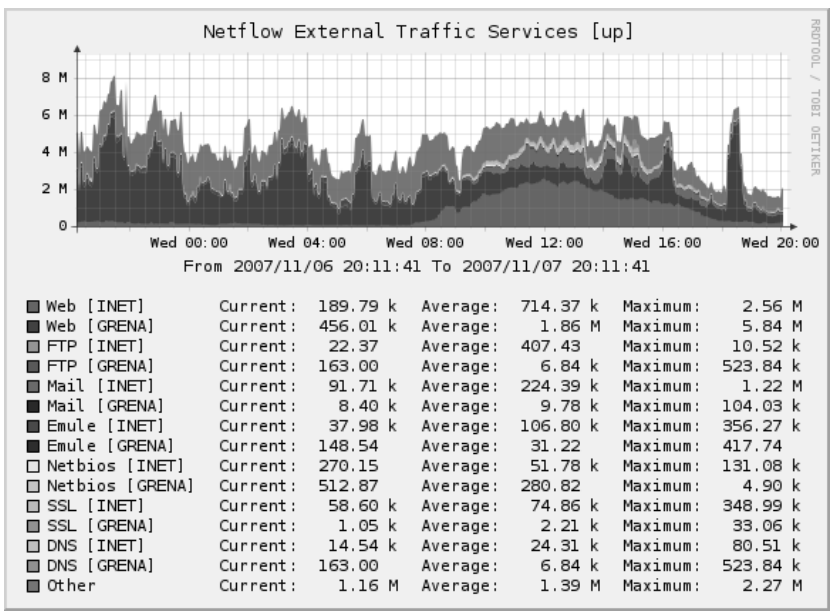

Fig.1- b)

Separate accounting was performed under the scope this research for the different data exchange directions: server is located in the Internet, client located in GRENA network (marked as [INET]) and the opposite - server located at GRENA side and client accessing it from the Internet (marked as [GRENA]). The research included the most widespread network services: Web service (HTTP), file transder service (FTP), e-mail service, peer-to-peer file shareing Service (Emule), network disk sharing service (Netbios), secure socket layer service (SSL), domain name resolution service (DNS). The rest of services with the neglible share in overall traffic were aggregated into single category (Other).

The main defferentiation criteria for network services for this research was chosen to be a transport protocol port number. This is the main reason of the fact, that multimedia protocols like H.323, SIP, RTP are not shown in the results as a separate category. As multimedia protocols do not use permanent port numbers to transport their flows and these ports are chosen dynamically for each session, it is necessary to use additional criteria in order to identify these flows correctly. The solution to this problem is the use of the special 8-bit field in the IP header called "Type of Service" (ToS). The value of this field for ordinary best effort data is 0, but the multimedia applications perform marking of this field with a custom value. As ToS field is different criteria, than the one used in this document, the analysis of multimedia flows must be subject of the upcoming research.

As it is shown in the graph in Fig 1.a), the highest share in the inbound traffic flow corresponds to the Web service consumed from the Internet web servers, which on average made up 58% (7,32Kbps) of the total throughput during analysis period, the share of other services is relatively neglible. The maximal load level was observed during working hours, as web service by its nature is highly interactive. We can make the following conclusions about outbound traffic based on the graph in Fig 1. b): the dominating part of the traffic is Web generated by the servers located inside GRENA network, the average share of which is 35% (1,86Mbps). During day hours the large portion of outbound traffic are web requests generated to the Internet web servers (5,84Mbps).

Besides creation of summary statistics, the presented system makes possible to analyse traffic loads for any IP address or groups of IP addresses (either source or destination). Inbound and outbound traffic patterns of the two largest universities – Tbilisi State University and Georgian Technical University were analysed. This is shown in the graphs presented in Fig 2. and Fig 3. a)

and b) correspondingly. As it can be observed from the graphs, the dominating share of both networks' traffic is web service.

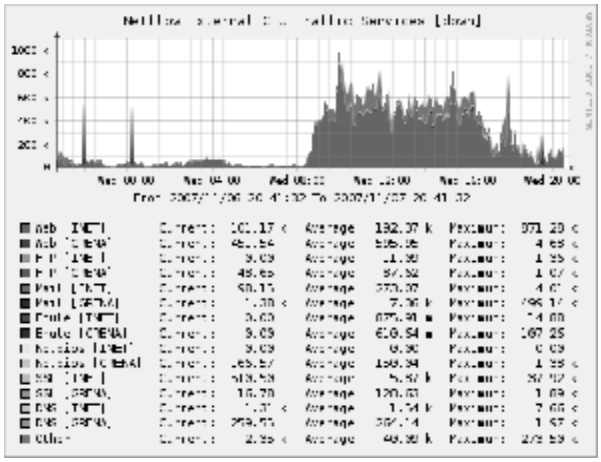

Fig.2-a)

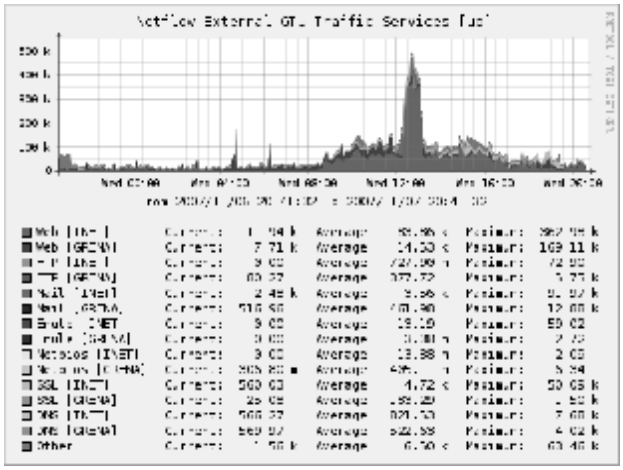

Fig.2-b)

In Fig 2. b) it is clearly noticable the significant portions of Netbios and SSL services. Netbios protocol is mainly used by Microsoft Windows operating systems for access to shared files and folders. This protocol is mostly used inside LANs and its appearance in the WAN traffic statistics is definitely an anomaly, which is the indication of the possible existance of one or several workstations that are infected by a virus or other malicious software. This observation definitely requires additional attention from the network security point of view.

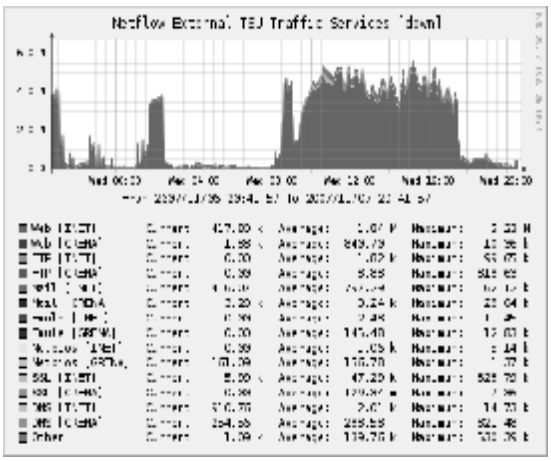

Fig.3-a)

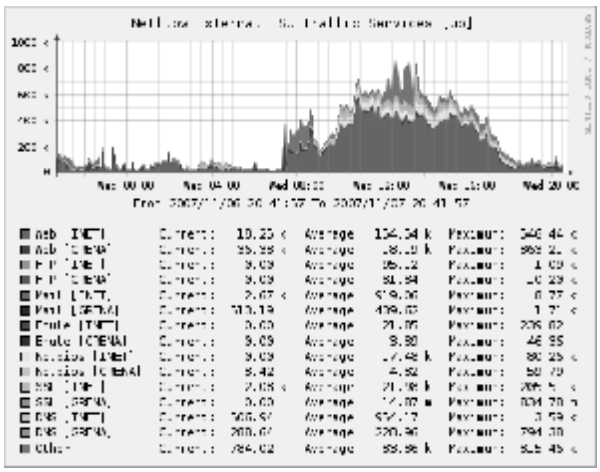

Fig.3-b)

3. **Conclusion**

The present research includes the analysis of service distribution of the inbound and outbound traffic of the Georgian Research and Educational network (GRENA), which became possible by creation of the network statistics collecting software system based on Netflow

protocol. The obtained graphs represent actual load generated by the whole network and separately by its different parts showing its component services. This gives opportunity to perform optimal tuning of traffic flows distribution among different paths to external networks and efficient monitoring of the network sercurity.

References

1.Configuring NetFlow and NetFlow Data Export (http://www.cisco.com/univercd/cc/ td/doc/ product/software/ios124/124cg/honf_c/chap05/ onf_bcf.htm)

2. Flow-capture Manual (http://www.splintered.net/sw/flow- tools/docs/flow- capture. html)

3. Flowscan Architecture (http://www.caida.org/tools/utilities/flowscan/arch.xml)

4. JKFlow Manual (http://users.telenet.be/jurgen.kobierczynski/jkflow/eindwerk.pdf)

5. Cacti Manual (http://docs.cacti.net/node/2)

6. M.Kartvelishvili, O.Kartvelishvili " The new mechanism of network statistics collection based on Netflow protocol ", GTU, "Shromebi", №1, 2008.

საგანმანათლებო ქსელში სერვისების განაწილების გამოკვლევა

მიხეილ ქართველიშვილი, ოთარ ქართველიშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

მოცემულია სამეცნიერო და საგანმანათლებლო ქსელში ინტერნეტის სერვისების განაწილების ანალიზი დამახასიათებელ და ანომალურ სქემების აღმოსაჩენად. გამოყოფილი იქნა ქსელში და მის ცალკეულ ნაწილებში ყველაზე მეტად გამოყენებული სერვისები. ქსელური სტატისტიკის შეგროვება შესრულდა პროგრამული სისტემის საშუალებით, რომელიც აგებული იქნა Netflow და SNMP პროტოკოლების ზოგიერთი პროგრამული კომპონენტების ოპტიმალურ შემადგენლობათა შეერთებით, რაც შესაძლებლობას იძლევა მიღებული იქნას ქსელის დეტალური სტატისტიკური ინფორმაცია.

ИССЛЕДОВАНИЕ РАСПРЕДЕЛЕНИЯ СЕВИСОВ В ОБРАЗОВАТЕЛЬНОЙ СЕТИ

Картвелишвили М., Картвелишвили О.
Грузинский Технический Университет

Резюме

Представлен анализ распределения Internet сервисов в науно-образовательной сети для выявления характерных и аномальных схем. Были выделены наиболее используемые сервисы в сети и ее отдельных частях. Сбор сетевой статистики производился с помощью программной системы, построенной из компонентов протоколов Netflow и SNMP, объединенных между собой оптимально. Это дает возможность получить детальную статистическую информацию сети.