"HENRI COANDA"
AIR FORCE ACADEMY
ROMANIA

GERMANY

"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY
SLOVAK REPUBLIC

INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER
AFASES 2011
Brasov, 26-28 May 2011

A PLATFORM MODULE AND A METHOD OF TRAFFIC ANALYSIS IN IP COMMUNICATION NETWORKS

Constantin GROZEA, Gigi-Daniel BUDARIU

Military Equipment and Technologies Research Agency, Bucharest, Romania,

Abstract: *This paper presents a hardware and software platform module based on open source applications for traffic analysis and optimization in communication networks with IP technology and a method of analysis which allows measurements of instantaneous and average traffic values allocated to various local network resources which are at the basis of module construction. These achievements are part of the research conducted within the "Complex system analysis and optimization of traffic in communication networks with technological diversity and convergence of services" (PNII-11029/2007).*

Keywords: *PNII-11029/2007, CNMP, ATRAF, analysis, method, IP networks*

I. INTRODUCTION

Measuring the dispersion of the average values for different traffic resources allocated IP communications networks offer real opportunities to highlight the existence of those portions of the network where traffic values required beyond the capabilities of network processing and transport in those areas, and other areas where the workload of resources in many cases does not exceed modest values of installed network capacity. Making traffic statistics and analysis of measurement results will be able to determine the choice of methods for optimization of traffic in these networks to be reflected in reduced operating costs.

The theme is quite broad scope and the approach has been facilitated by the sequencing of activities in a project launched in 2007, which was within the overall objectives of the Program 4 - Partnerships in priority areas, coordinated by the National Centre for Programme Management (CNMP), 2007 [1], [2]. Acronym of the project is ATRAF [3]. The project was based on a consortium of two higher education institutions (Military Technical Academy and Bucharest Polytechnic University), a research and development institutions (Military Equipment and Technologies Research Agency) and a private firm R&D activity (SC MARCTEL SIT SRL), thus encouraging collaboration between academia, R&D and business entities.

This article presents findings of preliminary studies, practical achievements and results of research conducted at the Military Equipment and Technologies Research Agency.

II. DESCRIPTION

Preliminary studies have considered the existing state of technology in support of communication and the desire to obtain a convergence in terms of services offered. So many topics were discussed of which I mention only some of the most important question: the architecture of computer networks (OSI layers, protocols, services access primitives, the relationship between services and protocols), Ethernet local area networks, applications, architecture, intelligence and support for ISDN services, mobile data communications (GSM) telephone networks and IP networks, Internet, local network traffic characteristics of the Ethernet protocol CSMA/CD Ethernet network performance, efficiency calculation channels communications, functional specifications and implementation of the driver and the Ethernet network communication other networks and communication protocols. Also review the functioning of converged networks in terms of communications services encompassing technological diversity.

The Military Equipment and Technologies Research Agency has developed a hardware platform and software module called ATRAF-MPMTFL-P2, with limited functionality as a stand-alone component of the overall hardware and software platform for modeling traffic in developed ATRAF project.

III. HARDWARE PLATFORM MODULE

Hardware platform module (Figure 1) is built on a LAN skeleton consisting of a server workstation and five client workstations. Separately, it also used an isolated workstation consists of a portable computer designed to work with a set of professional equipment, licensed software, for traffic generation and analysis, but are not part of the module. Hardware platform also includes networking components (switches, routers), computer peripheral equipment (uninterruptible power sources), external data storage devices (external HDD USB interface, SD memory cards for data storage), and several other inventory items.

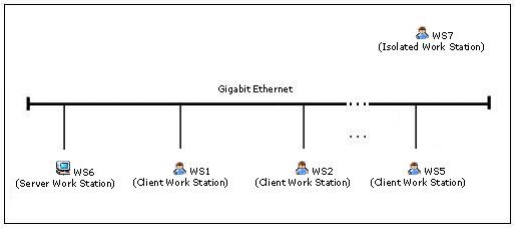

Figure 1. ATRAF-MPMTFL-P2 hardware components

Workstations are ordinary computers working under a common PC operating system (Windows, Linux [4], DOS, Unix) and can be used by ordinary users.

IV. SOFTWARE PLATFORM MODULE

Platform module include a set of software applications running under operating systems Debian/Linux, Ubuntu/Linux, or Windows XP SP2 and uses mostly open source software. Figure 2 is presented the application software operating systems operating under Debian/Linux, Ubuntu/Linux.

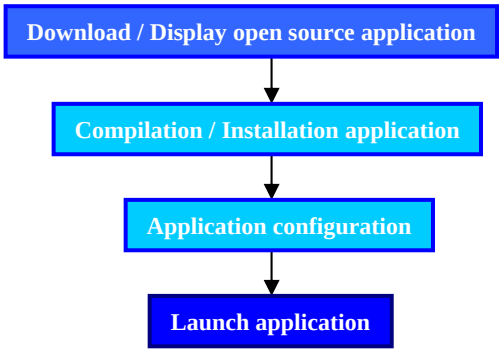

Figure 2. ATRAF-MPMTFL-P2 software components

Users are provided all necessary information about how to download and compilation of open source software, about installing software packages compiled under the Linux operating system (which can be compared with Microsoft software packages) in Debian and Ubuntu versions, or less under Microsoft Windows operating system and on setting up and launching applications. Depending on the workstation logged on, the user can access the server software or client software. The first use of open source software tools, these applications will be compiled from

open sources or packages will be installed automatically. Applications call functions from libraries and graphical user interfaces in the form of dialog or command line interface.

V. TRAFFIC ANALYSIS METHOD

The method of analysis of traffic in communication networks with IP technology begins with preliminary requirements specification, continue with step by step description of the set of tools used and the method continues with the actual steps necessary for analysis.

The set of tools used for applying the method comprising:

- a selection of the best open source software tools;
- representing some professional hardware generators and network analyzers licensed software.

The steps necessary for proper traffic analysis method allows the collection of statistical information IP network technology useful review. They are:

- configuration tools in the set used;
- traffic generation and testing;
- to obtain useful statistics about network traffic.

The method used both open-source software tools, free, which can be download from the Internet, hardware and software licensed professional.

The prerequisites followed in selecting open source software tools in the set were tested:

- Be very powerful even compared to similar commercial tools and already have very good references in benchmarks;
- Be as easy as possible to install;
- Have a good ergonomy and be easy to manage;
- Have an active and large community;
- Have no cost.

Even though some of the tools presented in our tutorials can be used on Microsoft Windows, they run better and increased security on Linux operating system.

Step by step description of open source software tools started from the premise that they can present very different levels of production, which can vary from basic scripts by software tools developed in a professional manner. The descriptions and information are included: hyper terminal application, term therapeutic application, advanced package management tools for Linux operating systems APT, the instrument software installation after compilation CheckInstall, Minicom serial communication program for Linux operating systems , installing the Microsoft fonts used, the use of MySQL commands, use PHP scripts, web browsers used for tests that require an Internet connection, etc.

The actual steps required to implement the method of traffic analysis, we tested a set of these software tools, test and still others will show you the steps necessary for analysis of traffic (including in terms of security) for each instrument in the test kit.

Figure 3 shows the main interfaces of network configuration (ifconfig, dhclient, ethtool, etc.), the instrument used to verify that the computer can be accessed via an IP network (ping), tcpdump [5], netstat , iperf / jperf [6], CDP.

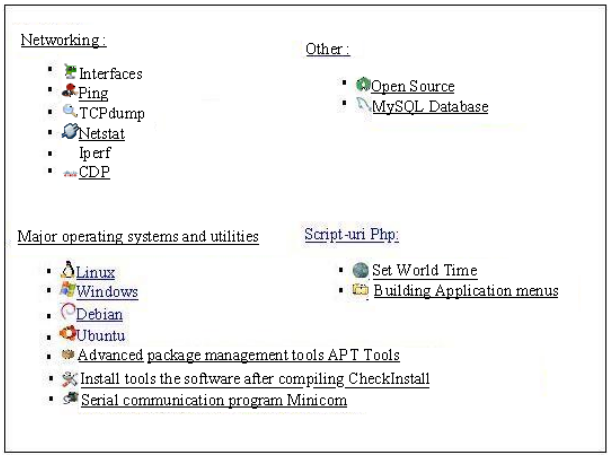

Figure 3. Configuration interfaces, operating systems, utilitaries, open sources, databases, PHP scripts

To generate traffic and testing applications using open source set of tools, shown in Figure 4 are software tools for analyzing traffic in IP networks (Wireshark [7], Ettercap [8], Snort & Base [9], Snort Inline & Base [10], Kismet, traffic monitoring (CACTI [11], PHP Weatermap), logging into the system (Php-syslog-ng, Rancid [12], Ipplan [13]), routing software (Vyatta [14] Quagga [15]), virtual private networking (OpenVPN) [16], software telephony (Trixbox) and emulation of links (WANem) [17].

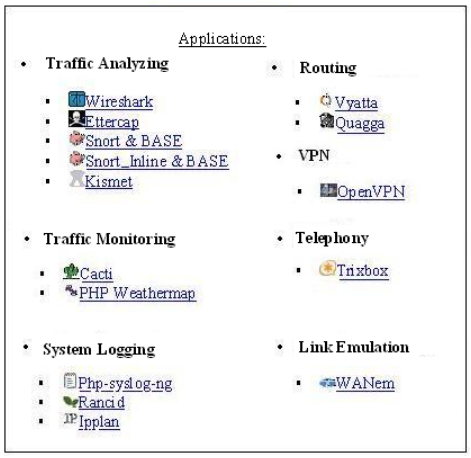

Figure 4. ATRAF-MPMTFL-P2 Software applications

Hardware professional licensed software, which are not part of the module are connected to the remote workstation and used to complete network statistics collected by the proposed method.

The method includes the steps necessary for a separate traffic analysis for the following four types of licensed software professional equipment:

Traffic generator and analyzer Spirent TestCenter SPT-2000A enables multi-user applications, while addressable multiple users of a test mode to increase efficiency of resource use device allows creation and execution of an extremely large number of tests complex and contains sequences of quick suggestions for reducing time to troubleshoot setup problems that may arise during the creation of new tests. SPT-2000A contains a large number of hardware and software, and chassis can be equipped with a variety of interchangeable modules. All chassis family of Spirent TestCenter equipment are compatible. All modules are easily operated remotely manageable via IP networks, to troubleshoot and replace.

Traffic test with Trend Multipro portable equipment is a test platform for Triple Play multiservice: IPTV, VoIP, Data, ADSL2+, VDSL2, QoE, MPEG, IP. This ensures fairness conduct tests for head-to-head operation between networking components that could be found for example in various converged networks, with multiple ways of making test performance and configurable services as required.

Digital pattern generator is PG3ACAB general purpose equipment that contains powerful tools for both work and production engineering. Generator emulation logic can be used as a stimulus for peripheral/ASIC, fixing/checking for confirmatory testing of large-scale production, small-scale testing products, and more generally for many other stimuli. When coupled with a Tektronix logic analyzer and / or a Tektronix digital oscilloscope, performing a complete test system.

TLA5202B logic analyzer is a portable device that combines high-speed timing resolution, fast state acquisition, long record time and sophisticated triggering circuit.

VI. RESULTS

By means of the traffic analysis module based on the proposed method, it was possible

to collect a large number of statistics about the network, such as for example:

- With open source software tools:
- For the traffic analysis:

• providing information about the data captured in the network and in the upper layers protocols, with Wireshark;

• using a software suite for attacks „man in the middle" within a local LAN network, with Ettercap;

• reading network traffic and display it on screen, with Snort, in sniffer mode;

• recording network traffic to a file, with Snort, in packet logger mode;

• recording network traffic according to security rules, with Snort, in IDS mode;

• using an intrusions prevention system, with Snort, in IPS mode;

• traffic analysis and security engine that displays logins generated by Snort IDS and send them into a database, with BASE;

• receiving and filtering of packets transmitted from the Netfilter Firewall, with Snort_Inline;

• detecting wireless networks with Kismet.

- To monitoring traffic:

• tracing the network bandwidth, used by the SNMP engine, using RRDTool, with CACTI;

• generating graphical maps of the load bandwidth network connections with PHP Weathermap.

- To log into the system:

• logins reading generated by a local server or remote workstations with Php-syslog-ng;

• automatic backup of the configuration of network devices and compare different versions of CVS (Concurrent Version System), with Rancid;

• IP address and DNS management via a very friendly Web interface, with Ipplan.

- For routing software:

•Traffic control for a wide range of standard network protocols such as those for: Routing: RIPv2, OSPF, BGP, Frame Relay or PPP encapsulation, network address translation (NAT) Protocol for redundancy (VRRP), DHCP server or relay, troubleshooting tcpdump, Stateful Firewall, with Vyatta;

• routing traffic through a set of "daemons", one for each routing protocol and a separate one called Zebra acting as manager kernel routing, with Quagga.

- To creating of virtual private networks (VPNs):

• building between two sites through SSL / TLS or pre-shared keys with OpenVPN.

- For telephony software:

• using a telephony packet, open source software based, for Asterisk PBX Voice-over-IP, with Trixbox.

- For link emulations:

• specific software to emulate the qualities of a link, to test the behavior of an application such as for example testing the remote possibility that an IP phone located in a low-bandwidth site to call the central site, with sufficient quality, with WANem.

- With some professional hardware equipment representing generators and network analyzers, with software licensed:

- To analyze the traffic performance:

• pentru măsurarea ratei de transfer, a întârzierilor şi a ratei de pierdere de cadre, conform RFC 2544, cu Generatorul şi analizorul de trafic Spirent TestCenter SPT-2000A şi cu echipamentul portabil de testare a traficului Trend MultiPro;

• to measure the transfer rate, latency and frame loss rate, according to RFC 2544, with the traffic generator and analyzer Spirent TestCenter SPT-2000A and the portable equipment for traffic test, Trend MultiPro.

- To analyze the conformance with IPSec standard:

• for ESP protocol layer 3 (IP Protocol 50), according to RFC 2406, with the traffic generator and analyzer Spirent TestCenter SPT-2000A;

• for ISAKMP (Internet Security Association and Key Management Protocol), used to establish security associations, according to RFC 2408, with the traffic generator and analyzer Spirent TestCenter SPT-2000A;

• for IKE protocol (Internet Key Exchange), used for automatic key exchange management through UDP port 500, according to RFC 2409, with the traffic generator and analyzer Spirent TestCenter SPT-2000A.

- That digital pattern generator:

• emulating as a stimulus for peripheral / ASIC, fixing / checking for maintenance, testing, production scale, small scale testing products, and more generally for many other stimuli, with digital pattern generator Moving Pixel Co. PG3ACAB;

- That logic analyzer:

• combining high-speed timing resolution, fast state acquisition, long record time and sophisticated triggering circuit with logic analyzer Tektronix TLA5202B.

The hardware and software platform module and the method of traffic analysis in networks with IP technology form a set of tools and a library of tests for measuring the dispersion of the values assigned to traffic on the various resources of communication networks with IP technology. General block diagram of the module is shown below:

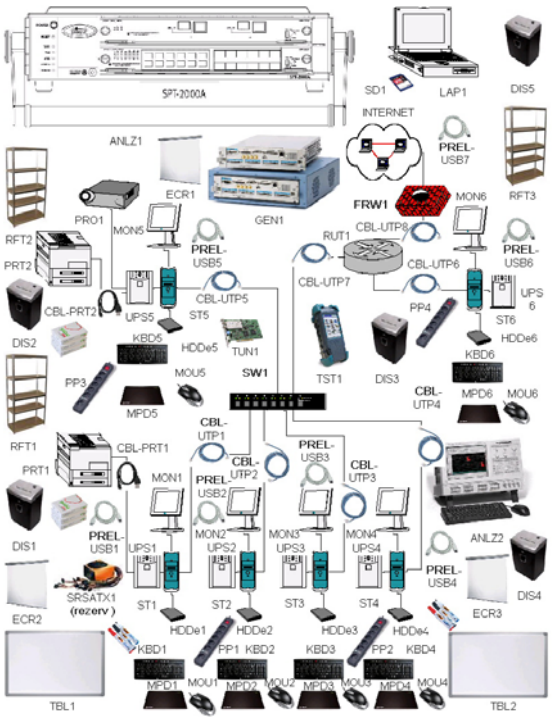

Figure 5. ATRAF -MPMTFL-P2
Hardware and software platform module

Legendă:
ST1 ... ST6 - Workstations 1 ... 6;
MON1 ... MON6 - Monitors 1 ... 6;
KBD1 ... KBD6 - Keyboards 1 ... 6;
MOU1 ... MOU6 - Mouse 1 ... 6;
MPD1 ... MPD6 - MousePad 1 ... 6;
HDDe1 ... HDDe6 - External HDD (USB) for data storage 1 ... 6;
UPS1 ... UPS6 - uninterruptible power supplies 1 ... 6;
TUN1 – Tv-Tuner 1;
SRSATX1 - Workstation Power Supply Unit ATX1 (rezervă)
LAP1 - Laptop 1;
SD1 SD Memory Card 1;
SW1 - Switch 1;
RUT1 - Router 1;
PRT1, PRT2 - Printers 1, 2;
CBL-PRT1, CBL-PRT2 - Printer Extension Cables 1, 2;
CBL-UTP1 ... CBL-UTP8 - UTP cables with RJ-45 connectors 1 ... 8;
PP1 ... PP4 - Multiple protection plugs 1 ... 4;
DIS1, ..., DIS5 - document shredders 1 ... 5;
RFT1 ... RFT3 - Metal racks 1 ... 3;
TBL1, TBL2 - Magnetic Tables 1, 2;
PRO1 - Projector 1;
ECR1 ... ECR3 - Projector screens 1 ... 3;
PREL-USB1 ... PREL-USB7 - USB Extension USB 1- 7;
ANLZ1 - Traffic generator and analyzer Spirent SPT-2000A 1;
TST1 - Portable Traffic Test Trend MultiPro 1;
GEN1 - Digital pattern generator Moving Pixel Co. PG3ACAB;
ANLZ2 - Logic analyzer Tektronix TLA5202B

VI. CONCLUSIONS

Module and method provides concrete opportunities to highlight the existence of those portions of the network where traffic values required beyond the capacity of processing and transportation network and other networks in other areas where the workload of resources in many cases does not exceed the modest values installed capacity of networks.

Method and the module contributes to the development of learning. The main news are made:

- the module allows to analyze adequacy of network management solutions through direct testing;
- the module is designed modular, to allow future development on emerging technologies and services;

the method can make a contribution to the development of new methods of optimizing resource allocation in communication networks with IP technology;

- the method has the ability to analyze network traffic in IP communications technology to extend research to other networks with different communications technology (ISDN / PSTN, GSM, VoIP, Eurocom, etc.).

After collecting network statistics, analysis of results of measurements made on the module based with the method application lead to finding new solutions to optimize network traffic measurement, which is reflected in reduced operating costs.

REFERENCES

1. Centrul Național de Management Programe (CNMP), „Program 4 - Parteneriate în domeniile prioritare - Prezentare", http://www.cnmp.ro, 2007
2. Centrul Național de Management Programe (CNMP), „Program 4 - Parteneriate în domeniile prioritare - Pachet de informații", http://www.cnmp.ro, 2007
3. Consorțiu ATRAF, „Site oficial ATRAF", http://www.atraf.ro
4. Informații despre instrumente software cu surse deschise, „Revhosts", http://fab.revhosts.net
5. TCPdump, „Code google mixtools", http://code.google.com/p/mixtools/wiki/sniff
6. Iperf, „Gennio", http://www.gennio.com/tags/iperf
7. Wireshark, „Wiki", http://wiki.backtrack-fr.net/index.php/Wireshark