Solutions for virtual laboratory

Peter Feciľak, Katarína Kleinová, František Jakab
Dept. of Computers and Informatics, Faculty of Electrical Engineering and Informatics
Technical University of Košice
Letná 9, 04001 Košice, Slovakia
Email: {Peter.Fecilak,Katarina.Kleinova,Frantisek.Jakab}@cnl.sk

***Abstract*—This paper deals with the solutions for next genaration virtual laboratory providing services for the operation of remote laboratory. The paper addresses problems related to requirement of flexible, secure and easy remote access to laboratory equipment. This paper also presents a unique concept for logical topology building with the usage of AToM, Q-in-Q tunneling and Frame relay technology, automated password-recovery procedure and knowledge evaluation.**

Keywords-Virtual laboratory; Q-in-Q tunneling; AToM, Knowledge evaluation; Automated password-recovery; Logical topology; Remote access

I. INTRODUCTION

Virtual laboratory in terms of this paper represents environment which is used for blended distance learning in Networking Academy program. Main purpose of virtual laboratory is to provide remote access to physical devices in network laboratory with the goal of doing exercises on real devices placed in virtual laboratory environment as well as combining them with virtual devices and providing services for wide range of applications used in complex labs (like Authentication server, Virtual Private Network server, Active directory (domain) server, etc.).

Main areas which must be reflected by modern virtual laboratory are:

- Remote access to real or virtualized devices (defined interface)
- Devices maintainance (password-recovery procedure, power on/off)
- Reservation system
- Content for exercises (labs)
- Physical/Logical topology re-configuration (dependent on exercise)
- Knowledge evaluation system

This paper describes several solutions for areas listed above with the contribution to the topic of virtual laboratories mainly with the unique approach to combination of real and virtualized devices as well as to logical topology building with the usage of technologies like Q-in-Q [5] tunneling, Frame relay and AToM [7]. Paper also describes physical lab environment components that we have used in our virtual laboratory at Regional Cisco Networking Academy at Košice.

II. DRAWBACKS OF EXISTING SOLUTIONS

In this section we will pass through each area of modern virtual laboratory (chapter I) and describe some drawbacks of solutions that are used in virtual laboratories.

A. Remote access to real or virtualized devices

Depending on devices used in virtual laboratory, it is necessary to define an interface for remote access to equipment. In case of remote laboratory for computer networks we usually use network devices like routers and switches that can be managed over telnet/ssh protocol or by serial or auxiliary interface. In general, it is TCP/IP or serial communication interface (RS232) that is using 9600 bits per second speed by default.

The cheapest way to access devices remotely is by using their own TCP/IP interface for remote access like using telnet or ssh protocol. This solution has its weaknesses in the need of correct configuration of TCP/IP stack at used devices. In case that IP address will be re-configured by user of virtual laboratory, then device of virtual laboratory will be no more accessible remotely at defined IP address. Even in case that we will put some kind of warning such as ”do not re-configure interface, etc.”, we are unable to guarantee accessibility of virtual laboratory as it might be malfunctioned by user. Therefore it is more stable if remote access is based on terminal server that has defined interface for accessing the remote devices connected to terminal server. Usually it is telnet or ssh protocol used for remote access.

There are a lot of laboratories that are using terminal server with telnet access on different ports for each device connected to terminal server. Terminal server based on Cisco integrated services router (terminal server) with 8 to 32 serial asynchronous interfaces is mostly used. There is also need for possibility of direct access to terminal server settings, like clearing frozen sessions and changing port speeds. If there is no other user interface to communicate settings directly to terminal server, then there is no way to access devices with different speeds of console port than default. This can be lack of this solution. As soon as user will change the speed of console port during lab exercise configuration, device becomes unusable for next reserved sessions.

 ISBN: 978-1-61208-133-5

Direct access (even relayed through terminal server) to devices using telnet protocol might be problematic in networks with too restrictive security policy. Due to security weakness of this protocol it is usually blocked in computer networks or service provider networks. Therefore there is strong need to provide secure way of communication with terminal server.

User interaction in remote network topology is also an important part of virtual laboratory. There is lack of virtual laboratories which combines remote laboratory equipment and user equipment with possibility of connecting own equipment (like user computer) into remote network topology. Usually remote network topology contains intermediate devices like routers and switches and there is lack of end devices like computers, IP phones and printers that can be controlled remotely. There is also strong need for terminal services not only for serial communication, but also for virtualization of operating systems and emulation of other network devices.

B. Devices maintainance

There are several actions that can be done by user and that can completely malfunction virtual laboratory. Therefore there is need for virtual laboratory equipment maintainance. These actions include:

- Re-configured passwords for console access or privileged exec mode *will cause inaccessibility of virtual laboratory for next users trying to access device*
- Changed speed of console or auxiliary port on device *will cause virtual lab device inaccessibility due to need for speed change at terminal server*
- Enabled security features that are blocking password-recovery procedure *will cause lab equipment to be unreachable due to impossibility of automatic password-recovery procedure*
- Erased flash memory *will cause device fails to boot and due to this problem it will not be accessible for lab training*

In modern virtual laboratories there is need for command authorization that cannot be done on Cisco ISR terminal server. Therefore a lot of virtual laboratories that are using Cisco terminal server are facing problems listed above and are solving them by person manually checking devices after each lab reservation. It is also possible to authorize commands on IOS application level with AAA server using tacacs or radius protocol. The solution using an authorization server has its weakness in that it relies on correct device configuration and its connectivity to AAA server. It is also limiting in case that authentication, authorization and accounting is part of exercise.

C. Reservation system

Each virtual laboratory has its own reservation system. Usually there is lack of easiness during reservation process. Some reservation systems are based on manual account creation (on devices or on terminal server) allowing user to access devices remotely. This process can be also partially or fully automated, which means that during reservation of lab session there is process including:

- Receival of lab reservation request from community using virtual laboratory. There are different forms of request receival - e-mail, web form, phone call to maintainer, etc.
- Approval and/or direct reservation
- Creating account and defining access rules
- Notification of person wishing to reserve lab equipment

Electronical requests (done via web form) can be almost fully automated, but there is also possibility of other non e-form requests to lab equipment maintainer. Therefore there is request for easy and fast process of equipment reservation integrated into traditional work user interfaces without spending too much time logging into reservation system, filling form items like e-mail of requester, date and time of lab reservation and notifying requester back.

D. Physical/Logical topology re-configuration

Sometimes it is necessary to re-configure network topology depending on the exercise that user wants to perform on virtual laboratory. There are a lot of virtual laboratories that do not allow topology re-configuration and all labs are based on the same topology or allow topology re-configuration only by technical staff physically changing network topology. There are also some approaches to automated change of physical topology based on connection matrices that are physically interconnecting wires by relay circuits. Some virtual laboratories are using logical topology change on ethernet network instead of physical topology re-configuration. There is issue for using solution based on VLANs for creating interconnection on L2 device for exercises related to L2 protocols like CDP, STP, VTP.

E. Content for exercises and knowledge evaluation

Every virtual laboratory has its technical limitations. Based on technical limitations there is limited set of exercises that can be done on set of equipment in virtual laboratory. Laboratories that did not solve technicaly topological re-configuration are usually dedicated to specific areas and therefore there is lack of scalability and possibility of doing wide range of excercies is typically missing. If laboratory is more static than dynamic in terms of topology creation, then there is usually no option for content creation (like connecting of devices together by web-oriented application of type similar to packet tracer [2] application).

Important part of modern virtual laboratory is a system for knowledge evaluation. Based on exercise that is user doing in virtual laboratory there should be system for configuration collection and configuration files evaluation. There are number of virtual laboratories that are evaluating

 ISBN: 978-1-61208-133-5

solution of exercise only by comparing solution file against user solution. Percentage of the difference between two solutions (template and user) is inverse percentage to 100%. There are still some problems with this solution as it is not so exact and also there is almost no variability in exercises (like IP address needs to be the same) and therefore exercise needs to be written so precisely that there is no other solution for the task.

III. Solutions for next generation virtual laboratory

In this section we will focus on solutions used in our virtual laboratory operated at our Regional Cisco Networking Academy. We have some unique approaches to logical topology management and knowledge evaluation that we will introduce in this chapter. Our virtual laboratory components are shown on Figure 1.

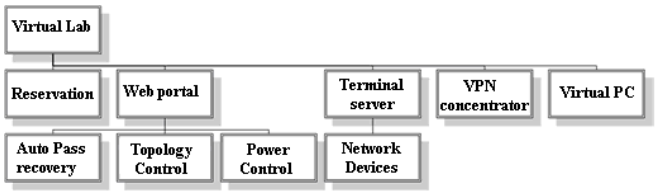

Figure 1. Virtual laboratory components

Our virtual laboratory is equipped with the following devices:

- 1x Virtual lab server with 8port PCI UART
- 1x APC switched rack PDU, 8 ports
- 1x Buttoner - mechanical MODE button pushing
- 3x WS-C3560-24-TS (1x MLS, 2x as SW1,SW2)
- 2x WS-C2960-24-TTL
- 4x Cisco 2811 router
- 2x ISDN B-link exchange
- 1x Frame relay switch (Cisco 2600 series router)

Features that are supported by our virtual laboratory are:

- Remote access to devices like routers and switches through the usage of terminal server with support of command authorization by regular expressions
- Speed change for each console connected to devices via Web user interface
- Automated password-recovery for routers and switches
- Automated topology re-configuration depending on exercise
- Content creation environment integrated to UI
- Knowledge evaluation system based on regular expression lookup
- Reservation system based on iCalendar events
- Virtualization of operating systems (end devices with MS Windows and OS Linux environment)
- Virtualization of routers with dynamips
- Secure connection to virtual laboratory by using VPN technologies with possibility of user interaction in remote topology
- HTTP tunneling for remote devices

A. Remote access via terminal server

History of our virtual laboratory started with specific hardware that was used as terminal server. It was TO108 hardware that had 8 serial ports and communication was multiplexed on one serial port used as management interface that was connected to virtual laboratory server. Main idea on this specific hardware was to have possibility of command authorization [6]. After some time of using this solution we have found one limitation of this terminal server. It was speed change limitation. Terminal server that we had used did not allow to change speed of console port (hardware limitation due to crystal oscilator and ICs used). Device became unavailable as soon as user in virtual laboratory applied command ”speed 115200” in line-console mode of the device. Therefore one of our pre-requisites for terminal server was ability to change speed of each console. As we wanted to avoid some situations causing virtual laboratory to malfunction (see chapter II-B) we have defined the need for command authorization as the second pre-requisite for terminal server.

Solution that we have used is based on multi-serial PCI card that we have inside of our virtual laboratory server. It is PCI8S950LP - 8 Port Low Profile RS232 PCI Serial Card with 16950 UART (Figure 2).

Figure 2. 8 Port low profile RS232 PCI RS232

As we have each serial console represented in UNIX-like system as /dev/ttyS*, it is possible to change speed of each console via setserial. This is really important for automated password-recovery procedure (chapter III-E). We are also using software based terminal server transforming telnet connection on specified port (one for each device) to physical serial interface of server. For this purpose we have modified serial to network proxy application (ser2net) [9]. We have modified this application to support regular expression based filtering for executed commands. This allows us to filter commands that can cause virtual laboratory failure (like erase flash and reload or changing speed of console port). Configuration of regular expression based filter is of Cisco ACL [1] style with definition of type of action - allow or deny. Table I shows an example of

 ISBN: 978-1-61208-133-5

ser2net filter configuration when we want to block specified commands.

Table I
SER2NET FILTERED COMMANDS

Command	*Regular expression statement*
H# erase startup-config	deny .*[#] erase star.*
H# write erase	deny .*[#] wr.* er.*
H(config)# line console 0 H(config-line)# speed 115200	deny .*[(]config-line[)][#] speed .*$
Allow everything else	allow .*

B. VPN concentrator

The goal of VPN concentrator is to allow secure connectivity to virtual laboratory with the option of user computer interaction with remote laboratory. For this purpose we have used openvpn [4] solution modified to allow connection via VPN client authenticated by username and password with pre-build package for end user. Depending on the time of lab reservation it allows connection for specified user and disconnect this user immediately after end of reservation. Due to unsecure nature of telnet protocol that is used on terminal server we do not allow direct telnetting to terminal server and we support direct telnetting (e.g., from user computer) only over VPN. In all our services we are using single sign-on to provide easy way to login to any service inside of virtual laboratory. Usage of VPN is only an option for those users that wants to access devices directly by telnetting from end user computer or to interact with own equipment like connecting end user computer to remote network topology. For this purpose we are using interface bridging so we are bridging VPN interface at end user computer with VLAN in network topology (802.1q and brctl is used on server side).

C. Reservation system

Key idea of reservation system is fast reservation with integration to daily used tools for time-management and communication like e-mail and calendar events. There is no need to develop special environment that is handling communication (messaging) and reservation of time/date based events as there are existing forms like iCalendar events that are handling time based events. One-click reservation system represents drag-and-drop action to visually select time slot of reservation and typing e-mail address of requester (see Figure 3). Reservation system on behind of this reservation process automaticaly parses information from iCalendar event, generates login and password information that is used for different services (VPN access, webGUI, Authentication server, virtual machines access (ssh/rdesktop/vnc), etc.). This information is sent to lab reservation requester automatically. Calendar systems have already solved problems related to read/write access to event reservation and automatic adding of events in case of non-coliding events (lab is free in defined timeslot) are added to calendar.

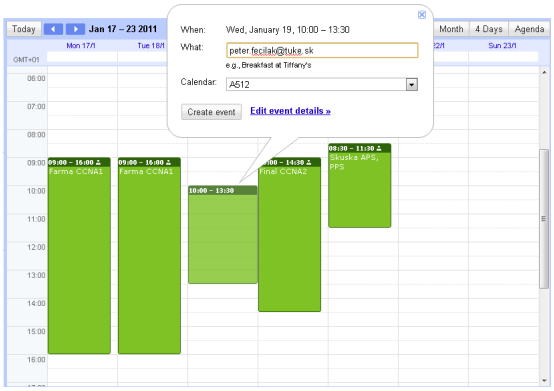

Figure 3. Reservation process using google calendar

D. Virtualized environment

The goal of virtualization is to equip virtual laboratory environment not only with real devices but to power options of virtual laboratory by operating virtual devices like end stations (computer is needed for testing of some features like port-security). From the early beginning of virtual laboratory operation we have been trying different virtualization techniques starting from linux-vserver, through XEN and finaly VMWARE ESXI [8]. Virtualized end stations with MS Windows or UNIX/Linux operating system are reachable via VPN or WebUI and VNC. By this we are powering options of virtual laboratory where user is able to interact with remote devices from user perspective (e.g., when testing port-security). Virtual machines created under ESXI are shown in Figure 4.

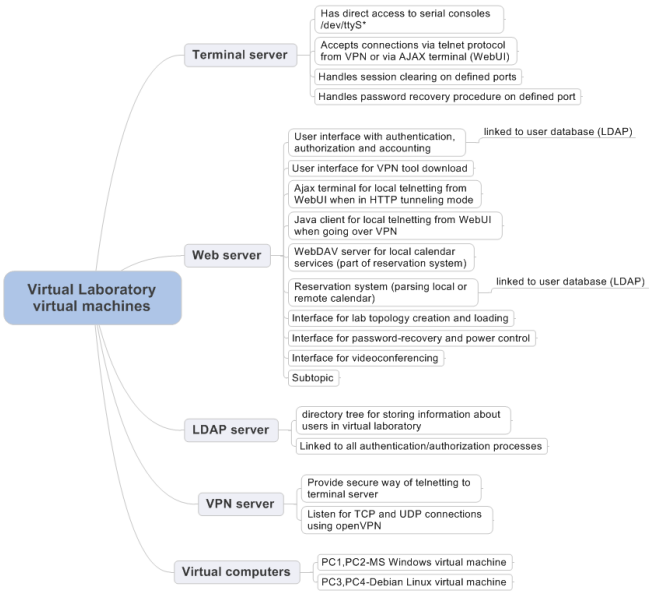

Figure 4. Virtual machines under VMWARE ESXI

E. Automated password-recovery

There are two different password-recovery actions that need to be supported by virtual laboratory. Password-recovery for routers is a bit different than for switches. There is strong need for speed change ability on each serial interface for successful password-recovery on router and mechanical push of MODE button for password-recovery on Catalyst switches. Key to password-recovery on routers is in control+break sequence generation. Practically this break sequence is generated by slowing speed down of console port lower than speed currently used and by sending 10 spaces. Therefore password-recovery on routers is done in following steps:

1) Power cycle the router (off/on)
2) Change speed of console port to 1200 bits per second
3) Send 10 spaces (0x20)
4) Change speed of console port back to default (9600 bits per second)
5) Configure config-register to 0x2142
6) Reload the router
7) Change config register back to default (0x2102)

Password-recovery procedure on Catalyst switches requires to manually push MODE button. The easiest way of how to do this is by shorting MODE button circuit by contact relay managed from server. As we want to keep warranty on our virtual lab equipment, we have developed a unique prototype for manual pressing of MODE button. ”Buttoner” device is managed by SNMP and is mounted in rack on the top of catalyst switch. For the purpose of power control we have used SNMP managed power distribution unit (Figure 5).

Figure 5. APC switched rack power distribution unit

F. Topology and its re-configuration

Our physical topology of virtual laboratory is shown on Figure 6.

This network topology is physically static, we do not use any connection matrices as there is no need for doing this. We have decided to manage topology more logically than physically by using provider technologies like Q-in-Q tunneling and any transport over MPLS (AToM). This technologies allows us to logically create interconnections between each devices by using separated VLANs and to tunnel layer 2 protocols like CDP/DTP/STP by using Q-in-Q tunneling. Also interconnections between devices using serial interfaces (WIC-2T) can be done by frame relay circuits or by using encapsulation (tunneling) to MPLS

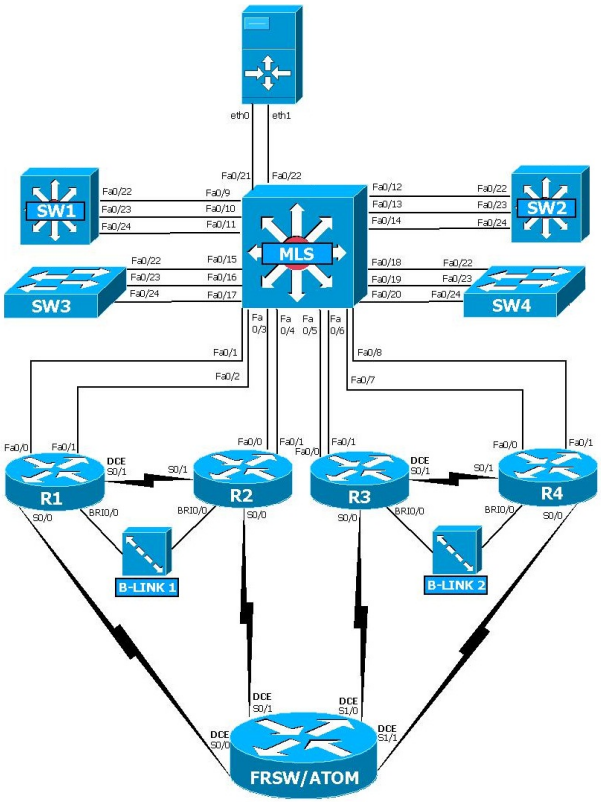

Figure 6. Virtual laboratory topology

(AToM). Table II shows configuration of virtual laboratory components when building logical topology from physical topology (Figure 6) shown on Figure 7.

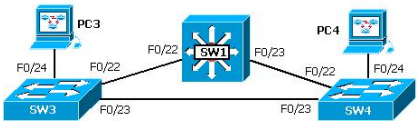

Figure 7. Example of virtual laboratory topology

Table II
EXAMPLE OF MLS CONFIGURATION FOR INTERCONNECTION SW1-SW3

```
MLS(config)# interface range Fa0/9, Fa0/15
MLS(config-if-range)# switchport mode dot1-tunnel
MLS(config-if-range)# l2protocol-tunnel cdp
MLS(config-if-range)# l2protocol-tunnel stp
MLS(config-if-range)# l2protocol-tunnel vtp
MLS(config-if-range)# switchport access vlan 10
MLS(config-if-range)# description SW1-SW3
```

G. Knowledge evaluation

Beyond technology there is content for exercises and knowledge evaluation. In our virtual laboratory we are able to practise exercises on CCNA and CCNP level without

 ISBN: 978-1-61208-133-5

any limitation. We have also some special labs on CCIP and CCIE R&S. Important part of virtual laboratory and its content is knowledge evaluation. For this purpose we have used our own regular expression based system for knowledge evaluation. Generally, we are collecting configuration files and different ”show” outputs from each device in virtual laboratory and comparing user solution against solution template.

Each template for specified lab exercise defines:

- start and end of block of evaluation by regular expression (e.g., only interface Fa0/0 configuration)
- line that should be evaluated within start-stop block by regular expression. This definition can contain fixed parts, variable parts and number-range parts
- scoring information - points for each occurence, minimal score per regular expression (important when penalty points are used), maximum number of occurences, penalty points per each occurence over the allowed maximum

Knowledge evaluation system used in our virtual laboratory is more described in [3].

H. Web user interface

Web user interface (Figure 8) acts as interface for communication with user. It is the central element for putting all the virtual laboratory pieces together. We have used some technologies like AJAX terminal that allows us to tunnel communication in case of limited access from user environment, PHP and Java technologies for running terminals from end station in non-firewalled environment.

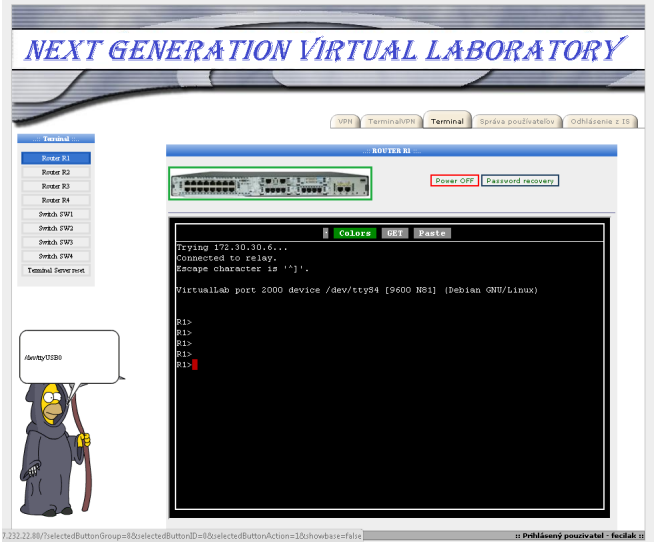

Figure 8. Web user interface of virtual laboratory

IV. Conclusion

In this paper we have presented several solutions for virtual laboratory operating at Regional Cisco Networking Academy at Košice. Our future work will be devoted to videoconferencing as a part of training in virtual laboratory and to special IPv6 training labs because we have joined to 7rp 6deploy project and as the only institution in this project from Slovakia we will be more focusing on IPv6 deployment.

Acknowledgment

THIS WORK WAS SUPPORTED BY THE SLOVAK CULTURAL AND EDUCATIONAL GRANT AGENCY OF MINISTRY OF EDUCATION OF SLOVAK 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%).

References

[1] Cisco Access Control Lists: *Overview and Guidelines*, [on-line 11.3.2011], URL: http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfacls.html

[2] Cisco Packet Tracer, [on-line 11.3.2011] URL: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html

[3] Feciľak, P. – Kleinová, K. – Jakab, F. – Bača, J.: *Automation in Knowledge Evaluation Process*, Proceddings of 6th International Conference on Emerging eLearning Technologies and Applications (ICETA 2008), Stará Lesná, Slovakia, 11. - 13. September, 2008, Košice, elfa, s.r.o., 2008, 1, 6, pp. 389-394, 978-80-8086-089-9

[4] Feilner, M.: *Building and Integrating Virtual Private Networks*, PACKT publishing 2006, ISBN:1-904811-85-X

[5] IEEE 802.1Q-in-Q VLAN Tag Termination, [on-line 11.3.2011] URL: http://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_ieee_802.1q.html

[6] Jakab, F. – Janitor, J. – Nagy, M.: *Virtual Lab in a Distributed International Environment* - SVC EDINET, The Fifth International Conference ICNS 2009 on Networking and Services, LMPCNA 2009, Valencia, 20.-25. April 2009, Valencia, Spain, IEEE Computer Society, 2009, 5, ISBN 978-0-7695-3586-9

[7] Lobo, L. – Lakshman, U.: *MPLS Configuration on Cisco IOS Software*, Cisco Press 2006, ISBN: 978-1-58705-199-9

[8] Olegsby, R. – Herold, S. – Laverick, M.: *VMware Infrastructure 3: Advanced Technical Design Guide and Advanced Operations Guide*, BrianMadden.com Publishing Group 2008, ISBN: 0971151083

[9] Serial port to network proxy project, [on-line 11.3.2011] URL: http://sourceforge.net/projects/ser2net/

 ISBN: 978-1-61208-133-5