ACTA UNIVERSITATIS AGRICULTURAE ET SILVICULTURAE MENDELIANAE BRUNENSIS

Volume LXI 119 Number 4, 2013
http://dx.doi.org/10.11118/actaun201361041077

DESIGN, IMPLEMENTATION AND SECURITY OF A TYPICAL EDUCATIONAL LABORATORY COMPUTER NETWORK

Martin Pokorný, Petr Zach

Received: March 4, 2013

Abstract

POKORNÝ MARTIN, ZACH PETR: *Design, implementation and security of a typical educational laboratory computer network*. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 2013, LXI, No. 4, pp. 1077–1087

Computer network used for laboratory training and for different types of network and security experiments represents a special environment where hazardous activities take place, which may not affect any production system or network. It is common that students need to have administrator privileges in this case which makes the overall security and maintenance of such a network a difficult task. We present our solution which has proved its usability for more than three years. First of all, four user requirements on the laboratory network are defined (access to educational network devices, to laboratory services, to the Internet, and administrator privileges of the end hosts), and four essential security rules are stipulated (enforceable end host security, controlled network access, level of network access according to the user privilege level, and rules for hazardous experiments), which protect the rest of the laboratory infrastructure as well as the outer university network and the Internet. The main part of the paper is dedicated to a design and implementation of these usability and security rules. We present a physical diagram of a typical laboratory network based on multiple circuits connecting end hosts to different networks, and a layout of rack devices. After that, a topological diagram of the network is described which is based on different VLANs and port-based access control using the IEEE 802.1x/EAP-TLS/RADIUS authentication to achieve defined level of network access. In the second part of the paper, the latest innovation of our network is presented that covers a transition to the system virtualization at the end host devices – inspiration came from a similar solution deployed at the Department of Telecommunications at Brno University of Technology. This improvement enables a greater flexibility in the end hosts maintenance and a simultaneous network access to the educational devices as well as to the Internet. In the end, a vision of a system of virtual machines preparation and automated deployment tailored for our needs is briefly outlined.

computer networks, network security, education, laboratory network, operating system virtualization

Laboratory of computer networking at the Department of Informatics (Faculty of Business and Economics, Mendel University in Brno) was founded in 2009 in order to support courses specialized in computer networking, network security and operating systems taught for bachelor and master degrees, and to provide an experimental environment for final thesis and for networking or security tests. The equipment of the laboratory covers basic areas in routing and switching, network security, wireless networking, VoIP, and server virtualization.

User requirements, design, implementation and maintenance of an educational network dedicated to laboratory experiments is a little bit different from a typical real network in that the students need to use a variety of different operating systems with administrator privilege which can be used for potentially dangerous network activities. The objective of this paper is to present our network laboratory design, implementation and experience with its maintenance, and to describe the concept of virtualized workstations. Our design can be used

as a template for other networking educational laboratories.

This paper follows our former paper Aulehlová, Pokorný and Zach (2012) which described the essential idea of the transition to the virtualized desktop computers but lacks an overall formal complex laboratory design. The same is true for the first paper describing our networking laboratory and the equipment purchased in 2009 (Kunderová, Motyčka, Pokorný and Serafinovič, 2009).

MATERIALS AND METHODS

User requirements

There are four basic user requirements on the laboratory computer network:

1. *Computer network providing access to educational network devices from the student workstations*. The connectivity is twofold, both the data connectivity (wired Ethernet between the workstation and the network device, UTP cable) and the console of the network device (workstation's RS-232 port – console cable – UTP cable – network device's console port) are required in the computer networking and security courses.
2. *Computer network providing access to laboratory network services from the student workstations*. A centralized authentication is needed in the Operating system course for the students to be able to log in with the same credentials on multiple workstations. Above that, a print server and a centralized storage space must be accessible from all workstations.
3. *Computer network providing Internet access* not only for the educational purposes but for the laboratory maintenance as well – operating system and application updates, antivirus database updates, new software installations, etc. In case of any dangerous network or security activity (e.g. antivirus protection or DoS protection experiment), there must be a possibility to isolate the laboratory network from the outside university production network to prevent any unwanted leakage of hazardous data.
4. *Possibility to log in with the administrator privileges on selected operating systems* because most of the configuration tasks in computer networking, security and operating systems courses can be accomplished only with a higher level of privilege access.

Basic security policy rules

In order to protect both the internal laboratory systems and the external university network, four basic security rules have been stipulated:

1. *All systems connected to the laboratory network, and particularly those systems allowed to access the university network and the Internet, must adhere to the basic security protection* which covers: an active antivirus protection including updates (except the Linux operating system), operating system updates, application software updates, activated firewall with a common filtering client-side policy, absence of any malicious software.
2. *Only authorized systems are allowed to access the laboratory network*, i.e. those systems operated by the laboratory administrator or other approved systems. The purpose of this rule is to prevent unsecured hosts that do not comply with the first rule of the security policy from connecting to the laboratory network.
3. *Those systems allowing the students to log in with administrator privileges are denied the university network and Internet access*. It is possible to affect the system security established in the first rule having the administrator privileges, that's why the network access is limited in this case.
4. *All the hazardous experiments are performed within a separate network infrastructure*. Above that, the overall laboratory Internet connectivity is temporarily blocked, and in case of a human failure (incorrect connection and/or forgotten connectivity isolation) there is a strict firewall which filters traffic between the internal and the external network according to the user requirement #3.

Technology overview

The essential idea behind the laboratory network design is the *Virtual Local Area Network (VLAN)* which enables segmentation of the computer network into smaller parts, usually individual IP networks, and thus facilitates the overall network maintenance, firewall policy design and its implementation. The concept of VLANs is based on *frame switching (L2)*, i.e. mapping of physical MAC addresses to switch ports together with the VLAN ID (numerical identifier of a VLAN), and related frame forwarding based on this information stored in the switch table. The communication between VLANs requires *routing (L3)* based on mapping of logical IP addresses of the destination network/host to ports leading to that destination, and related IP datagram forwarding based on this information stored in the router or multilayer switch routing table.

The data-link layer attacks can be avoided using a technique commonly called *Port Security*, which is able to provide a basic level of network access control based on the list of allowed MAC addresses. A more sophisticated method to enforce controlled network access is the *IEEE 802.1x framework* in which a supplicant (end host demanding access) must prove its identity against an authentication server (most commonly RADIUS, Remote Authentication Dial In User Service) before the supplicant's user payload is forwarded. This policy is enforced on a device standing between the supplicant and the authentication server – a so called authenticator (usually a switch or a wireless access point). The authentication data between the supplicant and the

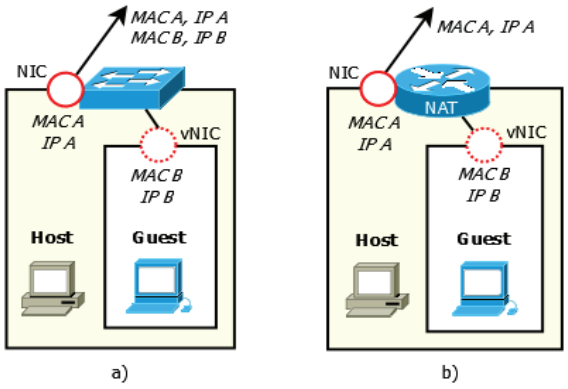
authenticator is transported in the EAP protocol (Extensible Authentication Protocol) defined in RFC 3748 and RFC 5247, and between the authenticator and the authentication server in the RADIUS protocol (RFC 2865, RFC 3575, RFC 5080). The authentication method used determines the particular EAP mutation, e.g. client authentication based on the public key infrastructure (PKI) and on the user X.509 certificate uses the EAP-TLS protocol (RFC 5216).

With respect to the technology employed in our laboratory, all the necessary settings of the functions related to the layer-2 switching and security can be found for example in the Cisco Systems product literature (Cisco Systems, 2013).

There are several *virtualization environment tools* such as VMware Player, Oracle VM VirtualBox or Parallels Desktop. The VirtualBox was chosen for its rich functionality and GNU GPL licensing.

The terms "host" and "guest" are used frequently in the text. The *host* is a base operating system providing resources to the guest system. The *guest* is an isolated and independent instance of an operating system running inside the host.

In terms of the system virtualization, there are different ways (called modes) how to connect the virtualized system (guest) to a computer network. Our solution uses two of them – the bridge mode and the NAT (Network Address Translation) mode. The bridge mode sends network packets directly to the guest system, circumventing host operating system's network stack (Oracle, 2013). The bridge mode inserts a virtual switch between the NIC (Network Interface Controller) and the guest's vNIC (virtual NIC), as depicted on Fig. 1a. Both the host and the guest can communicate as real PCs through a single NIC, each having an unique MAC addresses. The NAT mode, described on Fig. 1b, ensures that packets originated in the guest are routed by a virtual router and the NAT translation on the egress interface is applied. All packets (originated in the host as well as in the guest) exit the workstation with the workstation's MAC and IP address (Oracle, 2013).



1: *Two VirtualBox network modes deployed in our solution (a – Bridge mode, b – NAT mode)*

Other solutions

There are several ways how to fulfil the user requirements and the security policy rules defined above. The part of our design dealing with the user workstation virtualization was inspired by a similar solution in the Cisco Networking Academy laboratory at the Department of Telecommunication (Faculty of Electrical Engineering and Communication, Brno University of Technology) – specifically the idea of using a virtualized computer and two network interface cards to provide simultaneous access to both the educational network devices and to the Internet. The key features of the solution at the Department of Telecommunication are described in Jelínek *et al.* (2010) and in Morávek, Verner and Komosný (2010). The management of student workstations in a large scale using the computer virtualization is solved for example in the Austrian project VlizedLab – details in Matzinger (2013).

RESULTS AND DISCUSSION

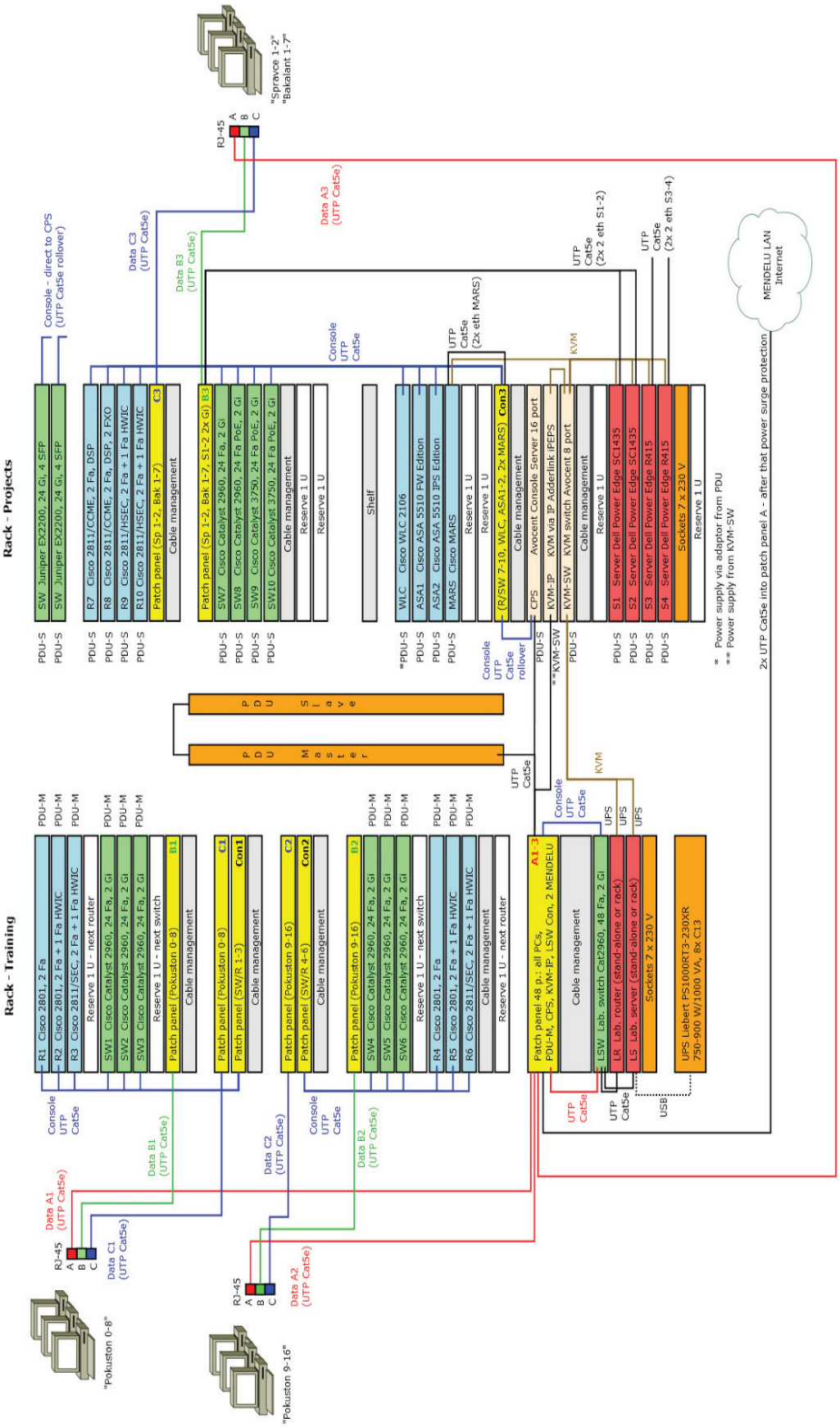
The original design and implementation

Physical schema

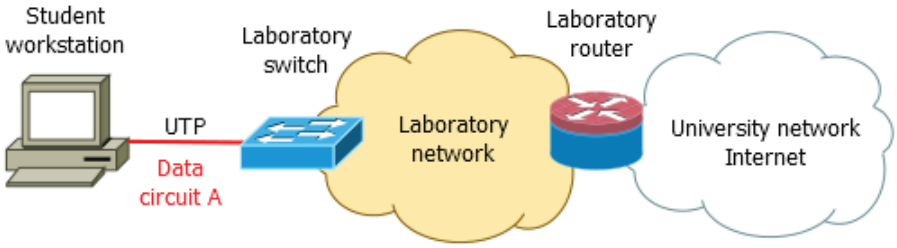
There are sixteen student workstations used for training, practical part of final theses, network experiments and Internet access – designated as "Pokuston 1–16" in our laboratory. These are divided into two groups (1–8 and 9–16) according to the physical placement in the room. Apart from these workstations, there is a teacher's workstation with a designation "Pokuston 0". Above that, there are seven workstations dedicated for special experiments – designated as "Bakalant 1–7". Two computers control the whole laboratory infrastructure ("Spravce 1" – primary, "Spravce 2" – backup). Two racks with educational network devices are interconnected with student workstations via three independent circuits A–C using UTP cables Cat5e. All the educational devices in racks are powered with two power distribution units (PDU) with a web management, devices' consoles are accessible either manually or via a console port server (CPS) with an IP access, all servers are connected to a KVM switch (keyboard, video, mouse) with an IP access. The whole laboratory network is connected to the university network with two UTP Cat5e 100 Mbps uplinks. The physical schema of the laboratory network is depicted on Fig 2.

Connection of the student workstations to the laboratory network

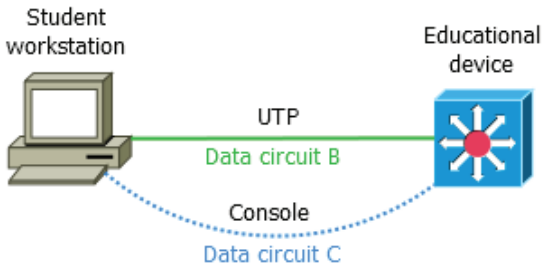
Most of the student workstations are equipped with one network interface card only, that's why there are two ways how to connect a particular workstation into the laboratory network. Fig. 3a shows a typical situation where the workstation is connected via the data circuit A to the laboratory network and can



2: *Physical schema of the laboratory network*



3a: *Connection of the student workstation to the laboratory network and possibly to the Internet*



3b: *Connection of the student workstation to an educational network device*

access laboratory servers providing network services (user requirement #2). If an operating system with an admission to connect to the Internet runs on the workstation at the moment, the laboratory firewall lets this type of communication to go through (user requirement #3), otherwise this communication is discarded. Fig. 3b depicts an access to an educational network device (user requirement #1, security rule #4) which covers both the data and the console connectivity (serial port). Students have to reconnect the workstation manually.

Topological diagram of the laboratory network

The overall logical diagram of the laboratory network is depicted on Fig 4. Student workstations are members of either VLAN 10 or VLAN 20, depending on the operating system which was selected to boot in the GRUB boot manager and which is running at the moment. There are several operating systems available (see Tab. I) on each workstation, each with a different application software set depending on the course requirements. Those systems that prevent students to log in with administrator privileges are dynamically assigned to VLAN 10 after a successful IEEE 802.1x/EAP-TLS authentication. The system must prove its identity using its X.509 certificate and its private key against the laboratory RADIUS server. Members of the VLAN 10 are allowed to access the university network and the Internet because there is a smaller chance to harm the system security without the administrator privileges (security rule #1). On the other hand, members of the VLAN 20 are denied access outside the laboratory network, and the students are allowed to log in with administrator privileges (user requirement #4, security rule #3).

The laboratory switch (Cisco Catalyst 2960, LAN Lite image) acts as an authenticator in the 802.1x framework, with the following configuration of a student workstation access port:

```
interface FastEthernet0/17
  switchport access vlan 10
  switchport mode access
  switchport port-security
  switchport port-security violation restrict
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky
  24be.0514.bec4
  dot1x pae authenticator
  dot1x port-control auto
  dot1x timeout quiet-period 3
  dot1x timeout tx-period 3
  dot1x guest-vlan 20
  storm-control broadcast level 70.00
  spanning-tree portfast
```

The port is a layer-2 port (switchport command), it is set to the access mode (mode access), and after a successful 802.1x/EAP authentication (dot1x port-control auto) it is assigned to the VLAN 10 (access vlan). If a system without an EAP client activated tries to access the port, it is assigned to the guest VLAN 20 (dot1x guest-vlan). If a system without a proper X.509 certificate but with the EAP client activated tries to access the port, it remains in an unauthorized state without the possibility to forward any user data (the restricted VLAN is not used). The Port Security commands prevent unauthorized MAC addresses

I: *Overview of operating systems deployed on the student workstations*

Course	Operating system	Administrator privileges	Internet access	VLAN	EAP
All	Windows 7, Linux CentOS	No	Yes	10	enabled*
Networking	Windows XP, 7, Linux CentOS	Yes	No	20	disabled
Operating systems	Linux CentOS	Yes	No	20	disabled
Experiments	Linux CentOS, Linux Debian	Yes	No	20	disabled

* With proper X.509 certificate (non-exportable) installed

from accessing the switch port (port-security violation restrict), only one legitimate MAC address of the student workstation is permitted and stored in the configuration (security rule #2).

VLAN 99 is dedicated for management purposes, members of this VLAN are two management workstations and infrastructure control devices (PDU, CPS, KVM-IP). The primary management workstation controls all important laboratory devices and servers, power distribution units, KVM (keyboard, video, mouse) of all servers, provides console access to some of the network devices, and controls the internet access. Above that, there is a central syslog server running on the primary management workstation gathering log messages from all important laboratory devices. Backups are stored on this workstation as well.

VLAN 40 and 50 have a special meaning – members ("Bakalant 1–7") of the VLAN 50 are allowed to access the Internet in a controlled fashion, usually temporarily to install or update all the necessary software on the workstations that are used for experiments or final theses. Normally, these systems are members of VLAN 40 which is administratively disabled with no network access. The membership status is changed via a script on the management workstation.

There are two laboratory servers (Linux CentOS and Windows Server 2003) virtualized with VMware vSphere 5 in the VLAN 30. The network services provided by these servers can be classified into three categories described below:

Network management services:
- DHCP server (IP configuration provided to the student workstations, static IP–MAC bindings).
- DNS server (name resolution inside the local laboratory network, cache server forwarding requests to the university nameserver).
- NTP server (time synchronization source for laboratory equipment, synced against the pool. ntp.org).
- RADIUS server (authentication server used for VLAN 10/20 assignment).

User services:
- LDAP server (centralized authentication of students in the Operating system course).
- NFS server (students' home directories accessed by workstations after a successful LDAP authentication).
- FTP server (centralized data storage space for teachers and students).
- CUPS server (laboratory print server).

Update services:
- Microsoft Update Services (software updates for Microsoft products, Windows, Internet Explorer and Microsoft Office).
- Yum repository (software updates for Linux operating systems).
- AVG Admin (centralized antivirus management system with an up to date antivirus database cache).

All the communication inside the VLANs is performed on the laboratory L2 switch, inter-VLAN routing is performed with a Linux router which runs a strict firewall (iptables) and masquerades (NAT) the whole laboratory network with the RFC 1918 private addressing behind the outer public university IP address.

Tab. II is an overview of all VLANs deployed in the laboratory computer network, the IP addressing scheme follows the logic of the VLAN ID encoded in the third byte of the private address space 10.0.0.0/8, i.e. 10.0.VID.0/24.

The new solution of virtualized student workstations

Shortcomings of the original design and implementation

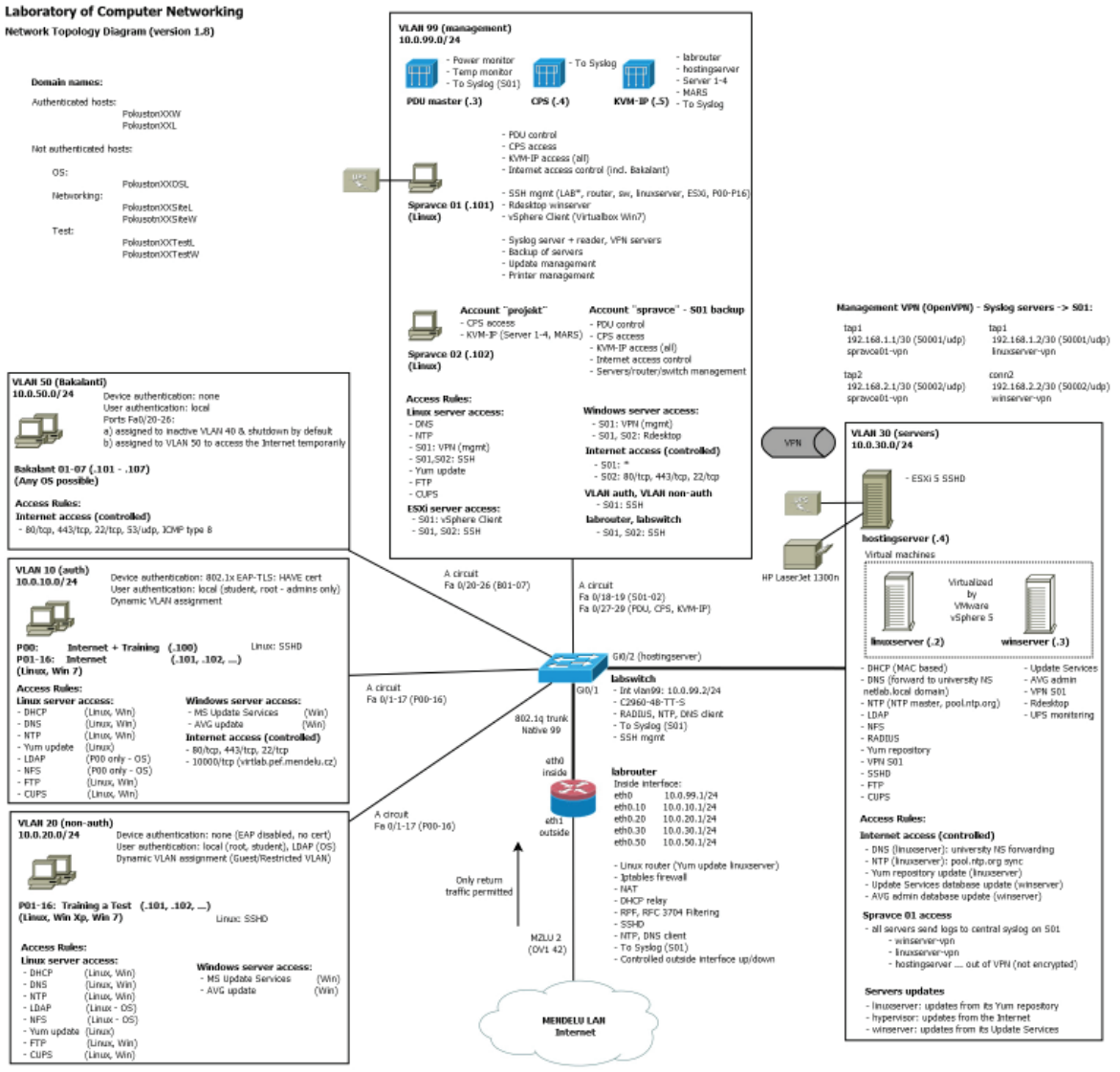
The original design and implementation has been successfully deployed for more than three years, but several shortcomings have arisen:

1. It is impossible to work with the educational network devices and to access the Internet from the same student workstation at the same time, moreover reboot is needed to change the operating system.
2. It is necessary for the students to switch the connectivity of the student workstations between the data circuit A and B manually to access the laboratory network/Internet and educational network devices respectively.
3. The flexibility of system updates is limited (reboot is needed with each operating system installed), deploying a new operating system

II: *Overview of all VLANs deployed in the laboratory computer network*

VLAN ID	VLAN members	Assignment type	Access level
10	Workstations "Pokuston 0*–16"	Dynamic – 802.1x auth.	Servers, Internet
20	Workstations "Pokuston 1–16"	Dynamic – guest VLAN	Servers
30	Servers	Static	Internet, Syslog to 99
40	Workstations "Bakalant 1–7"	Static – default shutdown	None
50	Workstations "Bakalant 1–7"	Static – manual auth.	Internet
99	Management	Static	All but 50

* Teacher's workstation (P0) is assigned to the VLAN 10 statically to gain a permanent Internet access.



4: *Topological diagram of the laboratory network*

requires a modification of the hard disk's partitions, potential errors in cloning makes the whole workstation unusable, all operating systems installed are hardware-dependent.

Concept of a virtualized operating system

The new proposed solution is based on multiple virtualized operating systems hosted on the student workstations. At the same time, all user requirements (#1–4) as well as all basic security policy rules (#1–4) must be met. With regard to the previous design and implementation, this approach brings changes especially in the design of the student workstations, the network architecture is affected minimally.

The new solution uses one base operating system (called host) hardly installed on the workstation and other virtualized operating systems (called guests) stored locally on each workstation. Using this approach, the operating systems present at the workstation were divided into two main categories according to their use:

- Host – a common OS with Internet access, equipped i.a. with a general office software (spreadsheet, word processor, etc.),
- Guest – an operating system equipped exactly according to the course needs (networking, experiments, Operating systems course, etc.).

The single host is the only entry point for the student to access the workstation. It means that the GRUB boot manager is not needed any more. User can start a particular guest with regard to the course from the host's GUI. From the user's perspective, the guest running in an emulation environment acts as a common application enclosed in a window of the host system, thus the user can easily switch between the environment of the guest and other applications (for example Internet browser) running in the host.

Implementation of the user requirements

Access to the laboratory network (user requirement #2) as well as the Internet access (user requirement #3) is provided by the host. The guests provide access to the educational network devices and to the console line (user requirement #1). Because of hardware resources sharing between multiple guests (serial port, MAC address – in some cases), one host and only one guest may be running on one workstation at the same time. More guests can be running on one workstation at the same time when no hardware resource sharing is needed.

The host provides only a non-super-user account for the students because of the essential security rule #3. On the other hand, providing the super-user rights for the students is usually necessary in case of guests, because students often need to train advanced tasks like settings of the IP configuration or disk partition maintenance (user requirement #4). The guests with super-user rights are denied access to the Internet (security rule #3).

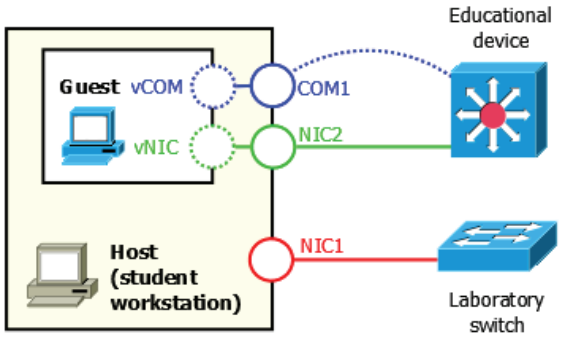
Simultaneous connection of one workstation to the local laboratory network as well as connection to the experimental infrastructure without the need of any reconnection (as with the previous solution) is achieved with implementation of virtualized systems and multiple workstation's NICs, as described in the next section.

Workstation design

The workstation is equipped with two network interface cards and with a serial port (COM). The Windows 8 Enterprise 64-bit is used as the host operating system. Guests' operating systems vary depending on their use.

In order to allow the guest to access external files (e.g. files stored on an USB disk or CD), the concept of a so called shared folder has been deployed. Shared folder is present in every operating system installed and its content is available to all of them. Moreover, this solution enables to run a network-isolated guest without any antivirus system. Before an external file is transferred into the guest, it is scanned by the host's antivirus system. Some of the guests cannot even be infected by a malicious software from the Internet, because these guests do not have access to external networks for security reasons. Infection cannot come from the students' laptops, because only approved systems are allowed to connect to the educational network.

In terms of network connectivity, this solution requires two NICs to provide simultaneous connectivity to the education network devices and to the Internet, and one COM port to access the console line. As depicted in Fig. 5, guests can reach both of the workstation's interface types. The virtual NIC can be mapped to a physical NIC using the NAT or the bridge mode, as described in the section Technology overview. Fig. 5 shows the mapping between the guest's virtual and workstation's



5: *Concept of multiple network interface cards on the student workstation*

physical ports to ensure this type of multiple connectivity.

Related to the VirtualBox network mode, the guests dedicated to the networking courses and networking experiments are mapped with the bridge mode to the NIC2 (circuit B) to gain access to a separate experimental network (security rule #4). The lack of administrator rights on the host system prevents unauthorized persons from changing the VirtualBox networking mode. (The same is true for a new unauthorized VM brought to or created on the student workstation.). Unauthorized reconnection of NIC2 to the circuit A causes an appropriate Port Security violation action on the switch's port (default action is Protect), and thus prevents the guest from accessing the laboratory network. Even if the administrator rights were misused to spoof the host's MAC address on the guest, the guest wouldn't gain any access because it is impossible for the guest without the proper host's X.509 certificate to authenticate the NIC1's port on the laboratory switch, and become member of the VLAN 10 (the port remains unauthorized on the laboratory switch, the guest VLAN 20 is not used in this solution). All these security precautions have been deployed to enforce security rules #2–3.

In order to ensure the connectivity of the guest for the Operating system course to the LDAP and NFS service (user requirement #2), the virtual NIC of this guest needs to be mapped with the bridge mode to the host's NIC1. It is not suitable to use the NAT mode in this case, because the students have the administrator rights in this particular guest system, and according to the security rule #3 it is impossible to enforce a proper security settings of such a system, and that's why it is necessary to prevent this guest from connecting to the university network and to the Internet. The easiest way how to implement this requirement is to filter the guest's traffic on the laboratory firewall filter based on the source IP address. And that's the reason why it is necessary to expose the guest's NIC in the bridge mode with its own unique IP address inside the laboratory network. In consequence, both of the end-hosts (the host and the guest) communicate over one switch port requiring a successful 802.1x authentication, thus a so called 802.1x multi-host

mode must be enabled on the port. Moreover, the maximum number of MAC addresses allowed on the port have to be increased to two (host and guest). Theoretically, a misuse of the super-user rights to spoof the host's IP address on the guest's vNIC could overcome the security rule #3, and an unauthorized Internet access could be gained, but the VirtualBox doesn't forward such a spoofed traffic in this case. Additional layer-2 security features like IP source guard or Port access control list applied to the laboratory switch port can reinforce the security of this design further.

Another guests might be required with new courses taught in the laboratory. These guests, prepared by teachers, typically contain a special software used for training. Above that, the Internet access is required, but usually no super-user rights for the students are necessary. To minimally affect the network infrastructure and to increase scalability, the best way is to map such a guest to the workstation's NIC1 through the NAT mode, as shown on Fig. 6.

To accomplish security rule #1, all systems allowed to access the university network and the Internet adhere to a basic security protection covered by the security rule #1. This condition must be met by the hosts, by the guests dedicated to the Operating System course and by other guests described in the previous paragraph. The guests dedicated to networking and experiments do not need to meet the security rule #1 because of network isolation.

Network infrastructure

As mentioned earlier, current network architecture is affected minimally with the new solution and this section is discussing required changes only.

The VLAN 20 is not needed any more because the systems used for networking and experiments stay apart from the laboratory network now, and the remaining systems access all the laboratory network services through the VLAN 10.

As discussed in the previous section, due to the guest supporting the Operating systems course, the Port Security parameters and the 802.1x host mode needed to be modified on the laboratory switch ports.

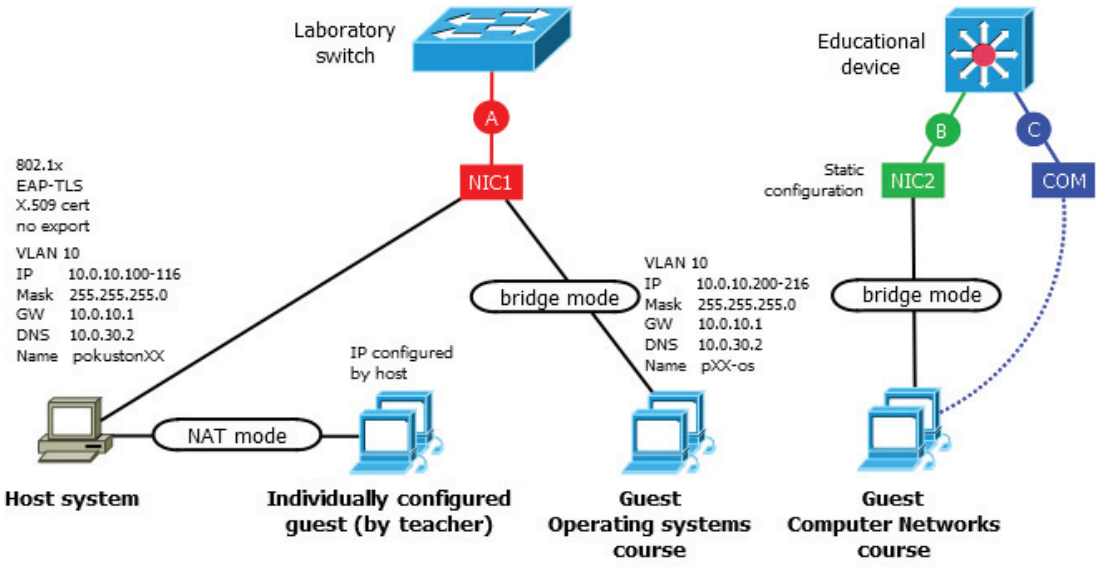
Note that with the 802.1x multi-host mode, the host is always the first one that authenticates the laboratory switch's port, and that's why it is not necessary for the guest supporting the Operating systems course to prove its identity.

Several changes in the configuration of the laboratory server network services were needed. As shown on Fig. 6, the hosts and the guests for Operating System course are using DHCP and DNS services (new pool and records required). Other guests are not facing the laboratory infrastructure. The Iptables firewall on the laboratory router was modified to prevent Operating systems guest from accessing the university network and the Internet, while the host's traffic is allowed to go through.

User services like FTP and CUPS are not affected by the new solution. To ensure proper access to operating system updates, all new hosts must be registered to the Microsoft Update Services and to the AVG Admin service.

Advantages of the new virtualized solution

In comparison to the original solution, the new concept of virtualized student workstations solved not only all the three shortcomings mentioned in the beginning of this chapter, but the flexibility in deploying a new system allows us to prepare a greater number of customized operating systems with specific educational needs. It is even possible to let a teacher download a default prototype guest system for his/her course, customize its software



6: *Virtualized solution of the student workstation from the network infrastructure perspective*

toolset or settings, and the administrators of the laboratory network deploy this guest system on all workstations with a simple copying process. There are even systems (e.g. the VlizedLab project) that accomplish this task in an automated fashion (Matzinger, 2013).

Above that, those guest systems used for networking and experiments, which are essentially isolated from the outside world, are run without any software or antivirus updates which facilitates their maintenance. On the other hand, it is easy for the administrator to change the networking mode of these guests temporarily from the bridge to the NAT, and to give these guests a possibility to update or install new software.

CONCLUSIONS

In this paper we presented two possible solutions that accomplished all the user requirements on a typical laboratory computer network, and which obeyed the defined security policy rules at the same time. There are other approaches as well – for example the desktop virtualization (described by Aulehlová, Pokorný and Zach, 2012) seems to be a suitable way how to accomplish the same goals as well, but this topic is beyond the scope of this paper.

SUMMARY

Computer network used for laboratory training and for different types of network and security experiments represents a special environment where hazardous activities take place, which may not affect any production system or network. It is common that students need to have administrator privileges in this case which makes the overall security and maintenance of such a network a difficult task. We present our solution which has proved its usability for more than three years. First of all, four user requirements on the laboratory network are defined (access to educational network devices, to laboratory services, to the Internet, and administrator privileges of the end hosts), and four essential security rules are stipulated (enforceable end host security, controlled network access, level of network access according to the user privilege level, and rules for hazardous experiments), which protect the rest of the laboratory infrastructure as well as the outer university network and the Internet. The main part of the paper is dedicated to a design and implementation of these usability and security rules. We present a physical diagram of a typical laboratory network based on multiple circuits connecting end hosts to different networks, and a layout of rack devices. After that, a topological diagram of the network is described which is based on different VLANs and port-based access control using the IEEE 802.1x/EAP-TLS/RADIUS authentication to achieve a defined level of network access. In the second part of the paper, the latest innovation of our network is presented that covers a transition to the system virtualization at the end host devices – inspiration came from a similar solution deployed at the Department of Telecommunications at Brno University of Technology. This improvement enables a greater flexibility in the end hosts maintenance and a simultaneous network access to the educational devices as well as to the Internet. In the end, a vision of a system of virtual machines preparation and automated deployment tailored for our needs is briefly outlined.

Acknowledgement

The equipment of the Laboratory of computer networking at the Department of Informatics FBE MENDELU was funded with the following projects: FRVŠ 1756/2011/A/b – Rozvoj laboratoře pro výuku předmětů se zaměřením na počítačové sítě a operační systémy. FRVŠ 2578/2009/A/b – Vybavení laboratoře pro výuku předmětů se zaměřením na operační systémy a počítačové sítě, FRVŠ 2639/2007/F1/a – Inovace praktické náplně předmětu Počítačové sítě a předmětů souvisejících, FRVŠ 743/2007/F1/a – Inovace předmětu Bezpečnost informačních systémů, and from the departmental fundings. There were plenty of our colleagues who helped us with the laboratory implementation and/or maintenance, in alphabetical order: Aulehlová B., Brázdil J., Daněk M., Halamíček P., Kunderová L., Kušnier J., Salák M., Šturma M., Vetr M.

REFERENCES

ABOBA, B. et al., 2008: Extensible Authentication Protocol (EAP) Key Management Framework. *RFC 5247* [online]. The Internet Society [cit. 2. March 2013]. Accessible on the Internet: <http://tools.ietf.org/html/rfc5247>.

ABOBA, B., 2003: IANA Considerations for RADIUS (Remote Authentication Dial In User Service). *RFC 3575* [online]. The Internet Society [cit. 2. March 2013]. Accessible on the Internet: <http://tools.ietf.org/html/rfc3575>.

AULEHLOVÁ, B., POKORNÝ, M., ZACH, P., 2012: Implementace virtualizovaných výukových stanic v Síťové laboratoři ÚI PEF MENDELU. [CD-ROM]. Brno: PEF MENDELU. In: *PEFnet 2012*. 1–11. ISBN 978-80-7375-669-7.

CISCO.COM, 2013: *Catalyst 2960 and 2960-S Switches Software Configuration Guide* [online]. Cisco

Systems, Inc. [cit. 2. March 2013]. Accessible on the Internet: <http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html>.

JELÍNEK, M., KOMOSNÝ, D., HOMOLKA, J., HRABAL, Z., SOUMAR, M., VERNER, L., 2010: Správa počítačových učeben na vysokých školách. *Elektrorevue – Internetový časopis (http://elektrorevue.cz)* [online]. 31: 1–5. ISSN 1213-1539. [cit. 2. March 2013]. Accessible on the Internet: <http://elektrorevue.cz/cz/download/sprava-pocitacovych-uceben-na-vysokych-skolach-1/>.

KUNDEROVÁ, L., MOTYČKA, A., POKORNÝ, M., SERAFINOVIČ, P., 2009: Nové síťové technologie na PEF MZLU v Brně. In: *UNINFOS 2009 (Univerzitné informačné systémy) Zborník príspevkov z medzinárodnej konferencie.* Nitra: SPU Nitra, 167–172. ISBN 978-80-552-0309-6.

LEELANIVAS, M. et al., 2003: Graceful Restart Mechanism for Label Distribution Protocol. *RFC 3748* [online]. The Internet Society [cit. 2. March 2013]. Accessible on the Internet: <http://tools.ietf.org/html/rfc3478>.

MATZINGER, R., 2013: *VlizedLab Project – An Open Source Solution for Running PC Labs in Schools and Educational Institutions* [online]. Matzinger [cit. 2. March 2013]. Accessible on the Internet: <http://www.vlizedlab.at/>.

MORÁVEK, P., VERNER, L., KOMOSNÝ, D., 2010: Automated configuration of network devices for laboratory purposes. In: *Sborník konference NEW INFORMATION AND MULTIMEDIA TECHNOLOGIES - NIMT 2010*. Brno: VUT Brno. 1–4. ISBN 978-80-214-4126- 2.

NELSON, D. et al., 2007: Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes. *RFC 5080* [online]. The Internet Society [cit. 2. March 2013]. Accessible on the Internet: <http://tools.ietf.org/html/rfc5080>.

ORACLE.COM, 2013: *Oracle VM VirtualBox®. User Manual* [online]. Oracle Corporation [cit. 3. March 2013]. Accessible on the Internet: <http://dlc.sun.com.edgesuite.net/virtualbox/4.2.8/UserManual.pdf>.

REKHTER, Y. et al., 1996: Address Allocation for Private Internets. *RFC 1918* [online]. The Internet Society [cit. 2. March 2013]. Accessible on the Internet: <http://tools.ietf.org/html/rfc1918>.

RIGNEY, C. et al., 2000: Remote Authentication Dial In User Service (RADIUS). *RFC 2865* [online]. The Internet Society [cit. 2. March 2013]. Accessible on the Internet: <http://tools.ietf.org/html/rfc2865>.

SIMON, D. et al., 2008: The EAP-TLS Authentication Protocol. *RFC 5216* [online]. The Internet Society [cit. 2. March 2013]. Accessible on the Internet: <http://tools.ietf.org/html/rfc5216>.

Address

Ing. Martin Pokorný, Ph.D., Ing. Petr Zach, Department of Informatics, Mendel University in Brno, Zemědělská 1, 613 00, Brno, Czech Republic, e-mail: martin.pokorny@mendelu.cz, petr.zach@mendelu.cz