Piloting Environment of Distributed Virtual Networking Laboratory

Petr Grygárek, Martin Milata
Department of Computer Science, VSB-Technical University of Ostrava, Czech Republic,
petr.grygarek@vsb.cz, +420 59 732 3243, martin.milata@vsb.cz

Abstract

This article presents implementation of an advanced task-based fully distributed virtual network laboratory management system that supports building on-demand variable topologies of laboratory devices located at multiple sites connected via Internet.

1. Introduction

In networking-oriented university courses it is necessary to provide enough opportunity for students to work with real network devices. It allows them to develop and develop a deeper knowledge of networking technologies and gain skills which will help them to learn how to operate the large-scale networking environment in practice. Since the time students spend in the laboratory during regular exercises is limited, it proved reasonable to provide students remote access to the laboratory networking equipment. For a couple of years we experimented with various technologies for controlled remote access to the network devices and methods of automatic interconnection of network topology [1]

2. Laboratory Equipment Sharing

During last months we finished our most advanced implementation of fully distributed architecture of virtual networking laboratory [2] [6] [7]. The architecture allows transparent mutual sharing of laboratory equipment and creating virtual topologies composed of real laboratory equipment scattered at multiple distant laboratory sites, connected together via Internet. In that semi-virtual distributed environment, students may reserve various topologies for particular time interval, suitable networking devices actually used for the virtual topology are searched dynamically in all participating sites. The set of devices chosen by mapping algorithm is automatically connected together into a virtual topology utilizing tunneling over Internet using our "Distributed Virtual Crossconnect" [2] [6] [7] which is a mixture of software-based configuration generators and hardware devices including our own prototypes [3] [4]. The distributed nature of the resulting educational network topology is completely hidden to users of the system.

By sharing of devices between multiple participant sites, we are able to implement very large temporary educational WAN topologies, which would be unattainable to create using only equipment of any single site. Moreover, the usage of dynamic selection of lab devices utilized for particular reservation brings lot of another advantages. Among others it allows sites to specialize on particular special technology and share expensive devices with users at other sites or easily substitute a failed device with other, possibly from a friendly institution (fig. 1).

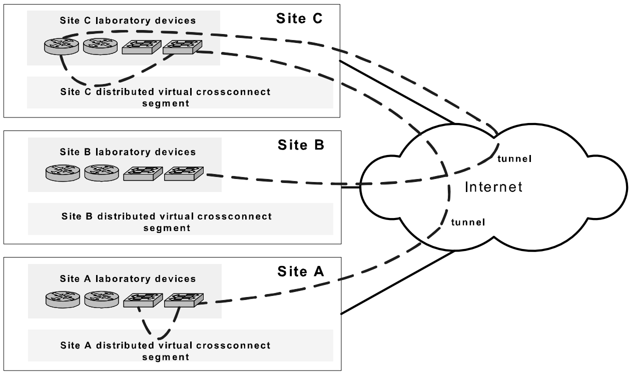
Site C laboratory devices
Site C
Site C distributed virtual crossconnect segment
Site B laboratory devices
Site B
Site B distributed virtual crossconnect segment
Site A laboratory devices
Site A
Site A distributed virtual crossconnect segment
tunnel
Internet
tunnel

Fig. 1. Distributed Laboratory Devices Sharing

2. Distributed Virtual Laboratory's Users and Tasks

There are four roles of Virtlab system users: instructor, student, tutor and administrator. Instructor prepare tasks which students may reserve to practice. Administrators sets up and maintains the system environment at individual sites. Tutors may support students remotely during their work on reserved tasks. They can see what every student does on the lab devices' consoles, demonstrate some configuration activity or invisibly make changes in the lab devices configurations to let student to practice troubleshooting of the problem. A single user may have multiple roles at the same time if desired.

To advice students recommended topics for practicing, the system offers students an extensible set of task they may choose from. Task specifications are completely described using HTML and may include not only obvious text and topology picture but also any additional multimedia elements. Teachers at every site may create it's own set of tasks and provide them to others. It proved very benefical that teachers may create task descriptions offline. After all multimedia materials related to task are prepared locally, they may be packaged together, accompanied with XML descriptor involving all parameters of the task, compressed and uploaded to the control server after teacher connects to the Internet. Currently we systematically work on implementation of a set of tasks focused on routing and switching prepared by experienced instructors of Regional Cisco Networking Academy to the Virtlab environment. In addition to selection of one of the predefined tasks, student may also define his or her own topology, which is appreciated mainly by more advanced students. The student's topology is defined in easily understandable XML format and student may prepare it on it's own computer in advance. For better orientation, predefined tasks may be categorized using multiple criteria.

A group of students may cooperate on solution of one reserved task together. The architecture even allows to incorporate students belonging to sites without lab equipment to share, which have appointments to borrow equipment from other sites (fig. 2).

In the current version, settings of individual sites' components is accomplished manually using set of text-based configuration files. To further simplify administration of the distributed environment, we currently work on GUI-based configuration system, which will allow administrators modify sites environment description (such as addition or temporary removal of lab devices or modification of time schedule) much more conveniently.

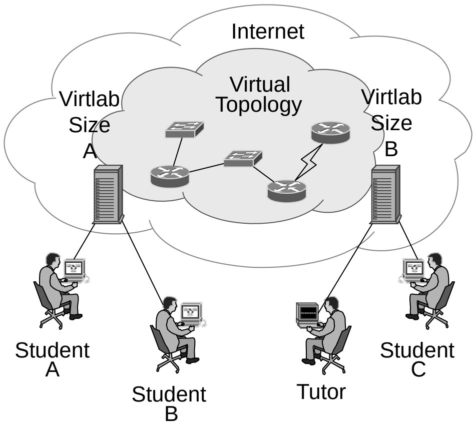

Fig. 2. Distributed Task in Virtual Network Laboratory

3. Distributed Nature of Virtual Laboratory

Our distributed networking laboratory implementation is highly modular based on open-source technologies. The property of the architecture we consider especially valuable is it's fully distributed nature. Since there is no central entity and thus no single point of failure, individual sites may continue to operate independently if equipment at other sites becomes unavailable due to network or software infrastructure outage. Moreover, administrators of individual sites have full control over the decision which network devices may be provided to users of other sites at particular time (they may specify weekly schedule to accomplish that.)

With regard to our planned participation in distributed e-learning project Edinet partially funded by EU grant, international operational context was taken into account during implementation. Every user may choose preferred language of user interface (currently we provide Czech and English). The distributed system also correctly handles actions of users located in different timezones (fig. 3).

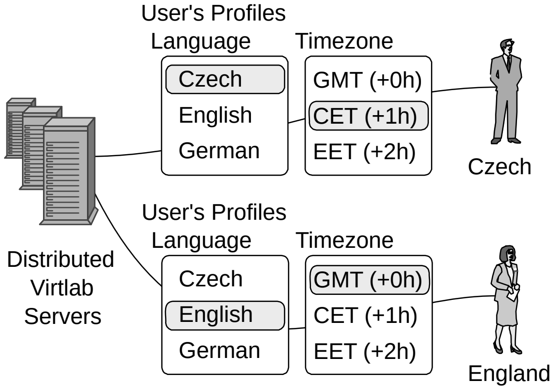

Fig. 3. User’s Profiles in Distributed Virtlab

We know well that industrial companies prefer to recruit employees with real-world day-to-day network operation maintenance and troubleshooting experience. Unfortunately, there is not enough time and equipment for practicing it during regular networking courses lab works. Moreover, standard lab objectives most often focus on making deeper knowledge of individual networking technologies in very simple usage scenario, but there is no opportunity to get experience with aspects of their long-term operation in large-scale environment, where the minimizing of network downtime is a crucial requirement. This is why we plan to work with industrial companies to develop real-world scenarios for day-to-day WAN network management training and troubleshooting. Since our Distributed Virtlab architecture allows to create both long-term and short-term virtual topologies and create multiple virtual topologies in parallel, it gives us an opportunity to setup large WAN topology and let it operate for a couple of days or weeks, without restricting other users in their individual practicing by selection one of individual pre-defined task for a short time (typically one or two hours).

By integrating freely available third-party components such as traffic generators or honeypots [10], we plan to create much more realistic exercising networking environment than can is obviously provided by traditional academic limited-extend lab settings. Using honeypots, we may efficiently simulate vast amount of end-user systems of various types, will be useful for practicing of implementation of security mechanisms. Traffic generator which will provide realistic load are necessary to let students gain experience with implementation of quality of service (QoS) in the real network. Another useful enhancement we currently work on is the ability to monitor traffic in any point of virtual topology by virtual network probes. We intent to allow student either to display captured traffic in his/her WWW browser or store it into file in well-known format and download to local computer for later offline analysis using tools like tcpdump or Wireshark. [9]

The implementation of architecture described above was finished in last months. Currently we set-up a piloting configuration, which will integrate networking laboratories of Department of Computer Science and Regional Cisco Networking Academy at VSB-Technical university of Ostrava and Local Cisco Networking Academy at Silesian University at Karvina. We also negotiate with third partner from Slovak Republic the possibility to join to the environment at the end of 2007.

Since we aim to operate the distributed virtual laboratory environment 24 hours 7 days per week, it was inevitable to carefully design the incident incident management system. From the previous experience with old (non-distributed) version of virtual laboratory [5] [9] [11] [12] [13] we learned that even short outage during student's reserved timeslot quickly demotivates student to use the virtual laboratory and breaks the trustworthiness of the whole system. This is why we spent a lot off effort to handle most of possible nonstandard situations in communication between system components and develop a unified system for detailed logging of important system events at various severity levels. The logging system allows us to follow all distributed transactions by inspecting appropriate syslog or browsing through stored records using WWW interface. It is also bound to the e-mail notification system informing administrators of affected sites about eventual critical outages of various system components. To allow users of the system report errors quickly and efficiently, we implemented bug reporting form directly to the GUI of system users of all possible roles. Users' reports are then forwarded to our internal web-based email-notification-capable bug tracking system and corrected by development team as soon as possible.

Since the distributed virtual laboratory exposed to the public Internet, security issues were taken into account from early stages of the architecture design. The traffic between sites is carried in IPSec tunnels. Access to control web application requires usage of encrypted HTTPS protocol. Users are authenticated using authentication infrastructure established in the particular user's home site. Access via firewalls was taken into account and number of conduits which have to be configured at sites' firewall was minimized (fig. 4).

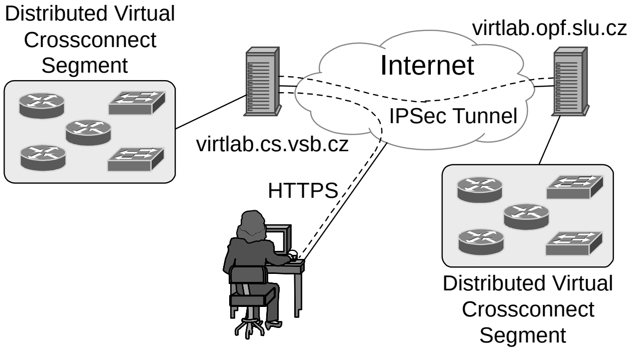
Distributed Virtual Crossconnect Segment
virtlab.opf.slu.cz
Internet
IPSec Tunnel
virtlab.cs.vsb.cz
HTTPS
Distributed Virtual Crossconnect Segment

Fig. 4. Security in Distributed Virtlab

Although the primary sense of the piloting stage of the distributed Virtlab implementation is to test it in the real operation and remove remaining error undetected during internal testing stage, we also intend to gather operational statistics which may help us to decide the right way to extend the system in the future. Primarily we want to monitor behavior of the device mapping algorithm to assess whether it works with acceptable efficiency. The monitoring will also help us to determine most busy device types which should be added to the lab equipment. We also plan to use the statistics to optimize user quotas so that the user is not limited unnecessarily but nobody is allowed to monopolize laboratory equipment at the expense of other users.

During setup of piloting environment, we proposed a lot of possible extensions to make the learning environment even more efficient. One of the most interesting we plan to implement in the near future is to incorporate remote user's station into the laboratory topology using VPN connection over the Internet. This option brings a lot of very interesting usages, because the user may utilize the full power of applications installed at his/her computer (such as hacking tools to test configured security mechanisms of laboratory network or GUI-based tools to control networking devices) to interact with semi-virtual laboratory network.

We hope that the platform which we are building will became well-equipped distributed networking laboratory, which will allow us to make scientific and technology research and also get students involved in solving of real networking problems of the industry. We will also welcome other academic partners willing to cooperate on the distributed laboratory environment. We also expect that the resulting environment may be successfully used in courses other than networking-oriented, like security or operating systems courses. During the current academic year, we plan to use our distributed networking laboratory in three subjects at both bachelor and MSc. level.

4. References:

[1] Grygárek, P., Seidl, D., Němec, P.: Enabling Access to Equipment of Computer Network Laboratory for Practical Trainging via the Internet. Proceedings of Technologies for E-Learning conference, FEL ČVUT Praha, 2005, ISBN 80-01-03274-4, pp. 43-52. [In Czech]

[2] Grygárek, P., Milata, M., Vavříček, J.: The Fully Distributed Architecture of Virtual Network Laboratory, In Proceedings of 5th International Conference on Emerging e-Learning Technologies and Applications, High Tatras, Stara Lesna, Slovakia 2007, ISBN 78-80-8086-061-5.

[3] Grygárek, P., Seidl, D.: Automatic WAN Topology Interconnection and it's Usage in CNAP Networking Laboratories, In Proceedings of 5th International Conference on Emerging e-Learning Technologies and Applications, High Tatras, Stara Lesna, Slovakia 2007, ISBN 978-80-8086-061-5.

[4] Seidl, D., Grygárek, P.,: System for Automated Network Topology Management. Seminar on Opensources Solutions in Computer Network III. Silesian University Karviná, 2005. Presentation available at http://www.cs.vsb.cz/vl-wiki/images/1/1c/ASSSK-SLU.pdf. [April 2007] [In Czech]

[5] Grygárek, P., Seidl, D., Němec P.: Virtual Network Laboratory for CNAP. Annual Conference of Cisco Networking Academy Program, Brno 2005. Available at http://www.cs.vsb.cz/vl-wiki/images/a/ad/Virtlab-prezentace-CNAP-Brno.pdf. [April 2007]. [In Czech]

[6] Vavříček J.: Enhancement of Virtual Networking Laboratory Control Software. Master's Thesis, Faculty of Electrical Engineering and Computer Science, VŠB-TU Ostrava, 2007 [In Czech]

[7] Hrabálek T.: Support for Creation of Virtual Topologies in Virtual Networking Laboratory Using Tunnelling Technology. Master's Thesis, Faculty of Electrical Engineering and Computer Science, VŠB-TU Ostrava, 2007 [In Czech]

[8] Němec, P.: Virtual Network Laboratory. Master's Thesis, Faculty of Electrical Engineering and Computer Science, VŠB-TU Ostrava, 2005 [In Czech]

[9] Novák R.: Traffic monitoring implementation on VLANs in Virtual Network Laboratory using tethereal or tcpdump. Bachelor's Thesis, Faculty of Electrical Engineering and Computer Science, VŠB-TU Ostrava, expected in May 2008 [In Czech]

[10] Hopp P.: Honeypots system integration into Virtual Network Laboratory. Bachelor's Thesis, Faculty of Electrical Engineering and Computer Science, VŠB-TU Ostrava, expected in May 2008 [In Czech]

[11] Grygarem P., Milata M., Jeníček P.: Applications of Virtualisation Technologies in Education of Computer Networks. Proceedings of Technologies for E-Learning conference, FEL ČVUT Praha, 2007, ISBN 978-80-01-03756-0, pp 45-54. [In Czech]

[12] Seidl, D.: System for Automatic Network Configuration Management. Master's Thesis, Faculty of Metallurgy and Materials Engineering, VŠB-TU Ostrava, 2005. [In Czech]

[13] Grygárek, P., Practical Experience with Implementiation of Virtual Computer Network Laboratory and Proposed Ways of its Further Development. Proceedings of Technologies for E-Learning conference, FEL ČVUT Praha, 2006, ISBN 80-01-03512-3, pp.58-68. [In Czech]