DOI: 10.17951/ai.2016.16.1.21

ANNALES
UNIVERSITATIS MARIAE CURIE-SKLODOWSKA
LUBLIN – POLONIA

VOL. XVI, 1 SECTIO AI 2016

REMOTE ACCESS ENVIRONMENT FOR COMPUTER NETWORKING LABORATORY: CHALLENGES AND SOLUTIONS

Karol Kuczyński [1], Rafał Stęgierski [1], Waldemar Suszyński [1], Dawid Królica[2]

[1] Institute of Computer Science,
Maria Curie Sklodowska University in Lublin
[2] Extreme Networks, San Jose, CA, USA

KEY WORDS: computer networking, remote access, remote learning

ABSTRACT: A variety of network management systems is commercially available. However, their applicability for computer networking laboratories that are used for scientific, educational or engineering purposes (in particular, as a test environment for network-based software engineering) is limited. Also dedicated remote access systems do not offer enough flexibility. Major challenges are discussed in the paper. Most of the proposed solutions have been already implemented and tested.

1. INTRODUCTION

Computer network management is a deeply studied subject. A variety of integrated network management systems is commercially available, to provide an administrator a holistic view of the network, and to facilitate network administration [1,2,3]. However, this is not the subject of our discussion here.

Many computer networks also exist as a test environment in a networking laboratory, rather than productive environment. They are used for educational or scientific purposes, engineering, prototyping, testing, demonstrations for potential customers, etc. In authors' opinion, available network management systems are not well suited for this application. Users (administrators) usually work directly with their network devices, so that they can for example connect their laptops to console ports, switch power outlets, connect cables.

In an era of e-learning [4] and teleworking [5], this approach seems to be very anachronistic. On the other hand, for students and beginner networkers, it is profitable to have the feeling of working on real hardware. The authors' aim is to design and implement a system that provides remote access to a laboratory network, with maximal flexibility. The system has been optimized for networking education, but can be used for any other purpose, where remote access is desirable. In particular, the system can provide a remotely available, fully functional test environment (with servers, PCs, full access to network infrastructure) for network-based software engineering. In order to be a reasonable alternative to physical access, the system is expected to meet the following criteria:

- Web-based client or client software installable with neither administrator privileges nor special non-standard libraries.
- Simultaneous access to multiple console (out-of-band) ports of the devices, out-of-band access to graphical consoles of remote PCs.
- Support for both physical and virtual devices.
- High responsiveness, no noticeable lags.
- Possibility to reset, turn on and off the devices on demand.
- Support for wireless solutions.
- Support for full 802.1x protocol in the lab network.
- Support for any multi-vendor environment.
- Support for group work.
- Precisely, centrally controlled user rights, comprehensive system administrator console.
- Possibility to share lab resources located in multiple localizations.
- Possibility to reserve access to lab bundles in advance, and to create configuration snapshots to be used later.
- High configurability, customizability and security.
- Simple licensing model.

Commercial network remote access system for e-learning do exist. However, in authors' opinion, none of currently available systems meets all or at least most of the listed above criteria. The main building box of the proposed solution have been already implemented and described in [6]. The system is currently used to provide Cisco NetAcad (CCNA, CCNA Security, CCNP), Extreme Networks (routing, switching, access control, wireless) courses (locally and remotely) and to access the same lab for scientific purposes. This paper is concentrated on its further development (for example an option of either client-based or clientless access) and performance tests.

2. MATERIALS AND METHODS

2.1. The hardware

The main server (Fig. 1) is running under VMware®ESXi™(either free or paid version, depending on requirements), thus any VMware-compatible machine with enough resources is suitable. KVM[1]-based version is also planned.

802.11 wireless network USB NICs (network interface cards) are used to connect virtual PCs to wireless lab networks (assuming that wireless solutions are to be explored). Similarly, USB Ethernet NICs are mapped to virtual PCs, so that for example full 802.1x authentication can be implemented on lab switches.

The terminal server provides network access to console ports of network devices to be managed. It can be a separate device or a multi-port RS-232 PCI card, attached to the server.

[1] http://www.linux-kvm.org

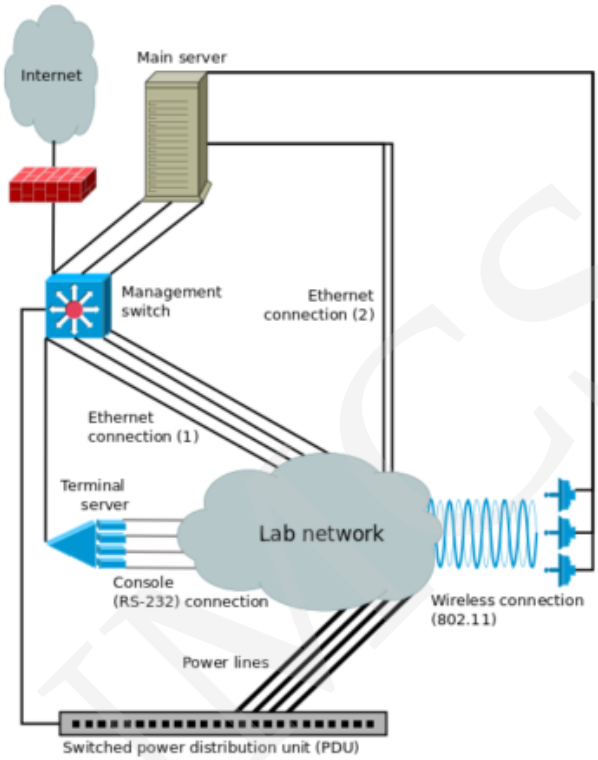

Figure 1 General system topology

The switched (IP-accessible) power distribution unit is the last crucial physical component. Physical devices are automatically turned on only when needed. Cold restart can be also performed by a remote user, for example to perform a password recovery procedure.

Connections inside a lab network are currently performed manually by an administrator, whose tasks need to be synchronized with bundles' configuration (described later).Application of a layer 1 system-managed-switch is considered in the future.

2.2. The software

Resources consumption of the main management server (Fig. 1) is limited, so the same physical machine (VMware®ESXi™server) can be also used by virtual machines (PCs, servers, virtual appliances, etc.) for the laboratory network or any other purpose. The remote access server performs the three main functions:

- lab resources access control,
- VPN concentrator,
- web server.

The management server acts as a secure point of access to the laboratory network. It gives granular control over time periods and resources availability for each user.

Virtual and physical devices are grouped into bundles (Fig. 2).

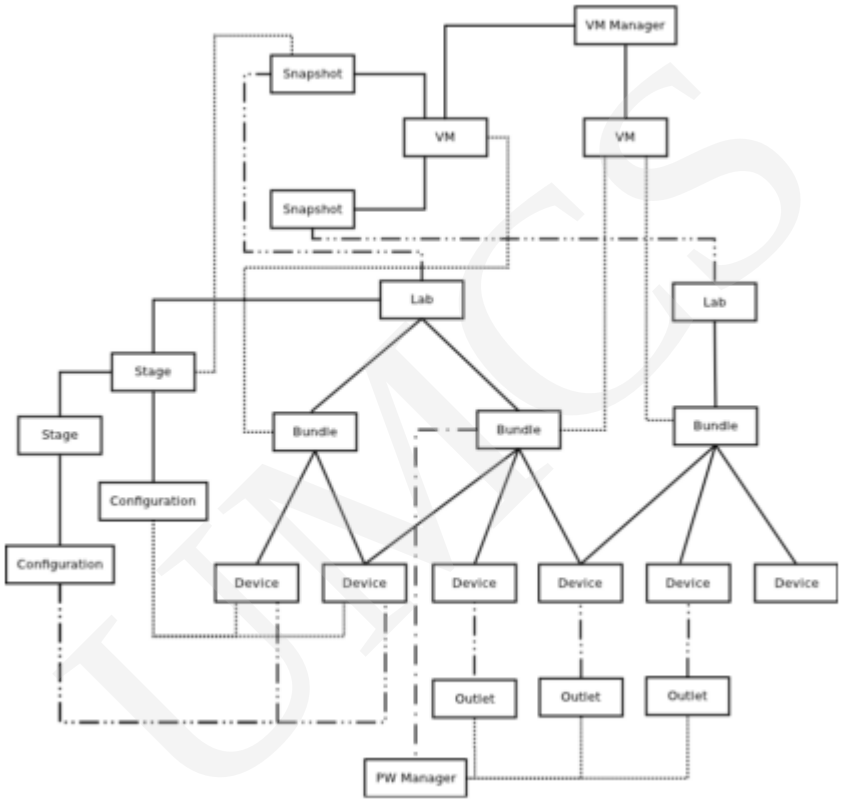

Figure 2 The system management software architecture diagram [6]

Users are authorised to access only the bundles assigned to them by the administrator. A bundle is accessible by a user in a time slot reserved in advance (through the scheduler). Bundles maybe available in defined periods only. It is the result of the fact that hardware could be bonded to different bundles, according to current hardware configuration. Bundle configuration (including server-managed VMware virtual switches and VLANs) is performed automatically by the system.

A user has three alternative options of remote access:

- A user has his own VNC, telnet, SSH software and SNMP tools. The server is used for access control and network traffic redirection. This option is useful for advanced users only.
- A standalone client program is used. Figs. 3, 4 present a client-based access to a laboratory preconfigured for Extreme Networks trainings, however the system is not limited to any particular vendor (provided that network devices are accessible in-band and/or out-of-band, by means of RS-232 interface, which is a standard now). The client provides a complete set of user tools. Traffic between the client

and the server is transmitted through a VPN tunnel. The client program can act also as a local server that offers parallel access to the laboratory equipment with user's software. Configuration like this provides also possibility to connect laboratory devices through a restricted firewall (connections to ports 443 and 22 only are established).

- Only a web browser is used at the client side. The server offers a web page with access to all user tools. The web application on the management server offers a full set of standalone client services. It is worth to point out that the whole solution is Java-less. Only a HTML5-compatible web browser with JavaScript is needed. In this solution the management server acts as a RFB, RDP, telnet and SSH proxy Only a connection to port 443 is necessary in this situation.

User's session state (configuration files and virtual machines' snapshots) can be saved and restored later.

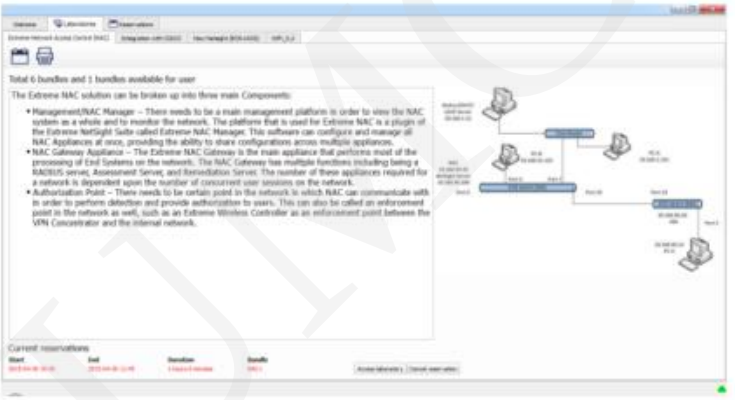

Figure 3 The lab information screen

Figure 4 VNC access to a remote virtual PC

The data is stored and managed centrally. Each laboratory can have stages (Fig. 2) defined by an administrator with proper configuration and/or VM snapshot. Such a stage could be restored by a user who wants to have faultless environment for a next part of an exercise.

3. RESULTS

It is important to know resources requirements (CPU, memory, network bandwidth) of a remote access system. This information is crucial for a system user, to scale an implementation accordingly to actual needs (number of users, devices, virtual machines, etc.).The testing procedure is described below. The other aspect is user satisfaction. According to a user satisfaction survey, the system is evaluated as simple, intuitive and fast.

The remote access server is running under VMware ®ESXi™system on a machine with Intel XEON E5-2640 processor and 32GB RAM. The server has two virtual CPUs assigned. The test remote lab consisted of 6 virtual PCs (Windows XP) and 6 Netsight [2] virtual appliances, running on the same machine as the remote access system. Six users were expected to perform the following procedure, at the same time:

- log into the virtual PC,
- start Netsight client (Java-based application) on the virtual PC,
- perform a few simple tasks (restore Netsight database, search for available devices, use the help),
- close the Netsight client, use a web browser intensively.

The procedure was repeated for each of the available access methods:

1. Users had their own VNC clients to connect to the virtual PC. The remote access server was then responsible only for access control, network traffic translation and redirection (between the virtual PC and the remote user).

2. The client application was used to access the lab. The application has its own VNC client and establishes a VPN tunnel with the remote access server.
3. Web-based (HTML5) access was used.

In the first case the access server CPU utilization was marginal (Fig. 5), up to 10%.

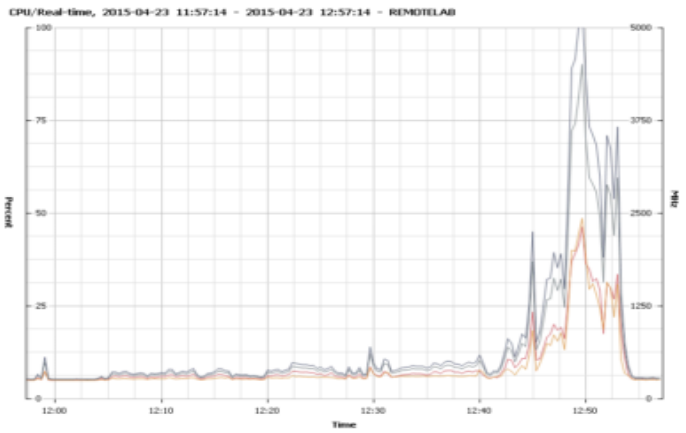

Figure 5 CPU utilization during the test (12:00-12:30 - 1st access method, 12:30-12:40 - 2nd access method, 12:40-12:55 – 3rd access method); dark grey line shows CPU usage in percent, the light grey one in MHz

Network bandwidth utilization remained below 1 MBps (Fig. 6).

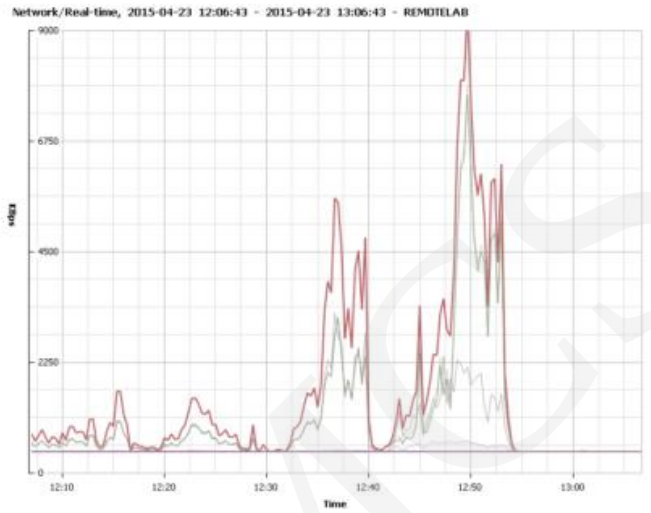

Figure 6 Network bandwidth utilization during the test (12:00-12:30 - 1st access method, 12:30-12:40 - 2nd access method, 12:40-12:55 - 3rd access method); the total network utilization (sent and received traffic) is shown by the thick red line

In the second access method, a slight CPU utilization growth is observed, because the server is additionally responsible for traffic encryption. Maximal network bandwidth utilization was about 5 MBps.

The last test (web-based access) was the most resources-intensive. It is natural, because the VNC client-side software runs on the server side rather than a user's machine. A user receives just web content, presenting current view of the remote machine's desktop. The access server CPU utilization was then about 50% during normal operation and up to 100% during intensive web browsing. Network maximal bandwidth utilization was about 9MBps.

It has to be noticed that maximal network bandwidth utilization takes place only during intensive web browser usage (many quickly changing, complex graphical objects to be transmitted), which is not a typical application of the presented system. A normal networker's work is much less bandwidth consuming.

4. DISCUSSION

The presented solution seems to be closely related to commercially available NDG NETLAB+[2]. The NETLAB is commonly used for regular trainings on dedicated equipment (provided that limitations like lack of 802.11 and 802.1x support are not an issue). The situation is much more complicated when the same devices are to be used for different purposes concurrently. In the presented system, a single device can be a member of a few

[2] http://www.netdevgroup.com/products/

different bundles, used for various courses and research purposes. Potential conflicts are resolved by the scheduler.

Scientific needs are often non-standard, unpredictable and thus inconsistent with license agreements. The presented solution is based mainly on free license solutions and authors' own code.

User interface of remote access systems is usually Java-based. This approach is natural and has obvious advantages. The latest Java versions have security extensions intended to make user systems less vulnerable to exploits. On the other hand, for some Java applications it is necessary to have appropriate Java version, web browser version and web browser security settings, to run properly. Security is an obvious issue. These requirements are not difficult to meet in a controlled environment, but it may be a serious problem to enforce them on remote users' computers. The described system offers alternative solutions. A user receives a standalone client program (Fig. 3, 4) for performing all user tasks. Network connection between the client and the server is SSL-encrypted. The client software installation requires neither administrator privileges nor any non-standard libraries. The program can be started from any directory or media (including a USB disk). Advanced users have also an option of using their own programs (VNS/RDP client, telnet client, etc.) on their local machines and have management traffic securely tunnelled to a remote lab network.

Required Internet connection quality (bandwidth, delay, jitter) is another issue that needs to be addressed. According to multiple tests (in a simulated environment and the real world: broadband connections, GSM-based access, etc.), no network-related problems are expected, unless the Internet connection is extremely poor.

5. CONCLUSIONS

The presented here combination of multiple physical and virtual network devices and hosts, with various in-band and out-of-band access methods and concurrent users, seems to be unique. There are some academic projects focused on networking remote learning, but they are either proprietary solutions, not available publicly, or (probably most commonly), NDG NETLAB+ is employed [7]. According to test users satisfaction survey and opinions expressed for several months of the system use, this solution is simple, intuitive and fast. During local networking trainings (routing, switching, wireless courses, currently on Cisco and Extreme Networks infrastructure), for beginners it is beneficial to have a direct access to lab network infrastructure. Advanced students are offered a choice of connecting directly to physical devices or using the access system. 100% of our students have chosen the remote access system-based option, since the system had been implemented. It gives features that make the work more comfortable, without noticeable responsiveness degradation, compared to direct physical access, plus possibility to continue lab work after regular class hours, remotely. The same infrastructure is used also for scientific purposes (various kinds of computer networking research) and to test and and refine network-based software in a controlled environment. The implementation in the networking lab has also significantly reduced the amount of lab administration work. It provides a centralized management tool for both physical and virtual infrastructure. The current form of the system constitutes a solid and flexible framework for future extensions and development.

LITERATURE

[1] Cisco Systems (2015) Cloud and Systems Management, http://www.cisco.com/c/en/us/products/cloud-systems-management/
[2] Extreme Networks (2015) Extreme Networks NetSight, http://www.extremenetworks.com/product/netsight
[3] Hewlett-Packard Development Company (2015) Network Management, http://www8.hp.com/pl/pl/software-solutions/network-management-automated-network-management/
[4] Bastidas C.E.C (2011) *41st Enabling Remote Access to Computer Networking Laboratories for Distance Education*. In ASEE/IEEE Frontiers in Education Conference, Rapid City, SD
[5] Ellison N.B (2004) *Telework and Social Change: how technology is reshaping the boundaries between home and work*, Westport, Connecticut: Praeger, p. 18, ISBN 9780313051715, OCLC 57435712
[6] K. Kuczynski, R. Stęgierski, W. Suszynski, M. Pellerin, *Versatile Remote Access Environment for Computer Networking Laboratory. In R. Choras* (ed.), Image Processing and Communication Challenges 6, Advances in Intelligent Systems and Computing 313, Springer Int. Publishing Switzerland 2015.
[7] C.E. Caicedo Bastidas, *Enabling Remote Access to Computer Networking Laboratories for Distance Education*, 41st ASEE/IEEE Frontiers in Education Conference, 2011.