Marek Bolanowski, Andrzej Paszkiewicz

Metody i środki zapewnienia dostępu do specjalizowanych zasobów laboratoryjnych

Edukacja - Technika - Informatyka 5/2, 334-341

2014

Marek BOLANOWSKI, Andrzej PASZKIEWICZ
Politechnika Rzeszowska, Polska

Metody i środki zapewnienia dostępu do specjalizowanych zasobów laboratoryjnych

Wstęp

Aspekt kształcenia praktycznego na kierunkach technicznych jest sprawą kluczową w procesie edukacji współczesnego inżyniera. Szeroki wachlarz dostępnych specjalności oraz coraz większa specjalizacja inżynierów stawia przed uczelnią wyższą nowe wyzwania związane z szerokim dostępem do zasobów laboratoryjnych. Jednym z kluczowych obszarów kształcenia w obszarze informatyki jest nauczanie przedmiotów specjalistycznych powiązanych z pracą na specjalizowanych urządzeniach. Studenci oprócz klasycznego wykładu powinni mieć powszechny, nieograniczony dostęp do możliwości praktycznej weryfikacji nabytej wiedzy oraz nauki w rzeczywistych lub testowych środowiskach dydaktycznych. Aby lepiej zrozumieć idee oraz specyfikę kształcenia praktycznego na kierunkach informatycznych, należy wprowadzić następującą klasyfikacji przedmiotów:

1. **Przedmioty oparte o uniwersalne platformy sprzętowe oraz specjalizowane oprogramowanie.** Dla tej grupy przedmiotów całość zajęć laboratoryjnych może być zrealizowana w oparciu o ogólnie dostępną architekturę komputera osobistego wyposażonego w specjalizowane oprogramowanie. Do tego obszaru możemy na przykład zaliczyć następujące przedmioty: programowanie, bazy danych, systemy operacyjne, metody obliczeniowe itp. W tym wypadku rola jednostki dydaktycznej (uczelni, szkoły średniej) sprowadza się do zapewnienia studentom odpowiednich licencji oraz dostępu do specjalizowanego oprogramowania. W efekcie uczeń może samodzielnie wykonywać ćwiczenia lub eksperymentować bez narzucania mu sztywnych ram czasowych, co skutkuje lepszym poznaniem danej technologii i pozwala mu zdobyć doświadczenie zawodowe potrzebne na rynku pracy. W chwili obecnej firmy produkujące specjalizowane oprogramowanie dysponują szeroką ofertą skierowaną do studentów, w ramach której bezpłatnie lub na preferencyjnych warunkach udostępniają swoje aplikacje do celów dydaktycznych (np. Microsoft Developer Network MSDN).
2. **Przedmioty oparte o specjalizowane platformy sprzętowe oraz specjalizowane oprogramowanie.** Zajęcia dla tej grupy przedmiotów prowadzone są w oparciu o drogą infrastrukturę sprzętową, a dostęp do niej jest możliwy tylko i wyłącznie w specjalizowanym laboratorium. Do tej grupy przedmio-

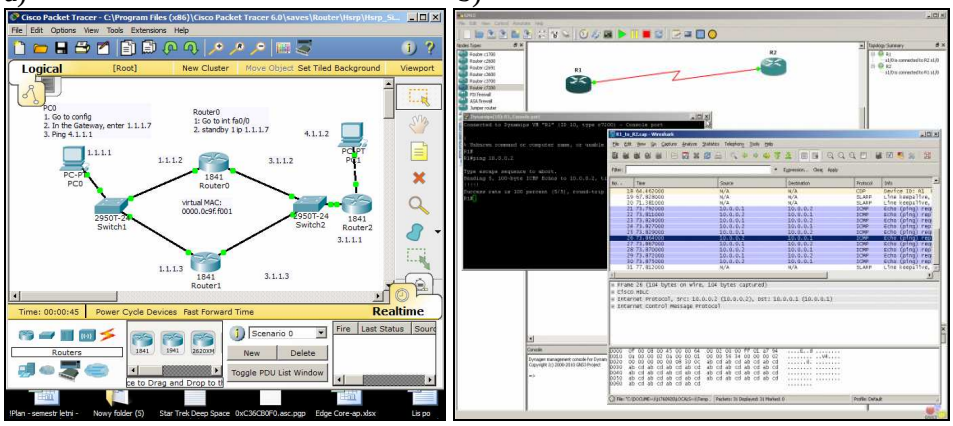
tów możemy zaliczyć między innymi: sieci komputerowe, automatykę i robotykę, oprogramowanie specjalizowanych obrabiarek. Samodzielna praca z taką specjalizowaną infrastrukturą laboratoryjną jest możliwa tylko i wyłącznie w godzinach pracy uczelni i pracowników technicznych nadzorujących prace w laboratorium.

Głównym celem tego artykułu jest zaproponowanie zdalnych metod dostępu do specjalizowanych zasobów laboratoryjnych na przykładzie przedmiotu sieci komputerowe. Zaproponowane zostaną zarówno metody oparte o symulatory sieciowe, jak również autorska topologia systemu umożliwiająca zdalną pracę na rzeczywistych urządzeniach.

1. Wirtualizacja środowiska sieciowego

Niektórzy producenci oprogramowania sieciowego mają w swojej ofercie symulatory urządzeń sieciowych, z wykorzystaniem których możemy symulować całe, złożone środowiska sieciowe. Sztandarowym przykładem takiego rozwiązania jest program Cisco Packet Tracer [Smith, Bluck 2010: 356–362]. W tym rozwiązaniu możemy zbudować własną topologię sieciową oraz wdrożyć na jej bazie różne protokoły, poczynając od prostej adresacji, a kończąc na złożonych architekturach routingu. W tego typu programach mamy dostęp za pośrednictwem konsoli do urządzeń, które są elementami testowanej topologii. Niestety, niejednokrotnie nie jest możliwe wykonanie wszystkich poleceń, ponieważ konsola symulowanego urządzenia zawiera tylko ich pewien podzbiór w porównaniu do urządzenia rzeczywistego.

a) b)

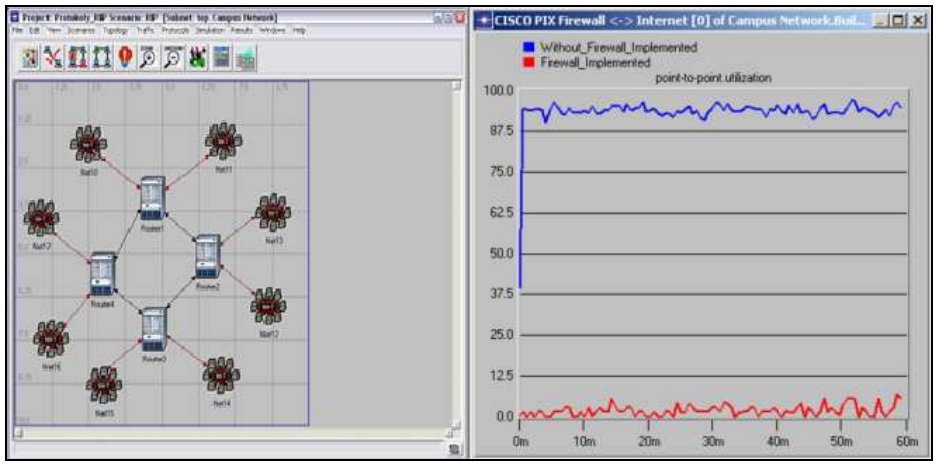


Rys. 1. Okno aplikacji: a) Cisco Packet Tracer, b) GNS3
Źródło: http://www.gns3.net/screenshots/

Problem ten po części rozwiązuje symulator GNS3 [GNS3, Graphical Network Simulator], w którym możemy uruchamiać wirtualne urządzenia (wybrane modele IOS urządzeń Cisco i Juniper), ale możliwe jest to tylko dla wybranych modeli urządzeń.

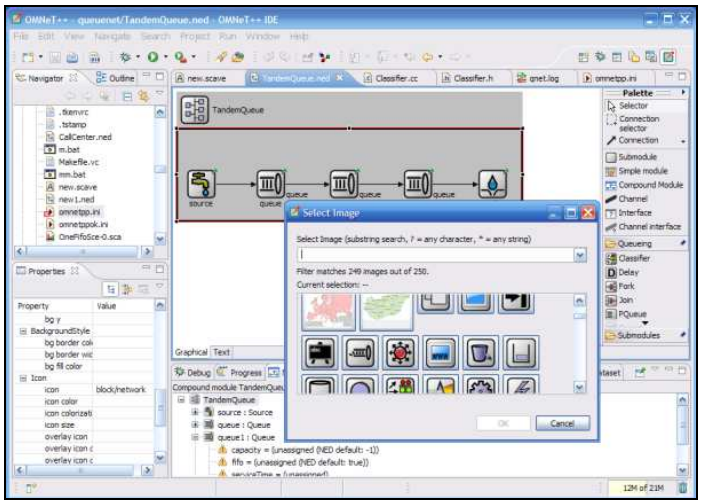
Niestety, opisywane powyżej podejścia umożliwiają symulacje sieci zbudowanych w oparciu o jednego producenta lub nawet o wybrane urządzenia jednego producenta. Jednak według raportu Gartnera [Duffy 2011], budowa sieci komputerowej właśnie w oparciu o urządzenia różnych producentów prowadzi do ograniczenia kosztów bez jednoczesnego wzrostu złożoności i niedostępności finalnego rozwiązania. Należy więc zapewnić studentom możliwość dostępu do środowisk symulacyjnych, pozwalających budować i symulować takie właśnie heterogoniczne środowiska.

Drugi obszar rozwiązań programowych to uniwersalne symulatory sieciowe bazujące na modelach matematycznych i algorytmicznych. Możemy tu wskazać trzy wiodące rozwiązania: Opnet (Riverbed Modeler) [Guo, Xiang, Wang 2007: 215–226; Opnet Modeler], Omnet++ [Cocorada 2011: 229–234] i NS-2 [http://www.isi.edu/nsnam/ns/]. Opnet to rozwiązanie komercyjne, które umożliwia symulowanie bardzo złożonych środowisk komunikacyjnych oraz ma odwzorowanych w swojej bazie bardzo wiele urządzeń sieciowych. Konfigurację urządzeń w tym środowisku wykonuje się w uproszczony sposób z wykorzystaniem środowiska GUI (ang. Graphic User Interface) poprzez zmianę poszczególnych parametrów urządzenia i kanału komunikacyjnego. Po stworzeniu modelu sieci możemy badać wybrane parametry sieci. Wadą tego rozwiązania są jednak duże koszty związane z zakupem licencji. Co prawda aplikacja dostępna jest w ramach programu IT Guru Academic Edition, ale w jej ramach nie są dostępne wszystkie funkcje programu i protokoły oraz ograniczony jest rozmiar symulowanego środowiska komunikacyjnego.



Rys. 2. Okna aplikacji OPNET IT Guru Academic Edition

Pozostałe dwa symulatory, tj. Omnet++ i NS-2 są symulatorami bardzo mocno zorientowanymi na samodzielne oprogramowanie własnych urządzeń i protokołów. Umożliwiają one realizacje bardzo złożonych symulacji, ale jednocześnie wymagają od użytkownika stosunkowo dużych umiejętności programistycznych, co predestynuje je bardziej do zastosowań naukowych niż dydaktycznych. Zarówno Opnet, Omnet++ i NS-2 nie udostępniają możliwości konfiguracji urządzeń sieciowych z wykorzystaniem charakterystycznych dla danego producenta konsol CLI. Dlatego ich zastosowanie w procesie dydaktycznym, który ma zaznajomić studentów z urządzeniami stosowanymi w przemyśle, wydaje się być ograniczone. Tego typu rozwiązania mogą być z powodzeniem stosowne przez doświadczonych inżynierów w procesie projektowania sieci i protokołów oraz przez jednostki naukowo-badawcze.



Rys. 3. Widok okna programu OMNET++
Źródło: http://www.omnetpp.org/

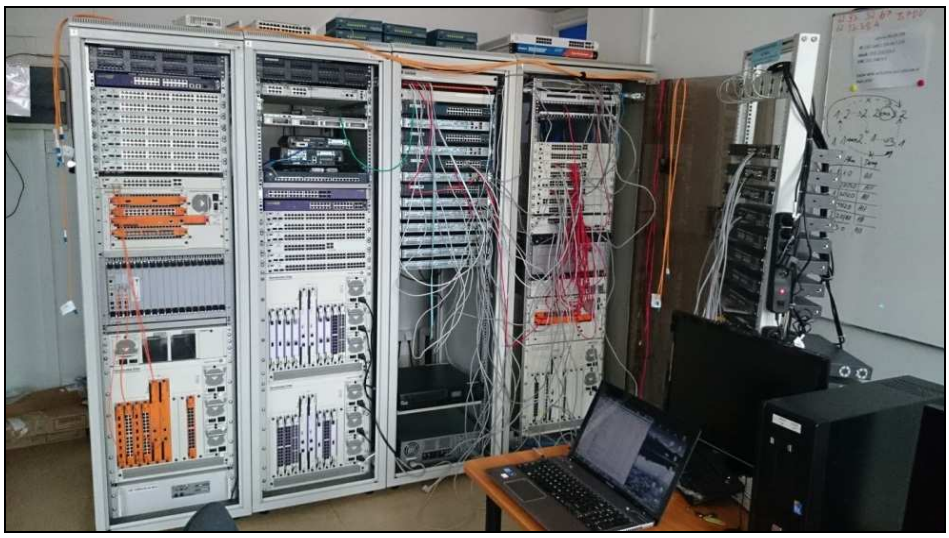
2. Udostępnienie zasobów rzeczywistego środowiska laboratoryjnego

Duże heterogeniczne środowiska laboratoryjne stwarzają możliwości testowania ogromnej gamy protokołów i topologii sieciowych. Głównym wyzwaniem, jakie powstaje w przypadku korzystania z takich zasobów, jest jak najszersze ich udostepnienie zainteresowanym osobom. Przy takim założeniu należy wziąć pod uwagę kilka aspektów:

– W odróżnieniu od programów symulacyjnych studenci mają dostęp do rzeczywistych wykorzystywanych przemysłowo urządzeń.
– Przy zakupie specjalizowanych urządzeń sieciowych dana jednostka ponosi znaczące koszty, tak więc jest z reguły zainteresowana umożliwieniem jak najszerszego do nich dostępu, również poza godzinami pracy – zdalnie.

– Jeżeli w danym laboratorium realizowane są ćwiczenia przez grupę studentów, która fizycznie go zajmuje, to bardzo rzadko wykorzystuje ona całość zainstalowanego sprzętu. Zatem możliwe jest korzystanie z urządzeń przez osoby będące fizycznie w laboratorium, jak i przez osoby łączące się do niego zdalnie.

W tym rozdziale zaproponowana zostanie metoda zdalnego udostępniania zasobów laboratorium sieciowego. Zdjęcie jednego ze stanowisk urządzeń sieciowych zostało zaprezentowane na rys. 4. Na rynku można znaleźć nieliczne rozwiązania komercyjne służące do realizacji dostępu do takich stanowisk, ale po ich analizie okazało się, że nie spełniają one oczekiwań, są stosunkowo drogie lub dedykowane dla urządzeń jednego producenta. Na podstawie ich analizy zidentyfikowano kilka podstawowych założeń realizowanego projektu: uniwersalność, niezależność od producenta urządzeń, łatwość w implementacji.

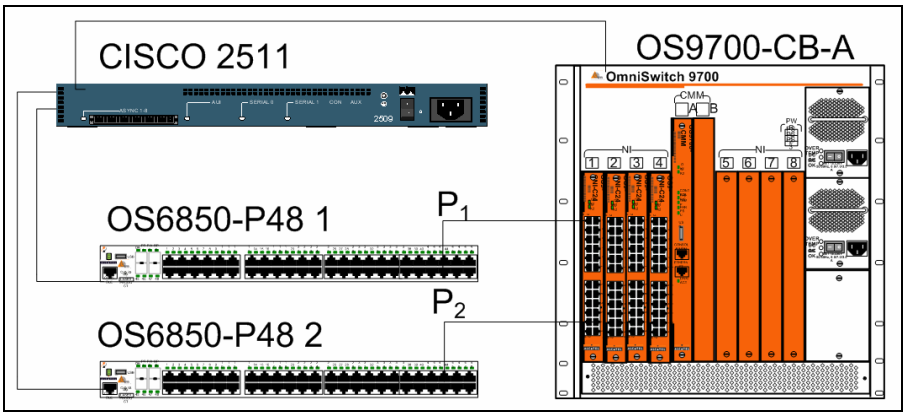


Rys. 4. Stanowisko urządzeń sieciowych, którego elementy były udostępniane w ramach testów

Podstawowe problemy, z jakimi należało się zmierzyć, to: jak zdalnie uzyskać dostęp do konsol urządzeń sieciowych w laboratorium (łączność realizowana jest z wykorzystaniem portu szeregowego), jak dynamicznie zmieniać fizyczne połączenia pomiędzy urządzeniami, jak zarządzać komputerami podłączonymi do infrastruktury zdalnego laboratorium. Poniżej omówione zostanie rozwiązanie każdego z tych problemów.

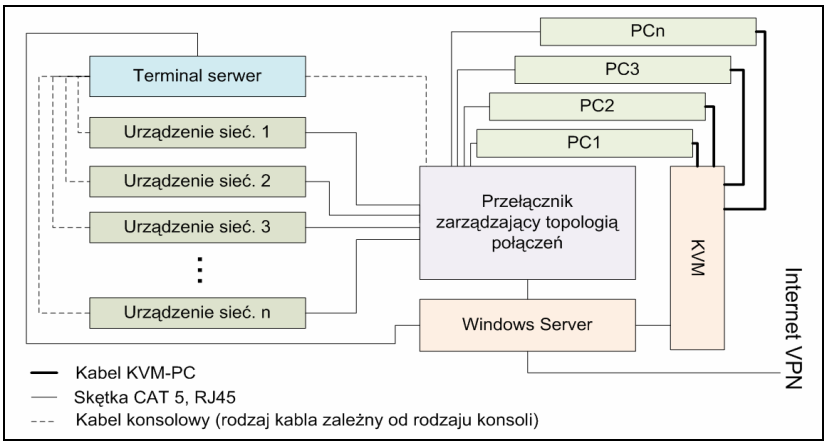
Dostęp do konsoli urządzenia został zrealizowany za pomocą rutera Cisco 2511, który pełni rolę serwera terminali. Na urządzeniu tym skonfigurowany został zdalny dostęp z wykorzystaniem protokołu SSH. Do portu ASYNC rutera

podłączony został kabel rozszyty na 8 kabli konsolowych podłączonych do urządzeń będących elementami udostępnianych zasobów. Użytkownik po zalogowaniu się poprzez SSH do rutera Cisco 2511 ma bezpośredni dostęp z wykorzystaniem funkcjonalności Reverse Telnet do konsoli 8 urządzeń sieciowych. W następnym kroku wykorzystywane urządzenia sieciowe zostały połączone dużą ilością portów (nie mniej niż 10 na każde urządzenie) z przełącznikiem modularnym (OmniSwitch 9700), tak jak to zostało pokazane na rys. 5. Jeżeli chcemy zestawić fizyczne połączenie pomiędzy portami P_1 na przełączniku OS6850-P48 1 i portem P_2 na przełączniku OS6850-P48 2, to wystarczy, że na przełączniku OS9700-CB-A porty, do których podłączone są P_1 i P_2, przenieść do osobnej sieci VLAN (ang. Virtual LAN). Komunikacje na porcie przełącznika testowego (w naszym przypadku OS6850-P48 1 lub 2) możemy wyłączyć poprzez wyłączenie portu administracyjnie z konsoli. Z wykorzystaniem zaprezentowanej topologii oraz łączenia portów za pomocą sieci VLAN jesteśmy w stanie zbudować dowolną topologię sieciową, **tworzyć i usuwać połączenia pomiędzy urządzeniami** oraz symulować awarie.



Rys. 5. Schemat podłączenia przełączników pozwalający dynamicznie budować połączenia fizyczne pomiędzy przełącznikami testowymi

Ostatnia kluczowa kwestia, która pozostała do rozwiązania, to dostęp do stacji roboczych podłączonych do urządzeń sieciowych. **Zarządzanie komputerami** zostało zrealizowane poprzez zastosowanie urządzenia KVM (ang. KVM switch – Keyboard Video Mouse) bazującego na protokole IP. Umożliwia on operatorom lokalnym i zdalnym monitorowanie i korzystanie z wielu komputerów. Użytkownicy zdalni korzystają z przełącznika przez sieć za pomocą przeglądarki internetowej i protokołu komunikacyjnego TCP/IP. Wykorzystane urządzenie CS1708i obsługuje do 32 użytkowników jednocześnie, przy zapewnieniu dostępu do komputera przez jedną magistralę.



Rys. 6. Schemat połączeń oraz komunikacji testowego stanowiska sieciowego z możliwością pracy zdalnej

Schemat zarządzania oraz komunikacji w tak połączonym środowisku testowym został przedstawiony na rys. 6. Urządzenia sieciowe, które chcemy udostępniać, mogą być dobieranie dowolnie, pod warunkiem że można nimi zarządzać z wykorzystaniem portu szeregowego lub protokołu TCP/IP. Użytkownik uzyskuje zdalnie dostęp do zasobów łącząc się z wykorzystaniem VPN (ang. Virtual Private Network) i RDP (ang. Remote Desktop) do Windows Server'a. Następnie loguje się do serwera terminali i przy wykorzystaniu przełącznika zarządzającego topologią połączeń ustala topologię fizyczną. W kolejnym kroku przystępuje do konfiguracji poszczególnych urządzeń w zależności od potrzeb. Dostęp do poszczególnych stacji PC użytkownik uzyskuje łącząc się z Windows Server'a do przełącznika KVM.

Zakończenie

W pracy zaprezentowano metody i środki zapewnienia dostępu studentom do specjalizowanych urządzeń sieciowych. Szczególny nacisk został położony na jak najwierniejsze odwzorowanie rzeczywistych warunków pracy. Zdaniem autorów, realizowanie zajęć laboratoryjnych na symulatorach urządzeń jest możliwe i w bardzo wielu przypadkach pożądane (np. w procesie certyfikacji inżyniera w ramach urządzeń danego producenta). Autorzy zaprezentowali model udostępniania rzeczywistych urządzeń sieciowych zdalnie. Zaprezentowana topologia pozwala zestawiać praktycznie dowolne środowiska testowe i umożliwia studentom ciągłą z nimi pracę. W kolejnych krokach system będzie rozwijany w dwóch obszarach: poprzez zbudowanie strony internetowej, która będzie stanowić interfejs dostępowy dla użytkowników, oraz poprzez dodanie kolejnej grupy urządzeń, których obrazy udostępniane są w postaci wirtualnej (np. Mikrotik), i zintegrowanie ich z fizycznym środowiskiem laboratorium.

Literatura

Cocorada S. (2011), *Integrating Omnet++ for teaching, learning and assessment in computer networking*, Conference proceedings of "eLearning and Software for Education" (eLSE), issue: 02/2011, www.ceeol.com.

Duffy J. (2011), *Gartner slams Cisco's single-vendor network vision*, January 21, http://www.networkworld.com/news/2011/012011-gartner-slams-cisco-single-vendor.html?source=NWWNLE_nlt_daily_am_2011-01-21

GNS3, Graphical Network Simulator, http://www.gns3.net/

Guo J., Xiang W., Wang S. (2007), *Reinforce Networking Theory with OPNET Simulation*, "Journal of Information Technology Education", vol. 6.

http://www.isi.edu/nsnam/ns/

Opnet Modeler, http://www.riverbed.com/

Smith A., Bluck C. (2010), *Multiuser Collaborative Practical Learning Using Packet Tracer, Networking and Services* (ICNS), Sixth International Conference on, 7–13 March 2010, IEEE.

Streszczenie

W artykule przedstawiono metody i środki dostępu do specjalizowanych środowisk laboratoryjnych na przykładzie stanowiska urządzeń sieciowych. Zaprezentowano możliwości wirtualizacji stanowisk urządzeń sieciowych oraz zaproponowano własną metodę zdalnego udostępniania rzeczywistych urządzeń sieciowych. Dzięki takiemu podejściu możliwe staje się realizowanie zajęć laboratoryjnych z sieci komputerowych w formie nauczania na odległość.

Słowa kluczowe: nauczanie na odległość, zdalny dostęp do laboratorium, wirtualne laboratorium, sieci komputerowe.

Methods and means of ensuring access to specialized laboratory resources

Abstract

The paper presents the methods and means of access to specialized laboratory environments on the example a network devices laboratory. The possibilities of virtualization of network devices stand are presented and own method of remote access to the network devices test stand are presented. With this approach it is possible to implement computer network laboratory classes in the form of distance learning.

Key words: distance learning, remote access to laboratory, virtual laboratory, computer network.