Robert Pękala, Tadeusz Kwater, Dariusz Strzęciwilk, Paweł Dymora

Technologie wirtualizacji i emulacji w badaniu sieci komputerowych

Edukacja - Technika - Informatyka nr 4(18), 371-376

2016

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

MUZEUM HISTORII POLSKI

© Wydawnictwo UR 2016 „Edukacja – Technika – Informatyka" nr 4/18/2016
ISSN 2080-9069 www.eti.rzeszow.pl
ISSN 2450-9221 online DOI: 10.15584/eti.2016.4.49

ROBERT PĘKALA[1], TADEUSZ KWATER[2], DARIUSZ STRZĘCIWILK[3], PAWEŁ DYMORA[4]

Technologie wirtualizacji i emulacji w badaniu sieci komputerowych

Virtualization and emulation technologies in the study of computer networks

[1] Doktor, Państwowa Wyższa Szkoła Techniczno-Ekonomiczna w Jarosławiu, Polska
[2] Doktor habilitowany inżynier profesor UR, Uniwersytet Rzeszowski, Wydział Matematyczno-Przyrodniczy, Katedra Inżynierii Komputerowej, Polska
[3] Doktor inżynier, Szkoła Główna Gospodarstwa Wiejskiego w Warszawie, Wydział Zastosowań Matematyki i Informatyki, Katedra Zastosowań Informatyki, Zakład Systemów Rozproszonych, Polska
[4] Doktor inżynier, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, Polska

Streszczenie

W artykule przedstawiono zagadnienia obrazujące możliwości zastosowania współczesnych technologii wirtualizacyjnych oraz emulacyjnych w procesie kształcenia studentów kierunków informatycznych. W szczególności dotyczy to treści związanych z tematyką usług w sieciach komputerowych. Autorzy wskazują na możliwości realizacji scenariuszy sieciowych, wykorzystujących obrazy *iso* systemów operacyjnych desktopowych i serwerowych w połączeniu z obrazem systemu operacyjnego Cisco IOS. Wykorzystanie platformy wirtualizacyjnej oraz emulacyjnej na zajęciach laboratoryjnych pozwoli studentom, w sposób porównywalny do warunków rzeczywistych, dokonywać konfiguracji oraz wdrażania usług sieciowych.

Słowa kluczowe: wirtualizacja, emulacja, serwer *Radius*, klient *NAS*, suplikant, uwierzytelnianie, autoryzacja, użytkownik.

Abstract

The article presents issues concerning the applicability of virtualization and emulation technologies in the teaching process for *IT* students. The presented content in particular relates to the subject of computer network services. The authors point to the possibility of simulating selected network scenarios, using *iso* images of desktop and server operating systems and *Cisco IOS* operating system image. The use of virtualization and simulation platform will allow in a manner similar to real conditions make the configuration and implementation of network services.

Key words: virtualization, emulation**,** *Radius* server, client *NAS*, supplicant, authentication, authorization, user.

Wstęp

Rozwój technologii informatycznych doprowadził do pojawienia się w słownikach stosunkowo nowego pojęcia – przetwarzanie w chmurze (z ang. *cloud computing*). W rzeczywistości dotyczy ono pewnego modelu dostarczania różnego rodzaju usług IT, których różnorodność staje się coraz bogatsza. Do niedawna usługi te były kojarzone głównie z udostępnianiem przestrzeni dyskowej, jednak obecnie ich oferta obejmuje m.in. pocztę elektroniczną, serwisy WWW, sklepy internetowe, a nawet takie ambitne rozwiązania, jak np. księgowość internetowa dla firm [„Computerworld" 2016; „Networld Trendy" 2013]. Wydaje się zatem, iż nie trzeba nikogo przekonywać, jak ważne jest to zagadnienie, szczególnie dla studentów kierunków informatycznych.

Z technicznego punktu widzenia, przetwarzanie w chmurze oparte jest przede wszystkim na technologii wirtualizacji. Pozwala ona m.in. na uruchamianie różnych systemów operacyjnych, a tym samym usług, w tzw. maszynach (komputerach) wirtualnych, funkcjonujących w ramach zasobów komputera fizycznego. Na jednej fizycznej maszynie teoretycznie może pracować wiele maszyn wirtualnych, przy czym zawsze należy zachować pewien umiar co do ich liczby, tak aby zachować odpowiednią wydajność przetwarzania.

Współczesne oprogramowanie wirtualizacyjne daje ogromne możliwości parametryzacji maszyn wirtualnych pod kątem dostępu do fizycznych zasobów komputera w postaci pamięci RAM, dysku bądź macierzy dyskowej, interfejsów *I/O*, a nawet liczby rdzeni procesora/procesorów. Należy jednocześnie mieć na uwadze pewne wady technologii, związane np. z wysokimi wymaganiami co do parametrów sprzętu fizycznego (wysokie koszty), czy też zwiększonym problemem bezpieczeństwa i kontroli dostępu do danych zwirtualizowanych.

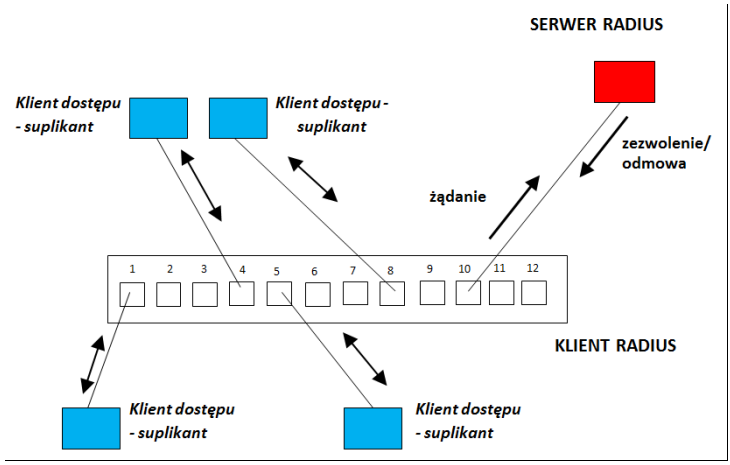
Pozytywne cechy oprogramowania mogą być nieocenione w funkcjonowaniu systemów komputerowych na uczelniach. Wystarczy wskazać tutaj chociażby na możliwość względnie łatwej reinstalacji systemu wirtualnego, co w warunkach funkcjonowania laboratoriów z dużą liczbą studentów znacząco może ułatwić zarządzanie oprogramowaniem stosowanym w dydaktyce. W

niniejszym artykule pragniemy wskazać na jeszcze jedną możliwość zastosowania wirtualizacji w kontekście realizacji pewnych treści nauczania w ramach przedmiotów związanych z technologiami sieci komputerowych. Jak wiadomo, realizacja treści z tego zakresu wymaga zwykle wykonywania przez studentów ćwiczeń laboratoryjnych, gdzie wykorzystuje się sprzęt w postaci urządzeń sieciowych. Prezentowane podejście pokazuje, iż alternatywą może być wykorzystanie środowiska wirtualizacyjnego oraz emulatora sieciowego. Dzięki temu studenci mogą realizować pewne scenariusze sieciowe w sposób, który nie odbiega od warunków rzeczywistych, ale bez konieczności używania fizycznego sprzętu. Wypracowane i zbadane w ten sposób konfiguracje mogą być później w tychże urządzeniach fizycznych implementowane.

Badanie usługi sieciowej RADIUS w środowisku VirtualBox oraz GNS3

Usługa sieciowa, działająca w oparciu o protokół RADIUS (z ang. *Remote Authentication Dial-In User Service*), stosowana jest głównie w celu uwierzytelniania i autoryzacji użytkowników sieci LAN, zbudowanej w technologii przewodowej, bezprzewodowej lub hybrydowej. Mówiąc inaczej, zadaniem protokołu jest potwierdzenie tożsamości logującego się w sieci użytkownika oraz upoważnienie go do korzystania z sieci LAN. To upoważnienie najczęściej związane jest z możliwością wykorzystania portu urządzenia dostępowego, co otwiera drogę użytkownikowi do korzystania z sieci kontrolowanej przez to urządzenie. Opcjonalnie protokół może także przetwarzać dane służące rozliczaniu użytkownika z wykorzystywanych przez niego zasobów sieciowych. Zatem RADIUS wpisuje się w tzw. model bezpieczeństwa AAA (z ang. *Authentication Authorization Accounting*).

Usługa działa w architekturze klient-serwer, przy czym dodatkowo należy jeszcze uwzględnić oprogramowanie w postaci tzw. klienta dostępu lub inaczej suplikanta (z ang. *supplicant*), działającego zwykle na stacjach desktopowych, z dowolnym rodzajem systemu operacyjnego i zgodnie z protokołem IEEE 802.1x. Wymagane komponenty usługi zostały przedstawione na rys. 1.

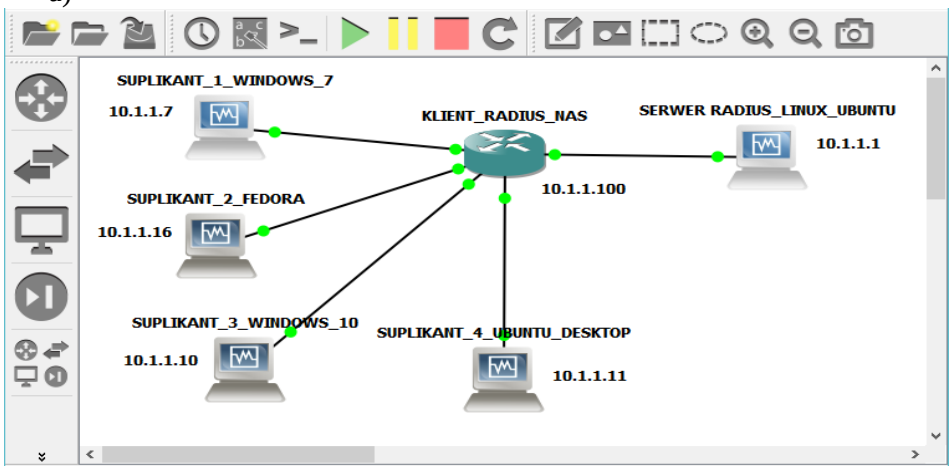


Rys. 1. Idea usługi *RADIUS* na przykładzie sieci przewodowej

Klientem może być urządzenie sieciowe, np. przełącznik zarządzalny (wspierający protokół IEEE 802.1x oraz RADIUS), natomiast rolę serwera RADIUS może pełnić oprogramowanie implementowane w systemach operacyjnych komercyjnych lub w systemach GNU/Linux. Na rys. 1 uwzględniono 4 stacje z oprogramowaniem suplikanta podłączone do interfejsów przełącznika Ethernet. Przełącznik, jak urządzenie dostępowe do sieci, zwany inaczej NAS (z ang. *Network Access Server*), jest jednocześnie klientem serwera RADIUS.

Podjęcie próby logowania użytkownika na stacji suplikanta powoduje, iż do przełącznika NAS zostają wysłane niezbędne dane do autentykacji i uwierzytelniania. Dzięki temu NAS może utworzyć komunikat żądania o nazwie Access--Request, umieszczając w nim m.in. zaszyfrowane wcześniej parametry logowania, a następnie wysłać go do serwera zgodnie z protokołem RADIUS. Serwer weryfikuje odebrany komunikat, sprawdzając, czy przysłane parametry są zgodne z danymi przechowywanymi we własnej bazie danych użytkowników. W zależności od wyniku weryfikacji serwer może wygenerować komunikat zezwalający na dostęp (Access-Accept) lub komunikat odmowy (Access--Reject). W pierwszym przypadku następuje odpowiednia reakcja NAS w stosunku do stacji suplikanta, w wyniku której uzyskuje ona dostęp do sieci, dzięki włączeniu interfejsu przełącznika. Może się także zdarzyć, iż przed wysłaniem sygnału akceptacji serwer RADIUS żąda od klienta NAS dodatkowych informacji, wysyłając mu komunikat typu Access-Chalange.

a)



b)

```
NAS(config)#aaa new-model
NAS(config)#aaa authentication dot1x default group radius
NAS(config)#aaa authorization network default group radius
NAS(config)#dot1x system-auth-control
NAS(config)#radius-server host 10.1.1.1 auth-port 1812 acct-port 1813 key haslo
NAS(config)#int fa1/0
NAS(config-if)#dot1x port-control auto
NAS(config-if)#
*Mar  1 00:05:46.455: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to down
NAS(config-if)#exit
NAS(config)#exit
NAS#
*Mar  1 00:05:54.771: %SYS-5-CONFIG_I: Configured from console by console
NAS#$.1.1.1 auth-port 1812 acct-port 1813 kowalski serwerownia10 legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.

NAS#
*Mar  1 00:07:41.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
```

Rys. 2. Topologia sieci wraz z adresami interfejsów *IP* (a) oraz okno konsoli klienta *NAS* (b)

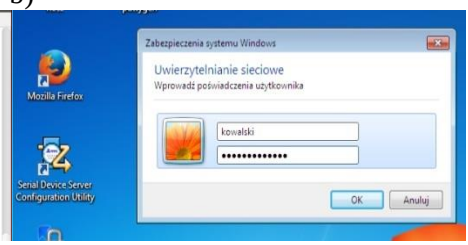
Ten krótki opis idei działania protokołu nie uwzględnia wielu dodatkowych mechanizmów, jednak jest wystarczający na potrzeby niniejszego artykułu. Należy zauważyć, że w warunkach rzeczywistych pełna konfiguracja usługi wymaga m.in. posiadania odpowiedniego przełącznika zarządzalnego. Na wielu uczelniach treści dydaktyczne z zakresu sieci komputerowych realizowane są w oparciu o sprzęt sieciowy firmy CISCO, z systemem operacyjnym IOS (z ang. *Internetworking Operating Sysytem*). To daje możliwość zastosowania darmowego oprogramowania o nazwie GNS3, które m.in. wspiera emulację tych urządzeń za pomocą obrazów systemu operacyjnego IOS. Ponadto może ono współpracować z darmowym środowiskiem wirtualizacyjnym VirtualBox, co z kolei stwarza warunki do budowy topologii sieciowych, w których jednocześnie występują zwirtualizowane systemy operacyjne serwerowe lub/oraz desktopowe, a także emulowane urządzenia sieciowe w postaci przełączników lub/oraz routerów [http://www.gns3.net; https://www.virtualbox.org]. Rysunek 2a przedstawia schemat topologii sieciowej zbudowanej za pomocą oprogramowania GNS3, będącej odpowiednikiem topologii z rys. 1.

a)

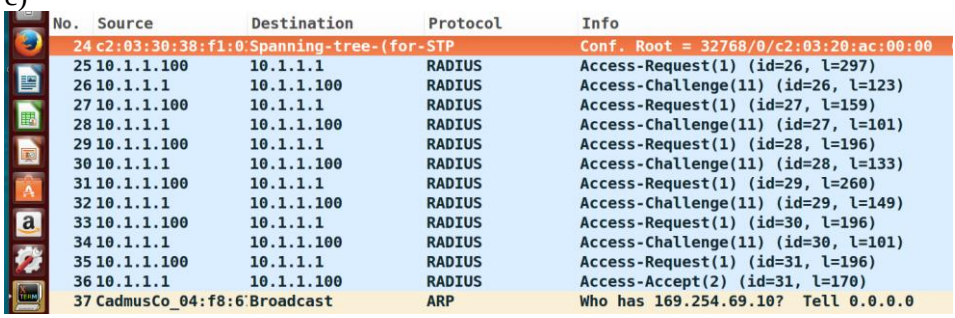
```
users ×
#
# Last default: rlogin to our main server.
#
#DEFAULT
#       Service-Type = Login-User,
#       Login-Service = Rlogin,
#       Login-IP-Host = shellbox.ispdomain.com

#
# On no match, the user is denied access.
kowalski Cleartext-Password := "serwerownia10"
        Auth-Type := Accept
```

b)



c)



No.	Source	Destination	Protocol	Info
24	c2:03:30:38:f1:0	Spanning-tree-(for-STP		Conf. Root = 32768/0/c2:03:20:ac:00:00
25	10.1.1.100	10.1.1.1	RADIUS	Access-Request(1) (id=26, l=297)
26	10.1.1.1	10.1.1.100	RADIUS	Access-Challenge(11) (id=26, l=123)
27	10.1.1.100	10.1.1.1	RADIUS	Access-Request(1) (id=27, l=159)
28	10.1.1.1	10.1.1.100	RADIUS	Access-Challenge(11) (id=27, l=101)
29	10.1.1.100	10.1.1.1	RADIUS	Access-Request(1) (id=28, l=196)
30	10.1.1.1	10.1.1.100	RADIUS	Access-Challenge(11) (id=28, l=133)
31	10.1.1.100	10.1.1.1	RADIUS	Access-Request(1) (id=29, l=260)
32	10.1.1.1	10.1.1.100	RADIUS	Access-Challenge(11) (id=29, l=149)
33	10.1.1.100	10.1.1.1	RADIUS	Access-Request(1) (id=30, l=196)
34	10.1.1.1	10.1.1.100	RADIUS	Access-Challenge(11) (id=30, l=101)
35	10.1.1.100	10.1.1.1	RADIUS	Access-Request(1) (id=31, l=196)
36	10.1.1.1	10.1.1.100	RADIUS	Access-Accept(2) (id=31, l=170)
37	CadmusCo_04:f8:6	Broadcast	ARP	Who has 169.254.69.10? Tell 0.0.0.0

Rys. 3. Okno logowania na stacji suplikanta (a), fragment bazy danych użytkowników serwera *Radius* (b), wymiana komunikatów protokołu *Radius* w analizatorze *Wireshark* (c).

W konsoli NAS prezentowanej na rys. 2b przedstawio kluczowe polecenia konfiguracji klienta, które zmierzają do autoryzacji użytkowników, polegającej na udstepnieniu przez NAS interfejsu, do którego podłączona jest stacja sie-

ciowa suplikanta, na której autentykuje się użytkownik. W rozważanym przypadku autentykacja dotyczy konta użytkownika *kowalski*. Użytkownik ten autentykuje się na stacji Suplikant_1_Windows 7, która podłączona jest do interfejsu FastEthernet1/0 klienta NAS. W oknie z rys. 2b widać także poprawną odpowiedź sewera Radius, uzyskaną w wyniku wymuszonego testu autentykacji użytkownika *kowalski* z poziomu NAS. Docelowo autentykacja i autoryzacja jest inicjowana na stacji suplikanta i wymaga podania przez użytkownika konta *kowalski* poprawnych danych w oknie logowania jak na rys. 3a. Dane te muszą odpowiadać definicji tego konta w bazie danych serwera RADIUS (*freeradius* [http://freeradius.org]) – rys. 3b.

Potwierdzeniem poprawności konfiguracji może być wynik prostej analizy wymiany komunikatów pomiędzy klientem a serwerem przeprowadzonej za pomocą oprogramowania Wireshark (rys. 3c). Widać, iż pakiet Access-Accept został uzyskany w wyniku żadania Access-Request, wysłanego wcześniej przez klienta NAS. Ponadto, w ostatnim wierszu konsoli z rys. 2b uchwycony jest komunikat od NAS, który informuje o włączeniu interfejsu nr 0/1 przełącznika, co jest wynikiem zakończonej sukcesem autoryzacji konta *kowalski*.

Wnioski

Prezentowane treści pokazują, iż istnieje możliwość badania zaawansowanych mechanizmów sieciowych na pojedynczym komputerze bez konieczności wykorzystywania fizycznego sprzętu sieciowego. Stosując darmowe oprogramowanie wirtualizacyjne oraz emulacyjne, można dokonać pełnej konfiguracji danej usługi, tak jak to odbywa się w realnej topologii sieciowej. Zatem takie podejście może stanowić niezwykle wygodne i skuteczne narzędzie dla nauczyciela akademickiego podczas wykładów, ale także może być środkiem wzbogacającym zajęcia laboratoryjne dla studentów. Wypracowane w środowisku wirtualizacyjnym konfiguracje mogą być przeniesione i testowane na urządzeniach rzeczywistych.

Literatura

„Computerworld” (2016), czerwiec.

http://freeradius.org.

http://www.gns3.net.

https://www.virtualbox.org.

„Networld Trendy” (2013).