DOI: 10.19279/TVZ.PD.2014-2-2-18

PODEŠAVANJE BEŽIČNE MREŽE UZ AUTORIZACIJU PREKO RADIUS SERVERA

Dario Pintarić[1], Zvonimir Begić[2], Dubravko Žigman[3]

[1]Nacionalna i sveučilišna knjižnica u Zagrebu
[2]Student TVZ-a diplomirao 2014.
[3]Tehničko velučilište u Zagrebu

Sažetak

Razvojem aplikacija podržanih preko eksterne-Internet ili interne mreže, povećalo se korištenje Radiusa-a kao protokola za autentifikaciju. Radius poslužitelj koji koristi AAA (Authentication, Authorization and Accounting) protokol, danas je u širokoj primjeni u informatici. Svoju je primjenu našao u mnogim informatičkim rješenjima zbog potrebe za provjerom identiteta, kontroliranjem „tko i što može raditi na mreži“ i prikupljanjem podataka o korištenju mrežnih resursa. Ograničena dostupnost uslugama i mrežnim tehnologijama i resursima od strane pružatelja takvih usluga, dovela je do potrebe za kontrolom i evidencijom tko do koje usluge može pristupiti i kako će je koristiti. Također „accounting“ svojstva Radius servera-a iskorištavala su se za izračun naplate usluge korištenja Interneta. Radius poslužitelj je bilježio kada se određeni korisnik spoji i odjavi s mreže. Aplikacija koja izračunava tarifu za korištenje te „Internet“ usluge koristi podatke iz log datoteka Radius poslužitelja. [1]

Ključne riječi: *Bežično, Implementacija, Autorizacija, Autentifikacija, Accounting, Radius, Aleph,C#.*

Summary

Application Development supported via external “Internet” or internal networks, increased use of Radius as the authentication protocol. Radius using AAA (Authentication, Authorization and Accounting) protocol, is now widely used in computer science and is one of the most popular AAA protocols. Its application is found in many IT solutions because of the need for verification of identity, controlling the “who and what you can do on the network” and collecting data on the use of network resources. The limited availability of services and network technologies and resources by providers of such services, has led to the need to control and records to anyone who can access the service and how it will be used. Also “accounting” properties Radius server-exploited and are used to calculate billing services using the Internet. Radius server has recorded when a particular user connects to the network and check-out. An application that calculates the rate of use and the “Internet” service uses data from log files Radius server [1]

Key words: *Wireless, Implementation, Authorization, Accounting, Autentification, Radius, Aleph, C #.*

1. Uvod

U svijetu informacijske tehnologije, sigurnosni model je siguran kao njegova najslabija karika. Postoji nekoliko slojeva sigurnosti i različite mjere koje se trenutno mogu provesti. Međutim, bez kontrole i koordinacije, potencijali narušavanja sigurnosti mogli bi ugroziti mrežu. Bežični pristup postaje norma, a korisnici zahtijevaju “komunikaciju u pokretu”. Razvojem aplikacija podržanih preko mreže, bilo eksterne ili interne, povećalo se korištenje Radius-a kao protokola za autentifikaciju. Tako se npr. kod pristupa elektroničkoj pošti putem web sučelja koristio Radius za autentifikaciju.

Također se počeo koristiti i kod nekih drugih aplikacija kao što su baze podataka, VPN i sl. i kao protokol pomoću kojeg se prenosi i neki drugi protokol. Primjer za to je enkapsulacija EAP (EAP-TLS, EAP-TTLS) paketa u Radius paketima. [1] Individualni pristup korisniku, aplikacijska rješenja, Freeradius i Daloradiu funkcionalnost, kontrola, platni mehanizni prednosti su instalacije i implementacije Freeradius poslužitelja.

2. Formulacija problema

Kada su bežične mreže dostupne bez upisivanja lozike ili kada je za sve korisnike lozinka ista, tada je teško ili nemoguće kvalitetno kontrolirati velik promet podataka u nekoj mreži. Također nemamo mogućnost stvaranja grupa korisnika, pregled izvještaja i statistike, naprednih pretraga itd., koju omogućuje instalacija i implementacija Freeradius poslužitelja.

Ukoliko se svakome dodjeli „jedinstvena“ lozinka, tada se u bazu podataka upisuju podaci o korisnicima, a „log“ datoteke na serveru i podaci iz MySql baze podataka omogiti će kontrolu i upravljanje kontrolu svim korisnicima mrežnih ili internih resursa.

Spajanje korisnika na Internet putem Radius servera omogućilo je autorizaciju korisnika na „otvorenu bežičnu mrežu“ bez sigurnosne „zajedničke“ lozinke za sve korisnike. Umjesto toga svakom korisniku bit će dodijeljeno korisničko ime i lozinka upisom podataka o korisniku u knjižnični software Aleph, te sinkronizacijom s Radius poslužiteljem koji će zatim omogućiti spajanje na mrežu. Korisnici će se tako slobodno spajati na AP (pristupnu točku), međutim spajanje na „Internet“ uvjetuje upis podataka u knjižnični (ili neki drugi) software, gdje će svaki korisnik zasebno dobiti svoje podatke za spajanje. Time se svakom korisniku zasebno može omogućiti pristup pojedinim uslugama. Programiranjem „desktop“ ili „web“aplikacija koje mogu povezati npr. MySQL bazu Freeradius poslužitelja i u ovom slučaju Oracle bazu Aleph poslužitelja, moguće je dobiti novu funkcionalnost sustava.

3. Rezultati istraživanja

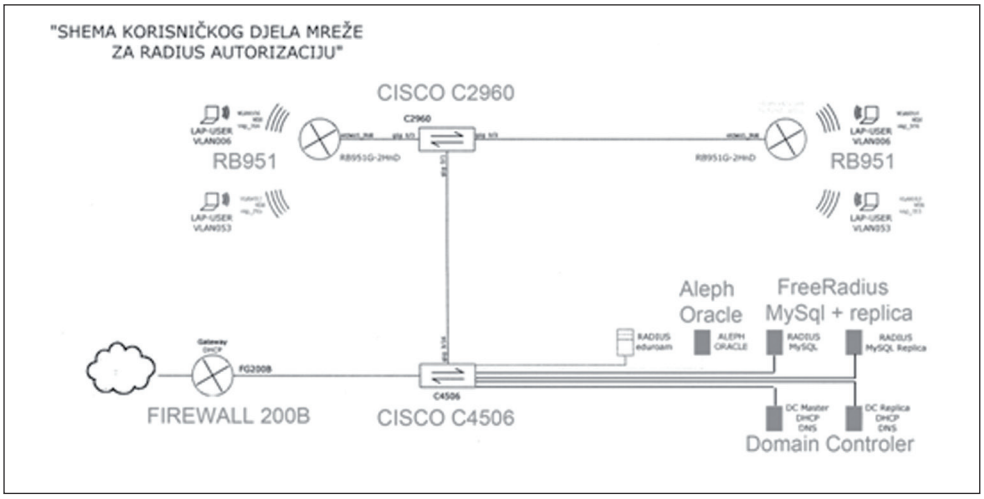
Implementacija nove bežične mreže (VLAN53) uz autorizaciju preko servera Freeradius na izdvojenoj mreži (VLAN 151), omogućila je sinkronizaciju podataka, kontrolu prometa i „log“ datoteka korisnika koji koriste bežični Internet unutar neke ustanove. Povezivanjem Microsoft i Linux distribucija i tehnologija, dobivena je nova funkcionalnost i omogućila nove usluge upravljanja korisnicima, grupama, Radius klijentima, pregled korisničke statistike, pregled accounting izvještaja i mogućnost provjere rada Freeradius poslužitelja. Funkcionalnost i dostupnost Radiusa omogućuje implementaciju i razvoj novih aplikativnih rješenja.

4. Tehnička izvedba

Podešavanje ovakvog sustava može se izvršiti na mnogo različitih načina, postavljajući sustav u samo jednu mrežu (VLAN) ili odvajajući svaki segment u različite mreže (VLAN-ove) što povećava kontrolu i sigurnost. U tomo slučaju kao u ovom primjeru, mreže se moraju oglasiti i podesiti na svim uređajima u mreži što uključuje Firewall Fortigate 200B uređaj, Cisco preklopnike, Freeradius servere, Domain Controler-e, usmjernike itd. Kako sav promet u mrežu prolazi kroz Fortigate firewall, potrebno je kreirati interface koji će povezivati firewall uređaj sa prvim preklopnikom „Cisco 4560“. Novu mrežu s gore navedenim adresama kreirat će se u Firewall 200B kako bi korisničke IP adrese mogle na kraju biti na raspolaganju korisnicima bežične mreže.[28] Podešavanja kao što je otvaranje interface-a vršit će se putem Firewall web sučelja. Ovisno s koje mreže ili VLAN-a se spajamo na Firewall, odgovarajuću adresu Firewalla potrebno je upisati u web preglednik te pristupiti grafičkom sučelju. Korištenjem Firewall -a olakšan je rad u smislu kontrole nad mrežama odnosno VLAN-ovima. [2]

Kako bi ostali uređaji ili hostovi u mreži imali informacije o novom VLAN-u 53 odnosno novoj bežičnoj mreži, ona mora biti „oglašena“ i na preklopniku C4506 (2). IP adresa interface-a za VLAN 53 je prva slobodna adresa 10.53.0.1 255.255.248.0. Preklopnik je postavljen kao VTP server, što znači da će na sve ostale Cisco preklopnike slati informacije o VLAN-ovima, ukoliko su ti ostali preklopnici postavljeni kao „VTP client“.

„Na preklopniku je već ranije podešen interface u „trunk“ port koji će oglašavati VLAN-ove sve do usmjernika Mikrotik. Nakon spajanja uređaja Cisco i RB951 usmjernika, te podešavanja VLAN-ova i Virtualnih pristupnih točaka, na usmjernik je potrebno povezati antenu preko „pigtail“ konektora. Postavljanje usmjernika i antene ovisi o prostoru u koji se planiraju postaviti. Potrebno je paziti na preklapanje signala, ali isto tako omogućiti dovoljno jak signal u cijelom prostoru. [4]



Slika 1. *Nacrt mreže*

Na slici 1. Prikazan je nacrt segmenta mreže u koju je implementirana nova bežična mreža. Sav promet podataka korisnika koji koriste pristupnu točku na RB951 usmjerniku, morat će prolaziti kroz VLAN 53 (VLAN nove bežične mreže) i VLAN 151 (VLAN Freeradius-a i Aleph servera), kako bi uspješno pristupili Internet-u ili uslugama omogućenim preko sustava AAA (Authentication, Authorization and Accounting). Korisnicima spojenim preko tih protokola može se također omogućiti spajanje preko VPN-a, sigurno korištenje e-pošte, sustav naplate i sl. Korištenje „log" datoteka i zapisa iz Freeradius MySql baze omogućuje nam kontrolu spajanja korisnika i prometa koji koriste.

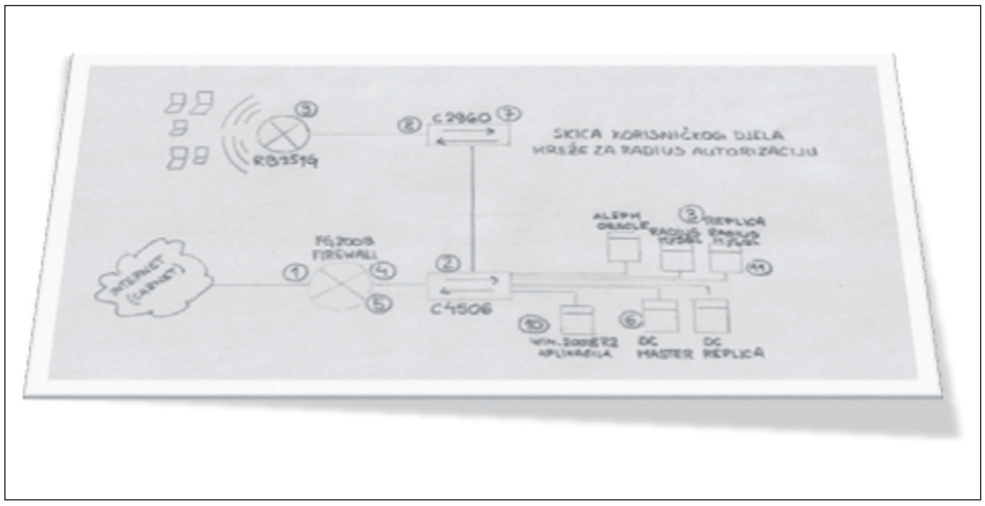
Domain Controler serveri (Microsoft Windows 2008 server) bit će podešeni za DHCP i DNS servis. Aleph software u koji se upisuju podaci o korisnicima će prosljeđivati podatke u Freeradius server. Freeradius serveri vršit će autorizaciju za spajanje na Internet. Unutar mreže servera (VLAN 151) u kojima se nalazi Aleph i Freeradius serveri može se dodati računalo ili server koji će biti „posrednik" između podataka o korisnicima (Ime i prezime, članarina,dugovanja i sl.) koje zaprima Aleph i podataka koje koristi Freeradius server za konačno propuštanje korisnika kroz mrežu do Interneta.

Firewall Fortigate 200B uređaj mora sadržavati pravila kojim se omogućuje promet između svih tih segmenata sve do „Internet"-a koji nam omogućuje „Internet provider" odnosno pružatelj internet usluge (Carnet ili sl.) Usmjernik RB951 s MikroTik OS-om, može se podesiti za distribuciju više VLAN-ova ili bežičnih mreža na koje se korisnici mogu spajati. Kreiranjem Virtualnih pristupnih točaka i upotrebom „bridge" i ostalih tehnologija na usmjerniku osim nove bažične mreže distribuirati će se i Eduroam mreža.[2]

Važno je predvidjeti mogućnosti ovakve implementacije kroz više različitih vrsta software-a i uređaja, koji ne moraju biti isti kao i u ovom primjeru. Aleph knjižnični software može biti zamijenjen nekim drugim software-om u koji će se upisivati podaci o članstvu, Freeradius server može biti zamijenjen Free radius.net, Tek radius, Electron ili nekim drugim „Radius" serverom itd.

Kroz deset aktivnosti omogućit će se autorizacija i sinkronizacija korisnika na Freeradius poslužitelju.

1. Otvaranje novog interfaceVLAN-a 53 na Firewall-u Fortigate B200
2. Oglašavanje VLANA 53 na glavnom preklopniku C4506 (VTP server)
3. Instalacija Freeradius poslužitelja sa replikom
4. Podešavanje postavki za radius servere na Firewallu
5. Podešavanje Firewall pravila za VLAN 53
6. DHCP „scope" na Domaincontroleru i DC repliciranom serveru
7. Postavljanje portova u VLAN 53 na preklopniku C2960
8. Spajanje Access Point-a na preklopnik
9. Podešavanje VLAN portova na MikroTik usmjerniku (AP)
10. Upotreba servera „Windows server 2008 R2" za povezivanje Oracle baze podataka Aleph-a s MySql bazom Radius servera



Slika 2: *skica i aktivnosti*

Koristit će se nekoliko VLAN-ova ili „virtualnih lokalnih mreža“. Potreba za nekoliko VLAN-ova primarno proizlazi iz sigurnosnih razloga. Poželjno je odvojiti djelatničku mrežu od korisničke, te također odvojiti nekoliko mreža za odsjeke unutar djelatničke mreže između ostalog i radi kontrola prometa po VLAN-ovima. Mreža Wireless_nova koja će imati pripadajući VLAN 53 na Firewallu, bit će podešena na rasponu od 2046 IP adrese. [4]

VLAN53 – Bežična mreža Wireless_nova uz autorizaciju

Adresa mreže: 10.53.0.0/21
Prva adresa hosta: 10.53.0.1
Zadnja adresa hosta: 10.53.7.254
Broadcast adresa: 10.53.7.255
Upotrebljivih adresa: 2046

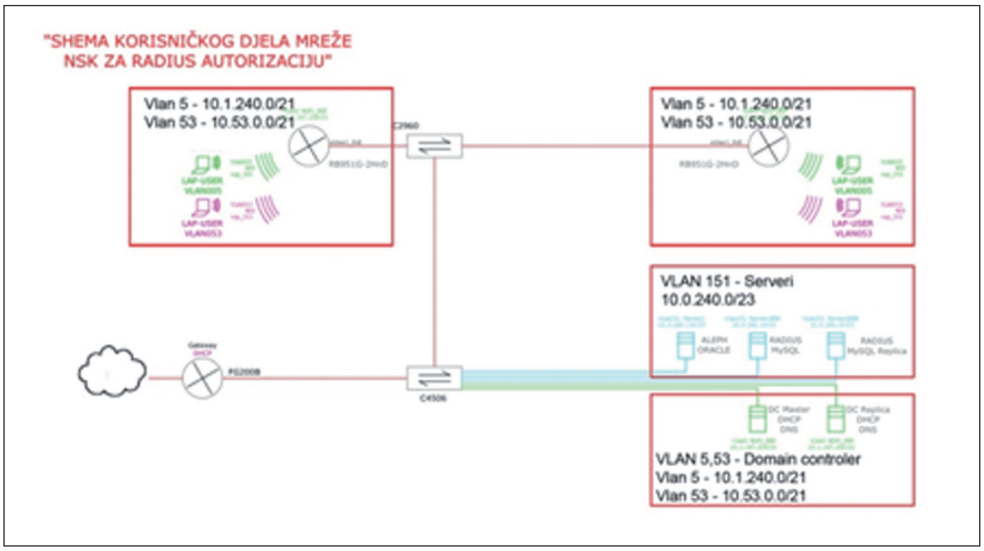
Osim Wireless_nova mreže odnosno VLAN-a 53, podešeni su i VLAN-ovi za mrežu servera (VLAN151), te za korisničku bežičnu mrežu Wireless_lib na kojoj nema autorizacije (VLAN 5).

VLAN 151 – Serveri (radius1, radius2, Aleph,Aplikacija za usporedbu podataka na serveru Microsoft Windows 2008)

Adresa mreže: 10.0.240.0/23
Prva adresa: 10.0.240.1
Zadnja adresa: 10.0.241.254
Broadcast adresa: 10.0.241.255
Upotrebljivih adresa: 510

VLAN 5 – Bežična mreža Wireless_lib bez autorizacije

Adresa mreže: 10.1.240.0/21
Prva adresa: 10.1.240.1
Zadnja adresa: 10.1.247.254
Broadcast adresa: 10.1.247.255
Upotrebljivih adresa: 2046



Slika 2: *Shema „VLAN“-ovi*

Instalacija Freeradius poslužitelja

Osnovu funkcioniranja Freeradius poslužitelja čine njegove konfiguracijske datoteke.

Prilikom procesiranja zahtjeva, poslužitelj uspoređuje parametre zahtjeva sa odgovarajućim podacima iz konfiguracijskih datoteka. [3]

Glavne konfiguracijske datoteke su:

- radiusd.conf – centralna lokacija za konfiguriranje Freeradius servera
- clients.conf – opisuje klijente i sastoji se od zapisa o podacima klijenta

Neke od aktivnosti instalacije Freeradius poslužitelja na Linux Ubuntu distribuciji:

- Podešavanje root password-a
- Instalacija„Joe“ tekst editor
- Podešavanje DNS nameservera /etc/resolv.conf
- DHCP client-a - knjiga.nsk.hr
- Podesiti BOND Interface i IP adresu
- Instalacija Ntp Time servisa
- Podešavanje Local Host /etc/hosts
- Installacija MySQL Server apt-get install mysql-server
- Installacija PhP5 apt-get install php5-gd php-pear php-db
- Instalacija FreeRADIUS i FreeRADIUS-MySQL apt-get install freeradius freeradius-mysql
- Instalacija PhPMyAdmin apt-get install phpmyadmin
- Instalacija Daloradiusa
- Podešavanje MySQL baze podatka

Podešavanje MikroTik usmjernika

a. Upisati System identify
b. Kreiranje bridge interface-a za svaki VLAN
c. Promjena imena za ethernet interface – označavanje portova spojenih na druge uređaje u LAN mreži
d. Kreiranje VLAN-ova za svaki interface
e. Wireless security „Profiles“
f. Podesiti „wireless“ interface – za 2 virtualna AP interface-a
g. Kreirati „virtual access point“ za svaki vlan na koji će se spajati korisnici
h. Upisati VLAN ove u „bridge“ port-ove i otvoriti „bridge“ portove na navedenim interface-ima
i. Upisati IP adrese za management usmjernika
j. Upisati DNS na usmjerniku
k. Upisati „default route! za management usmjernika
l. Postaviti sat
m. Podesiti SNTP client
n. Dodati default usera

Da bi se omogućila funkcionalnost distribucije više VLAN-ova koristit će se „bridge“ opcija, te virtualni „access point“ za svaki VLAN. Time će se dobiti mogućnost odvajanja bežičnih mreža različitim VLAN-ovima, zbog sigurnosnih razloga, te mogućnosti kontrole prometa po mrežama. Na MikroTik RB912 spajanje se izvodi preko Winbox aplikacije koja upisom IP adrese usmjernika daje mogućnost podešavanja i kontrole mreža odnosno VLAN-ova.

Upotreba servera „Windows server 2008 R2“ za povezivanje Oracle baze podataka Aleph-a s MySql bazom Radius servera

Za ovakvo aplikacijsko rješenje nije nužno potreban poslužitelj, već računalo u mreži čija je baza podataka spojena na bazu podataka Freeradius poslužitelja. Korišten je Microsoft Visual basic i C# programski jezik.

PROGRAM KOJI DNEVNO PUNI RADIUS MySQL BAZU

1. Podaci iz tablice Aleph baze za podatke RADIUS MySQL
   - ID-KARTICE_BARCODE
   - PREZIME_IME
   - GODINA_ MJESEC_DATUM_ROĐENJA
   - EXPIRE _DATE
   - E-MAIL
   - OIB
2. Upisati izvađene podatke u RADIUS MYSQL, uz uvjete
   - EXPIRE_DATE < “NOW” (ako je istekla članarina) → Ne upisuje se u RADIUS
   - EXPIRE_DATE > "NOW" (nije istekla članarina) → Provjeri je li ID-KARTICE postoji u RADIUS BAZI
   - ID-KARTICE_BARCODE = DA POSTOJI → Ne upisuj u RADIUS
   - ID-KATRICE_BARCODE = NE POSTOJI → Generira se PASSWORD = OIB ***

- OIB = "NULL" (ako nema podatak o OIB-u) → generiraj password od 6 znakova

3. Brisati podatke u RADIUS MySQL
   - EXPIRE_DATE < "NOW" (ako je istekla članarina)
   - PREZIME, IME + GODINA, MJESEC, DATUM ROĐENJA à Viae odijeljenih ID-KARICE_BARCODE (ako je istom korisniku dodijeljeno više ID-KARTICA (novo izdana, zagubljena, oštećena kartica), izbrisati sve osim najveći ID-KARTICE_ BARCODE koji ima korisnik (zadnja kartica)

Aplikacija je razvijena u C# programskom jeziku. Vrši provjeru podataka u Alephu, te ih uspoređuje s podacima u MySql bazi podataka. Podaci koji se obrađuju su sljedeći: Ime i prezime, OIB, datum prestanka valjanosti kartice i ID kartice. Aplikacija se pokreće sekvencijalno tri puta dnevno ne windows serveru 2008 R2. Prilikom provjere podataka u Alephu kontrolira sevrijeme isteka članske iskaznice, te ukoliko su podaci ispravni, upisuju se u MySql Radius bazu. Aplikacija ili servis za takvu usporedbu podataka može se kreirati i u nekom drugom programskom jeziku.

5. Zaključak

Širok spektar mogućnosti Freeradius poslužitelja i Daloradius-a pružaju sigurnost i kvalitetu, kako na lokalnim tako i na bežičnim mrežama. Kontrolom prometa, odnosno upotrebom Daloradius, Adminradius ili nekih drugih aplikacija za upravljanje Freeradius poslužiteljem, povećat će se kvaliteta mreže i razina sigurnosti, te će biti omogućene nove funkcionalnosti mrežne i serverske infrastrukture.

Podešavanjem FirewallFortigate-a (kreiranje radius grupe, kreiranje pravila za komunikaciju između VLAN-ova i uređaja), oglašavanjem VLAN-ova na preklopnicima, postavljanjem MikroTik usmjernika i instalacijom Freeradius poslužitelja, dobivena je funkcionalnost nekoliko povezanih uređaja i operativnih sustava, te je time i povećana uspješnost poslovanja.

Nakon implementacije nove bežične mreže uz autorizaciju preko Radius poslužitelja budući ciljevi su proširenje mreže, omogućavanje naplate i iskoristivosti novih usluga kao npr. elektronske pošte, mogućnosti rezervacije najma prostora,kontrolirani pristup resursima i poslužiteljima, mogućnost korištenja nekog uređaja ili aplikacije.

6. Reference

[1] M.Šikić, M.Stanke, Comparisonofthe RADIUS andDiameterProtocols Proceedingof ITI 2008 pp893-989, 23.06.2008

[2] Engst, Adam C.,GlennFleishman, Bežično umrežavanje(praktični priručnik za Wi-Fi umrežavanje), 2004

[3] Adelstein Tom, Lubanovic Bill, Administriranje Linux sustava, 2007

[4] Kunštek, Zlatko.,Računalne mreže II, 2011

AUTORI

Mr. sc. Dubravko Žigman- nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 2, No. 1, 2014.