Eduroam- servis u istraživačkim i edukacionim mrežama

Vladimir Gazivoda dipl.ing.[1] , prof. dr Božo Krstajić[2]

***Sadržaj* — EDUROAM je konfederacija Nacionalnih Roaming Operatora koja omogućava korisnicima članica eduroama pristup mrežnim resursima bilo gdje u konfederaciji. Primarni cilj projekta je da se olakša rad internacionalnom društvu edukacije i istraživanja prilikom rada u drugim institucijama. Projekat je zasnovan na Radius proxy hijerarhijskoj infrastrukturi i 802.1x standardu. Osim u Evropi, eduroam je takođe uspostavljen i u Azijsko-Pacifičkom dijelu, tako da možemo reći da se radi o svojevrsnom globalnom servisu.**

***Ključne reči* — 802.1X, AAA, hijerarhijska infrastruktura, NREN, NRO, Radius.**

I. UVOD

OVAJ rad opisuje princip funkcionisanja Eduroama, kao i osvrt na tehnologiju na kojoj je zasnovan.

Eduroam, naziv sastavljen od riječi EDUcation ROAMing [1][8], omogućava korisnicima članica eduroam zajednice zaštićen Internet pristup u instituciji članici eduroam zajednice u kojoj se trenutno nalaze. Sam princip eduroam-a je sličan roaming-u u mobilnoj telefoniji, gdje se koriste resursi institucije u kojoj se korisnik trenutno nalazi, dok se autentifikacija vrši na serverima u instituciji iz koje korisnik potiče. Ukratko, suštinu eduroama najbolje opisuje njen slogan „otvorite laptop i budite online“. Naravno, ovo uveliko zavisi od broja i rasprostranjenosti hotspot-ova koje članice postave.

Međutim, da bi ovo bilo moguće neophodna je velika usklađenost i koordinacija između institucija. Za razliku od mobilnog rominga koji je takođe zasnovan na korištenju infrastrukture druge mreže, kod eduroama ne postoji komercijalni benefit korištenja ove usluge. Samim tim je i teže stvoriti zavidnu zajednicu koje će biti u potpunosti u duhu slogana eduroama. Jedino “ljepilo“ koje veže organizacije je stvaranje globalne eduroam zajednice za benefit članova akademskih institucija širom Evrope.

Evropska eduroam zajednica pruža legalni okvir za organizacije koje su članice eduroam zajednice. Samo korištenje eduroama je ograničeno na zatvoreno društvo koje čine Nacionalne mreže za istraživanje i edukaciju (NREN – National Research and Education Network). Članovi Evropske eduroam zajednice su organizacije odgovorne za operaciju nacionalnog roaming servisa. Ove organizacije (NRO – National Roaming Operator) su u najvećem broju slučajeva i sami NREN-ovi. Ako NRO nije i NREN, onda taj NRO mora imati precizno definisan odnos sa NREN u ovom slučaju[1][2].

Ovaj rad je podijeljen u dva dijela. Prvi dio opisuje tehnologije koje su primjenjene u realizaciji eduroam servisa. U drugom dijelu je pažnja posvećenja opisivanju eduroam servisa i njegovo funkcionisanje.

II. TEHNOLOGIJE PRIMJENJENE U EDUROAMU

Eduroam koristi sljedeće komponente kako bi realizovala svoj servis:

- Network Access Server (NAS) – svič ili wireless access point koji pruža klijentima pristup lokalnoj mreži.
- Klijent/Supplicant – klijentski uređaj koji omogućava korisničku autentifikaciju na mreži. Suplicant je softver koji je interisan unutar OS-a ili zasebna aplikacija.
- Autentifikacioni server (AS) – za autentifikaciju i autorizaciju klijenata i dinamičku konfiguraciju servera za pristup mreži. AS posjeduje korisničku bazu koja sadrži korisničke kredencijale koji se koriste za autentifikaciju klijenata. Termin „Autentifikacioni Server“ je generički termin. Nekoliko protokola se može koristiti da prenose korisničke kredencijale. Najpoznatiji su TACACS+, Radius i Diameter. Radius serveri imaju do sada najveću primjenu i veliki broj dostupnih implementacija.
- IEEE 802.1X – Standard za kontrolu pristupa mreži baziranoj na portovima.
- IEEE 802.1Q – Standard za VLAN dodjeljivanje

A. IEEE 802.1X

IEEE 802.1X je standard za kontrolu pristupa mreži preko portova. Mrežni uređaj koji podržava 802.1X može kontrolisati svoje portove tako da je klijentima dozvoljeno da komuniciraju samo preko njih ukoliko se poklapaju kriterijumi autentifikacije i autorizacije. Takvi mrežni uređaji mogu biti svičevi ili wireless Access Point-i.
Tri komponente uključene u IEEE 802.1X autentifikacionom procesu su:

1. Supplicant je klijentski softver koji šalje zahtjev kroz port.
2. Autentifikator je mrežni uređaj, tj. NAS

[1] Vladimir Gazivoda, Centar Informacionog Sistema Univerziteta Crne Gore, Crna Gora (telefon: +382 20 414 290; fax: +382 20 414 283; e-mail: vladg@ac.me)

[2] Prof. dr Božo Krstajić, Elektrotehnički fakultet Univerziteta Crne Gore, Crna Gora (telefon: +382 20 414 284; fax: +382 20 414 283; e-mail:bozok@ac.me)

3. Autentifikacioni Server (AS), u većini slučajeva RADIUS server.

Korisnička autentifikacija putem 802.1X zahtjeva korištenje Extensible Authentication Protocol (EAP, [RFC3748]). EAP transportuje autentifikacione podatke preko LAN-a (EAPoL) i takođe u okviru RADIUS protokola ([RFC2869]). Autentifikator je nadležan samo za status i VLAN pripadanje portova, kao i da li je ili nije supplicant povezan[7].

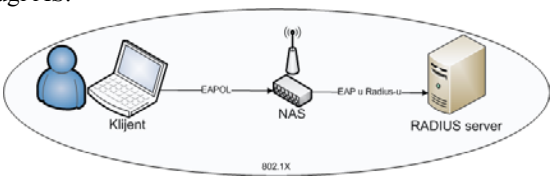
Drugi aspekt 802.1X koji ga čini svestranim je veliki broj različitih autentifikacionih metoda koji se mogu koristiti u okviru EAP-a. Neki od primjera su EAP-MD5, EAP sa One-Time Password (EAP-OTP), Generic Token Card (EAP-GTC) i EAP-SIM[5]. Kako bi se što bolje zaštitila komunikacija, posebno u bežičnim mrežama, koriste se metode koje omogućavaju uzajamnu autentifikaciju, pri čemu korištenje pomenutih metoda nije obligatorno. Važno je za supplicanta da zna da može imati povjerenje u autentifikacioni server prije nego što otvori osjetljive informacije kao što su korisničko ime i lozinka. Primjeri pogodnih autentifikacionih metoda su EAP-TLS (certificate/certificate), EAP-TTLS(certificate/user name + password) and EAP-PEAP (certificate/user name + encrypted password). U svakom od ovih metoda RADIUS server prvo šalje svoje sertifikate, koji sadrže javni ključ, klijentu. Klijent može da provjeri ovaj sertifikat na osnovu instalirane kopije Certificate Authority (CA) javnog ključa i moguće instalirane Certificate Revocation Liste (CRL) prije nego što se autentifikacioni proces nastavi.

Važno je napomenuti da enkripcija autentifikacionog procesa ne znači i enkripciju podataka od/ka strane klijenta nakon uspješne autentifikacije. Odvojena enkripcijska šema je neophodna kako bi zadovoljile ovu osobinu. Ipak, 802.1X zajedno sa odgovarajućom autentifikacionom metodom može biti korišten da se distribuiraju enkripcioni ključevi koje klijenti mogu koristiti za svoj saobraćaj. Za bežične mreže, metodi enkripcije su WEP (40 ili 104 bita) sa rotacionim ključevima, TKIP ili AES. Korištenje 802.1X autentifikacije sa AES enkripcijom je poznato pod nazivom WPA2, koji je široko ekvivalentan sa IEEE 802.11i standardom.

B. *RADIUS serveri*

RADIUS je akronim za "Remote Authentication Dial In User Service" i definisan je IETF RFC 2865 i RFC 2866. Radius je protokol između NAS-a i AS-a. On prenosi autentifikacione, autorizacione, konfiguracione i obračunske poruke[5].

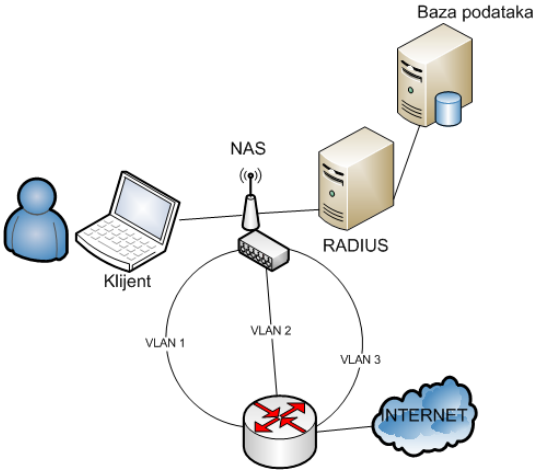
IEEE 802.1X protokol koji se koristi je Extensible Authentication Protocol (EAP preko LAN-a između klijenta i NAS-a). NAS enkapsulira EAP sadržaj i transportuje autenifikacione poruke do RADIUS servera. RADIUS server vrši autentifikaciju i ili prihvata ili odbija zahtjev(slika 1). NAS takokođe reaguje sa odbijanjem ili prihvatanjem klijenta za pristup mreži. Odgovor od AS-a može takođe sadržati konfiguracione elemente koje utiču na to kako će klijent koristiti servis. Nekoliko NAS uređaja se može povezati kao klijent na AS. AS takođe sarađuje sa ostalim AS-ovima kroz backbone autentifikacionu mreži gdje jedan AS služi kao proxy za drugi AS.



Sl. 1. Radius server

AS može podržati veliki broj autentifikacionih metoda, zaviseći od implementacije. Unix login, tekstualni fajlovi, SQL baza podataka, Certification Authority i LDAP baza su neke od primjera izvora kredencijala koje AS može koristiti kako bi verifikovao korisnički identitet. Takođe je moguće da se koriste neke metode u kombinaciji sa ostalim kriterijumima kao što su prefiks i sufiks korisničkom imenu, identitet zahtjeva NAS-a, itd.

U slučaju uspješne autentifikacije, lokalni RADIUS server šalje konfiguracione opcije do NAS-a kako bi kontrolisao kojem VLAN-u je klijent dodijeljen. Različiti VLAN-ovi mogu imati različita prava pristupa i mogu biti povezani na različite djelove kampusa(slika 2).



Sl. 2. Struktura lokalne mreže i VLAN podjela

C. *Mrežna infrastruktura i klijentski softver za pristup eduroam servisu*

Eduroam ne uslovljava hardverske karakteristike neophodne za pristup mreži. Korisnici eduroama mogu pristupiti eduroam servisu bilo preko bežične (koju eduroam preferira) ili žičane konekcije. Međutim, zbog specifične konfiguracije, korisnici moraju imati određeni softver kojim se šalju zahtjevi za pristup eduroam mreži. Naime, po propoziciji eduroama, Access pointi ili svičevi moraju podržavati IEEE 802.1X standard koji obuhvata korištenje EAP protokola (Extensible Authentication Protocol)[3]-[5]. Korištenjem odgovarajuće EAP metode, vrši se ili uspostavljanje obezbijeđenog tunela od klijentskog računara do servera matične institucije kojim se vrši razmjena autentifikacionih informacija (EAP-TTLS ili PEAP), ili međusobna autentifikacija putem javnih X.509 sertifikata (EAP-TLS). Tri prethodno pomenuta autentifikaciona metoda uspostavljaju sigurni TLS tunel od klijentskog računara do servera matične institucije i ne mogu biti prisluškivana na svom putu. Takođe, poželjno je da mrežni uređaji mogu klijenta dodijeliti određenom

VLAN na osnovu informacija koje su dobili od Radius servera.

Softver koji koristi 802.1X da bi slali zahtjev za pristup eduroam mreži putem EAP-a je obično ugrađen u Operativni Sistem, kao što je slučaj kod Windows XP operativnog sistema, a može biti i odvojena aplikacija kao što je SecureW2. Korisnici moraju da podese pomenuti softver na osnovu eduroam podešavanja. Ovako podešen softver se može koristiti bilo gdje u okviru eduroam zajednice.

EAP-TTLS se smatra kao najlaši način da se eduroam implementira u velikim institucijama, međutim Microsoft Windows nema ugrađenu podršku za EAP-TTLS. Tako da je u ovom slučaju neophodno korištenje dodatnog softvera koji podržava EAP-TTLS.

III. REALIZACIJA EDUROAM SERVISA

A. Hijerarhija eduroama

Evropski eduroam servis je konfederacijski servis kreiran hijerarhijski na distribuiranom sistemu AAA servera. Na vrhu se nalazi servis konfederacijskog nivoa, tj top level servis. Njegova primarna namjena je pružanje neophodne infrastrukture kako bi se dozvolio mrežni pristup svim članicama u svakom trenutku. Ovaj konfederacijski servis je iznad nacionalnih roming servisa, za koje su nadležni nacionalni roming operatori. Nacionalni roming operatori su nadležni za eduroam servis na nacionalnom nivou. U zavisnosti od slučaja, ispod nacionalnih roming operatora mogu biti ostale organizacije akademskog tipa, kao što su Univerziteti, naučne akademije i slično[2]-[5].

Trenutna implementacija koristi RADIUS kao AAA protokol, i implementiran je kao hijerahijski sistem RADIUS servera kako bi se prenosili autentifikacioni zahtjevi korisnika iz druge institucije do nativne institucije, kao i vraćanje odgovarajućeg odgovora nazad.

1) Radius serveri konfederacijskog nivoa (Top Level Radius Server - TLRS)

Top level radius serveri služe kako bi usmjeravale AAA zahtjeve ka odgovarajućim institucionalnim ili federacijskim RADIUS serverima. Trenutno za Evropsku konfederaciju postoji par top levele radius servera, i svaki od njih je nadležan za određenu grupu federacijskih servera. Ukoliko nekom od njih dodje zahtjev za federacijski server za koji nijesu nadležni, taj TLRS će proslijediti zahtjev TLRS-u koji je nadležan za pomenuti federacijski server.

Osim Evropske eduroam konfederacije, postoje eduroam učesnici i u ostalim djelovima svijeta. Ovi učesnici su takođe povezani sa Evropskom eduroam konfederacijom, ali njihovi NREN-ovi nijesu i članovi Evropske konfederacije[2][6].

2) Radius serveri federacijskog nivoa (Federation level Radius Servers - FLRS)

Federacijski RADIUS server sadrži listu povezanih institucionalnih servera i odgovarajućih domena. Oni primaju zahtjeve od konfederacijskih servera i institucija povezanih na njih, i prosleđuje ih odgovarajućoj instituciji. Ovdje moramo da napomenemo da federacijski RADIUS server može takođe služiti i kao institucionalni RADIUS server.

3) Nativni i udaljeni institucionalni radius serveri (Home and Remote Institutional Radius)

Institucionalni RADIUS serveri su nadležni za autentifikaciju sopstvenih korisnika, bilo da su u nativnoj mreži ili u udaljenoj. Osim ove uloge, ovi serveri prosleđuju zahtjeve korisnika koji su u posjeti do federacijskog servera.

Za razliku od prethodna dva tipa RADIUS servera (konfederacijski i federacijski) koji su u suštini proxy serveri koji prosleđuju zahtjeve, institucionalni serveri su mnogo kompleksniji. Ovi serveri, osim što su i sami u jednom dijelu proxy serveri, takođe obrađuju zahtjeve, i samim tim kompletiraju EAP zahtjeve i vrše pretragu sistema za korisničke kredencijale.

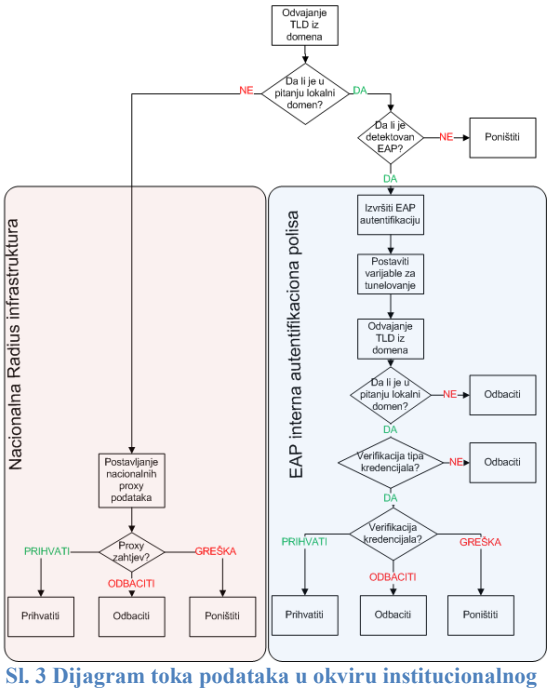
B. Funkcionisanje eduroama

RADIUS serveri formiraju osnovnu strukturu eduroam infrastrukture. Posebno važnu ulogu imaju kada se koriste kao proxy serveri za autentifikacione zahtjeve. Svaki NREN koji participira u eduroamu ima jedan RADIUS server federacijskog nivoa sa makar još jednim RADIUS serverom federacijskog nivoa postavljenim na drugu lokaciju radi redundanse. Ovi serveri federacijskog nivoa imaju kompletnu listu podređenih eduroam institucija u toj federaciji, od kojih je svaka odgovorna za autentifikaciju svojih korisnika. Svaki radius server insitucionalnog nivoa treba samo da ima informaciju o svom radius serveru federacijskog nivoa. Radius server federacijskog nivoa je takođe konfigurisan i kao Radius proxy klijent za Evropske eduroam Radius servere konfederacijskog nivoa.

Obzirom da Radius serveri takođe funkcionišu kao proxy serveri za ostale servere, oni omogućavaju gostujućem korisniku da se autentifikuje za pristup mreži sa kredencijalima koje koristi u svojoj matičnoj instituciji. Ovo je moguće jer lokalni radius serveri jednostavno prosleđuju autentifikacione poruke do korisnikove matične institucije bez potrebe za daljom analizom zahtjeva. Sve što je relevantno jeste da lokalni NAS prihvati ili odbije korisnički zahtjev za pristup na osnovu ishoda autentifikacionog zahtjeva matičnoj instituciji.

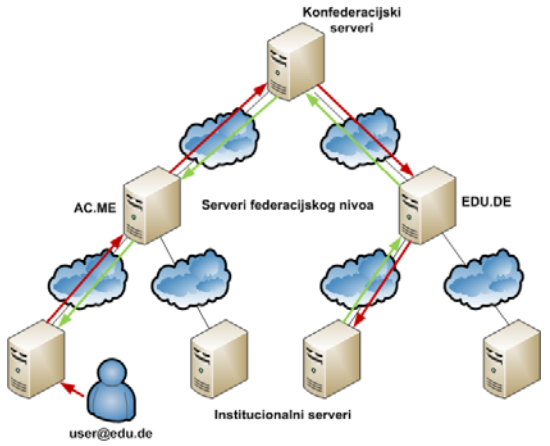
U poglavlju gdje smo opisivali tehnologiju koja stoji iza eduroam servisa, pomenuli smo da AS može koristiti različite autientifikacione metode u kombinaciji sa ostalim kriterijumima. Upravo je ova mogućnost iskorištena kako bi se na fleksibilan način obezbjedilo identifikacija matične institucije korisnika i adekvatno prosleđivanje. Kada korisnik uputi zahtjev za autentifikaciju, korisnički domen odlučuje gdje će se zahtjev poslati. Domen je sufiks korisničkog imena, odvojen znakom „@“ i izveden iz institucionalnog DNS domenskog prefiksa[4].

Kada korisnik pošalje zahtjev za autentifikaciju, prvi institucionalni server vrši razdvajanje korisničkog domena iz korisničkog imena, i vrši algoritamsku provjeru domena kao što je prikazano na slici 3.



Sl. 3 Dijagram toka podataka u okviru institucionalnog Radius servera

Ukoliko je u pitanju lokalni domen, sledeći korak je ispitivanje EAP-a, a zatim i korisničkih kredencijala. Ukoliko je korisnički domen iz iste federacije, federacijski radius server prosleđuje zahtjev do nadležnog institucionalnog servera, koji će nastaviti algoritamsku provjeru kredencijala. Ukoliko je domen iz različite federacije, federacijski radius server će proslijediti zahtjev na konfederacijski nivo, a zatim će se zahtjev proslijediti do nadležnog insitucionalnog servera u matičnoj federaciji korisnika, kao što je prikazano na slici 4. Nakon obrade kredencijala, radius server će NAS-u vratiti informaciju o validnosti korisničkih kredencijala, uz moguće konfiguracione opcije[2]-[5].



Sl. 4. Prosleđivanje zahtjeva ka matičnoj instituciji

Međutim, mora se uzeti u obzir da postoje značajne razlike između organizacija u okviru eduroam konfederacije koje se tiču autentifikacionih i enkripcionih šema koje su izabrali za svoje mreže. Konfiguracija zavisi od lokalne sklonosti, kompatabilnosti klijenata i hardverskim/softverskim limitima u access point-ima i/ili u RADIUS serverima. Ipak, uzimajući da je IEEE 802.1X sistem svuda, lokalni metod autentifikacije je nevažan za klijente posjetioce[5][7]. Klijentski autorizacioni proces je proslijeđen od strane RADIUS proxy servera do klijentske nativne organizacije i procesuiran kao da je klijent u nativnoj organizaciji. Moguće je da klijent mora adaptirati enkripcionu šemu na osnovu lokalne konfiguracije. Većina organizacija posjeduje access point-e koji podržavaju više enkripcionih metoda; što bi značila da postoji velika mogućnost da klijent koristi nativnu enkripcionu metodu. U drugom slučaju, on mora da izabere metodu koja je implementirana u datoj instituciji.

LITERATURA

[1] www.eduroam.org

[2] Miroslav Milinović (CARNet/Srce), Juergen Rauschenbach (DFN), Stefan Winter (RESTENA), Licia Florio (TERENA), David Simonsen (UNI-C), Josh Howlett (UKERNA), SA5 and JRA5 group, *GN2-07-327v2-DS5_1_1-_eduroam_Service_Definition*, 2008

[3] S. Winter (RESTENA), T. Kersting (DFN), P. Dekkers (SURFnet), L. Guido (FCCN), S. Papageorgiou (NTUA/GRNET), Janos Mohacsi (NIIF/HUNGARNET), R. Papez (ARNES), M. Milinovic (CARNet/Srce), D. Penezic (CARNet/Srce), J. Rauschenbach (DFN), J. Tomasek (CESNET), K. Wierenga (SURFnet), T. Wolniewicz (Nicolaus Copernicus University, Torun), José-Manuel Macias-Luna (RedIRIS), I. Thomson (DANTE), JRA5 group, *GN2-08-230-DJ5.1.5.3-eduroamCookbook*, 2008

[4] K. Wierenga (SURFnet, main editor), S. Winter (RESTENA, main editor), R. Arends (Telematica Instituut), R. Castro (RedIRIS), P. Dekkers (SURFnet), H. Eertink (Telematica Instituut), L. Guido (FCCN), J. Leira (UNINETT), M. Linden (CSC), M. Milinovic (SRCE), R. Papez (ARNES), A. Peddemors (Telematica Instituut), R. Poortinga (Telematica Instituut), J. Rauschenbach (DFN) , D. Simonsen (UNI-C), M. Sova (CESNET), Manuela Stanica (DFN), and with contributions from other GN2 JRA5 group members: *Deliverable DJ5.1.4:Inter-NREN Roaming Architecture:Description and Development Items,*2006

[5] Erik Dobbelsteijn, Klaas Wierenga (SURFnet bv), Paul Dekkers (SURFnet bv), Henny Bekker (SURFnet bv), James Sankar (UKERNA), Tim Chown (University of Southampton), Sami Keski-Kasari Tampere (University of Technology, Finland):*Mobility Task Force Deliverable D Inventory of 802.1X-based solutions for inter-NRENs roaming*, 2003

[6] http://www.aarnet.edu.au/services/eduroam.aspx

[7] http://www.terena.org/activities/tf-mobility/deliverables/delanddoc.html

[8] http://en.wikipedia.org/wiki/Eduroam

ABSTRACT

EDUROAM is confederation of National Roaming Operators that enables users of eduroam member institutions access to network resources anywere in confederation. Primary goal of this project is to help international society of research and education during visiting other institutions. Project is established upon Radius proxy hierarchy infrastructure and 802.1X standard. Beside Europe, eduroam is present also in Asia-Pacific region, so we can say that eduroam is a sort of global service.

EDUROAM- SERVICE IN RESARCH AND EDUCATION NETWORKS

Vladimir Gazivoda dipl.ing. , prof. dr Božo Krstajić