CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosni elementi RADIUS protokola

NCERT-PUBDOC-2010-07-306

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument je vlasništvo Nacionalnog CERT-a. Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u izvornom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet–a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. Uvod

RADIUS (eng. *Remote Authentication Dial In User Service*) je mrežni protokol koji omogućava centralizirano upravljanje autentikacijom, autorizacijom i administracijom korisnika (eng. AAA – *Authentication, Authorization, Accounting*) prilikom spajanja računala na mrežu i korištenja mrežnih usluga. Pojavio se 1991. godine kao protokol za autentikaciju i administraciju korisnika na mrežnim pristupnim uređajima. Zbog široko dostupne podrške i sveprisutnosti RADIUS protokola, često ga koriste pružatelji Internet usluge kao i mnoge organizacije za upravljanje pristupom Internetu ili privatnim i bežičnim mrežama te integriranim *e-mail* uslugama. Te mreže mogu sadržavati modeme, DSL-ove, pristupne točke (eng. *access points*), virtualne privatne mreže (VPN) i sl.

RADIUS je protokol koji radi na principu komunikacije klijent-poslužitelj, spada u skupinu protokola aplikacijskog sloja i koristi UDP (eng. *User Datagram Protocol*) transportni protokol. Poslužitelji za udaljeni pristup (eng. *Remote Access Server*), poslužitelji virtualne privatne mreže (eng. *Virtual Private Network server*), mrežni preklopnici (eng. *Network switch*) i mrežni pristupni poslužitelji (eng. *Network Access Server*) su sučelja koja nadziru pristup mreži i imaju komponentu RADIUS klijenta koja komunicira s RADIUS poslužiteljem. RADIUS poslužitelj se obično izvršava kao pozadinski proces na računalu s UNIX/Linux ili Windows operacijskim sustavom. Poslužitelj ima tri funkcije:

- autenticirati korisnike ili uređaje prije odobravanja pristupa mreži,
- autorizirati korisnike ili uređaje za određene mrežne usluge i
- pratiti aktivnosti korisnika tih usluga.

U ovom dokumentu će se prikazati na koji način RADIUS protokol obavlja pobrojane funkcije kroz detaljnu analizu samog protokola, navesti će se poznati problemi vezani uz njegovo korištenje te mogući alternativni protokoli za korisnike kojima RADIUS ne ispunjava sve zahtjeve.

2. Povijest i razvoj RADIUS protokola

Merit Network Inc. je neprofitna organizacija osnovana 1966. godine sa svrhom povezivanja računala na 3 sveučilišta u Michiganu, čime je odigrala veliku ulogu u oblikovanju današnjeg Interneta. Merit je razvio vlastitu mrežu, korištenjem uglavnom ARPAnet protokola. Ona se isprva koristila samo za povezivanje centralnih računala na sveučilištima University of Michigan, Michigan State University i Wayne State University. No, razvojem sustava do 1990. godine ova mreža je povezivala većinu učilišta i sveučilišta u Michiganu i podržavala distribuirani *dial-in*[1] pristup. Na taj način se, primjerice, student koji polazi Michigan State University mogao prijaviti na sustav svog sveučilišta s računala koje je u mreži sveučilišta University of Michigan.

1991. godine Merit Network je objavio natječaj za dobavljača *dial-in* poslužitelja. Potreba za distribuiranim *dial-in* uslugama je bila veliki izazov većini mladih poduzeća koja su se javila na natječaj. U to vrijeme je samo jedan od dobavljača (Xylogic) koji se javio mogao ponuditi autentikacijski protokol na daljinu. Nekoliko mjeseci nakon objavljivanja natječaja, javila se organizacija Livingston i opisala mogućnosti svog RADIUS poslužitelja. RADIUS je odgovarao traženim zahtjevima i prihvaćen je. Nakon što su ga kupili i implementirali, Merit Network ga je doradio kako bi imao dodatne mogućnosti kao što su *proxy* za distribuiranu autentikaciju i podrška za specifične *dial-in* usluge koje je pružala mreža u Michiganu. Unutar godine dana od nabavljanja, razvijen je sasvim drugačiji RADIUS – Merit RADIUS poslužitelj. On i njegovi nasljednici (Interlink Networkova RAD-serija RADIUS poslužitelja) se danas koriste u stotinama tisuća mreža diljem svijeta, osiguravajući i bežične i mobilne, a ne više samo *dial-in* mreže.

U jesen 1992. godine je IETF (Internet Engineering Task Force) osnovao radnu grupu NASREQ (Network Access Server Requirement). 1994. godine, organizacija Livingston je predala skicu RADIUS protokola NASREQ-u i ponudila da kôd RADIUS poslužitelja bude otvoren i dostupan svima. Na taj način je RADIUS-ov kôd postao osnova mnogim sličnim implementacijama na poslužiteljima.

Puno se raspravljalo o tome da li bi RADIUS uopće trebao biti standard, pogotovo zbog njegove upitne sigurnosti. No, unatoč svim službenim raspravama, nakon što je RADIUS-ov kôd izašao u javnost, gotovo svi NAS (*Network Access Server*) dobavljači su ga počeli primjenjivati na svojim proizvodima. Neslužbeno se podrazumijevalo da svaki NAS na tržištu podržava RADIUS, pa je on postao *defacto* standard.

S vremenom je pritisak korisnika i prodavača postao toliko jak da je krajem 1995. IETF osnovao radnu grupu za RADIUS, čiji je rad bio ograničen na dokumentiranje i „pročišćavanje" postojeće skice RADIUS protokola, bez ikakvih dodataka i promjena u protokolu.

Prvotni RADIUS RFC dokument (2058) je izdan početkom 1997. godine. Trenutni standard, RADIUS RFC (2865), je izdan sredinom 2000. godine. Kao dodatak standardnom RFC-u, napravljena su i dva informativna (nestandardna) RFC dokumenta. RADIUS *accounting* RFC (2866) pokriva mogućnosti praćenja aktivnosti korisnika (eng. *accounting*), dok RADIUS *Extensions* RFC (2869) pokriva dodatne mogućnosti i nadogradnje na službeni standard.

1997. godine, IETF je prihvatio RADIUS kao standard. Od tada i službeni i neslužbeni RADIUS RFC dokumenti predstavljaju standard svima koji implementiraju RADIUS protokol u svoju opremu.

Kompletna kronologija razvoja RADIUS protokola dana je u tablici 1.

[1] *Dial-in* pristup se odnosi na pristup postojećoj mreži putem udaljene telefonske-modem veze

Broj dokumenta	Naslov dokumenta	Datum izdavanja	Zamijenjen dokumentom
RFC 2058	*Remote Authentication Dial In User Service (RADIUS)*	siječanj 1997.	RFC 2138
RFC 2059	*RADIUS Accounting*	siječanj 1997.	RFC 2139
RFC 2138	*Remote Authentication Dial In User Service (RADIUS)*	travanj 1997.	RFC 2865
RFC 2139	*RADIUS Accounting*	travanj 1997.	RFC 2866
RFC 2548	*Microsoft Vendor-specific RADIUS Attributes*	ožujak 1999.	
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*	lipanj 2000.	Nadopunjavaju ga RFC 2868, 3575 i 5080
RFC 2866	*RADIUS Accounting*	lipanj 2000.	Nadopunjava ga RFC 2867
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*	lipanj 2000.	Nadopunjava RFC 2866

Tablica 1. Kronografski redoslijed izdavanja RFC dokumenata o RADIUS protokolu

3. Analiza protokola

RADIUS je protokol koji koristi arhitekturu klijent-poslužitelj. RADIUS klijent je obično poslužitelj pristupa mreži ili NAS (eng. *Network Access Server*), a RADIUS poslužitelj pozadinski (eng. *daemon*) program koji se izvršava na računalu s UNIX/Linux ili Windows operacijskim sustavom. Prilikom prijave u mrežu, korisnik šalje svoje podatke RADIUS klijentu koji potom izmjenjuje RADIUS poruke specifičnog formata s RADIUS poslužiteljem. Svrha tih poruka je ostvarivanje tri funkcije „AAA" koncepta: autentikacije, autorizacije i administracije korisnika (eng. *accounting*).

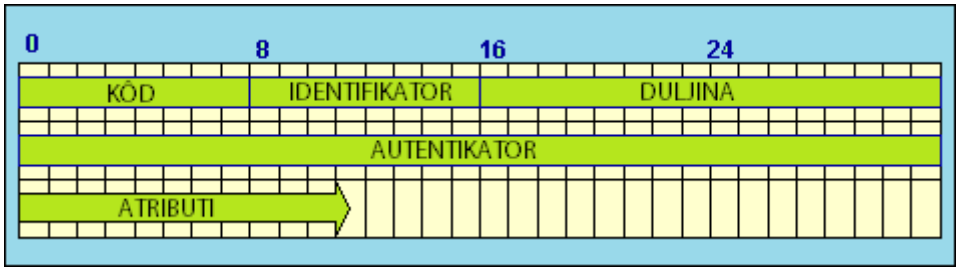
- **Autentikacija** je proces kojim se potvrđuje korisnikov digitalni identitet, obično putem neke vrste identifikatora i pripadnih podataka. Primjeri tih podataka su lozinke, tokeni, digitalni certifikati i brojevi telefona.
- **Autorizacijom** se utvrđuje je li određeni entitet ovlašten izvoditi neku aktivnost (što se najčešće provodi prijavom pomoću lozinke). Autorizacija se može provoditi nizom ograničenja poput vremenskog, ograničenja fizičke lokacije ili ograničenja protiv višestrukih prijava istog entiteta ili korisnika. Primjeri tipova usluga su filtriranje IP adrese, dodjeljivanje adrese, dodjeljivanje puta usmjeravanja, kvaliteta usluge (QoS), diferencijalne usluge, kontrola pojasne širine, upravljanje prometom, obavezno tuneliranje do određene krajnje točke i enkripcija.
- ***Accounting* ili administracija korisnika** je proces praćenja korištenja mrežnih resursa. Ti podaci se mogu koristiti za upravljanje, planiranje, naplaćivanje i usluge te u druge (specifične) svrhe. *Accounting* u stvarnom vremenu se odnosi na podatke koji se dostavljaju za vrijeme korištenja resursa. Skupni *accounting* (eng. *batch accounting*) se odnosi na podatke koji se čuvaju i kasnije dostavljaju pružatelju mrežne usluge. Podaci koji se obično prikupljaju su identitet korisnika, vrsta pružene usluge, kad je usluga počela i kad je završila.

3.1. Format RADIUS poruke

RADIUS poruke se izmjenjuju kad korisnik želi pristupiti mreži čijim pristupom upravlja RADIUS klijent (npr. NAS). Klijent izmjenjuje poruke s RADIUS poslužiteljem, čime se odobravaju ili odbijaju zahtjevi korisnika. RADIUS poruka sadrži 8-bitni kôd poruke, 8-bitni identifikator, 16-bitnu duljinu poruke, 32-bitni autentikator i, opcionalno, atribute. Format poruke je prikazan na slici 1. Kôd određuje tip poruke, a moguće vrijednosti su:

- (1) zahtjev za pristupom (*Acces-Request*),
- (2) odobren pristup (*Access-Accept*),
- (3) odbijen pristup (*Access-Reject*),
- (4) accounting zahtjev (*Accounting-Request),*
- (5) accounting odgovor (*Accounting-Response*),
- (11) osporavanje pristupa (*Access-Challenge*),
- (12) status poslužitelja (*Status-Server*),
- (13) status klijenta (*Status-Client*),
- (255) rezervirano (*Reserved*).

Identifikator je vrijednost koja omogućava RADIUS klijentu da poveže RADIUS odgovor s ispravnim neispunjenim zahtjevom, dok „Duljina" označava duljinu poruke uključivo sa zaglavljem. Autentikator polje koristi se za provjeru autentičnosti odgovora od RADIUS poslužitelja, a zaštićeno je lozinkom pomoću algoritma za kriptiranje. U polje atributa se upisuje proizvoljni broj atributa kao što su npr. korisničko ime (User-Name) i lozinka (User-Password). RADIUS nudi 256 mogućih atributa, od kojih su 49 još nedodijeljena [2].



Slika 1. RADIUS poruka

3.2. Primjer komunikacije

U nastavku će se prikazati najčešći oblik komunikacije RADIUS porukama, zahtjev za pristupom na temelju korisničkog imena i lozinke. Dvije strane u komunikaciji su klijent koji želi ovjeriti pristupne podatke koje je dobio od korisnikai poslužitelj koji ima pristup bazi podataka s podacima o korisnicima.

Slika 2. Entiteti potrebni za razmjenu RADIUS poruka

Slijede koraci koji se poduzimaju tijekom komunikacije.

1. Klijent stvara *Access-Request* poruku koja od atributa mora sadržavati barem korisničko ime i lozinku. Polje identifikatora poruke nije specificirano RADIUS protokolom već je riječ o jednostavnom brojaču koji je stvoren na klijentu i koji se povećava sa svakim zahtjevom. Poruka sadrži autentikator zahtjeva (eng. *Request Authenticator*), što je zapravo slučajno odabran niz bitova duljine 256. Osim atributa s lozinkom, cijela poruka je nezaštićena. Lozinka je zaštićena pomoću zajedničkog ključa klijenta i poslužitelja. Zajednički ključ je niz znakova koji služi kao lozinka između RADIUS klijenta i poslužitelja, klijenta i posrednika (eng. *proxy*) ili posrednika i poslužitelja. Može se dobiti programom za generiranje i mora biti poznat objema stranama prije početka komunikacije. Zajednički ključ i *Request Authenticator* unose se u MD5 *hash* algoritam [4] čime se dobije 256-bitni sažetak koji se kombinira[2] s lozinkom korisnika.
2. Poslužitelj prima *Access-Request* poruku i provjerava posjeduje li zajednički ključ tog klijenta, o čemu ovisi da li se zahtjev obrađuje. Ako poslužitelj ima isti ključ kao i klijent, može dešifrirati korisničku lozinku. Nakon toga traži u bazi podataka dobiveno korisničko ime i lozinku kako bi ih ovjerio. Ako su podaci valjani, poslužitelj šalje klijentu *Access-Accept* poruku. Ako nisu, poslužitelj šalje *Access-Reject* poruku.
3. Obje poruke koriste vrijednost identifikatora iz dobivene *Access-Request* poruke, a polje autentikatora postavljaju u vrijednost autentikatora odgovora (eng. *Response Authenticator*). Primjenom ranije spomenutog MD5 *hash* algoritma na niz koji čine ulančana poruka zahtjeva i zajednički ključ dobiva se *Response Authenticator*. Ovaj postupak prikazan je jednadžbom u nastavku:

Response Authenticator = MD5(kôd + ID + duljina + *Request Authenticator* + Atributi + zajednički ključ)

   gdje znak „+“ označava ulančavanje.
4. Nakon što klijent primi odgovor, koristi polje identifikatora da ga poveže s neispunjenim zahtjevom. U slučaju kad nema zahtjeva s istim identifikatorom, poruka se zanemaruje. U

[2] Računa se XOR operacija između pojedinih bitova sažetka i lozinke

suprotnom, klijent provjerava vrijednost polja *Response Authenticator*, računajući ga na isti način na koji je to učinio poslužitelj. Ako zaprimljena vrijednost nije ista izračunatoj, poruka se zanemaruje.

5. Ako je klijent primio ovjereni *Access-Accept* paket, smatra se da su korisničko ime i lozinka ispravni te je korisnik ovjeren. Ako je klijent primio ovjereni *Access-Reject* paket, smatra se da su korisničko ime i/ili lozinka neispravni te korisnik nije ovjeren.

Opisana komunikacija se može prikazati na slici Slika 3.

Slika 3. Tijek razmjene RADIUS poruka

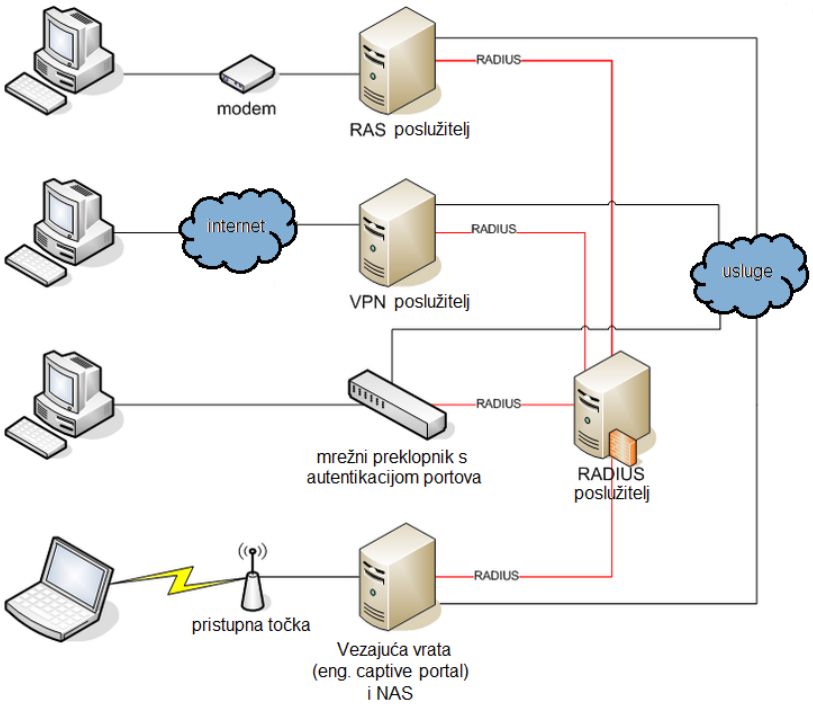
4. Sigurnosni elementi i njihova izvedba

RADIUS poslužitelji ostvaruju „AAA“ koncept za upravljanje mrežnim pristupom – autentikaciju, autorizaciju i administraciju korisnika. Tzv. „AAA transakcija“ se odvija u dva koraka opisana u potpoglavljima koji slijede. Prvi, autentikacija i autorizacija, je opisan u RFC 2865 specifikaciji [5], a drugi (*accounting)* u RFC 2866 [6].

Uređaji koja nadziru pristup mreži su:

- poslužitelji za udaljeni pristup (eng. *Remote Access Server*),
- poslužitelji virtualne privatne mreže (eng. *Virtual Private Network server*),
- mrežni preklopnici (eng. *Network switch*) i
- poslužitelji pristupa mreži – NAS (eng. *Network Access Server*).

U daljnjem tekstu će biti opisan pristup RADIUS poslužitelju putem poslužitelja pristupa mreži (NAS).



Slika 4. Upravljanje pristupom u organizaciji korištenjem RADIUS-a

4.1. Autentikacija i autorizacija

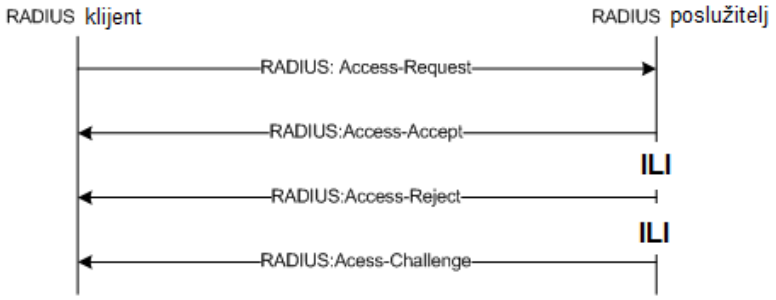
Korisničko računalo šalje NAS-u zahtjev za pristup određenim mrežnim resursima (npr. *web* stranici, FTP arhivi, bazi podataka ili privatnoj mreže) koristeći svoje identifikacijske podatke specifične za tu mrežu. Ti podaci se proslijeđuju NAS uređaju putem protokola sloja podatkovne veze kao što je na primjer PPP (*Point-to Point Protocol*). Nakon toga NAS šalje *Access-Request* poruku RADIUS poslužitelju tražeći autorizaciju za pristup putem RADIUS protokola. Zahtjev za autorizacijom sadrži pristupne podatke, obično u obliku korisničkog imena i lozinke ili sigurnosnog certifikata korisnika. Podaci mogu uključivati i druge podatke koje NAS ima o korisniku poput IP adrese, broja telefona i detalja o korisnikovom fizičkom mjestu priključivanja na NAS.

RADIUS poslužitelj vraća jedan od tri moguća odgovora na zahtjev (prikazano na slici Slika 5):

- *Access-Reject* – korisniku je bezuvjetno osporen pristup svim traženim mrežnim resursima. Razlog tome mogu biti nemogućnost dokazivanja identiteta, nepoznat ili neaktivan korisnički račun.
- *Access-Challenge* – zahtjevaju se dodatni podaci, poput naknadne lozinke, PIN-a i sl. Ova poruka se koristi i u složenijim autentikacijskim dijalozima gdje se uspostavlja sigurni tunel između korisničkog računala i RADIUS poslužitelja tako da se pristupni podaci skrivaju od NAS-a.

- *Access-Accept* – korisniku je odobren pristup. Kad je korisnik autenticiran, RADIUS poslužitelj će provjeriti da li je korisnik autoriziran za korištenje tražene mrežne usluge. Korisniku tako može na primjer biti dozvoljen pristup poslovnoj bežičnoj mreži, ali ne i VPN-u.

Sva tri odgovora mogu sadržavati atribut *Reply-Message* koji daje razlog odbijanja, zahtjev za dodatnim podacima ili poruku dobrodošlice.



Slika 5. Komunikacija NAS (RADIUS Client) - RADIUS poslužitelj prilikom autentikacije
Izvor: wikipedia.org

RADIUS poslužitelj provjerava ispravnost podataka koristeći autentikacijske protokole kao što su PAP (*Password Authentication Protocol*), CHAP (*Challenge Handshake Authentication Protocol*) ili EAP (*Extensible Authentication Protocol*). Poslužitelj koristi bazu podataka da ovjeri identifikacijske podatke korisnika kao i dodatne informacije povezane sa zahtjevom (poput IP-a korisnika, članskog statusa i privilegija pristupa mrežnoj usluzi). Na taj način se određuje da li korisniku dati dozvolu pristupa i koje ovlasti mu pripadaju. U prošlosti su RADIUS poslužitelji provjeravali korisničke podatke isključivo u lokalno smještenoj bazi podataka. Danas, uz taj pristup, postoji i mogućnost korištenja vanjskih izvora, kao što su vanjske SQL baze podataka [7], Kerberos [8], LDAP [9] ili Active Directory [10] poslužitelja.

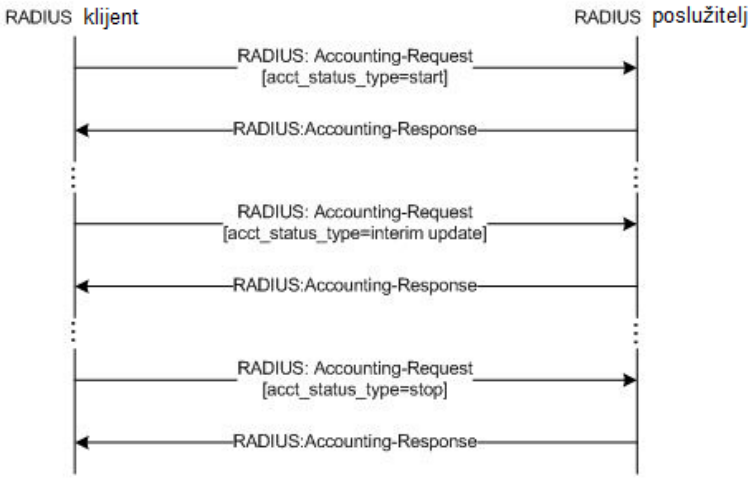
4.2. Administracija korisnika

Nakon što je NAS odobrio pristup korisniku, on šalje poruku *Accounting Start* (RADIUS *Accounting Request* poruka koja sadrži atribut *Acct-Status-Type* s vrijednošću „start“) RADIUS poslužitelju. Slanje te poruke označava početak korisnikovog pristupa mreži. *Accounting Start* poruke obično sadrže identifikaciju korisnika, njegovu IP adresu, mjesto pristupa i jedinstveni identifikator sjednice. Kao odgovor, poslužitelj uzvraća porukom *Accounting-Response*.

Nakon uspostave sjednice, NAS može povremeno slati *Interim Update* poruke poslužitelju. Riječ je o RADIUS *Accounting-Request* porukama koje sadrže atribut *Acct-Status-Type* s vrijednošću „interim-update“. Uobičajeno, *Accounting Interim* poruke prenose podatke o trajanju trenutne sjednice i o trenutnom korištenju podataka, što je korisno za praćenje osobnih troškova, odnosno za nadgledanje rada korisnika u mreži.

Na kraju, prilikom isključivanja korisnika iz mreže, NAS šalje *Accounting Stop* poruku (RADIUS *Accounting Request* poruka s vrijednošću „stop“ atributa *Acct-Status-Type*). Poruka sadrži detalje o ukupnom vremenu trajanja sjednice, prenesenoj količini podataka, razlogu isključivanja i ostale informacije vezane uz pristup mreži.

Klijent obično šalje Accounting-Request poruke u određenim intervalima sve dok ne primi Accounting-Response odgovor. Osnovna svrha ovih podataka je ta da se korisniku može naplatiti usluga u skladu s njegovom potrošnjom. Uz naplatu potrošnje, podaci se koriste i za računanje statistike kao i za nadzor same mreže. Opisana komunikacija prikazana je na slici 6.

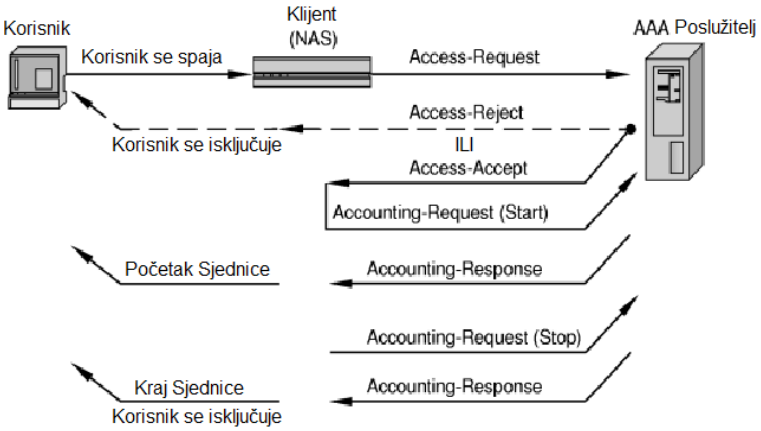


Slika 6. Razmjena accounting poruka
Izvor: wikipedia.org

4.3. Sažetak sjednice

Kad se uzmu u obzir sve poruke koje izmjenjuju RADIUS klijent i poslužitelj, kao i sami zahtjevi korisnika, komunikacija se može prikazati slikom 7.

1. Korisnik šalje svoje identifikacijske podatke RADIUS klijentu u želji da mu se odobri pristup određenim mrežnim resursima.
2. Klijent provodi proces autentikacije i autorizacije razmjenom poruka s RADIUS poslužiteljem
    a. klijent šalje *Access-Request*
    b. poslužitelj odgovara s *Access-Reject* (u ovom slučaju se korisnikov zahtjev za pristupom jednostavno odbacuje) ili s *Access-Accept.*
3. Klijent provodi proces administracije korisnika (*accounting*)
    a. klijent šalje poslužitelju poruku *Accounting-Request (Start)*
    b. poslužitelj odgovara s *Accounting-Response*, čime počinje sjednica
    c. kad korisnik želi završiti sjednicu, klijent šalje poslužitelju *Accounting-Request (Stop)*
    d. poslužitelj odgovara s *Accounting-Response*, čime se završava sjednica i korisnik isključuje iz mreže.



Slika 7. Sjednica koja koristi RADIUS protokol
Izvor: hp.com

4.4. Protokoli autentikacije

RADIUS sustavi mogu provoditi autentikaciju korisnika pomoću nekoliko autentikacijskih protokola. To su PAP, CHAP, MS-CHAP i EAP.

- PAP (*Password Authentication Protocol*) je slaba metoda autentikacije jer se lozinke šalju u otvorenom tekstu. Postupak autentikacije PAP protokolom je prikazan na slici 7.
- CHAP (*Challenge Handshake Authentication Protocol*) je snažnija metoda povezivanja od PAP-a. Razmjena poruka korištenjem ovog protokola analogna je PAP metodi uz jednu razliku. Prilikom spajanja korisnika na NAS (koji je ujedno i RADIUS klijent), NAS šalje korisniku upit. Korisnik mora posjedovati posebni uređaj, poput *smart* kartice ili posebnog programa, pomoću kojih će kriptirati dobiveni upit, te ga poslati natrag NAS klijentu. NAS prosljeđuje kriptirani upit zajedno s *Access-Request* porukom RADIUS poslužitelju, koji na temelju dobivenih podataka autenticira korisnika.
- MS-CHAP (*Microsoft Challenge Handshake Authentication Protocol*) je primjena CHAP protokola koju je oblikovao Microsoft za autentikaciju udaljenih Windows radnih stanica. MS-CHAP je uglavnom identičan CHAP-u, uz sitne razlike. MS-CHAP je baziran na enkripciji i *hash* algoritmima koje koriste Windows mreže, a format kriptiranog upita je specifičan za Windows operacijske sustave.
- EAP (*Extensible Authentication Protocol*) je sigurnija metoda povezivanja od PAP-a, i nudi veću fleksibilnost s više mogućnosti kriptografskih algoritama pri obradi autentikacijskih zahtjeva. EAP poruke mogu biti enkapsulirane u paketima drugih protokola, poput RADIUS-a, kako bi se postigla kompatibilnost sa širokim spektrom autentikacijskih mehanizama. Ova fleksibilnost omogućava da se EAP primjenjuje u oblicima koji su prikladniji za bežične i mobilne mreže od drugih autentikacijskih protokola (npr. LEAP – *Lightweight EAP*). EAP omogućava autentikaciju direktno između korisnika i RADIUS poslužitelja, bez sudjelovanja pristupnog poslužitelja (kao što je slučaj s npr. CHAP-om).

5. Sigurnosni problemi

U nastavku slijedi opis sigurnosnih problema kod RADIUS protokola i mogućih napada na RADIUS poslužitelje. Iskorištavanje sigurnosnih ranjivosti protokola ovisi o sposobnosti napadača da presretne RADIUS poruke na putu od pristupnog (NAS) do RADIUS poslužitelja. U navedenim slučajevima se podrazumijeva da napadač posjeduje fizički pristup mreži i da se nalazi na putu usmjeravanja između pristupnog i RADIUS poslužitelja.

5.1. Neautenticirane klijentske Access-Request poruke

U RADIUS poslužitelju se obično ne provodi kriptografska ovjera kojom bi se korištenjem ključeva ili *hash* sažetka provjerila autentičnost dolaznih *Access-Request* poruka. Poslužitelj ovjerava IP adresu RADIUS klijenta koji je poslao poruku, ali IP adresa se u RADIUS porukama lako može lažirati.

Problemu se može doskočiti tako da poslužitelj zahtjeva atribut *Message-Authenticator* za sve *Access-Request* poruke. Atribut *Message-Authenticator* je MD5 *hash* sažetak cijele *Access-Request* poruke, izračunat korištenjem zajedničkog ključa poslužitelja i klijenta. Pristupni poslužitelj mora koristiti navedeni atribut u svojim porukama RADIUS poslužitelju, a RADIUS poslužitelj mora odbaciti poruke koje ga ne sadržavaju ili u kojima on ne prolazi ovjeru. Atribut *Message-Authenticator* standardno zahtjevaju samo EAP/RADIUS poruke.

5.2. Slabosti zajedničkog ključa

Mnogi RADIUS poslužitelji koriste jedan ključ za više parova klijent-poslužitelj, a generiranjem se ne postiže dovoljno velik broj različitih ključeva da bi se uspješno spriječio napad rječnikom (eng. *dictionary attack*). Da bi se pogodio zajednički ključ, potrebno je izračunati polje *Response Authenticator* i sadržaj *Message-Authenticator* atributa. Dobiveni rezultati se uspoređuju s vrijednostima u presretnutom *Access-Accept*, *Access-Reject* ili *Access-Challenge* odgovoru. U sustavu u kojem se jedan ključ koristi više puta, nakon što se jednom izračuna, isti se lako može zloupotrijebiti (npr. slanjem lažnog zahtjeva koji koristi ispravni ključ). Situaciju dodatno pogoršavaju RADIUS klijenti i poslužitelji koji ograničavaju duljinu ključa na znakove koji se mogu unijeti s tipkovnice (94 od mogućih 256 ASCII znakova).

Postoje dva moguća rješenja za ovaj problem:

1. Korištenje različitih ključeva za svaki par klijent-poslužitelj.
2. Ako ključ mora biti niz znakova s tipkovnice, treba odabrati niz od barem 22 slučajno odabrana velika i mala slova, brojke i interpunkcijskih znakova. Ako ključ mora biti slijed heksadecimalnih znakova, treba koristiti barem 32 slučajno odabrana heksadecimalna broja. U dokumentu RFC 2865 preporuča se duljinu ključa od 16 znakova, ali za potpunih 128 bitova entropije[3], svaki znak mora sadržavati punih 8 bita entropije. Ako je ključ ograničen na znakove s tipkovnice (za razliku od heksadecimalnih znakova), svaki znak sadržava 5.8 bitova entropije. Da bi se postigla 128-bitna entropija, RADIUS klijent, poslužitelj i, ako se koristi, *proxy* poslužitelj moraju omogućiti duljinu ključa od barem 22 znaka.

5.3. Osjetljivi atributi šifrirani RADIUS-ovim skrivajućim mehanizmom

RADIUS ima ugrađeni mehanizam koji osigurava minimalnu razinu zaštite osjetljivih atributa. Mehanizam prikrivanja korisničke lozinke (eng. *User-Password hiding mechanism*) koristi MD5 hash algoritam kako bi generirao ključni niz (eng. *key stream*) iz zajedničkog ključa klijenta i poslužitelja i vrijednosti *Request Authenticator*. Prilikom autentikacije korisnika PAP (Password Authentication Protocol) protokolom (koji prenosi lozinku u otvorenom tekstualnom obliku), promatrajući razmjenu RADIUS poruka, moguće je skupiti ključne nizove koji odgovaraju određenoj vrijednosti *Request Authenticator*. Uz poznatu korisničku lozinku, može se odrediti ključni niz i povezati s danom vrijednošću *Request Authenticator*. Pošto je napadač prilikom navedene komunikacije mogao odrediti ključni niz, može se pretpostaviti da je svaka sljedeća poruka koja sadrži isti *Request Authenticator* ugrožena.

[3] Entropija označava količinu informacije sadržanu u nekom podatku.

Ovaj problem je poznat IETF-u, te je u RFC 2865 navedeno da korisnici sami procijene ozbiljnost prijetnje, te razmisle o dodatnim sigurnosnim mehanizmima. Standardni način dodatne zaštite skrivenih atributa je korištenje IPSec (*Internet Protocol Security*) protokola s ESP[4]-om (*Encapsulating Security Payload*) i enkripcijskim algoritmom kao što je 3DES (*Triple Data Encryption Standard*), kako bi se osigurala povjerljivost podataka za cijelu RADIUS poruku. Ukoliko nije moguće koristiti IPSec s ESP-om i enkripcijskim algoritmom, mrežni administratori mogu smanjiti ranjivost poduzimajući sljedeće korake:

1. Zahtjevati korištenje atributa *Message-Authenticator* u svim *Access-Request* porukama.
2. Koristiti kriptografski jake *Request Authenticator* vrijednosti.
3. Zahtjevati korištenje jakih korisničkih lozinki.
4. Koristiti autentikacijski mehanizam brojanja i zaključavanja kako bi se spriječio *online* napad rječnikom na korisničku lozinku.
5. Koristiti zajednički ključ sa 128-bitnom entropijom.

5.4. Dekriptiranje enkriptiranih atributa pomoću slabih Request Authenticator vrijednosti

Kao što je navedeno u dokumentu RFC 2865 [5], sigurni *Request Authenticator* mora biti vremenski i prostorno jedinstven. *Request Authenticator* i zajednički ključ se kombiniraju da bi se odredio slijed ključeva (eng. *key stream*) za enkripciju korisničke lozinke i ostalih atributa. Napadač koji zna kako presresti promet između RADIUS klijenta i poslužitelja i kako ostvariti mrežni pristup, može napraviti rječnik RADIUS *Request Authenticator* vrijednosti s odgovarajućim slijedovima ključeva. Ako pristupni poslužitelj ikad ponovi *Request Authenticator* s istim zajedničkim ključem, mogu se odrediti korisnička lozinka i ostali atributi sadržani u porukama.

Ukoliko generator vrijednosti atributa *Request Authenticator* nije dovoljno nasumičan, odnosno ako nema mogućnost dovoljno različitih vrijednosti, korištena vrijednost se može predvidjeti jer je velika vjerojatnost da će se ponoviti u razumno kratkom vremenskom periodu. Generator mora biti kriptografske kvalitete, a ako to nije, može se koristiti IPSec s ESP-om [11] i enkripcijskim algoritmom poput 3DES-a kako bi se postigla povjerljivost podataka za cijelu RADIUS poruku.

[4] ESP osigurava autentičnost izvora, integritet i povjerljivost poslanih paketa. Podržava postavke enkripcije i autentikacije (svaku zasebno).

6. Alternativni protokoli

Iako vrlo popularan, RADIUS nije jedini protokol koji koristi AAA princip. U nastavku slijedi kratki pregled protokola koji se koriste s istom ili sličnom svrhom.

6.1. TACACS

TACACS (*Terminal Access Controller Access-Control System*) [14] je autentikacijski protokol koji omogućava komunikaciju pristupnog poslužitelja s udaljenim autentikacijskim poslužiteljem u UNIX mrežama. Jednako kao i kod RADIUS-a, autentikacijski poslužitelj ovjerava korisnika koji traži pristup mreži.

TACACS omogućava klijentu da preuzme korisničko ime i lozinku i šalje upite TACACS autentikacijskom poslužitelju, ponekad zvanom i TACACS *daemon*[5] ili TACACSD. Taj poslužitelj je obično program koji se izvršava na domaćinu, s tim da domaćin odlučuje o prihvaćanju ili odbijanju zahtjeva i slanju odgovora. Na taj način je proces odlučivanja otvoren, a korišteni algoritmi i podaci pomoću kojih se donosi odluka su pod potpunom kontrolom domaćina na kojem se izvršava TACACSD.

6.2. TACACS+

TACACS+ [15] i RADIUS su u novijim mrežama zamijenili TACACS protokol. Iako je baziran na TACACS protokolu, TACACS+ je sasvim novi proizvod i nekompatibilan je s prethodnim verzijama. Od RADIUS-a se razlikuje po tome što koristi pouzdani transportni protokol TCP (*Transmission Control Protocol*) naspram nepouzdanog UDP-a (*User Datagram Protocol*) i po tome što odvaja operacije autentikacije i autorizacije.

TACACS+ se može rastaviti na 3 različita protokola, gdje svaki obavlja jednu od funkcija autentikacije, autorizacije i *accountinga*. Oni se mogu, po želji, implementirati na odvojenim poslužiteljima. Pruža podršku drugim protokolima, poput IP-a i AppleTalk-a. Kao Ciscovo poboljšanje TACACS protokola, TACACS+ izvršava operaciju enkripcije cijelog tijela paketa za sigurniju komunikaciju.

Kriterij	RADIUS	TACACS+
Transportni protokol	UDP (nepouzdani prijenos)	TCP (pouzdani prijenos)
Autentikacija i autorizacija	Povezani	Mogu se odvojiti, čime se ostvaruje veća fleksibilnost
Podrška drugih protokola	Samo IP	Podržava (IP, Apple, NetBIOS, Novell, X.25)
Pristup naredbenom sučelju usmjeritelja	Ne podržava	Podržava 2 metode kontroliranja autorizacije naredbi usmjeritelja – po osobi i po grupi
Enkripcija	Samo lozinke	Enkripcija cijelog paketa

Tablica 2. Usporedba protokola RADIUS i TACACS+

6.3. Diameter

Već u vrijeme prvih službenih IETF sastanaka radne grupe za RADIUS počeli su neslužbeni dogovori o nasljedniku koji je trebao biti njegova pročišćena verzija. Isprva je bilo predloženo ime RADIUS v2, no IETF ga nije dozvolio jer je naziv RADIUS v1 još uvijek bio u postupku ratifikacije. Umjesto toga su ga nazvali Diameter (jer je „dva puta bolji od RADIUS-a“). Diameter [16] pruža jaču kontrolu pristupa koja rješava mnoge nedostatke RADIUS-ovog dizajna. Na primjer, RADIUS podržava samo nepouzdani UDP transportni protokol, dok Diameter podržava pouzdane TCP i SCTP (*Stream Control Transmission Protocol*) protokole, čime je prikladniji za širu lepezu aplikacija.

[5] Daemon je program čija je svrha obavljati zadatke u pozadini, neovisno i bez komunikacije s korisnikom.

Drugi očiti napredak je u slučaju atributa. Atributi RADIUS protokola koriste 8-bitne identifikacijske vrijednosti, a 206 od 256 mogućih vrijednosti je već dodijeljeno [2]. Diameter koristi 32-bitne kôdove što znači da podržava 4,294,967,296 (preko 4 milijarde!!) različitih atributa.

Karakteristike	RADIUS	Diameter
Transportni protokol	Nepouzdani (UDP)	Pouzdani (TCP ili SCTP)
Transportna sigurnost	Neobavezni IPSec	Obavezni IPsec ili TLS (eng. *Transport Layer Security*)
Konfiguracija klijenta	Statička konfiguracija.	Statička konfiguracija i otkrivanje korisnika.
Status poslužitelja	Poslužitelj ne objavljuje svoj status (radi, ne radi)	Podržava poruke o stanju poslužitelja (*keepalive, running, going down*)
Potvrda o prijmu	Klijent ne zna da li je poslužitelj primio poruku ili je ona odbačena (zbog greške ili netočnih podataka)	Poslužitelj može slati poruke o greškama, autentikaciji i o prekidama sjednica.
Sigurnosni model	Podržava sigurnost „korak-po-korak“ (eng. *hop-by-hop*). Svakim skokom se mijenjaju podaci te im se ne može otkriti podrijetlo.	Podržava sigurnost „s kraja na kraj“ i „korak-po-korak“. Sigurnost „s kraja na kraj“ osigurava da se podaci ne mogu mijenjati bez upozorenja.
Veličina atributa	Rezervirano je 8 bitova za kôd atributa u zaglavlju.	Rezervirana su 32 bita za kôd atributa u zaglavlju.
Podrška različitih nabavljača	Podržava specifične atribute.	Podržava specifične atribute i poruke.

Tablica 3. Usporedba protokola RADIUS i Diameter

7. Budućnost RADIUS protokola

Kad se RADIUS tek pojavio, uloga mu je bila jednostavno pružiti uslugu autentikacije na distribuiranim *dial-in* pristupnim poslužiteljima. Od tad se prilagođavao potrebi svake nove mrežne pristupne tehnologije koja bi se pojavila. Danas se najčešće koristi za autenticirani pristup VPN mrežama, mrežnim preklopnicima i bežičnim pristupnim točkama. Mnoštvo usluga aplikacijskog sloja koristi RADIUS za centraliziranu autentikaciju, a stalne nadogradnje ovog protokola obećavaju još mnoge nove mogućnosti u budućnosti.

Uz stalni napredak RADIUS-a, treba uzeti u obzir i protokol koji je nastao s glavnom svrhom da ga zamijeni - Diameter. No, ako je nastao s tom svrhom, postavlja se pitanje zašto ga još nije zamijenio?

Za početak, dok je prvi RADIUS RFC objavljen 1997. godine, specifikacije Diameter protokola su objavljene tek 2003. godine. Tijekom tih 6 godina korisnici su se dobro upoznali s načinom rada RADIUS-a, a njegove primjene su se proširile svijetom, dok je Diameter relativno nov, neupoznat i s puno manje implementacija. Najočitiji dokaz toga su 2 najraširenija operacijska sustava, Windows i Linux, koji oboje koriste RADIUS poslužitelje u svojim platformama (Microsoftov *Internet Authentication Service* i Linuxov *FreeRADIUS*).

Osim toga, RADIUS se nije prestao razvijati dok se stvarao Diameter. Njegov razvoj je pratio evoluciju internetskih pristupnih tehnologija, od modema do ADSL veza. Alan DeKok, predsjednik RADIUS arhitekture za Infoblox i programer na FreeRADIUS projektu tvrdi: „RADIUS je nekada podržavao 90% funkcionalnosti koju ima Diameter, no uza sva trenutna i planirana poboljšanja, doseći će 99% i biti će rijetke situacije u kojima će Diameter još uvijek biti potreban."

8. Zaključak

Od skromnih početaka u umrežavanju sveučilišta u Americi, RADIUS se proširio dalje nego što se ikad nadalo. S konceptom koji je konstantno dorađivan, nadopunjavan i prilagođavan, RADIUS služi mnogim korisnicima diljem svijeta već 15-ak godina. Iako je u početku postavljano pitanje da li ga uopće proglasiti službenim standardom, pošto je IETF shvatio koliko je RADIUS postao popularan, proglasio ga je standardom kako bi pomogao širenju njegovog izvornog oblika. Na taj način su htjeli dati javnosti sliku toga kako je RADIUS trebao izgledati prije brojnih izmjena i dodataka koje je doživio šireći se Internetom.

RADIUS i danas korisnicima pruža centraliziranu kontrolu nad autentikacijom, autorizacijom i administracijom korisnika. Iako ima određene slabosti, one se uglavnom mogu premostiti korištenjem dodatnih sigurnosnih mehanizama i poštivanjem pravila. Stoga ne čudi što većina korisnika ne osjeća potrebu za prelaskom na napredniji i „jači" protokol Diameter.

No unatoč svim subjektivnim prednostima RADIUS-a, Internet se i dalje razvija, a s njim neizbježno i tehnologija. Kroz nekoliko godina trebale bi se prepoznati tehničke prednosti Diametera i tad se očekuje njegovo brzo širenje i dugo očekivano preuzimanje RADIUS-ovog mjesta.

9. Reference

[1] History of the RADIUS server, http://www.interlinknetworks.com/app_notes/History_of_RADIUS.htm , 2006.-2007.

[2] IANA, RADIUS Types, http://www.iana.org/assignments/radius-types/, lipanj 2010.

[3] HP-UX AAA Server A.06.01 Getting Started Guide, http://docs.hp.com/en/T1428-90058/ch01s01.html, 2001.-2004.

[4] MD5, http://en.wikipedia.org/wiki/MD5, srpanj 2010.

[5] IETF, Remote Authentication Dial In User Service (RADIUS), http://www.ietf.org/rfc/rfc2865.txt, lipanj 2000.

[6] IETF, RADIUS Accounting, http://www.ietf.org/rfc/rfc2866.txt, lipanj 2000.

[7] SQL, http://en.wikipedia.org/wiki/SQL, srpanj 2010.

[8] Kerberos (protocol), http://en.wikipedia.org/wiki/Kerberos_(protocol), srpanj 2010.

[9] LDAP, http://en.wikipedia.org/wiki/LDAP, srpanj 2010.

[10] Active Directory, http://en.wikipedia.org/wiki/Active_Directory, srpanj 2010.

[11] IPsec, http://en.wikipedia.org/wiki/IPsec, srpanj 2010.

[12] AAA protocol, http://en.wikipedia.org/wiki/AAA_protocol, lipanj 2010.

[13] RADIUS Protocol Security and Best Practices, http://technet.microsoft.com/en-us/library/bb742489.aspx, siječanj 2002.

[14] TACACS, http://en.wikipedia.org/wiki/TACACS, lipanj 2010.

[15] TACACS+, http://en.wikipedia.org/wiki/TACACS%2B, lipanj 2010.

[16] Diameter (protocol), http://en.wikipedia.org/wiki/Diameter_(protocol), srpanj 2010.

[17] High-Level Comparison of RADIUS, TACACS+, and Diameter, http://etutorials.org/Networking/network+management/Part+II+Implementations+on+the+Cisco+Devices/Chapter+9.+AAA+Accounting/High-Level+Comparison+of+RADIUS+TACACS+and+Diameter/, 2008.-2010.

[18] Eric A. Hall, RADIUS Reinvigorated, http://www.eric-a-hall.com/articles/20060101itf1.html, 2006.