CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

DIAMETER protokol

NCERT-PUBDOC-2010-07-305

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.

Sadržaj

1. Uvod

Posljednjih godina svjedoci smo velikog porasta broja ponuđenih mrežnih usluga. Značajan broj navedenih usluga u svom radu koristi metode autentikacije, autorizacije i administracije (eng. *accounting*) korisnika. Možda najbolji primjer njihove uporabe je pružanje usluge pristupa Internetu. Da bi pružatelji mrežnih i internetskih usluga (eng. *Internet Service Provider, ISP*) uspješno omogućili pristup Internetu svojim korisnicima, potrebno je dodijeliti im mrežne identitete, provjeravati ih, omogućiti im pristup sadržajima, ovisno o njihovim ovlastima, te pratiti mrežne i računalne resurse koje su pritom potrošili. Tako metode autentikacije služe za uspostavljanje i provjeru digitalnog identiteta korisnika, metode autorizacije određuju korisniku dopuštene informacijske i komunikacijske aktivnosti, a metode administracije služe za evidenciju potrošnje mrežnih i računalnih resursa u svrhu upravljanja, planiranja ili naplate.

Kako bi mrežna arhitektura mogla pratiti takav trend porasta broja ponuđenih usluga, potrebne su stalne nadogradnje postojećih usmjeritelja, pristupnih mrežnih poslužitelja (eng. *Network Access Server, NAS*) i ostalih mrežnih elemenata. Ipak, velikim ISP-ovima se ne isplati rekonfigurirati sve svoje pretplatnike pri svakoj promjeni opreme na, primjerice, pristupnim mrežnim poslužiteljima. Da bi se to izbjeglo, za sada se prilično uspješno primjenjuju raznovrsni protokoli za autentikaciju, autorizaciju i administraciju. Danas najpopularniji takav protokol je RADIUS (eng. *Remote Access Dial-In User Service*). Ipak, velikim porastom složenosti broja mrežnih usmjeritelja, pristupnih mrežnih poslužitelja i ostalih elemenata mrežne infrastrukture sve više se osjeća ograničenost njegove arhitekture i javlja potreba za razvojem novog i kvalitetnijeg nasljednika.

Još jedan argument za nastajanje kvalitetnijeg protokola za autentikaciju, autorizaciju i administraciju korisnika može se pronaći u nedostatku fleksibilnosti postojećih. Naime, pojavom raznih usluga (*Voice over IP, Fax over IP, Mobile IP* itd.) koje zahtijevaju slične mehanizme autentikacije, prikupljanja i praćenja podataka o korisničkim ovlastima i potrošenim resursima, došlo je do pojave vrlo čudne filozofije unutar organizacije IETF (eng. *Internet Engineering Task Force*). Za svaku od uvedenih usluga krenuo se razvijati specifičan protokol koji bi obavljao navedene zadatke bez obzira na njihovu sličnost. Osnovni razlog tomu bio je upravo nedostatak fleksibilnosti i proširivosti postojećih rješenja. Takva filozofija, naravno, nije bila održiva te se krenulo u potragu za boljim rješenjem.

Upravo ovdje na scenu stupa protokol DIAMETER. Razvijen iz protokola RADIUS te zamišljen kao njegov nasljednik, DIAMETER je protokol za autentikaciju, autorizaciju i administraciju korisnika koji donosi čitav niz poboljšanja i prednosti u odnosu na svojeg prethodnika. Uz to, donosi i toliko traženu fleksibilnost koja omogućuje ostvarenje čitavog spektra različitih usluga jednostavnom nadogradnjom osnovnog rješenja.

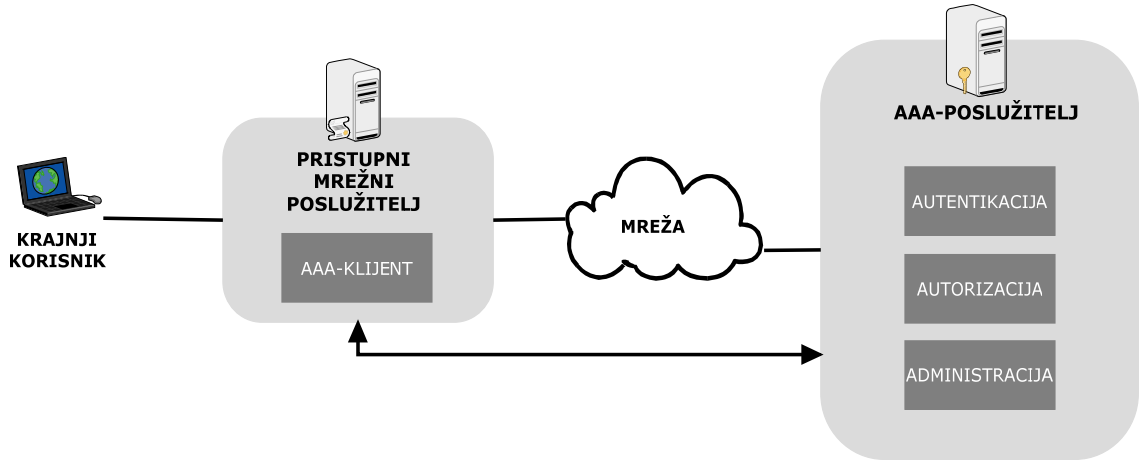
U ovom dokumentu bit će predstavljen protokol DIAMETER, ukratko opisan njegov nastanak i razvoj te analizirane njegove razlike i prednosti u odnosu na protokol RADIUS. Osim toga, predstavit će se većina njegovih funkcionalnosti, opisati arhitektura te razmotriti njegova primjena danas zajedno s idejama vezanim uz budući razvoj.

2. Nastanak protokola DIAMETER i njegove funkcionalnosti

2.1. Općenita arhitektura protokola za autentikaciju, autorizaciju i administraciju

S obzirom na stalan rast broja mrežnih usluga, aplikacija i njihovih korisnika te sve veću složenost cjelokupne mrežne arhitekture, logično je da su se pojavili sve veći i značajniji sigurnosni problemi. Samim time javila se i potreba za ozbiljnijim razvojem protokola zaduženih za autentikaciju, autorizaciju i administraciju korisnika. Tako se u jedinstvenom rješenju nalaze objedinjeni mehanizmi koji omogućuju osnovne sigurnosne preduvjete: provjere identiteta komunicirajućih strana, ograničenja njihova pristupa ovisno o dodijeljenim pravima te praćenje potrošenih računalnih i mrežnih resursa u svrhu upravljanja, planiranja ili naplate. Naravno, cilj je da takvo rješenje bude što jednostavnije, skalabilnije te fleksibilnije u suradnji s mnoštvom dostupnih mrežnih platformi i tehnologija. S druge strane, protokoli za autentikaciju, autorizaciju i administraciju korisnika omogućuju pohranu velikog broja autentikacijskih i administrativnih parametara različitih korisnika na jednom, središnjem poslužitelju. To uvelike olakšava administraciju velikog broja korisnika te smanjuje dodatni pritisak na resurse klasičnih mrežnih elemenata poput usmjeritelja, preklopnika, modema i ostalih.

Pojednostavljen princip rada protokola ove vrste objašnjen je pomoću sljedeće slike (Slika 1). Valja napomenuti da se kratica AAA (eng. *authentication, authorization and accounting*) često koristi za skraćeno pisanje koncepta autentikacije, autorizacije i administracije korisnika. Primjerice, nerijetko se u literaturi umjesto protokola za autentikaciju, autorizaciju i administraciju korisnika pojavljuje termin AAA-protokol.



Slika 1. Pojednostavljena arhitektura sustava koji pruža AAA-usluge

Na gornjoj slici mogu se primijetiti osnovni elementi rješenja koje omogućuje autentikaciju, autorizaciju i administraciju korisnika: AAA-poslužitelj i AAA-klijent, smješten na pristupnom mrežnom poslužitelju. AAA-poslužitelji služe kao središnji čvorovi zaduženi za pohranu i distribuciju svih relevantnih AAA-podataka. Tipične pristupne točke u mrežama ovakve arhitekture pristupni su mrežni poslužitelji koji imaju ugrađene klijentske AAA-funkcije. Postupak korištenja AAA-usluge teče otprilike ovako:

- krajnji korisnik se spaja na uređaj koji ima funkciju pristupne točke (primjerice pristupni mrežni poslužitelj) i zahtijeva pristup mreži,
- klijentska AAA-funkcija pristupnog mrežnog poslužitelja prikuplja korisničke autentikacijske podatke (korisničko ime, lozinka...) i prosljeđuje ih AAA-poslužitelju,
- AAA-poslužitelj obrađuje primljene podatke i vraća pozitivan ili negativan odgovor zajedno s ostalim podacima potrebnim AAA-klijentu,
- AAA-klijent na pristupnom poslužitelju obavještava krajnjeg korisnika o uspješnom ili neuspješnom pristupu traženim resursima.

Pristupni mrežni poslužitelj može, u suradnji s AAA-poslužiteljem, pratiti resurse koje je korisnik potrošio od uspostave do prekida veze. Tako se, uz prethodno opisan postupak autentikacije, ostvaruju i mehanizmi autorizacije i administracije korisnika.

2.2. Protokol RADIUS i njegova ograničenja

RADIUS je trenutno najkorišteniji protokol za autentikaciju, autorizaciju i administraciju korisnika. Radi se o protokolu aplikacijskog sloja koji se temelji na modelu klijent-poslužitelj te na transportnom sloju koristi protokol UDP. U principu, njegova arhitektura vrlo je slična općenitoj arhitekturi protokola ove vrste opisanoj u prethodnom potpoglavlju. Umjesto AAA-klijenata ovdje se koriste RADIUS klijenti, najčešće smješteni na pristupnim mrežnim poslužiteljima. Funkciju AAA-poslužitelja obnašaju RADIUS poslužitelji koji prihvaćaju upite, provjeravaju dobivene korisničke parametre te ovisno o ishodu provjere vraćaju odgovarajuće konfiguracijske parametre koji će omogućiti pružanje adekvatne usluge korisniku. Osim toga, RADIUS poslužitelji mogu se koristiti i kao posrednički klijenti ostalim RADIUS poslužiteljima ili nekim drugim sustavima za autentikaciju korisnika. Sama komunikacija između klijenta i poslužitelja temelji se na dijeljenom tajnom ključu koji se iz sigurnosnih razloga nikada ne šalje računalnom mrežom.

Usprkos njegovim kvalitetnim rješenjima i pozitivnim karakteristikama valja uzeti u obzir da je protokol RADIUS razvijen sredinom 90-ih godina prošloga stoljeća s namjerom da pruži usluge autentikacije, autorizacije i administracije za potrebe tadašnje mrežne arhitekture. Skalabilnost protokola tada je bila u drugom planu. Zahtjevi su se s godinama, razvojem novih tehnologija te porastom broja korisnika i složenosti usluga, uvelike promijenili. Kako bi se nosio sa sve zahtjevnijim trendovima te podržao brojne nove usluge, RADIUS je za svaku veću promjenu zahtjeva dobivao nove i složenije zakrpe. S vremenom je broj ugrađenih dodataka postao toliko velik da se pri izradi novih jednostavno prestalo voditi računa o njihovom uzajamnom djelovanju. Osim nedostatka skalabilnosti, s vremenom su postala očita i ostala ograničenja. Jedno od njih svakako je isključiva uporaba nesigurnog i nepouzdanog UDP protokola na transportnom sloju. Mnoga ograničenja protokola RADIUS proizlaze iz činjenice da je on dizajniran kako bi pružio infrastrukturu za usluge autentikacije, autorizacije i administracije u tradicionalnim mrežama s komunikacijom temeljenom na PPP (eng. *Point to Point Protocol*) tehnologiji. Usluge se danas kreću u potpuno drugom smjeru, prema tehnologiji pokretnog IP-a (eng. *Mobile IP*), pokretljivosti korisnika, terminala i osoba. Uzevši u obzir navedena ograničenja u kombinaciji s nedostatkom fleksibilnosti i slabom proširivosti protokola jasno je da je došlo do potrebe za razvojem novijeg i naprednijeg nasljednika.

2.3. Nastanak i razvoj protokola DIAMETER

Na samom početku razvoja protokola koji bi po svojoj funkcionalnosti naslijedio RADIUS pojavilo se pitanje - od kuda krenuti? Naime, s obzirom na relativno zastarjelu i krutu arhitekturu protokola RADIUS nametnula se ideja da kao temelj u izradi nasljednika posluži neki drugi, noviji i sigurniji protokol. Ipak, u tom trenutku takav "adekvatniji" protokol nije postojao. S druge strane, početi iz temelja kao što je protokol RADIUS ipak je bilo logičnije nego početi ni iz čega.

Sam naziv novog protokola - DIAMETER (eng. *diameter* – promjer) upućuje na njegove karakteristike u odnosu na RADIUS (eng. *radius* – polumjer). Protokol DIAMETER nastao je 1998. godine. Prvu verziju razvili su Pat R. Calhoun, Glen Zorn i Ping Pan. Većina posla oko razvoja svodila se na uklanjanje nedostataka i funkcionalnih ograničenja preuzetih iz protokola RADIUS. Iako je jezgrena funkcionalnost protokola RADIUS ostala netaknuta, način njene implementacije poprilično se promijenio. Uz to, dodana su brojna proširenja i ostvarene nove mogućnosti. Premda DIAMETER nije izravno kompatibilan s protokolom RADIUS, njihova suradnja moguća je uporabom jednog od mnogobrojnih proširenja. Upravo je jednostavna proširivost protokola DIAMETER bila jedna od osnovnih ciljeva njegova razvoja.

Dodatni razvoj protokola DIAMETER potaknule su organizacije poput IETF-a i 3GPP-a (eng. *The 3rd Generation Partnership Project*) stalnim doradama i iscrpnim specifikacijama. Napokon, valja napomenuti kako je 3GPP odabrao upravo DIAMETER kao osnovni signalizacijski protokol za autentikaciju, autorizaciju i administraciju te upravljanje pokretljivošću unutar njihovog velikog projekta, višemedijskog podsustava zasnovanog na protokolu IP (eng. *IP Multimedia Subsystem, IMS*).

2.4. Funkcionalnosti protokola DIAMETER

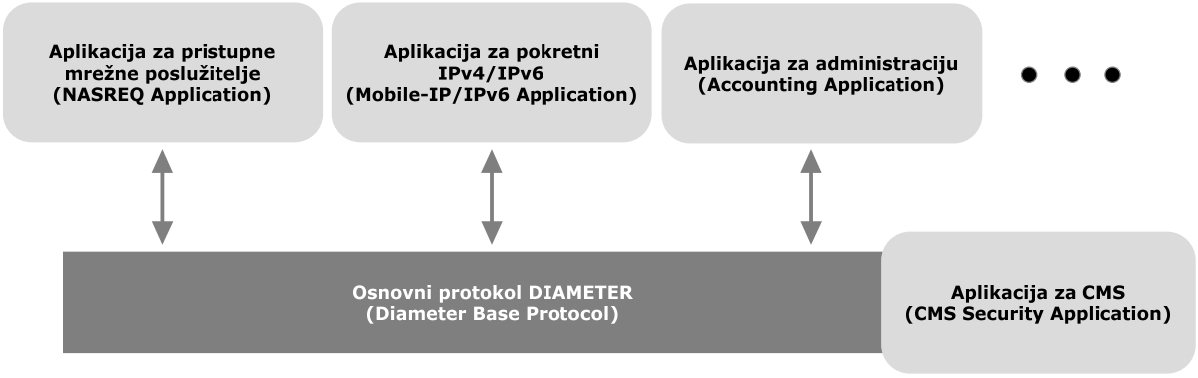
DIAMETER je protokol nove generacije koji pruža usluge autentikacije, autorizacije i administracije korisnika. U odnosu na svoje prethodnike, na čelu s protokolom RADIUS, DIAMETER nudi unaprjeđenja na području sigurnosti, pouzdanosti, skalabilnosti i fleksibilnosti u gotovo svim mogućim aspektima.

Neke od najvažnijih funkcionalnosti protokola DIAMETER i njegovih proširenja su:

- prijenos korisničkih autentikacijskih podataka i pružanje usluge autentikacije korisnika pomoću DIAMETER poslužitelja,
- razmjena karakterističnih autorizacijskih informacija između klijenata i poslužitelja, čime se ostvaruje provjera ovlasti korisničkog pristupa pojedinim resursima,
- razmjena i praćenje podataka o korištenim resursima radi administracije korisnika, naplate, planiranja i sl.,
- arhitektura temeljena na *peer-to-peer* modelu koja svakom elementu omogućuje pokretanje komunikacije,
- sigurnosni mehanizmi u slučaju ispada usluge, mreže ili primarnih poslužitelja (eng. *failover*) ostvareni pozitivnim potvrdama na aplikacijskom sloju, sigurnosnim algoritmima i mehanizmima dojave pogrešaka,
- sigurnost prijenosa podataka na transportnom i mrežnom sloju ostvarena podrškom za protokole IPsec i TLS,
- pouzdanost prijenosa podataka na transportnom sloju uporabom protokola TCP ili SCTP,
- implementacija vremenskih oznaka koje onemogućavaju napade ponavljanjem (eng. *replay attacks*),
- podrška za raznovrsne mrežne agente poput posrednika (eng. *Proxy*), preusmjeritelja (eng. *Redirect*) i agenata za prosljeđivanje podataka (eng. *Relay*),
- podrška za ostvarenje sigurnosti podatkovnih objekata (eng. *data object security*),
- ostvarenje sigurnosti "s kraja na kraj" uporabom CMS-a (eng. *Cryptographic Message Security*),
- mogućnost suradnje s RADIUS protokolom,
- mehanizmi obrade pogrešaka,
- mehanizmi otkrivanja mogućnosti klijentsko-poslužiteljskih elemenata arhitekture te dogovora oko istih,
- podrška za obavezne i neobavezne parove atributa i vrijednosti,
- dinamično otkrivanje i konfiguracija klijentsko-poslužiteljskih elemenata pomoću DNS-a,
- podrška za mrežnu pokretljivost i protokol Mobile IP,
- predodređen prostor za dodatna proširenja.

3. Arhitektura i rad protokola DIAMETER

Protokol DIAMETER osmišljen je kao kombinacija osnovnog protokola te širokog spektra aplikacija koje mu nude jednostavnu mogućnost proširenja za ostvarenje raznovrsnih dodatnih usluga. Takav koncept pregledno je prikazan na sljedećoj slici (Slika 2).



Slika 2. Odnos osnovnog protokola DIAMETER i njegovih aplikacija

Osnovni protokol nudi temeljne mehanizme i funkcionalnosti zajedničke svim aplikacijama. Većina njih temelji se na osnovnoj funkcionalnosti protokola RADIUS dok je ostatak rezultat novih rješenja i poboljšanja postojećih ideja. Konkretno, ovdje su definirani osnovni formati poruka, temeljni mehanizmi prijenosa podataka i upravljanja pogreškama, metode komunikacije između pojedinih elemenata arhitekture te osnovne sigurnosne funkcije.

Aplikacije ovdje nisu klasične programske aplikacije nego protokolna rješenja koja se nadovezuju na funkcionalnosti osnovnog protokola. Svaka aplikacija određena je posebnom oznakom i u osnovnu strukturu može unijeti nove naredbe i nove obavezne parove atributa i vrijednosti čime se stvaraju dodatne funkcionalnosti. Primjeri su aplikacija za podršku pokretnom IP-u (eng. *Diameter Mobile IPv4 Application, MobileIP*), aplikacija za pristupne mrežne poslužitelje (eng. *Diameter Network Access Server Application, NASREQ*), aplikacija za podršku protokola EAP (eng. *Diameter Extensible Authentication Protocol Application*), aplikacija za podršku kontrole naplate (eng. *Diameter Credit-Control Application*), aplikacija za CMS (eng. *Diameter Cryptographic Message Security Application*) te aplikacija za podršku protokola SIP (eng. *Diameter Session Initiation Protocol Application*). Više informacija o primjeni nekih od nabrojanih aplikacija nalazi se u posljednjem poglavlju dokumenta.

3.1. Elementi arhitekture

Arhitektura protokola DIAMETER temelji se na modelu *peer-to-peer*. Tako je svaki njen element ujedno i klijent i poslužitelj ovisno o trenutnim potrebama mreže. Elementi također mogu biti i mrežni agenti. Stoga, elemente arhitekture protokola DIAMETER po trenutnim ulogama i zaduženjima u mreži možemo podijeliti na klijente, poslužitelje i agente.

3.1.1. Klijenti i poslužitelji

Element koji primi zahtjev krajnjeg korisnika za spajanjem na mrežu automatski postaje klijent. U većini slučajeva klijent je ujedno i pristupni mrežni poslužitelj. Nakon prikupljanja korisničkih autentikacijskih podataka klijent šalje poruku s pristupnim zahtjevom jednom od elemenata arhitekture protokola DIAMETER koji će taj zahtjev poslužiti. Takav element u ovom slučaju bit će ili poslužitelj ili jedan od agenata. Pretpostavi li se da je spomenuti element poslužitelj, on će biti zadužen za mehanizme autentikacije korisnika temeljem primljenih podataka. Ako je autentikacija bila uspješna, konfiguracijski podaci i podaci vezani uz korisnički pristup bit će poslani natrag klijentu kao odgovor na pristupni zahtjev. U protivnom, zahtjev će se odbiti.

Ovako opisan postupak komunikacije između klijentskih i poslužiteljskih elemenata jako podsjeća na klasičnu arhitekturu protokola za autentikaciju, autorizaciju i administraciju temeljenu na

modelu klijent-poslužitelj. Arhitektura temeljena na *peer-to-peer* modelu puno je fleksibilnija jer dopušta da svaki od mrežnih elemenata bude ili klijent ili poslužitelj te obavlja i jedne i druge funkcije ovisno o potrebi.

3.1.2. Agenti

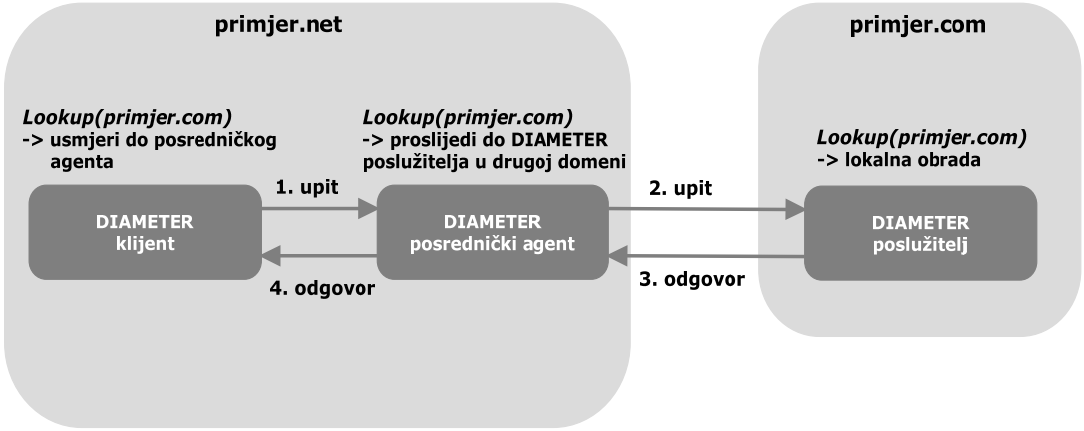
Osim klijenata i poslužitelja, važan dio arhitekture protokola DIAMETER su i agenti. Po svojoj ulozi, agenti mogu biti zaduženi za prosljeđivanje (eng. *Relay Agent*) i preusmjeravanje (eng. *Redirect Agent*), posredništvo (eng. *Proxy Agent*) te prevođenje (eng. *Translation Agent*) protokola.

Agenti zaduženi za prosljeđivanje:

Ovi agenti koriste se za prosljeđivanje poruka na odgovarajuće odredište, ovisno o informacijama dobivenim iz pristigle poruke. Jedna od njihovih prednosti sposobnost je prikupljanja i agregacije zahtjeva pristiglih iz različitih domena i područja te njihovo usmjeravanje prema zajedničkom odredišnom području. Time se eliminiraju zahtjevni postupci konfiguracije pristupnih poslužitelja za svaku promjenu poslužiteljskog elementa DIAMETER mreže.

Posrednički agenti:

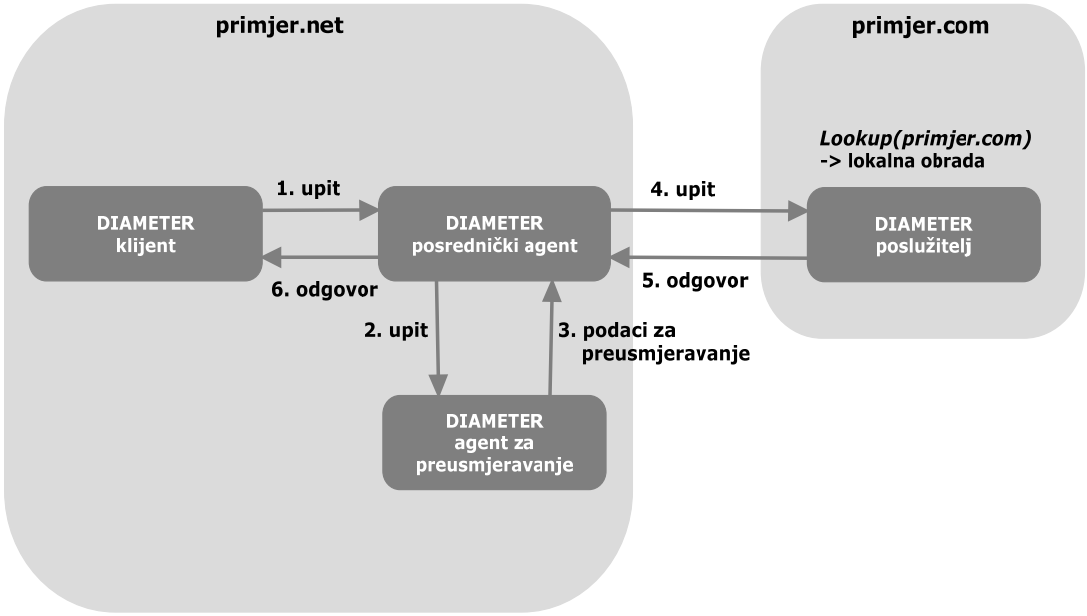
Posrednički agenti također se koriste za prosljeđivanje poruka no, za razliku od agenata zaduženih samo za prosljeđivanje, sposobni su i za promjenu sadržaja tih poruka. To omogućuje ostvarenje brojnih usluga dodane vrijednosti (eng. *Value-Added Services*), uvođenje pravila obrade ovisno o pojedinim porukama te obavljanje administrativnih zadataka za pojedino područje ili domenu. Na sljedećoj slici (Slika 3) može se vidjeti mehanizam kojim posrednički agent prosljeđuje poruku prema drugoj domeni. U slučaju da ovdje nije potrebno mijenjati sadržaj poruke, ulogu posredničkog agenta može preuzeti i agent zadužen za prosljeđivanje.



Slika 3. Rad posredničkog agenta

Agenti zaduženi za preusmjeravanje:

Ovi agenti služi kao središnji konfiguracijski repozitoriji za sve ostale elemente DIAMETER arhitekture. Po primitku poruke agent provjerava svoju tablicu usmjeravanja i kao odgovor šalje informacije vezane uz preusmjeravanje. Ostali elementi tako ne trebaju imati lokalno implementirane tablice usmjeravanja već uvijek mogu poslati poruke agentima zaduženim za njihovo preusmjeravanje. Slika na sljedećoj stranici (Slika 4) prikazuje rad agenta ovog tipa.

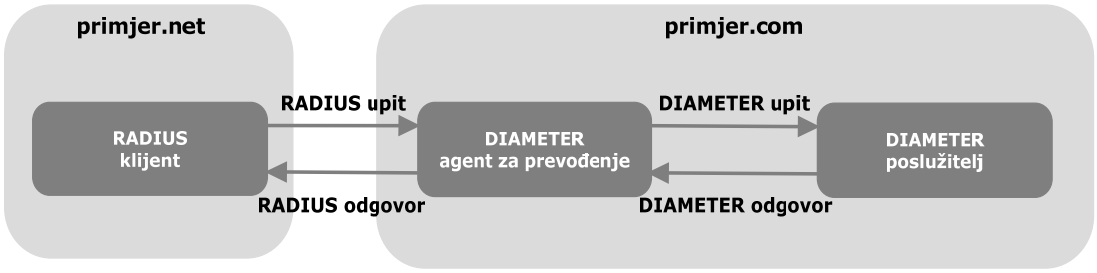


Slika 4. Rad agenta zaduženog za preusmjeravanje

Scenarij prikazan na gornjoj slici gotovo je identičan onom na slici prije, s tom razlikom da ovdje posrednički agent ne zna adresu poslužitelja kojem treba proslijediti poruku pa tu informaciju saznaje pomoću agenta zaduženog za preusmjeravanje.

Agenti zaduženi za prevođenje:

Ovi agenti predstavljaju posebnu vrstu agenata unutar arhitekture protokola DIAMETER. Njihova je zadaća prevođenje poruka raznih protokola za autentikaciju, autorizaciju i administraciju u poruke protokola DIAMETER i obrnuto. Ova funkcionalnost vrlo je korisna pri integraciji s ostalim, trenutno više korištenim, protokolima za autentikaciju, autorizaciju i administraciju koje predvodi protokol RADIUS. Na sljedećoj slici (Slika 5) prikazan je rad agenta zaduženog za prevođenje poruka protokola RADIUS u protokol DIAMETER i obratno.



Slika 5. Rad agenta zaduženog za prevođenje

3.2. Struktura paketa i poruke

Poruke protokola DIAMETER osnovno su sredstvo komunikacije između elemenata protokolne arhitekture. Osnovni protokol DIAMETER koristi preko deset različitih poruka za ostvarenje temeljnih funkcionalnosti. One se međusobno razlikuju po kodu naredbe. Neki primjeri su poruka *Accounting-Request* koja označava da paket sadrži podatke vezane uz administraciju korisnika te poruka *Capability-Exchange-Request* koja označava da paket sadrži podatke s opisom mogućnosti određenog elementa protokolne arhitekture. Ostatak poruka koje koristi osnovni protokol DIAMETER popisan je u sljedećoj tablici (Tablica 1).

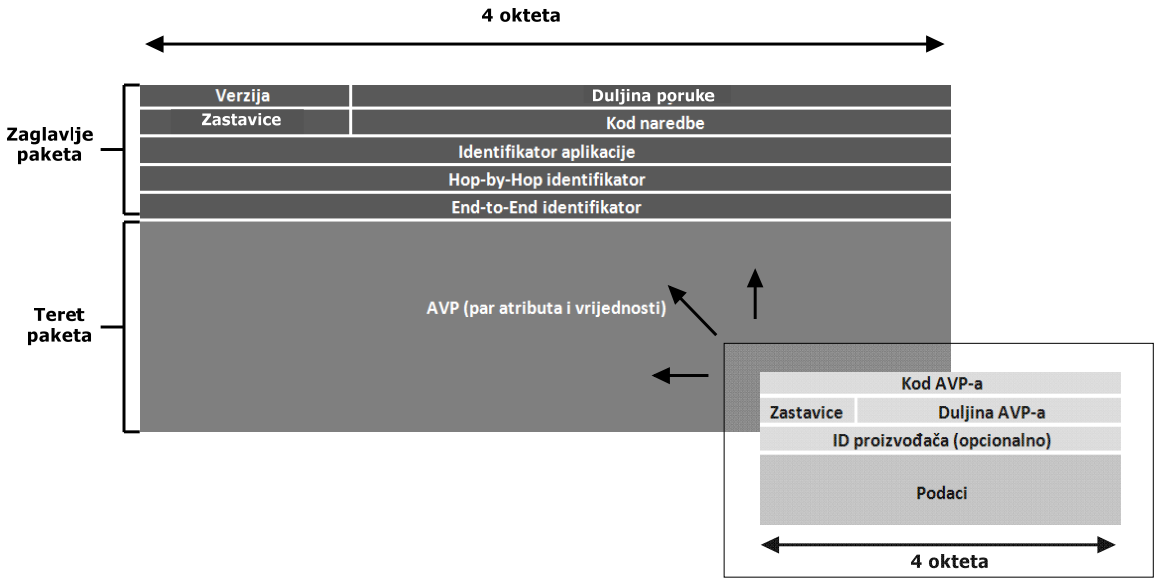
Naziv poruke:	*Kratica:*	*Kod naredbe:*
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Capabilities-Exchanging-Request	CER	257
Capabilities-Exchange-Answer	CEA	257
Device-Watchdog-Request	DWR	280
Device-Watchdog-Answer	DWA	280
Disconnect-Peer-Request	DPR	282
Disconnect-Peer-Answer	DPA	282
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258
Session-Termination-Request	STR	275
Session-Termination-Answer	STA	275

Tablica 1. Poruke osnovnog protokola DIAMETER

U gornjoj tablici može se primijetiti da svaki zahtjev ima odgovarajući odgovor s kojim dijeli kod naredbe. Razlog je implementacija sinkronog mehanizma razmjene poruka.

Kod naredbe koristi se pri određivanju tipa poruke koja se u nekom paketu prenosi i nalazi se u njegovu zaglavlju. Konkretni podaci koji se paketom prenose nalaze se u teretu paketa u obliku skupa parova atributa i njihovih vrijednosti (eng. *Attribute-Value-Pair, AVP*). Protokol DIAMETER definira skup osnovnih atributa i svakom od njih pridjeljuje odgovarajuću semantiku. Parovi atributa i vrijednosti prenose sve podatke vezane uz autentikaciju, autorizaciju, administraciju te usmjeravanje, sigurnost i opis mogućnosti između para elemenata protokolne arhitekture. Dodatno, svaki par atributa i vrijednosti povezan je s posebnim podatkovnim formatom također definiranim unutar protokola DIAMETER pa vrijednosti moraju odgovarati pridruženim formatima.

Na sljedećoj slici (Slika 6) nalazi se prikaz strukture paketa protokola DIAMETER.



Slika 6. Struktura paketa protokola DIAMETER

Osim opisanog koda naredbe, u zaglavlju paketa mogu se primijetiti polje za oznaku verzije protokola (stavlja se vrijednost 1 za oznaku prve verzije protokola DIAMETER), duljina poruke (tri okteta koja sadrže podatak o duljini poruke), zastavice za postavljanje specifičnih parametara, identifikator aplikacije (četiri

okteta koja sadrže informaciju o aplikacijama koje koriste navedenu poruku), *Hop-by-Hop* identifikator (pomoć kod pridruživanja zahtjeva i odgovora) te *End-to-End* identifikator (pomoć pri otkrivanju višestrukih poruka).

3.3. Rad protokola

3.3.1. Otkrivanje čvorova

U klasičnoj arhitekturi protokola za autentikaciju, autorizaciju i administraciju bila je nužna ručna konfiguracija pristupnog mrežnog poslužitelja kako bi on posjedovao adresu AAA-poslužitelja kojem bi slao zahtjeve kod prijave korisnika. Takvi postupci mogu biti prilično naporni u složenim i velikim mrežama.

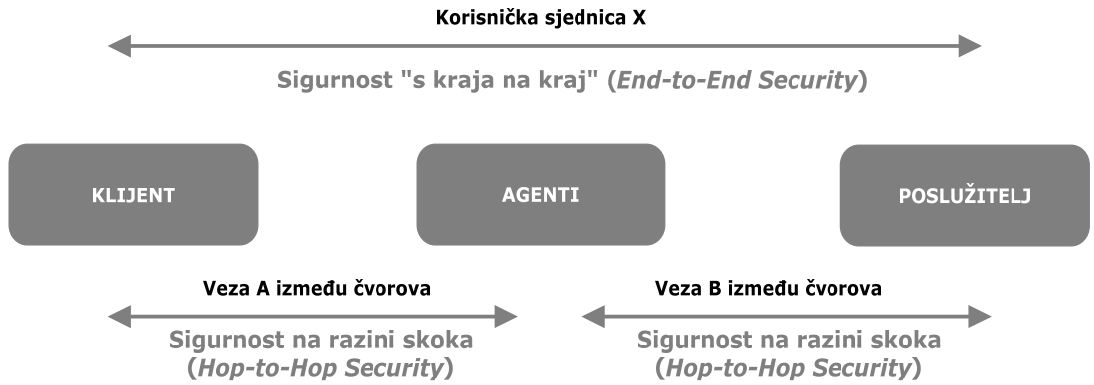
Uz podršku ručnoj konfiguraciji, protokol DIAMETER donosi mogućnost dinamičnog otkrivanja ostalih DIAMETER čvorova (eng. *peers*). Dinamično otkrivanje moguće je s obzirom na činjenicu da DIAMETER poslužitelji i agenti razašilju poruke s obavijestima o vlastitim mogućnostima i podržanom stupnju sigurnosti obližnjim elementima. Klijenti tako, ovisno o korištenim aplikacijama, traženom stupnju sigurnosti i ostalim parametrima, mogu odabrati odgovarajući čvor kojem će proslijediti korisnički upit. Za pojedini element (u ovom slučaju za klijenta) novootkrivena lokacija odgovarajućeg čvora pohranjuje se lokalno preko tablice čvorova (eng. *Peer Table*) i tablice usmjeravanja čvorovima (eng. *Peer Routing Table*).

3.3.2. Tijek sjednice

Nakon otkrića odgovarajućeg čvora kojem će se zahtjev proslijediti potrebno je uspostaviti vezu s tim čvorom jer DIAMETER na transportnom sloju koristi protokole TCP ili SCTP. U odnosu na UDP ovi protokoli pružaju pouzdan prijenos vrlo važan za aplikacije koje izmjenjuju podatke vezane uz administraciju.

S obzirom na *peer-to-peer* model, pojedini DIAMETER čvor može imati i više uspostavljenih veza u jednom trenutku. Protokol DIAMETER eksplicitno definira da u jednom trenutku pojedini čvor mora uspostaviti barem dvije veze prema čvorovima unutar istog područja ili domene koji onda postaju primarnim i sekundarnim kontaktnim čvorom.

Radi boljeg razumijevanja rada protokola DIAMETER valja razlikovati pojmove veze i sjednice. Na sljedećoj slici (Slika 7) prikazana je razlika između tih koncepata.



Slika 7. Veza i sjednica u protokolu DIAMETER

Veza i sjednica razlikuju se u tome što sjednica predstavlja povezanost DIAMETER čvorova na logičkoj razini i može sadržavati više uspostavljenih veza. Sjednica se može zamisliti kao slijed poruka razmijenjenih između klijentskog i poslužiteljskog čvora u određenom vremenskom periodu. Svaka sjednica određena je jedinstvenim identifikatorom *Session-Id* kojeg stvara klijent.

Pokretanje sjednice:

Pokretanje sjednice slično je kao kod većine klijentsko-poslužiteljskih modela. Sjednica počinje slanjem zahtjeva klijenta poslužitelju. U kontekstu protokola DIAMETER klijent poslužitelju šalje

poruku *Auth-Request* koja, između ostalog, sadrži i identifikator sjednice. U slučaju da je potrebno proslijediti poruku, ona na putu do poslužitelja prolazi odgovarajućim agentima. Valja napomenuti da poruka *Auth-Request* nije definirana u skupu poruka osnovnog protokola DIAMETER jer atributi koje prenosi ovise o aplikaciji koja se koristi.

Nakon prihvaćanja poruke *Auth-Request* poslužitelj u odgovor može uključiti atribut *Authorization-Lifetime* koji određuje količinu vremena (u sekundama) unutar kojeg klijent mora biti ponovno autoriziran. Nakon eventualnog isteka vremenske kontrole poslužitelj briše sjednicu iz liste aktivnih sjednica i oslobađa sve za nju rezervirane resurse.

Trajanje sjednice:

Tijekom trajanja sjednice poslužitelj može započeti postupak ponovne autentikacije ili ponovne autorizacije. Ovaj postupak koristan je za praćenja trenutne aktivnosti korisnika radi naplate kod, primjerice, *prepaid* usluga. Za kontrolu sjednice i praćenje uzroka eventualnih nepredviđenih prekida koristi se atribut *Origin-State-Id*.

Ostatak komunikacije između klijenta i poslužitelja koji uključuje dogovore oko svih potrebnih korisničkih parametara ili razmjenu informacija za pružanje i izvršavanje ostalih usluga također se obavlja preko različitih parova atributa i njihovih vrijednosti definiranih u pojedinim aplikacijama.

Prekid sjednice:

Poruke vezane uz prekid sjednice koriste se samo kod pružanja usluga autentikacije i autorizacije i to onda kada se prati i održava stanje sjednice. Za usluge administracije koriste se poruke za prekid administracije.

Prekid sjednice može započeti ili klijent ili poslužitelj. Želi li klijent prekinuti sjednicu, poslužitelju će poslati poruku *Session-Termination-Request* u koju je uključen atribut *Termination-Clause* koji sadrži opis razloga prekida sjednice. Želi li to učiniti poslužitelj (npr. zbog administrativnih razloga), poslat će klijentu poruku *Abort-Session-Request*. Ipak, postoje situacije kada klijent nije obvezan prekinuti sjednicu po primitku poruke za prekid sjednice od poslužitelja. Sjednica se prekida odgovorom na zahtjeve za prekidom čvorova koji su ih zaprimili.

4. Usporedba protokola DIAMETER i RADIUS

Već je spomenuto kako je protokol DIAMETER nastao na temelju protokola RADIUS te da je po svojoj funkcionalnosti zapravo njegov punokrvni nasljednik. Premda je funkcionalnost vrlo slična, način na koji je ostvaren te brojna proširenja koja su pridodana protokolu DIAMETER, ipak čine razlike između navedenih protokola značajnim. U ovom poglavlju dana je usporedba navedenih protokola po sljedećim kategorijama:

- autentikacija,
- autorizacija,
- administracija i
- općenite razlike.

4.1. Autentikacija

Autorizacija bez postupka autentikacije:

Protokol RADIUS ne podržava ovakav način autorizacije s obzirom na činjenicu da za slanje klijentskih upita zahtijeva barem neki oblik autentikacijskih podataka. Protokol DIAMETER ovdje ne inzistira na slanju autentikacijskih podataka u upitima. Valja napomenuti kako je autorizacija bez autentikacije jedan od trenutnih zahtjeva IETF-ove radne grupe NASREQ (eng. *Network Access Server Requirements*) koja se bavi uslugama podržanim na pristupnim mrežnim poslužiteljima. Jednostavno, poslužitelji ovako ne moraju popunjavati upite inače neupotrebljivim, lažnim autentikacijskim podacima kako bi se zaobišlo to ograničenje.

Podrška za PAP (eng. Password Authentication Protocol):

Premda je PAP danas prilično nesiguran protokol, mnoge aplikacije i dalje ga koriste. Tako se javlja potreba da protokoli za autentikaciju, autorizaciju i administraciju sigurno prenose obične, tekstualne lozinke velikim i često pokretnim mrežama. Da bi to bilo ostvarivo, tajnost lozinki mora biti osigurana. Takve lozinke ne smiju biti izložene posredničkim poslužiteljima koji se nalaze duž staza usmjeravanja. S obzirom na to da protokol RADIUS podržava samo sigurnost na razini skoka između pojedinih mrežnih čvorova (eng. *hop-by-hop security*), ne može spriječiti izlaganje lozinki posredničkim poslužiteljima niti osigurati tajnost lozinke "s kraja na kraj". Protokol DIAMETER to ostvaruje pomoću aplikacije za CMS.

Napadi ponavljanjem i uskraćivanjem usluge:

S obzirom na činjenicu da RADIUS nema implementiranu mogućnost autentikacije "s kraja na kraj", ne postoji način obrane od napada ponavljanjem. Konkretno, neispravan poslužitelj ili zlonamjerni korisnik mogu neprekidno ponavljati slanje starih paketa bez mogućnosti opažanja. Postupak može uzrokovati nemogućnost pružanja daljnje usluge na opterećenom poslužitelju. Također, napadi ponavljanjem mogu prouzročiti slanje višestrukih administrativnih poruka čime se remeti praćenje potrošenih korisničkih resursa, a samim time, primjerice, i naplata. Protokol DIAMETER pruža učinkovite mehanizme obrane od napada ponavljanjem utjelovljene pomoću vremenskih oznaka i CMS-a.

Obavezni dijeljeni tajni ključ:

Protokol RADIUS zahtijeva postojanje dijeljenog tajnog ključa između klijenata i poslužitelja. Kod podrške za pokretljivost ovo predstavlja popriličan problem. Naime, pretpostavi li se kretanje čvorova između različitih administrativnih cjelina, u tom slučaju bi tajni ključ, jednak onom domaćeg poslužitelja pokretnog čvora, trebali posjedovati svi agenti u domenama kroz koje je taj pokretni čvor prošao. Samim time, baze podataka agenata sadržavale bi praktički beskonačne količine tajnih ključeva korisnika. Protokol DIAMETER ne koristi mehanizme dijeljenog tajnog ključa već se oslanja na IPSec i TLS kako bi osigurao povjerljivost komunikacije klijenata i poslužitelja.

4.2. Autorizacija

Podrška za RADIUS prilaze (eng. RADIUS gateway capability):

Već je nekoliko puta spomenuto kako je protokol RADIUS trenutno najkorišteniji protokol za autentikaciju, autorizaciju i administraciju. Stoga je ključno da eventualni nasljednici što jednostavnije surađuju s njim. Ovdje su ključni elementi RADIUS prilazi. Protokol DIAMETER u principu ima ostvarenu podršku za rad s protokolom RADIUS preko takvih elemenata, no kompatibilnost još uvijek nije potpuna. Brojni IETF-ovi zahtjevi za proširenjem osnovnog protokola DIAMETER u kombinaciji s različitim implementacijama i verzijama protokola RADIUS ponekad ipak uzrokuju međusobnu nekompatibilnost.

Uskladivost stanja (eng. State-Reconciliation):

Posjedovanje ovog svojstva kod protokola za autorizaciju, autentikaciju i administraciju znači da njihovi poslužitelji pomažu klijentima pri obavljanju simultane kontrole korisničke prijave, ograničenjima uporabe pojedinih priključnica, ograničenjima kod tuneliranja te smanjenju vremena spajanja. Sve skupa je moguće osigura li se oporavak stanja u slučajevima gubitka podataka kod ispada ili grešaka u sustavu. To se obično ostvaruje porukama za praćenje stanja sjednice ili resursa te porukama za osvježavanje ili prekid veze. Protokol RADIUS ne sadrži naredbe koje bi se mogle primijeniti za ostvarenje takvih poruka. Također, zbog modela arhitekture svaki element nije u mogućnosti samostalno započeti komunikaciju slanjem poruka bez prethodnog upita. Protokol DIAMETER već u svojoj osnovnoj specifikaciji podržava potrebne poruke.

Poslužiteljem potaknut prekid komunikacije:

Protokol DIAMETER sadrži niz poruka koje se mogu koristiti prilikom nepredviđenih prekida komunikacije, najčešće potaknutih s poslužiteljske strane. U najnovijim verzijama RADIUS također sadrži niz poruka za prekid veze no bez mogućnosti da takve poruke budu poslane s poslužitelja.

Ponovna autorizacija na zahtjev:

Ponovna autorizacija na zahtjev odnosi se na mogućnost ponovnog traženja autorizacije klijenta ili poslužitelja. Protokol RADIUS podržava tek mogućnost periodične ponovne autorizacije i to bez prethodnih zahtjeva. DIAMETER ju podržava u potpunosti kroz svoj sjednički orijentiran, *peer-to-peer* odnos između "klijenata" i "poslužitelja".

4.3. Administracija

Potpora za slanje netraženih poruka (eng. support of unsolicited messages):

Netražene poruke, u ovom kontekstu, bile bi poruke koje nisu odgovor na neki eksplicitan upit. Protokol RADIUS ne dozvoljava poslužiteljima slanje ovakvih poruka klijentima. Ograničenje prvenstveno proizlazi iz arhitekture temeljene na klasičnom modelu klijent-poslužitelj gdje su isključivo klijenti ti koji šalju upite (netražene poruke). S obzirom na različit model arhitekture, kod DIAMETER-a je to jednostavno omogućeno. Naime, u *peer-to-peer* arhitekturi svaki čvor ujedno je i klijent i poslužitelj, pa samim time i u bilo kojem trenutku bez prethodnog upita može poslati poruku nekom drugom čvoru. Ovo svojstvo najčešće se koristi za potrebe administracije, u trenucima kada pristupni mrežni poslužitelj treba prekinuti određenu korisničku sjednicu ili za podršku uslugama gdje podatke o sjednici treba mijenjati tijekom njena trajanja.

4.4. Općenite razlike

Skalabilnost:

O nedostatku skalabilnosti protokola RADIUS već je bilo riječi. Osnovni problem leži u veličini polja za oznaku sjednica u zaglavljima RADIUS paketa. Predodređena veličina od jednog okteta jednostavno je premalena za današnje potrebe. Protokol DIAMETER za identično polje ima osigurana četiri okteta i drugačiju filozofiju njegova korištenja čime je zahtjev vezan uz skalabilnost ispunjen.

Tajnost podatkovnih objekata:

Protokol RADIUS ne može pružiti tajnost poruka "s kraja na kraj" što posredničkim poslužiteljima omogućuje dohvat nezaštićenih podataka. S druge strane, DIAMETER omogućuje takav stupanj zaštite čime su podaci sigurni čak i kada putuju kroz razne posredničke poslužitelje.

Integritet podatkovnih objekata:

Slično kao i do sada, protokol RADIUS ne podržava zaštitu integriteta podataka "s kraja na kraj", a protokol DIAMETER to ostvaruje uporabom CMS-a.

Transparentnost prijenosa:

Pri uporabi posredničkih poslužitelja, protokol DIAMETER omogućuje praćenje njihova usmjeravanja kroz mrežu. Protokol RADIUS to ne podržava.

Proširivost:

Osnovno ograničenje proširivosti protokola RADIUS može se pronaći u ograničenju broja atributa koje prosječan paket ovog protokola može prenijeti. Takvo ograničenje nastalo je zbog veličine polja oznake broja atributa od samo jednog okteta. Kod protokola DIAMETER veličina sličnog polja iznosi ponovno četiri okteta. Usporedbe radi, RADIUS omogućuje najviše 256 parova atributa i vrijednosti po paketu, a DIAMETER njih čak 2^{32}. RADIUS, također, omogućuje uporabu višestrukih atributa istog tipa što je prilično nepovoljno za poslužitelje i klijente koji trebaju odrediti jesu li višestruki identični atributi zapravo jedan fragmentirani ili više neovisnih. Također, premda protokol RADIUS podržava atribute specifične za razne proizvođače (eng. *vendor-specific attributes*), ne podržava takve naredbe (eng. *vendor-specific commands*). Protokol DIAMETER podržava i te naredbe kroz aplikacije koje proizvođači mogu ostvariti.

Sigurnost na razini skoka (eng. Hop-by-Hop security):

Protokol RADIUS koristi sigurnost na razini skoka što znači da svakim sljedećim skokom mreža posredničkih poslužitelja dodaje autentikacijske podatke koje koristi sljedeći element na putu usmjeravanja. S obzirom na to da svaki takav skok mijenja poruku koja se prenosi, javlja se već spomenuta nemogućnost ostvarenja sigurnosti "s kraja na kraj". DIAMETER ne podržava sigurnost na razini skoka.

Postupci retransmisije:

Postupci retransmisije ostvareni kod protokola RADIUS prilično su komplicirani i stvaraju dodatno kašnjenje te iziskuju dodatne poslužiteljske resurse. Ponovno je razlog način na koji je ostvareno praćenje i identificiranje pojedinih transmisija. S druge strane, DIAMETER koristi pouzdane protokole na transportnom sloju koji automatski nude mehanizme retransmisije čime se smanjuje pritisak na poslužiteljske resurse.

Kontrola toka prema poslužiteljima:

Kod protokola RADIUS kontrola toka zbog uporabe protokola UDP praktički je nepostojeća. Uporaba pouzdanih transportnih protokola poput TCP-a ili SCTP-a protokolu DIAMETER omogućuje kontrolu toka prvenstveno mehanizmom klizećih prozora.

Zahtjevi veličine zaglavlja:

Većina današnjih procesora optimalno radi s objektima podešenim tako da im je veličina višekratnik od 32 bita. Svaki noviji IETF-ov protokol zahtijeva upravo tako uređene podatke. Tako i protokol DIAMETER zahtijeva postavljanje veličine svih zaglavlja i podataka na višekratnik od 32 bita. Suprotno njemu, protokol RADIUS nema zahtjeve takve vrste čime se dodatni teret stavlja upravo na poslužitelje koji sporije obrađuju takve pakete.

Ignoriranje i odbacivanje paketa (eng. silent discarding of packets):

Politika protokola RADIUS je takva da se sve poruke koje ne sadrže očekivanu informaciju ili sadrže pogreške ignoriraju i odbacuju. Tako može doći do slučaja da pristupni mrežni poslužitelj pretpostavi da

mu je lokalni RADIUS poslužitelj postao nepristupačan jer ne dobiva nikakve odgovore na poslani upit. Posljedica toga ponovno je slanje svih neodgovorenih zahtjeva s pristupnog poslužitelja, ali drugim poslužiteljima. No niti oni neće promijeniti općenitu politiku ignoriranja i odbacivanja te pristupni usmjeritelj ponovno neće dobiti odgovor. Sve skupa ponavljat će se dok pristupni poslužitelj napokon ne odustane od upita. Takva situacija jasno pokazuje nedostatke opisane filozofije. Uz iznimku nekoliko pogrešaka vezanih uz sigurnost, protokol DIAMETER zahtijeva da svaka poruka bude potvrđena ili pozitivnim odgovorom ili odgovorom koji sadrži šifru i opis greške. Pristupni poslužitelji tako odmah saznaju kada i u kojoj poruci je došlo do pogreške.

5. Primjena i budućnost

Premda je na tržištu protokola za autentikaciju, autorizaciju i administraciju i dalje najpopularniji protokol RADIUS, njegova popularnost i dominacija imaju izraženu tendenciju pada. Osnovni razlog tome sve su izraženija ograničenja koja se posebno očituju razvojem novih i sve popularnijih tehnologija.

Samim time, nameće se pitanje protokola koji će ga zamijeniti. S obzirom na trenutne prednosti, uvedena poboljšanja, fleksibilnost i proširivost, IETF-ovu i 3GPP-ovu podršku te podršku velikih kompanija kao što su Microsoft, Sun Microsystems, Nortel Networks, LM Ericsson, Cisco Systems, Nokia Research Center, Blackstorm Networks, Merit Networks i ostali, vrlo su veliki izgledi da ta uloga pripadne upravo protokolu DIAMETER.

Trenutna primjena protokola DIAMETER može se podijeliti na standardnu uporabu vezanu uz osnovne funkcionalnosti autentikacije, autorizacije i administracije korisnika te na pružanje proširenih AAA-usluga u suvremenim pokretnim mrežama i mrežama temeljenim na novim tehnologijama. Velik udio trenutne primjene protokola DIAMETER i njegovih aplikacija otpada na pružatelje mrežnih usluga i mrežne operatore koji svojim korisnicima moraju omogućiti usluge autentikacije, autorizacije i administracije. Kod njih se prilično jasno očituje trend prelaska s uporabe izvornih AAA-protokola na AAA-protokole nove generacije. Značajna prednost protokola DIAMETER ovdje je njegova mogućnost suradnje s protokolom RADIUS i ostalim izvornim AAA-protokolima što uvelike olakšava spomenutu tranziciju.

U nastavku poglavlja bit će opisane neke od najvažnijih aplikacija koje protokolu DIAMETER omogućuju proširenu primjenu i podršku za nove usluge i tehnologije. Osim toga bit će opisano i trenutno najznačajnije područje primjene protokola DIAMETER - primjena unutar 3GPP-ova IMS-a, višemedijskog podsustava zasnovanog na protokolu IP.

5.1. Najznačajnije aplikacije protokola DIAMETER

Iako u svim implementacijama protokol DIAMETER koristi osnovnu verziju protokola, ona se nikada ne koristi samostalno. Prema specifikacijama, osnovni protokol uvijek se koristi proširen barem jednom aplikacijom.

Trenutno najznačajnije aplikacije za proširenje osnovnog protokola DIAMETER su aplikacija za podršku pokretnom IP-u, aplikacija za pristupne mrežne poslužitelje i aplikacija za CMS, tj. redom *Mobile-IP*, *NASREQ* i *CMS Security*.

5.1.1. Aplikacija za podršku pokretnom IP-u

Mobile-IP predstavlja mehanizam kojim pokretni čvor može mijenjati točke pristupa Internetu koje se nalaze u različitim domenama ili podmrežama bez promjene izvorne IP adrese. Da bi pokretni čvor uopće mogao dobiti pristup mrežnim resursima, potrebni su postupci autentikacije i autorizacije za što se koristi AAA-arhitektura. Takva arhitektura može se koristiti i za distribuciju sigurnosnih ključeva kako bi se osiguralo prelaženje korisnika iz domaće u stranu mrežu (eng. *roaming*), potporu mehanizama pokretljivosti i optimizaciju postupaka autentikacije, autorizacije i upravljanja pokretljivošću. Protokoli za autentikaciju, autorizaciju i administraciju poput protokola DIAMETER omogućuju pokretnim korisnicima prelaženje iz jedne mreže u drugu i dohvaćanje adekvatnih usluga ovisno o mjestu gdje se nalaze bez obzira na to jesu li u domaćoj ili stranoj mreži. Funkcionalnosti protokola DIAMETER u kombinaciji s mehanizmima pokretnog IP-a omogućuju tako daljnji razvoj protokola *Mobile-IP* prvenstveno u pogledu komunikacije između mreža ili pojedinih domena.

Aplikacija za podršku pokretnom IP-u proširuje osnovni protokol DIAMETER kako bi omogućila DIAMETER poslužiteljima da učinkovito vrše mehanizme autentikacije, autorizacije i prikupljanja podataka za naplatu i administraciju korisnika u pokretnim mrežama temeljenim na protokolu *Mobile IPv4*. U kombinaciji s mehanizmima komunikacije između pojedinih domena koje nudi osnovni protokol DIAMETER, pokretnim čvorovima nudi se mogućnost primanja usluga unutar stranih mreža ili domena. Sama aplikacija određuje način na koji domaći i strani agenti razmjenjuju podatke o administraciji korisnika kako bi prenijeli korisničke podatke prema DIAMETER poslužiteljima.

5.1.2. Aplikacija za pristupne mrežne poslužitelje

Ovo proširenje definira skup naredbi za autentikaciju i autorizaciju kojima se omogućuje podrška za protokole CHAP (eng. *Challenge-Handshake Authentication Protocol*), PAP (eng. *Password Authentication Protocol*) i EAP (eng. *Extensible Authentication Protocol*), te poboljšanje njihovih mehanizama. Svrha te aplikacije pružanje je učinkovitih usluga autentikacije, autorizacije i administracije u okruženju temeljenom na *dial-in* PPP tehnologijama, najčešće implementiranih na pristupnom mrežnom poslužitelju.

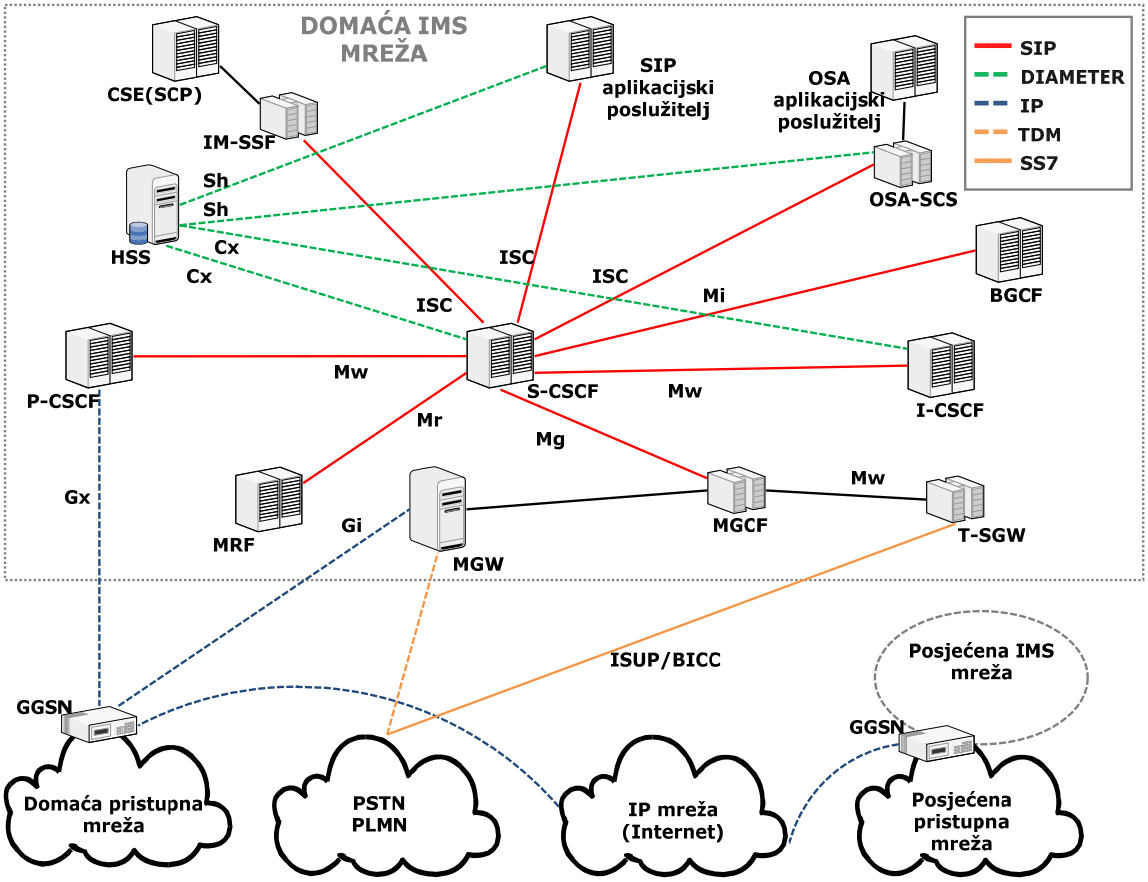
5.1.3. Aplikacija za CMS

Osnovni protokol DIAMETER omogućuje sigurnost komunikacije unutar mrežne arhitekture po principu “skok po skok“. CMS omogućuje pojačanu sigurnost osnovnog protokola definiranjem načina učahurivanja CMS-ovih objekata u klasične parove atributa i vrijednosti. Dvije osnovne tehnike koje CMS koristi su metoda digitalnih potpisa i metoda šifriranja podataka. Digitalni potpisi zajedno s digitalnim certifikatima omogućuju mehanizam autentikacije, zaštite integriteta i očuvanja neporecivosti (sudionici ne mogu poreći aktivnosti u kojima su sudjelovali). Šifriranje podataka omogućuje očuvanje njihove povjerljivosti. Implementacija obje metode istovremeno omogućuje protokolu DIAMETER učinkovitu zaštitu “s kraja na kraj“.

5.2. Primjena unutar IMS-a

Opisane prednosti protokola DIAMETER na čelu s onima koje se tiču pružanja usluga autentikacije, autorizacije i administracije unutar pokretnih mreža jedan su od osnovnih razloga zbog kojih se 3GPP posvetio njegovu razvoju. DIAMETER je odabran kao osnovni signalizacijski protokol za spomenute usluge unutar IMS-a. Višemedijski podsustav zasnovan na protokolu IP ili IMS, sustav je koji obuhvaća sve elemente jezgrene mreže koji omogućuavaju pružanje višemedijskih usluga. Trenutno se IMS koristi kod pokretnih mreža treće generacije no budući planovi njegove uporabe odnose se na okosnicu arhitekture koja će podržati konvergenciju usluga iz fiksnih, bežičnih, pokretnih i privatnih mrežnih sustava. IMS nudi relativno siguran posredni pristup uslugama dodane vrijednosti i mrežnim resursima koji se nalaze unutar jezgrene mreže temeljene na protokolu IP uz otvoreno sučelje za vanjske davatelje usluge i platformu za usluge samih mrežnih operatera.

Arhitektura IMS-a i položaj protokola DIAMETER unutar takve arhitekture prikazani su na sljedećoj slici (Slika 8).



Slika 8. Arhitektura IMS-a i najvažnija sučelja

Čvor označen kao HSS (eng. *Home Subscriber Server*) je poslužitelj koji sadrži bazu podataka s popisom svih domaćih pretplatnika i njihovih podataka poput korisničkih identifikatora, upravljačkih informacija vezanih uz autentikaciju i autorizaciju korisnika, podataka vezanih uz trenutnu lokaciju u mreži i podatke vezane uz korisničke profile.

Čvor koji je označen kao CSCF (eng. *Call Session Control Function*) predstavlja element s ugrađenom funkcijom za upravljanje sjednicom poziva. Njegova je zadaća upravljanje sjednicama temeljeno na protokolu SIP (eng. *Session Initiation Protocol*). Signalizacija protokolom SIP koristi se, primjerice, prilikom registracije korisnika u domaćoj mreži preko S-CSCF-a (eng. *Serving Call Session Control Function*). Sam S-CSCF koristi protokol DIAMETER na sučelju Cx kako bi zatražio potrebne autorizacijske podatke od HSS-a, radi potvrde korisničke registracije te kako bi prikupio ostale korisničke podatke iz domaćeg poslužitelja.

Protokol DIAMETER također se koristi i na sučelju Sx koje koriste aplikacijski poslužitelji ili OSA prilazi kako bi prikupili ili osvježili podatke o pretplatničkim profilima ili korisničke podatke koje koriste zajedničke baze podataka.

Naplata korištenja usluga u IMS-u također je ostvarena preko protokola DIAMETER.

5.3. Budućnost razvoja

Budući trendovi razvoja protokola DIAMETER odnose se prije svega na daljnja poboljšanja postojećih rješenja razvojem novih i učinkovitijih aplikacija. Također, očekuje se i brži razvoj dodatnih proširenja koja će osnovnom protokolu omogućiti neke nove funkcionalnosti s obzirom na pojavu novih i naprednijih usluga. Cjelokupni proces daljnjeg razvoja svakako će nadgledati IETF i 3GPP, a nova rješenja bit će jasno i precizno specificirana odgovarajućim dokumentima. Vjerojatno najveći utjecaj na popularnost i daljnji razvoj ovog protokola imat će svakako uspjeh IMS-a te ideje da upravo tako zamišljen sustav posluži kao okosnica sveobuhvatnoj i sveprisutnoj mreži budućnosti.

6. Zaključak

Trendovi razvoja novih tehnologija i usluga svakim danom postavljaju nove izazove ostvarenju mehanizama autentikacije, autorizacije i administracije. Jasno je kako su ti mehanizmi danas prijeko potrebni zbog načina rada samih usluga i zbog stupnja sigurnosti kojeg one moraju ponuditi.

Protokoli koji su svih ovih godina bili zaduženi za ostvarenje navedenih mehanizama danas jednostavno ne mogu u potpunosti zadovoljiti suvremene potrebe. Razlog je najčešće zastarjela, kruta i nefleksibilna arhitektura te složenost implementacije proširenja. Takve karakteristike vrlo lako se mogu uočiti kod trenutno najpopularnijeg protokola ove vrste, protokola RADIUS. Logičan postupak stoga je bio razvoj novog protokola koji će omogućiti upravo sve ono što dosadašnji protokoli ne mogu, a na temelju već ostvarenih i provjerenih principa.

Primjer takvog novog protokola je DIAMETER. Osnovna i najznačajnija njegova karakteristika je jednostavna proširivost osnovnog rješenja. U kombinaciji s usavršenim funkcionalnostima koje nude svi ostali protokoli za autentikaciju, autorizaciju i administraciju stvoreno je kvalitetno novo rješenje. Prednosti takvog rješenja prepoznali su brojni proizvođači, organizacije i samostalni programeri.

S obzirom na sve opisane karakteristike, prednosti u odnosu na RADIUS i ostalu konkurenciju te veliku podršku razvojne zajednice i velikih kompanija, izvjesno je da će DIAMETER smijeniti protokol RADIUS i ostalu konkurenciju. Preostaje samo pitanje trajanja ove tranzicije te pojave eventualne značajnije konkurencije na tržištu.

7. Reference

[1] XMPP Working Group: Request For Comment 3588, Diameter Base Protocol, IETF, rujan 2003.

[2] Calhoun, Pat R. et al: Diameter Framework Document, AAA Working Group, veljača 2001.

[3] Liu, J., Jiang, S., Lin, H.: Introduction to Diameter: Get the next generation AAA protocol, http://www.ibm.com/developerworks/library/wi-diameter/index.html, IBM, siječanj 2006.

[4] Diameter Tutorial, http://www.ulticom.com/html/products/signalware-diameter-what-is.aspx, Ulticom, Inc., 2010.

[5] Ventura Håkan: DIAMETER: next generation's AAA protocol, završni rad, Linköpings Universitet, Linköpings, Švedska, 2002.

[6] Wikipedia: Diameter (protocol), http://en.wikipedia.org/wiki/Diameter_%28protocol%29, svibanj 2010.