ANALIZA PROTOKOLA RADIUS I DIAMETER SA ASPEKTA TARIFIRANJA TELEKOMUNIKACIONIH SERVISA

Vesna M. Radonjić, *Andrijana* N. Todosijević, *Milica* R. Petrović, *Mirjana* D. Stojanović, *Aleksandra* K. Kostić-Ljubisavljević, Univerzitet u Beogradu, Saobraćajni fakultet, Beograd

DOI: 10.5937/vojtehg61-2221

OBLAST: telekomunikacije
VRSTA ČLANKA: stručni članak

Sažetak:

Tarifiranje servisa povezano je sa funkcijama utvrđivanja verodostojnosti i autorizacijom. Ove funkcije obično se razmatraju zajedno i implementiraju na istom serveru uz pomoć zajedničkog protokola. Najpoznatiji protokoli za verifikaciju, autorizaciju i tarifiranje jesu protokoli RADIUS i Diameter.

Iako protokol RADIUS ima široku upotrebu za mehanizme kontrole verodostojnosti, autorizacije i tarifiranja, ima i određene nedostatke koji mogu biti prouzrokovani samim protokolom ili lošom implementacijom i korišćenjem protokola.

Diameter protokol je skalabilni protokol koji je dizajnirala IETF radna grupa sa ciljem da zameni RADIUS protokol u skoroj budućnosti. Diameter protokol fokusira se na fleksibilno proširenje, napredne algoritme rutiranja, dinamičko ispravljanje grešaka i sigurnosne karakteristike transportnog sloja.

U radu je prikazan opšti pregled RADIUS i Diameter protokola, uključujući njihove osnovne operacije sa težištem na aplikacijama tarifiranja. Sličnosti ovih protokola ogledaju se u podršci istim funkcijama i u sličnom formatu paketa. Razlike se odnose na arhitekturu protokola, način utvrđivanja verodostojnosti, mehanizme autorizacije i tarifiranja. Sa aspekta tarifiranja, najvažnije prednosti protokola Diameter jesu mogućnost prenosa tarifnih informacija u realnom vremenu, kao i implementirani mehanizmi za ispravljanje grešaka sa ciljem da se minimizira gubitak tarifnih podataka u situacijama otkaza. Zahvaljujući ovim karakteristikama protokol Diameter ostvaruje znatnu prednost u odnosu na RADIUS u mrežama naredne generacije.

Key words: *tarifni sistem, verodostojnost, autorizacija, obračun, funkcionalnost, arhitektura protokola, nadgledanje u realnom vremenu, telekomunikacione mreže.*

Zahvalnica: Ovaj rad je deo rezultata istraživanja na projektu „TR32025“ koji finansira Ministarstvo prosvete i nauke Republike Srbije.

v.radonjic@sf.bg.ac.rs

Uvod

S obzirom na sve veći broj telekomunikacionih servisa i činjenicu da su ranije telekomunikacione mreže podržavale ili samo jedan servis ili mali broj različitih servisa, problem tarifiranja u novim mrežama postaje sve složeniji i značajniji. Tarifiranje servisa je proces koji je bitan za upravljanje, planiranje i naplaćivanje servisa. Čuvanje i razmena tarifnih podataka posebno su važni u mrežama u kojima se zahteva tarifiranje korisnika u realnom vremenu.

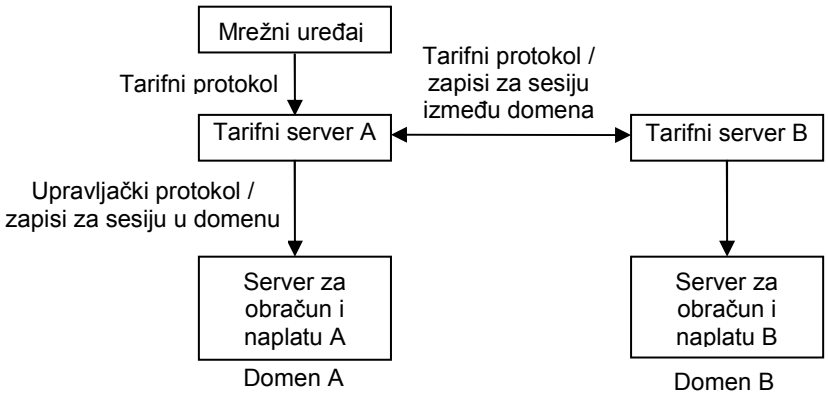
Funkcije tarifiranja povezane su sa funkcijama utvrđivanja verodostojnosti i autorizacijom. Utvrđivanje verodostojnosti je neophodno kako bi se osigurala naplata korišćenja servisa pravom korisniku, dok autorizacija osigurava raspoloživost relevantnih podataka samo ovlašćenim osobama. Zbog toga se funkcije utvrđivanja verodostojnosti, autorizacije i tarifiranja (AAA, *Authentication, Authorization and Accounting*) obično razmatraju zajedno i implementiraju na istom serveru, uz pomoć zajedničkog protokola (Aboba, et al, 2000), (Pras, et al, 2001, pp.108-113), (Zseby, et al, 2002). U kontekstu obezbeđivanja ovih funkcija izdvajaju se protokoli RADIUS (*Remote Authentication Dial In User Service*) i Diameter.

Razvojem i uvođenjem novih tehnologija postavljaju se novi zahtevi za AAA protokole. U ovom radu analiza je usmerena na tehničke mogućnosti protokola RADIUS, kao najviše korišćenog AAA protokola i protokola Diameter, koji uvodi nova funkcionalna poboljšanja.

U prvom delu rada izložen je radni okvir za upravljanje tarifiranjem, koji je definisao IETF. Zatim su opisani mehanizmi funkcionisanja protokola RADIUS i Diameter i prikazana je njihova uporedna analiza. Posmatrani su, pored AAA funkcija, i opšti aspekti. Na kraju su predočena zaključna razmatranja.

Funkcije AAA i odgovarajući protokoli

IETF je ustanovio radni okvir za upravljanje tarifiranjem sa ciljem da definiše skup alata koji se mogu koristiti da ispune zahteve različitih aplikacija (Aboba, et al., 2000). Na slici 1 prikazana je arhitektura upravljanja tarifiranjem, koja obuhvata interakcije između elemenata mreže, tarifnih servera i servera za obračun i naplatu. Elementi mreže prikupljaju informacije o iskorišćenju resursa i prosleđuju ih tarifnom serveru posredstvom odgovarajućeg protokola ili u formi zapisa za svaku sesiju. Tarifni server zatim generiše i prosleđuje relevantne podatke serveru za obračun i naplatu, koji takođe može da obavlja funkcije fakturisanja, verifikacije obračuna, analize trendova i planiranja kapaciteta. Kada se primenjuje tarifiranje prema korišćenju, neophodni su tarifni podaci radi fakturisanja. U slučaju primene ravnomerne šeme tarifiranja, tarifni podaci se koriste prevashodno za verifikaciju obračuna, analizu trendova i planiranje kapaciteta.



Slika 1 – IETF arhitektura upravljanja tarifiranjem
Figure 1 – IETF accounting management architecture

Utvrđivanje verodostojnosti je proces kojim se potvrđuje korisnikov digitalni identitet, obično putem neke vrste identifikatora i pripadajućih podataka. Primeri tih podataka su lozinke, tokeni, digitalni sertifikati i brojevi telefona. Autorizacijom se utvrđuje da li je određeni entitet ovlašćen da izvrši neku aktivnost. Ona se može izvršiti preko niza ograničenja, poput vremenskog, ograničenja fizičke lokacije ili ograničenja protiv višestrukih prijava istog entiteta ili korisnika. Primeri tipova usluga su filtriranje IP adrese, dodeljivanje adrese, dodeljivanje rute, QoS, diferencijalne usluge, upravljanje tokom saobraćaja, obavezno tunelovanje do određene krajnje tačke i enkripcija. Tarifiranje korisnika u novijim mrežama podrazumeva praćenje korišćenja mrežnih resursa. Tarifni podaci mogu se koristiti za upravljanje, planiranje i naplaćivanje servisa, kao i za druge (specifične) svrhe. Tarifiranje u realnom vremenu odnosi se na podatke koji se dostavljaju tokom vremena korišćenja resursa. Grupno tarifiranje odnosi se na podatke koji se čuvaju i kasnije dostavljaju provajderu servisa. Podaci koji se obično prikupljaju su identitet korisnika, vrsta pružene usluge i vreme početka i završetka usluge.

Radna grupa IETF-a za AAA prvenstveno se bavi pristupom mreži i odgovarajućim protokolima:

– RADIUS je razvijen za potrebe komutiranog pristupa.

– TACACS (*Terminal Access Controller Access Control System*) jeste razvijen za potrebe terminalskog pristupa.

– SNMP (*Simple Network Management Protocol*) omogućava upravljanje pojedinačnim elementima mreže i služi za potrebe konfigurisanja mrežnih elemenata.

– COPS (*Common Open Policy Service*) zasniva se na klijent/server modelu, sa tipičnom primenom u protokolu RSVP.

– Diameter predstavlja poboljšanu verziju RADIUS protokola i razvijen je za pristup mreži i mobilni IP.

Razvojem i širenjem interneta i uvođenjem novih tehnologija pristupa, kao što su DSL, Ethernet, bežični pristup i mobilni IP, dizajn rutera i pristupnih servera je sve kompleksniji i postavlja nove zahteve za AAA protokole (Zseby, et al., 2002). Protokoli kao što su RADIUS i TACACS ne odgovaraju zahtevima novih tehnologija.

Protokol SNMP ima važnu ulogu u upravljanju tarifiranjem. Funkcionalnost SNMP u tarifiranju povezana je sa daljinskim pretraživanjem rezultata merenja tokova saobraćaja koji su relevantni za tarifiranje, a memorišu se u elementima mreže kao deo standardizovane baze upravljačkih informacija (MIB, *Management Information Base*).

COPS je relativno jednostavan protokol koji se zasniva na klijent/server modelu i obuhvata procedure za uspostavljanje dijaloga i identifikaciju zahteva. COPS koristi transportni protokol TCP (*Transmission Control Protocol*) da osigura pouzdan prenos signalizacionih informacija između krajnjih sistema. Daljinsko konfigurisanje elemenata mreže uključenih u proces tarifiranja može se obavljati posredstvom protokola SNMP ili COPS.

IETF je usvojio i preporučio protokol Diameter kao najpogodniji AAA protokol, koji je, pored primene za pristup mreži i u mobilnim IP komunikacijama, takođe predviđen za rad sa lokalnim AAA funkcijama, kao i za rad u roaming-u. Protokol se zasniva na modelu upit/odziv, a informacije se razmenjuju u formi parova vrednosti atributa (AVP, *Attribute Value Pair*). Razmena tarifnih podataka obavlja se posredstvom para poruka: *Accounting Request* i *Accounting Answer*. AVP-ovi pridruženi ovim porukama omogućavaju prenos informacija o verodostojnosti i autorizaciji, iskorišćenosti resursa relevantnih za tarifiranje određenog servisa, planiranju kapaciteta i dr. Osnovni protokol može se koristiti samo za potrebe tarifiranja ili sa specifičnim Diameter aplikacijama, kao što su mobilni IP ili pristupni server mreže.

Osnovne funkcije protokola RADIUS

RADIUS je najčešće korišćen AAA protokol (Rigney, 1997). Danas postoje razni komercijalni i *open-source* RADIUS serveri. Najčešću primenu nalazi kod mrežnih uređaja poput rutera, svičeva, modema i sl. Protokol se bazira na klijent-server modelu i na transportnom sloju koristi UDP protokol. Na strani klijenta koristi se NAS (*Network Access Server*), koji obavlja zadatke vezane za prosleđivanje korisničkih parametara RADIUS serveru, kao i za obradu primljenih odgovora (Metz, 2001). Sa druge strane nalaze se RADIUS serveri koji su zaduženi za primanje upita, proveru primljenih korisničkih parametara i zatim vraćanja potrebnih konfiguracijskih parametara koji će omogućiti pružanje adekvatne usluge korisniku od strane klijenta.

RADIUS protokol koristi se iz više razloga: mrežni uređaji u osnovi ne poseduju mogućnost čuvanja velikog broja autentifikacijskih parametara različitih korisnika, s obzirom na ograničene resurse kojima raspolažu, olakšava i centralizuje tarifiranje korisnika, pruža određeni nivo zaštite protiv aktivnih napada neovlašćenih korisnika, ima veliku podršku različitih proizvođača mrežne opreme (Hashmathur, et al, 2010, pp.48-54). RADIUS se, iz navedenih razloga, danas smatra standardom za udaljeno utvrđivanje verodostojnosti korisnika.

Pored utvrđivanja verodostojnosti i autorizacije, primena protokola RADIUS podrazumeva i prenos informacija o tarifiranju između NAS i tarifnog (*accounting*) servera. Ključne osobine su (Tuomimäki, 2003, pp.1-16):

– klijent/server model: NAS predstavlja klijenta RADIUS tarifnog servera. Klijent je odgovoran za prosleđivanje informacija i tarifiranje određenom RADIUS serveru. Server prima upit i šalje potvrdu klijentu o uspešnom prijemu upita. RADIUS tarifni server može da radi kao *proxy* klijent drugim tarifnim serverima;

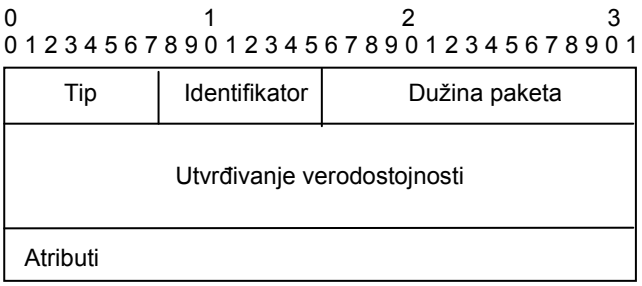
– bezbednost mreže: transakcije između klijenta i servera su verodostojne, što se postiže korišćenjem zajedničkog tajnog ključa koji se nikada ne šalje mrežom;

– mogućnost proširenja: sve transakcije sastoje se od *Attribute-Length-Value* trojki varijabilne dužine. Nove vrednosti atributa mogu biti dodate bez remećenja već postojeće implementacije protokola.

Kada je klijent konfigurisan da koristi RADIUS tarifiranje, na početku isporuke servisa biće generisan *Accounting Start* paket, koji opisuje tip servisa i korisnika servisa, i poslat serveru, koji šalje potvrdu o uspešnom prijemu. Na kraju će biti generisan *Accounting Stop* paket koji opisuje tip isporučenog servisa i opcino statistike poput proteklog vremena, ulaznih i izlaznih okteta ili ulaznih i izlaznih paketa. To će biti poslato serveru koji šalje potvrdu da je paket uspešno primljen.

Accounting-Request (bilo *Start* ili *Stop*) šalje se RADIUS tarifnom serveru putem mreže. Ako u određenom periodu nema potvrde, upit se šalje određeni broj puta. Klijent može i da prosledi upit alternativnom serveru ili serverima koji se koriste u slučaju pada ili nedostupnosti prvog servera. Alternativni server može se koristiti i nakon neuspelih pokušaja slanja primarnom serveru zbog pada. Algoritmi za vraćanje ili oporavak od pada su predmet mnogih istraživanja.

RADIUS tarifni server može zahtevati druge servise radi ispunjenja zahteva i u tom slučaju on je klijent. Ako RADIUS tarifni server nije u mogućnosti da uspešno primi paket, on ne sme da pošalje *Accounting-Response* potvrdu klijentu. Tačno jedan RADIUS tarifni paket je enkapsuliran u UDP polje podataka, pri čemu UDP koristi port 1813. Kada je generisan odziv, portovi izvora i destinacije su obrnuti. Na slici 2 prikazan je format RADIUS paketa.



Slika 2 – Format RADIUS paketa
Figure 2 – RADIUS packet format

– **Tip** (*Code*): ovo polje je dužine jednog okteta i opisuje tip RADIUS paketa. Kada se paket primi sa pogrešnim *Code* poljem, odbacuje se. RADIUS *Accounting Code* polja su redom:

4 – Accounting-Request

5 – Accounting-Response

– **Identifikator** (*Identifier*): ovo polje je dužine jednog okteta i pomaže u slaganju upita i odziva.

– **Dužina paketa** (*Length*): zauzima dva okteta. Označava dužinu paketa, uključujući *Code*, *Identifier*, *Length*, *Authenticator* i *Attributes*. Okteti koji su duži ili kraći od polja *Length* treba da budu ignorisani i odbačeni. Minimalna dužina je 20, a maksimalna 4096 okteta.

– **Utvrđivanje verodostojnosti** (*Authenticator*): polje je dužine šesnaest okteta. Najvažniji oktet se prenosi prvi. Ova vrednost koristi se da utvrdi verodostojnost poruka između klijenta i RADIUS tarifnog servera.

– **Atributi** (*Attributes*): mogu imati više slučajeva. Red atributa istog tipa treba da bude sačuvan, što se ne zahteva za red atributa različitog tipa.

Prilikom prijave u mrežu, korisnik šalje svoje podatke RADIUS klijentu koji zatim izmenjuje RADIUS poruke specifičnog formata s RADIUS serverom. Svrha tih poruka je ostvarivanje tri funkcije AAA koncepta: utvrđivanje verodostojnosti, autorizacije i tarifiranja korisnika.

Kada se uzmu u obzir sve poruke koje razmenjuju RADIUS klijent i server, kao i sami zahtevi korisnika, komunikacija izgleda ovako:

1. Korisnik šalje svoje identifikacione podatke RADIUS klijentu sa željom da mu se odobri pristup određenim mrežnim resursima.

2. Klijent izvršava proces utvrđivanja verodostojnosti i autorizacije razmenom poruka sa RADIUS serverom:

   a. klijent šalje upit – *Access-Request*,

   b. server odgovara odzivom, koji može da bude: *Access-Reject* (ako se korisnikov upit za pristup odbacuje) ili *Access-Accept* (ukoliko se korisnikov upit za pristup prihvata).

1. Klijent izvršava proces tarifiranja korisnika:
   a. klijent šalje serveru poruku Accounting-Request (Start), koja predstavlja zahtev za početak sesije,
   b. server odgovara sa Accounting-Response, čime počinje sesija,
   c. kada korisnik želi da završi sesiju, klijent šalje serveru Accounting-Request (Stop),
   d. server odgovara sa Accounting-Response, čime se završava sesija i korisnik se isključuje iz mreže.

Nakon što je NAS odobrio pristup korisniku, on šalje poruku *Accounting Start* (RADIUS *Accounting-Request* upit koji sadrži atribut *Acct-Status-Type* sa vrednošću „start") RADIUS serveru. Slanje te poruke označava početak korisnikovog pristupa mreži. *Accounting Start* poruke obično sadrže identifikaciju korisnika, njegovu IP adresu, mesto pristupa i jedinstveni identifikator sesije. Kao odgovor, server uzvraća odzivnom porukom *Accounting-Response.*

Nakon uspostavljene sesije, NAS može povremeno slati *Interim Update* poruke serveru. Radi se o RADIUS *Accounting-Request* porukama koje sadrže atribut *Acct-Status-Type* sa vrednošću *Interim Update*. Uobičajeno*, Accounting Interim* poruke prenose podatke o trajanju trenutne sesije i o trenutnom korišćenju podataka, što je korisno za praćenje ličnih 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 vrednošću „stop" atributa *Acct-Status-Type*). Poruka sadrži detalje o ukupnom vremenu trajanja sesije, prenesenoj količini podataka, razlogu isključivanja i ostale informacije vezane za pristup mreži.

Klijent obično šalje *Accounting-Request* poruke u određenim intervalima, sve dok ne primi *Accounting- Response* odgovor. Osnovna svrha ovih podataka jeste 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 (Rigney, 1997).

Arhitektura i rad protokola Diameter

Protokol Diameter razvijen je sa ciljem da ukloni nedostatke i funkcionalna ograničenja protokola RADIUS. Sam naziv ovog protokola – Diameter (prečnik) upućuje na njegove karakteristike u odnosu na RADIUS (poluprečnik). Iako je jezgrena funkcionalnost protokola RADIUS ostala netaknuta, način njene implementacije je promenjen. Uz to, dodata su brojna proširenja i ostvarene nove mogućnosti. Iako Diameter nije potpuno kompatibilan sa protokolom RADIUS, njihova saradnja je moguća upotrebom jednog od mnogobrojnih proširenja. Upravo je jednostavna proširivost protokola Diameter bila jedna od osnovnih ciljeva njegovog

razvoja. Dodatni razvoj protokola Diameter podstakle su organizacije poput IETF-a i 3GPP-a (*The 3rd Generation Partnership Project*) stalnim doradama i iscrpnim specifikacijama.

Protokol Diameter namenjen je za rad u lokalnom AAA i roming okruženju za aplikacije poput pristupanja mreži i IP mobilnosti. Osnovnu aplikaciju protokola treba da podrže sve Diameter aplikacija. Diameter omogućava:

– isporuku AVP-ova,
– mogućnost pregovaranja,
– notifikaciju grešaka,
– mogućnost proširenja dodavanjem novih komandi i AVP-ova,
– osnovne servise neophodne za aplikacije, kao što su upravljanje korisničkim sesijama ili tarifiranje.

Svi podaci preneseni protokolom su u formi AVP-a. Neke od ovih AVP vrednosti koriste se za sam protokol, dok su neke povezane sa posebnim aplikacijama koje omogućava Diameter. Parovi se mogu dodati proizvoljno u Diameter poruke sve dok su uključeni zahtevani parovi, a nisu obuhvaćeni oni nezahtevani. AVP-ovi se koriste u okviru ovog protokola kako bi omogućili sledeće karakteristike:

– prenos informacija o verodostojnosti korisnika, radi omogućavanja servera da verifikuje korisnika,
– prenos specifičnih informacija o autorizaciji između klijenta i servera, koji omogućava donošenje odluke o odobravanju korisničkog upita,
– razmenu informacija o korišćenju resursa, koja može biti korišćena u svrhe tarifiranja, planiranja kapaciteta itd.,
– prosleđivanje, posredništvo i preusmeravanje poruka kroz hijerarhiju servera.

Osnovni protokol Diameter može se koristiti samo za tarifiranje, ili sa aplikacijama poput mobilnog IPv4 ili mrežnog pristupa. Takođe, postoji mogućnost proširenja protokola za nove aplikacije, dodavanjem novih komandi ili AVP-ova.

Protokol Diameter osmišljen je kao kombinacija osnovnog protokola i širokog spektra aplikacija koje mu nude jednostavnu mogućnost proširenja za ostvarenje raznovrsnih dodatnih usluga. Osnovni protokol nudi temeljne mehanizme i funkcionalnosti zajedničke svim aplikacijama. Većina njih temelji se na osnovnoj funkcionalnosti protokola RADIUS, dok je ostatak rezultat novih rešenja i poboljšanja postojećih ideja. Ovde su definisani osnovni formati poruka, mehanizmi prenosa podataka i upravljanja greškama, metode komunikacije između pojedinih elemenata arhitekture i osnovne sigurnosne funkcije. Aplikacije nisu klasične programske aplikacije nego protokolna rešenja koja se nadovezuju na funkcionalnosti osnovnog protokola. Svaka aplikacija određena je posebnom oznakom i u osnovnu strukturu može uneti nove naredbe i nove obavezne parove atributa i vred-

nosti, čime se stvaraju dodatne funkcionalnosti. Primeri su: aplikacija za podršku mobilom IP-u (*Mobile* IP, *Diameter Mobile* IPv4 *Application*), aplikacija za pristupne mrežne servere (NASREQ, *Diameter Network Access Server Application*), aplikacija za podršku protokola EAP (Diameter Extensible Authentication Protocol Application), aplikacija za podršku kontrole naplate (*Diameter Credit-Control Application*), aplikacija za CMS (*Diameter Cryptographic Message Security Application*) i aplikacija za podršku protokola SIP (*Diameter Session Initiation Protocol Application*).

Arhitektura protokola Diameter temelji se na modelu *peer-to-peer*. Na taj način je svaki njen element ujedno i klijent i server, zavisno od trenutnih potreba mreže. Elementi takođe mogu biti i mrežni agenti. Stoga, elemente arhitekture ovog protokola po trenutnim ulogama i zaduženjima u mreži možemo podeliti na klijente, servere i agente (Calhoun, et al, 2003).

Element koji primi zahtev krajnjeg korisnika za spajanjem na mrežu automatski postaje klijent. U većini slučajeva klijent je ujedno i pristupni mrežni server. Nakon prikupljanja korisničkih podataka o verodostojnosti, klijent šalje poruku s pristupnim upitom jednom od elemenata arhitekture protokola koji će taj upit opslužiti. Takav element u ovom slučaju biće ili server ili jedan od agenata. Pretpostavi li se da je pomenuti element server, on će biti zadužen za mehanizme utvrđivanja verodostojnosti korisnika na osnovu primljenih podataka. Ako je verodostojnost bila uspešna, konfiguracijski podaci i podaci vezani za korisnički pristup biće poslati natrag klijentu kao odziv na pristupni upit. U protivnom, upit će biti odbijen. Protokol podržava i iniciranje poruka od strane servera, kao što je obustava servisa određenom korisniku. Arhitektura temeljena na modelu *peer-to-peer* puno je fleksibilnija, jer dopušta da svaki od mrežnih elemenata bude ili klijent ili server i, prema potrebi, omogućava obavljanje i jedne i druge funkcije.

Osim klijenata i servera, važan deo arhitekture protokola Diameter su i agenti. Diameter agent je čvor koji ne omogućava verodostojnost/autorizaciju lokalno, već server vrši ove operacije, dok jedan čvor može biti i klijent i server istovremeno. Po svojoj ulozi, agenti mogu biti zaduženi za prosleđivanje (*Relay Agent*), preusmeravanje (*Redirect Agent*), posredništvo (*Proxy Agent*) i prevođenje (*Translation Agent*) protokola.

Agenti zaduženi za prosleđivanje koriste se za prosleđivanje poruka na odgovarajuće odredište, zavisno od informacija dobijenih iz pristigle poruke. Jedna od njihovih prednosti je sposobnost prikupljanja i agregacije zahteva pristiglih iz različitih domena i područja i njihovo usmeravanje prema zajedničkom odredišnom području. Time se eliminišu zahtevni postupci konfiguracije pristupnih servera za svaku promenu serverskog elementa Diameter mreže.

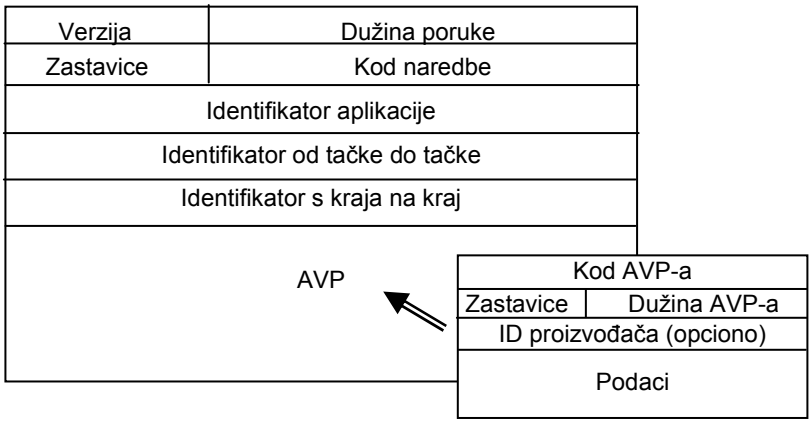
Posrednički agenti se, takođe, koriste za prosleđivanje poruka, ali, za razliku od agenata zaduženih samo za prosleđivanje, sposobni su i za promenu sadržaja tih poruka. To omogućava ostvarenje brojnih servisa dodatne vrednosti, uvođenje pravila obrade zavisno od pojedinih poruka i

obavljanje administrativnih zadataka za pojedino područje ili domen. U slučaju da nije potrebno menjati sadržaj poruke, ulogu posredničkog agenta može preuzeti i agent zadužen za prosleđivanje.

Agenti zaduženi za preusmeravanje služe kao središnji konfiguracijski nosilac za sve ostale elemente Diameter arhitekture. Po prijemu poruke agent proverava svoju tabelu rutiranja i, kao odziv, šalje informacije vezane za preusmeravanje. Razlika između posredničkog agenta i agenta zaduženog za preusmeravanje jeste što posrednički agent ne zna adresu servera kojem treba da prosledi poruku već tu informaciju saznaje pomoću agenta zaduženog za preusmeravanje.

Agenti zaduženi za prevođenje imaju zadatak da prevode poruke raznih protokola za utvrđivanje verodostojnosti, autorizaciju i tarifiranje u poruke protokola Diameter i obrnuto. Ova funkcionalnost je veoma korisna pri integraciji sa ostalim, trenutno više korišćenim AAA protokolima, posebno sa protokolom RADIUS.

Struktura zaglavlja Diameter protokola prikazana je na slici 3.



Slika 3 – Format zaglavlja Diameter paketa (Calhoun, et al., 2003)
Figure 3 – Diameter packet format

Značenje svakog od polja zaglavlja je sledeće:

– **Verzija** (*Version*): vrednost polja je 1 da bi se naznačilo da je u pitanju Diameter protokol verzije 1.

– **Dužina poruke** (*Message lenght*): ovo polje zauzima 3 okteta i ukazuje na dužinu cele poruke koja se prenosi, uključujući pri tome i polja koja se nalaze u zaglavlju Diameter poruke.

– **Zastavice naredbi** (*Command flags*): dužina polja zastavice naredbi je 8 bita. Dodeljivanje vrednosti bitima vrši se na sledeći način:

  – **R** *(request)* – Upit/Odziv. Ukoliko je vrednost ovog bita 1, poruka predstavlja upit, u suprotnom je u pitanju odziv.

– **P** *(proxiable)* – Mogućnost prosleđivanja. Ako ovo polje nije setovano poruka se mora obraditi isključivo lokalno. Ukoliko je vrednost ovog bita 1 Diameter poruka može se proslediti, prenositi i uputiti i na drugi administrativni domen.
– **E** *(error)* – Greška. Ovaj bit ukazuje na to da li poruka sadrži grešku u protokolu. Ukoliko je vrednost polja E u poruci 1, smatra se da je u pitanju poruka sa greškom. Ukoliko je u pitanju zahtev, ovo polje ne sme da bude setovano.
– **T** *(re-transmitted)* – Mogućnost ponovnog slanja. Ova zastavica se aktivira nakon greške u slanju, a da bi se onemogućilo dupliranje poslatih upita. Ukoliko se ne dobija odgovor na poslati upit, ova zastavica se postavlja na 1 prilikom ponovnog slanja iste poruke, sa ciljem da ukaže na mogućnost umnoženih upita zbog otkaza linka. Ukoliko se poruka sa upitom šalje prvi put bit mora biti 0. Na taj način Diameter agenti se brinu isključivo o broju upita koje su poslali na osnovu jednog primljenog upita. Sve retransmisije koje su drugi entiteti obavili ne uzimaju se u obzir i ne moraju se posebno pratiti. Agenti koji su primili poruku sa aktivnim poljem T moraju zadržati ovu vrednost prilikom prosleđivanja poruke. Takođe, ukoliko je za poslati upit primljen odgovor u vidu greške u protokolu, zastavica se ne sme aktivirati i njena vrednost mora ostati 0. Samo u slučaju kada se za poslati upit ne dobije odgovor, polje se postavlja na 1.

– **Kod naredbe** (*Command code*): koristi se za saopštavanje naredbi pridruženih poruci. Ovo polje podržava više od 16 miliona različitih komandi. Kodovi od 0 do 255 su tzv. RADIUS tipovi kodova i koriste se za obezbeđivanje kompatibilnosti sa RADIUS protokolom. Vrednosti od 256 do 16.777.213 namenjene su za nepromenljive, standardne komande koje je dodelio IETF. Ostale vrednosti polja namenjene su za eksperimentalnu upotrebu.

– **Identifikator aplikacije** (*Application ID*): koristi se da identifikuje aplikaciju za koju je poruka namenjena.

– **Identifikator od tačke do tačke (***Hop-by-hop Identifier*): predstavlja 32-bitno polje koje potpomaže uparivanje upita i odgovora. Pošiljalac upita mora obezbediti da ovo polje bude jedinstveno za datu konekciju u datom trenutku, dok pošiljalac odziva mora obezbediti poklapanje vrednosti ovog polja sa vrednošću polja odgovarajućeg upita.

– **Identifikator s kraja na kraj (***End-to-end Identifier***)**: predstavlja polje dužine 4 okteta čija je namena da detektuje duplicirane poruke.

– **AVP**: Parovi vrednosti atributa predstavljaju konkretne podatke koji se prenose porukom. Diameter protokol definiše skup osnovnih atributa i svakom od njih dodeljuje odgovarajuću semantiku. AVP prenose sve podatke vezane za verodostojnost, autorizaciju i tarifiranje, kao i za rutira-

nje, sigurnosne informacije i detalje konfiguracije upita i odziva. Takođe, AVP ima svoje sopstveno zaglavlje.

Zaglavlje AVP-a čine:

– AVP kod (AVP *code*): ovo polje u kombinaciji s poljem identifikatora proizvođača jedinstveno označava atribut. Dužine je 3 okteta.

– AVP zastavice (*Flags*): sastoji se od 8 bita i obuhvata zastavice koje definišu da li je podrška za AVP obavezna (M bit), da li postoji polje identifikatora proizvođača (V bit), da li je potrebna enkripcija (P bit). Ostalih 5 bitova se trenutno ne koristi.

– AVP dužina (AVP *length*): polje je veličine 3 okteta i ukazuje na ukupan broj okteta koji čine AVP (zaglavlje i korisne informacije).

– Identifikator proizvođača (*Vendor* ID): vrednost ovog polja, ukoliko postoji, predstavlja 32-bitni kod koji dodjeljuje IETF.

Svaka Diameter poruka mora sadržati kod naredbe u svom zaglavlju i na taj način se utvrđuje aktivnost koja će se izvršiti po prijemu poruke. Tako, na primer, naredba ACR označava da poruka sadrži informacije vezane za tarifiranje. Razmena tarifnih podataka obavlja se posredstvom para poruka ACR/ACA. Za svaki par komandi tipa upit/odziv postoji jedan kod naredbe, a zastavicom naredbi R (koja je ranije definisana) vrši se diferencijacija podtipa.

U klasičnoj arhitekturi protokoli za verifikaciju, autorizaciju i tarifiranje zahtevali su ručnu (statičku) konfiguraciju adresa mrežnog pristupnog servera i klijenata kako bi se slali upiti prilikom prijave korisnika. Takvi postupci unose dodatno opterećenje u složenim i velikim mrežama.

Diameter protokol, uz podršku ručnoj konfiguraciji, donosi i mogućnost dinamičkog otkrivanja ostalih Diameter čvorova (Ooms, 2007). Dinamično otkrivanje moguće je s obzirom na činjenicu da Diameter serveri i agenti šalju poruke sa informacijama o sopstvenim mogućnostima i podržanom nivou sigurnosti obližnjim čvorovima. Klijenti tako, u zavisnosti od korišćenih aplikacija, traženog nivoa sigurnosti i ostalih parametara, mogu odabrati odgovarajući čvor kojem će proslediti korisnički upit. Za pojedini čvor (u ovom slučaju za klijenta) novootkrivena lokacija odgovarajućeg čvora čuva se lokalno preko tabele čvorova i tabele rutiranja čvorova.

Nakon pronalaženja odgovarajućeg čvora kojem će zahtev biti prosleđen potrebno je uspostaviti konekciju sa tim čvorom, jer Diameter na transportnom sloju koristi protokole TCP ili SCTP (*Stream Control Transmission Protocol*). U odnosu na UDP ovi protokoli pružaju pouzdan prenos koji je vrlo važan za aplikacije koje razmenjuju podatke vezane za tarifiranje.

S obzirom na *peer-to-peer* model, pojedini Diameter čvor može imati i više uspostavljenih konekcija u jednom trenutku. Protokol Diameter eksplicitno definiše da u jednom trenutku pojedini čvor mora uspostaviti bar dve konekcije prema čvorovima unutar istog područja ili domena, koji se tada nazivaju primarnim i sekundarnim čvorom.

Radi boljeg razumevanja rada protokola Diameter treba razlikovati pojmove konekcije i sesije. Sesija predstavlja logičku vezu pristupnog uređaja i servera na nivou aplikacije. Konekcija je veza na transportnom nivou, uspostavlja se između dva čvora i služi za razmenu Diameter poruka. Jednu sesiju može činiti više uspostavljenih konekcija. Sesija se može zamisliti kao niz poruka razmenjenih između klijentskog i serverskog čvora u određenom periodu. Svaka sesija određena je jedinstvenim identifikatorom – *Session-Id* kojeg definiše klijent.

Pokretanje sesije slično je kao kod većine klijent-server modela. Sesija počinje slanjem upita klijenta ka serveru. U okviru protokola Diameter, klijent serveru šalje poruku koja sadrži poruku *Auth-Request,* a koja, pored ostalog, sadrži i identifikator sesije. U slučaju kada je potrebno proslediti poruku, ona se na putu do servera prosleđuje odgovarajućim agentima. Treba napomenuti da poruka Auth-Request nije u potpunosti definisana u skupu poruka osnovnog protokola Diameter, jer atributi koje prenosi zavise od aplikacije koja se koristi.

Nakon prihvatanja poruke *Auth-Request* server u poruku odziva može uključiti atribut *Authorization – Lifetime,* kojim se određuje vreme (u sekundama) u okviru kojeg klijent mora biti ponovno autorizovan. Nakon eventualnog isteka vremenske kontrole server briše sesiju iz liste aktivnih sesija i oslobađa sve za nju rezervisane resurse. Klijent zatim mora ponovo poslati poruku sa upitom za uspostavljanje autentifikacije sesije.

Tokom trajanja sesije server može započeti postupak ponovnog utvrđivanja verodostojnosti ili ponovne autorizacije. Ponovno utvrđivanje verodostojnosti i/ili autorizacija izvršavaju se slanjem upita od servera ka klijentu, a koji sadrži naredbu *Re-Auth-Request*. Ovaj postupak koristan je za praćenje trenutne aktivnosti korisnika radi tarifiranja i naplate odgovarajućih servisa, kao na primer kod *prepaid* usluga, kada je serveru potrebna potvrda da korisnik još uvek koristi određeni servis. Nakon uspešno poslatog *Re-Auth-Answer* odziva, klijent mora poslati i odgovarajuću poruku za utvrđivanje verodostojnosti i/ili autorizaciju specifičnu za datu aplikaciju. Autentifikacija sesije uspostavlja se tek nakon što server pošalje odziv. Za kontrolu sesije i praćenje uzroka eventualnih nepredviđenih prekida koristi se atribut *Origin-State-Id*.

Ostatak komunikacije između klijenta i servera, koji uključuje dogovore oko svih potrebnih korisničkih parametara ili razmenu informacija za pružanje i izvršavanje ostalih servisa, takođe se obavlja preko različitih parova atributa i njihovih vrednosti definisanih u pojedinim aplikacijama.

Poruke vezane za prekid sesije koriste se samo u slučaju pružanja usluga utvrđivanja verodostojnosti i autorizacije i to onda kada se prati i održava stanje sesije. Za usluge tarifiranja koriste se poruke za prekid tarifiranja. Prekid sesije može započeti ili klijent ili server. Ukoliko klijent želi da prekine sesiju, serveru će poslati poruku *Session-Termination-*

Request u koju je uključen atribut *Termination-Clause* koji sadrži opis razloga prekida sesije. Na taj način serveru se stavlja na znanje da se sesija prekida. Nakon prijema upita, server šalje odgovarajući odziv i briše sesiju iz liste aktivnih sesija i oslobađa zauzete resurse. Ako prekid inicira server (npr. zbog administrativnih razloga kao što je manjak memorijskog prostora), poslaće klijentu poruku *Abort-Session-Request*. Klijent treba da pošalje odziv na ovaj upit, a zatim da pokrene postupak prekida sesije. Ipak, postoje situacije kada klijent nije obavezan da prekine sesiju nakon primanja poruke za prekid sesije od servera. Sesija se prekida odgovorom na upite za prekidom sesije od strane čvorova koji su ih primili.

Diameter protokol omogućava prenos tarifnih informacija u realnom vremenu i u njega je ugrađeno nekoliko metoda za ispravljanje grešaka sa ciljem da se minimizira gubitak tarifnih podataka u slučaju otkaza. Uređaj koji generiše tarifne podatke dobija informacije ili od autorizovanog servera (ukoliko je povezan sa njim) ili od tarifnog servera, uzimajući u obzir način prosleđivanja tarifnih podataka. Ove informacije uključuju pravovremeno zahtevane tarifne zapise.

Prenos tarifnih informacija u realnom vremenu jedan je od osnovnih zahteva sistema, kao što je i potreba za izvršavanjem provere kreditnog limita i detektovanje prevara. Nasuprot tome, grupno tarifiranje nije jedan od osnovnih zahteva i nije podržano od Diameter protokola. Međutim, iako Diameter obrađuje tarifne upite pojedinačno, za većinu aplikacija sasvim je dovoljno što transportni protokoli koji se koriste obično u jednom paketu prenose grupu upita u slučaju gustog saobraćaja.

Serveri za autorizaciju upravljaju odabirom odgovarajuće strategije prenosa, pri čemu se izbor bazira na poznavanju korisnika i njegovih veza sa roming saradnicima. Server (ili agenti) koriste *Acct-Interim-Interval* i *Accounting-Realtime-Required* vrednosti parova atributa za kontrolu rada Diameter klijenata. *Acct-Interim-Interval* AVP daje instrukciju Diameter čvoru koji ima ulogu klijenta da neprekidno šalje tarifne zapise, čak i za vreme trajanja sesije. *Accounting-Realtime-Required* AVP koristi se za kontrolu ponašanja klijenta u slučaju kada je prenos tarifnih zapisa neuspešan ili je zakasnio.

Diameter tarifni server može da poništi privremeni interval ili zahtev za prenosom u realnom vremenu tako što će u *Accounting-Answer* odzivnoj poruci poslati *Acct-Interim-Interval* ili *Accounting-Realtime-Required* AVP. Kada je prisutan jedan od ova dva AVP-a u odzivu, poslednja primljena vrednost treba da se koristi za buduće tarifne aktivnosti u istoj sesiji.

Diameter čvor koji uspešno primi autentifikacionu i/ili autorizovanu poruku od baznog AAA servera mora prikupiti tarifne informacije za tu sesiju. *Accounting-Request* upit koristi se da prenese tarifne informacije do

lokalnog AAA servera, pri čemu server mora poslati *Accounting-Answer* odziv kao potvrdu o prijemu. Odziv sadrži Result-Code AVP, koji može ukazati na prisustvo greške u tarifnoj poruci. Odbačen upit može dovesti do prekida korisničke sesije, u zavisnosti od vrednosti Accounting-Realtime-Required AVP-a koji je za datu sesiju primljen ranije.

Svaka Diameter aplikacija mora definisati svoje specifične AVP-ove koji moraju biti prisutni u *Accounting-Request* poruci u delu nazvanom „Tarifni AVP-i". Aplikacija mora pretpostaviti da će AVP-ovi definisani RFC preporukom biti prisutni u svim tarifnim porukama, tako da se u ovom delu definišu isključivo njihovi AVP vezani za specifičan servis.

Mehanizam Diameter protokola kreiran je tako da prevaziđe manje gubitke poruka, kao i povremene otkaze mreže. Diameter čvorovi koji imaju ulogu klijenta moraju implementirati odgovarajuće procedure zaštite od otkaza servera ili mrežnih linkova. Oni mogu imati neizbrisivu memoriju za sigurno čuvanje tarifnih zapisa tokom ponovnog podizanja sistema ili dužih mrežnih i serverskih otkaza. Klijent ne bi trebalo da ukloni tarifne podatke iz bilo koje memorijske lokacije sve dok ne primi odgovarajući Accounting-Answer odziv. Takođe, klijent može ukloniti najstarije, nedostavljene ili još uvek nepotvrđene tarifne podatke ukoliko više nema dovoljno memorijskih resursa. Diameter čvorovi koji imaju ulogu agenta moraju detektovati duplirane tarifne zapise nastale zbog slanja istog zapisa ka više servera, kao i umnožene poruke u tranzitu. Ova detekcija vrši se na osnovu inspekcije parova *Session-Id* i *Accounting-Record-Number* AVP-ova. Ukoliko se zahteva strogo utvrđivanje verodostojnosti od agenata, za ovu svrhu može se koristiti sigurnost sa kraja na kraj.

U zavisnosti od tipa tarifnog servisa i uputstava servera za autorizaciju postoje i različite vrste tarifnih zapisa. Ukoliko je tarifni servis takav da su početak i kraj događaja istovremeni, mora postojati par atributa Accounting-Record-Type sa setovanom vrednošću na EVENT_RECORD. Ako je u pitanju privremen tarifni servis merljivog trajanja, moraju se koristiti parovi atributa sa posebnim vrednostima za početak i kraj zapisa – START_RECORD i STOP_RECORD. Ukoliko autorizacioni server nije dozvolio privremeno tarifiranje za odgovarajuću sesiju, moraju se generisati dva tarifna zapisa za svaki servis s obzirom na tip sesije. Kada je za datu sesiju poslat početni tarifni upit, Accounting-Record-Type par atributa mora se podesiti na vrednost START_RECORD. Kada se pošalje poslednji tarifni upit, vrednost mora biti STOP_RECORD. Ako je server za autorizaciju dozvolio privremeno tarifiranje, Diameter klijent mora kreirati i dodatni zapis, označen kao INTERIM_RECORD. Za jednu sesiju mora postojati samo jedan privremeni zapis koji traje u tom trenutku na pristupnom uređaju. Ukoliko se za istu sesiju generiše novi zapis on će se sačuvati preko prethodnog privremenog tarifnog zapisa.

Poređenje radius i diameter protokola

Iako je na tržištu protokola za AAA funkcije i dalje najpopularniji protokol RADIUS, njegova popularnost i dominacija imaju izraženu tendenciju pada. Osnovni razlog za to su sve izraženija ograničenja koja se posebno zapažaju pri razvoju novih i sve popularnijih tehnologija. Samim tim, nameće se pitanje protokola koji će ga zameniti. S obzirom na trenutne prednosti, uvedena poboljšanja, fleksibilnost, mogućnost proširenja, IETF-ovu i 3GPP-ovu podršku i podršku velikih kompanija, veliki su izgledi da ta uloga pripadne upravo protokolu Diameter. Kratak pregled najznačajnijih razlika protokola RADIUS i Diameter prikazan je u tabeli 1.

Tabela 1 – Uporedni prikaz karakteristika protokola RADIUS i Diameter
Table 1 – Comparison of the RADIUS and Diameter protocols

	RADIUS	Diameter
Arhitektura	klijent-server	*peer-to-peer*
Protokol na transportnom sloju	UDP	TCP i SCTP
Sigurnost	Nedovoljna podrška sigurnosti s kraja na kraj. Ne podržava poruke greške.	Koristi napredne algoritme rutiranja i omogućava dinamičko ispravljanje grešaka.
Autentifikacija	Nedovoljna podrška mobilnosti.	Puna podrška mobilnosti.
Autorizacija	Podržava samo periodičnu ponovnu autorizaciju.	Sadrži niz poruka koje se mogu koristiti prilikom nepredviđenih prekida komunikacije.
Tarifiranje	Nema mogućnost tarifiranja u realnom vremenu.	Ima mogućnost prenosa tarifnih informacija u realnom vremenu.

U slučaju primene RADIUS protokola, klijent-server koncept podrazumeva da se serveri mogu koristiti i kao posredni klijenti ostalim RADIUS serverima. Sama komunikacija između klijenta i servera temelji se na deljenom tajnom ključu koji se iz sigurnosnih razloga nikada ne šalje mrežom. Uprkos njegovim kvalitetnim rešenjima i pozitivnim karakteristikama treba uzeti u obzir da je protokol RADIUS razvijen sredinom 90-ih godina prošlog veka s namerom da pruži usluge AAA za potrebe tadašnje mrežne arhitekture. Skalabilnost protokola tada je bila u drugom planu. Zahtevi su se s godinama, razvojem novih tehnologija, porastom broja korisnika i složenosti usluga uveliko promenili. Kako bi odgovorio sve zahtevnijim trendovima i podržao brojne nove usluge, RADIUS je za svaku veću promenu zahteva dobijao nove i složenije dodatke. Vremenom je broj ugrađenih dodataka postao toliko veliki da se pri izradi novih prestalo voditi računa o njihovom uzajamnom delovanju. Osim nedostatka skalabilnosti, postala su očigledna i ostala ograničenja. Jedno od njih svakako

je isključiva upotreba 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 AAA u tradicionalnim mrežama sa komunikacijom baziranom na tehnologiji PPP (*Point to Point Protocol*). Usluge se danas kreću u potpuno drugom smeru, prema tehnologiji mobilnog IP-a. Uzevši u obzir navedena ograničenja u kombinaciji s nedostatkom fleksibilnosti i slabom proširivošću protokola jasna je potreba za razvojem novijeg i naprednijeg naslednika.

AAA protokoli, kao što su TACACS i RADIUS, inicijalno su mogli da obezbede *dial-up* PPP i pristup terminalnom serveru. Razvojem interneta i novih pristupnih tehnologija, ruteri i NAS postali su kompleksniji i složeniji, postavljajući nove zahteve pred AAA protokole.

Protokol RADIUS ne podržava autorizaciju bez utvrđivanja verodostojnosti s obzirom na to da za slanje klijentskih upita zahteva i podatke o verodostojnosti. Protokol Diameter ne insistira na slanju ovih podataka u upitima, što predstavlja jedan od trenutnih zahteva IETF-ove radne grupe NASREQ (*Network Access Server Requirements*) koja se bavi uslugama podržanim na pristupnim mrežnim serverima.

Iako je PAP *(Password Authentication Protocol)* danas prilično nesiguran protokol, mnoge aplikacije ga i dalje koriste. Otuda se javlja potreba da AAA protokoli prenose obične, tekstualne ključeve preko velikih mreža. Da bi to bilo ostvarivo, tajnost ključeva mora biti osigurana. Takvi ključevi ne smeju biti izloženi posredničkim serverima koji se nalaze duž ruta. S obzirom na to da protokol RADIUS podržava samo sigurnost od tačke do tačke, ne može sprečiti izlaganje ključeva posredničkim serverima, niti osigurati tajnost ključa s kraja na kraj, što posredničkim serverima omogućava kontakt sa nezaštićenim podacima. Protokol Diameter omogućava takav stepen zaštite upotrebom CMS-a, u kojem su podaci sigurni, čak i kada putuju kroz razne posredničke servere. Pri upotrebi posredničkih servera, Diameter omogućava njihovo praćenje kroz mrežu, dok protokol RADIUS to ne podržava. Takođe, implementacije RADIUS-a tipično zahtevaju da ime ili adresa servera ili klijenta bude ručno konfigurisana, zajedno sa odgovarajućim deljenim tajnim ključevima. To rezultira velikom administracijom i može dovesti do narušavanja sigurnosti ako *Request Authenticator* nije konstantno jednak sa zahtevanim u RADIUS-u. Kroz DNS (*Domain Name System*) Diameter omogućava dinamičko otkrivanje parova. Dodela dinamičkih ključeva sesije omogućena je kroz sigurnost transportnog sloja.

S obzirom na to da RADIUS nema mogućnost utvrđivanja verodostojnosti s kraja na kraj, neispravan server ili zlonamerni korisnik mogu neprekidno ponavljati slanje starih paketa. Postupak može uzrokovati nemogućnost pružanja dalje usluge na opterećenom serveru. Takođe, napadi ponavljanjem mogu prouzrokovati slanje višestrukih administrativnih

poruka, čime se remeti praćenje potrošenih korisničkih resursa, a samim tim i naplata. Protokol Diameter pruža efikasne mehanizme odbrane od napada ponavljanjem pomoću vremenskih oznaka i CMS-a.

Protokol RADIUS zahteva postojanje deljenog tajnog ključa između klijenata i servera, što predstavlja problem kod podrške mobilnosti. Ukoliko se pretpostavi kretanje čvorova između različitih administrativnih celina, tajni ključ, jednak onom na domaćem serveru mobilnog čvora, trebalo bi da poseduju svi agenti u domenima kroz koje je taj mobilni čvor prošao. Samim tim, baze podataka agenata sadržale bi beskonačno mnogo tajnih ključeva korisnika. Protokol Diameter ne koristi mehanizme deljenog tajnog ključa, već se oslanja na IPSec (IP *Security*) i TLS (*Transport Layer Security*) kako bi obezbedio sigurnost komunikacije klijenata i servera.

RADIUS definiše verodostojnost na aplikacionom sloju i šemu integriteta koja se zahteva samo za upotrebu sa paketima odziva. S obzirom na to da RFC 3162 definiše upotrebu IPsec sa RADIUS-om, podrška IPsec se ne zahteva. Nije moguće definisati odvojene šeme autorizacije za svaku aplikaciju. To ograničava korist IPsec u domenu AAA aplikacija (kao što je roming), gde može biti definisana različita sertifikaciona hijerarhija za upotrebu u AAA okruženju. Radi pružanja univerzalne podrške za sigurnost na transportnom sloju, IPsec je obavezan u Diameter-u, dok je TLS opciona.

Pošto je protokol RADIUS trenutno najčešće korišćen protokol za AAA, veoma je važno da potencijalni naslednici ovog protokola što jednostavnije sarađuju s njim. Ovde su ključni elementi RADIUS prilazi. Iako Diameter ima ostvarenu podršku za rad sa protokolom RADIUS preko takvih elemenata, kompatibilnost još uvek nije potpuna. Brojni IETF-ovi zahtevi za proširenjem osnovnog protokola Diameter, u kombinaciji s različitim implementacijama i verzijama protokola RADIUS, ponekad ipak uzrokuju međusobnu nekompatibilnost.

Posedovanje svojstva usklađivanja stanja kod AAA protokola znači da njihovi serveri pomažu klijentima pri obavljanju simultane kontrole korisničke prijave, ograničenjima pri tuneliranju i smanjenju vremena povezivanja. To je moguće ako se osigura oporavak stanja u slučajevima gubitka podataka pri ispadu ili greškama u sistemu. To se obično ostvaruje porukama za praćenje stanja sesije ili resursa i porukama za osvežavanje ili prekid veze. Protokol RADIUS ne sadrži naredbe koje bi se mogle primeniti za ostvarenje takvih poruka. Takođe, zbog modela arhitekture nije svaki element u mogućnosti da samostalno započne komunikaciju slanjem poruka bez prethodnog upita. Protokol Diameter već u svojoj osnovnoj specifikaciji podržava potrebne poruke.

Protokol Diameter sadrži niz poruka koje se mogu koristiti prilikom nepredviđenih prekida komunikacije, najčešće iniciranih sa serverske strane. U najnovijim verzijama RADIUS takođe sadrži niz poruka za prekid veze, ali bez mogućnosti da takve poruke budu poslate sa servera.

Ponovna autorizacija na zahtev odnosi se na mogućnost ponovnog traženja autorizacije klijenta ili servera. Protokol RADIUS podržava tek mogućnost periodične ponovne autorizacije i to bez prethodnih zahteva. Diameter je podržava u potpunosti kroz svoj sesijski orijentisan, *peer-to-peer* odnos između klijenata i servera.

Neželjene poruke, u kontekstu podrške za slanje neželjenih poruka, bile bi poruke koje nisu odgovor na neki eksplicitan upit. Protokol RADIUS ne dozvoljava serverima slanje ovakvih poruka klijentima. Ograničenje prvenstveno proizlazi iz arhitekture temeljene na klasičnom modelu klijent–server, gde isključivo klijenti šalju upite (neželjene poruke). Kod Diameter-a to je jednostavno omogućeno, jer je u *peer-to-peer* arhitekturi svaki čvor ujedno i klijent i server, pa samim tim u bilo kom trenutku bez prethodnog upita može poslati poruku nekom drugom čvoru. Ovo svojstvo najčešće se koristi za potrebe tarifiranja, u trenucima kada pristupni mrežni server treba da prekine određenu korisničku sesiju ili za podršku uslugama gde podatke o sesiji treba menjati tokom njenog trajanja.

U kontekstu formata paketa, osnovni problem je u veličini polja za oznaku sesija u zaglavljima RADIUS paketa, jer veličina od jednog okteta ne odgovara današnjim potrebama. Protokol Diameter za identično polje ima osigurana četiri okteta.

Osnovno ograničenje proširivosti protokola RADIUS sastoji se u ograničenju broja atributa koje prosečan paket ovog protokola može preneti. Takvo ograničenje nastaje zbog veličine polja oznake broja atributa od samo jednog okteta. Kod protokola Diameter veličina sličnog polja iznosi četiri okteta. Rezultat toga jeste da RADIUS omogućuje najviše 256 parova atributa i vrednosti po paketu, a Diameter čak 2^{32}. RADIUS, takođe, omogućava upotrebu višestrukih atributa istog tipa, što je nepovoljno za servere i klijente koji treba da odrede da li su višestruki identični atributi zapravo jedan fragmentisani ili više nezavisnih. Takođe, iako protokol RADIUS podržava atribute specifične za razne proizvođače, ne podržava takve naredbe. Protokol Diameter podržava i te naredbe kroz odgovarajuće aplikacije proizvođača.

Postupci retransmisije, ostvareni kod protokola RADIUS, prilično su složeni, stvaraju dodatno kašnjenje i iziskuju dodatne serverske resurse. Ponovno je razlog način na koji je ostvareno praćenje i identifikovanje pojedinih transmisija. S druge strane, Diameter koristi pouzdane protokole na transportnom sloju, kao što su TCP i SCTP protokoli, koji automatski nude mehanizme retransmisije, čime se smanjuje pritisak na serverske resurse. RADIUS koristi UDP protokol i ne definiše retransmisiju, pa, kao rezultat, pouzdanost zavisi od implementacije. To je glavni problem u tarifiranju, gde se gubitak paketa može direktno odraziti na prihod. Osim toga, kod protokola RADIUS kontrola toka zbog upotrebe protokola UDP praktično ne postoji. Upotreba pouzdanih transportnih protokola poput

TCP-a ili SCTP-a protokolu Diameter omogućuje kontrolu toka prvenstveno mehanizmom kliznih prozora.

Politika protokola RADIUS je takva da se sve poruke koje ne sadrže očekivanu informaciju ili sadrže greške ignorišu i odbacuju. Tako može doći do slučaja da pristupni mrežni server pretpostavi da mu je lokalni RADIUS server postao nepristupačan, jer ne dobija nikakve odgovore na poslati upit. Posledica toga je ponovno slanje svih neodgovorenih zahteva sa pristupnog servera drugim serverima. Međutim, oni neće promeniti opštu politiku ignorisanja i odbacivanja, niti će pristupni ruter ponovno dobiti odgovor. Ceo proces će se ponavljati dok pristupni server napokon ne odustane od upita, što jasno pokazuje nedostatke opisane procedure. Protokol Diameter zahteva da svaka poruka bude potvrđena ili pozitivnim odgovorom ili odgovorom koji sadrži šifru i opis greške. Pristupni server na ovaj način odmah saznaje kada i u kojoj poruci je došlo do greške.

Diameter podrazumeva podršku upravljanju greškama, sposobnost pregovaranja, obavezne/neobavezne parove atributa, za razliku od protokola RADIUS koji ne omogućava direktnu podršku agentima, pa ponašanje agenata varira u zavisnosti od implementacije. Diameter eksplicitno definiše ponašanje agenata.

Kako RADIUS ne omogućava eksplicitnu *proxy* podršku, nedostatak mogućnosti revizije sigurnosnih karakteristika na transportnom sloju dovodi do toga da je roming podležan spoljnim napadima, kao i prevarama partnera. Zbog toga RADIUS nije odgovarajući za široku primenu u internetu. Obezbeđivanjem eksplicitne podrške za roming unutar domena i rutiranje poruka, reviziju i sigurnost na transportnom sloju, Diameter omogućava siguran i skalabilan roming (Calhoun, et al, 2003).

Značajan napor utrošen je u omogućavanju kompatibilnosti protokola Diameter sa RADIUS-om i funkcionisanja oba istovremeno, u istoj mreži. Inicijalno, očekuje se da će Diameter biti ugrađen u mrežne uređaje, kao i u gejtveje, omogućujući komunikaciju RADIUS uređaja i Diameter agenata. Ova sposobnost omogućava da se Diameter podrška doda postojećoj mreži, dodavanjem gejtveja ili servera oba protokola.

Zaključak

Trendovi razvoja novih tehnologija i usluga svakim danom postavljaju nove izazove ostvarenju AAA mehanizama. Jasno je da su ti mehanizmi danas preko potrebni zbog načina rada samih usluga i zbog stepena sigurnosti koji one moraju ponuditi.

Sa konceptom koji je konstantno dorađivan, dopunjavan i prilagođavan, protokol RADIUS služi mnogim korisnicima širom sveta skoro dve decenije. Ovaj protokol korisnicima pruža centralizovanu kontrolu nad funkcijama utvrđivanja verodostojnosti, autorizacije i tarifiranja korisnika.

Do sada su se nedostaci ovog protokola uglavnom prevazilazili korišćenjem dodatnih sigurnosnih mehanizama. Međutim, protokol RADIUS ne može u potpunosti da ispuni sve veće zahteve koji se postavljaju pred AAA funkcije. Razlog je najčešće zastarela, kruta i nefleksibilna arhitektura, kao i složenost implementacije proširenja.

Radi prevazilaženja ovih nedostataka usledio je razvoj novog protokola koji bi, na temelju već ostvarenih i proverenih principa, omogućio upravo sve ono što dosadašnji protokoli ne mogu. Primer takvog novog protokola je Diameter. Njegova osnovna i najznačajnija karakteristika je jednostavna mogućnost proširenja osnovnog rešenja. U kombinaciji sa usavršenim funkcionalnostima koje nude svi ostali AAA protokoli stvoreno je kvalitetno novo rešenje. Prednosti takvog rešenja prepoznali su brojni proizvođači, organizacije i samostalni programeri. Treba napomenuti da je 3GPP odabrao upravo Diameter kao osnovni signalizacioni protokol za utvrđivanje verodostojnosti, autorizaciju i tarifiranje i upravljanje pokretljivošću unutar njihovog velikog projekta, multimedijalnog podsistema zasnovanog na protokolu IP (IP *Multimedia Subsystem*, IMS) (Kumar, Harihar, 2012, pp.266-269).

S obzirom na opisane karakteristike protokola Diameter, tehničke prednosti u odnosu na RADIUS i ostale konkurentne protokole, veliku podršku razvojne zajednice i velikih kompanija, u narednom periodu se očekuje da Diameter potpuno potisne trenutno više korišćeni protokol RADIUS. Pitanje je samo koliko će trajati ova tranzicija i da li će doći do eventualne značajnije konkurencije na tržištu.

Literatura

Aboba, B., Arkko, J., Harrington, D., 2000, *Introduction to Accounting Management*, RFC 2975 (Informational), IETF.

Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J., 2003, *Diameter Base Protocol*, RFC 3588 (Standards Track), IETF.

Hashmathur R., Govardhan, A., Venkat Narayana Rao, T., 2010, *Design and Implementation of RADIUS – An Network Security Protocol*, Global Journal of Computer Science and Technology, 10(7) Ver. 1.0, pp.48-54.

Kumar, V, Harihar, M., 2012, *Diameter-based Protocol in the IP Multimedia Subsystem*, International Journal of Soft Computing and Engineering, 1(6), pp.266-269.

Metz, C., 2001, *AAA PROTOCOLS: Authentication, Authorization, and Accounting for the Internet*, IEEE Internet Computing online.

Ooms, W., 2007, *Providing AAA with the Diameter protocol for multi-domain interacting services*, Master Thesis, Faculty of Electrical Engineering, Mathematics and Computer Science, Design and Analysis of Communication Systems, University of Twente.

Pras, A., Van Beijnum, B-J., Sprenkels, R., Parhonoyi, R., 2001, *Internet Accounting*, IEEE Communications Magazine, 39(5), pp.108-113.

Rigney, C., 1997, *RADIUS Accounting*, RFC 2139 (Informational), IETF.

Tuomimäki, J., 2003, *Overview, Details and Analysis of Radius Protocol*, pp.1-16, Seminar on Internetworking, Helsinki University of Technology.

Zseby, T., Zander, S., Carle, G., 2002, *Policy Based Accounting*, RFC 3334 (Experimental), IETF.

ANALYSIS OF THE RADIUS AND DIAMETER PROTOCOLS IN TERMS OF PRICING TELECOMMUNICATION SERVICES

FIELD: Telecommunications
ARTICLE TYPE: Professional Paper

Summary:

Introduction

Accounting of telecommunication services is closely related to the functions of authentication and authorization. These functions are usually considered together and implemented within the same server using a common protocol. The most renowned protocols for authentication, authorization and accounting are the RADIUS and Diameter protocols.

AAA functions and related protocols

In this chapter, the accounting management architecture developed by IETF is presented. It includes the interaction between network elements, accounting servers and billing and charging servers. Accounting data can be used for management, planning and charging users as well as other (specific) purposes. Authentication is the process of confirming a user's digital identity, usually through some type of identifiers and related data. Authorization determines whether a particular entity is authorized to perform an activity.

Basic Functions of the RADIUS Protocol

The RADIUS architecture is based on a client-server model. It uses UDP on the transport layer. Transactions between the client and the server are authenticated, which is achieved by using a common secret key that is never sent through the network. Given the limited resources available to network devices, RADIUS facilitates and centralizes charging end users, provides some protection against active attacks by unauthorized users and it has great support from different network equipment vendors. Although RADIUS is a widely accepted protocol for the mechanisms of authentication, authorization and accounting, it has certain shortcomings that may be caused by the protocol itself or by its poor implementation.

Architecture and Operation of the Diameter Protocol

Diameter is a scalable protocol designed by the IETF working group in order to eliminate shortcomings and functional limitations of the RADIUS protocol and eventually to replace it in the near future.

Most of the basic Diameter mechanisms and its functionality are based on the fundamental functionality of the RADIUS protocol and the rest is a result of new solutions and improvements to the existing ideas. The Diameter protocol focuses on the expansion of flexible, advanced routing algorithms, dynamic troubleshooting and safety characteristics of the transport layer. This paper defines the basic packet formats, data transfer mechanisms and error management, methods of communication between individual elements of the architecture and basic security functions. The Diameter protocol architecture is based on the peer-to-peer model. Besides clients and servers, network agents can be the elements of this architecture. The Diameter agent is an element that does not allow authentication / authorization locally, but the server performs this operation, while one node can be both the client and the server simultaneously. The role of agents can be forwarding (Relay Agent), redirection (Redirect Agent), mediation (Proxy Agent) and translation (Translation Agent). Since the peer-to-peer model is applied, each Diameter element can establish more connections at the same time. Diameter enables the delivery of attribute value pairs, the possibility of negotiation, error notification, extensibility by adding new commands and attribute value pairs, the basic services necessary for applications such as managing user sessions or accounting.

Comparison of the RADIUS and Diameter protocols

Although at the protocol market for authentication, authorization and accounting, the RADIUS protocol remains the most popular, its popularity and dominance has a decreasing tendency. The main reasons for this are more prominent limitations which are particularly perceived due to new and increasingly popular technology. Therefore, the main issue is about a protocol that will replace RADIUS. The peer-to-peer architecture used by Diameter is much more flexible than the client-server model because in the peer-to-peer architecture every element can be both the client and the server, depending on the current needs of the network. At the transport layer, Diameter uses the TCP or SCTP protocols. When compared to UDP, these protocols provide reliable transmission which is very important for applications exchanging data related to accounting. In addition, the Diameter protocol allows the transmission of accounting information in real time and it incorporates several methods for troubleshooting in order to minimize the loss of accounting data when a failure occurs, which is not the case with RADIUS. Given the present benefits, introduced improvements, flexibility, expandability, IETF and 3GPP's support and the support of big companies, there is a great chance that Diameter will replace RADIUS.

Conclusion

This paper presents a general overview of the RADIUS and Diameter protocols, including some of their basic operations with a special emphasis on accounting applications. The similarities of these pro-

tocols are reflected in the support of the same functions in a similar format of the packages. The differences are related to the protocol architectures and the methods of determining authentication, authorization and accounting mechanisms. Regarding accounting aspects, the most important advantages of the Diameter protocol are its possibility to transmit accounting information in real time and implemented mechanisms for troubleshooting in order to minimize the loss of accounting data in case of failure. Owing to to these characteristics, the Diameter protocol achieves a significant advantage over RADIUS in next generation networks.

Key words: Accounting system, Authentication, Authorization, charging, functionality, Protocol architecture, real-time monitoring, telecommunication networks.

Datum prijema članka/Paper received on: 07. 07. 2012.
Datum dostavljanja ispravki rukopisa/Manuscript corrections submitted on: 03. 12. 2012.
Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 05. 12. 2012.