

Mobilni pristup klaudu primenom mehanizma višeprotokolnog komutiranja labela

Tamara Sević, dr Dušan Vujošević

Sadržaj — U ovom radu se predstavlja jedan od pristupa klaudu preko mobilnih uređaja. Analiziraju se prednosti klauda, virtuelizacije i balansiranja resursima u kontekstu mobilnog pristupa. Opisuje se jedna moguća serverska infrastruktura koja ovakav pristup podržava. Diskutuju se izazovi koje pred rešenje postavlja potreba za osiguranjem bezbednosti podataka. Sagledava se potencijal koji upotreba mobilnog pristupa klaudu donosi organizacijama. Predlažu se pravci daljeg istraživanja.

Ključne reči — 2G/3G, APN, GGSN, IP/MPLS, klaud, virtuelizacija

I. UVOD

RAZVOJEM računarskih tehnologija, zahtevi i potrebe malih i srednjih preduzeća pokazuju da je *cloud computing* jedna od najbitnijih tehnologija budućnosti. Sve je češća pojava da korisnici imaju potrebu da preko mobilnih uređaja pristupaju poslovnim aplikacijama sa terena. U prvo vreme bilo je dovoljno pristupiti elektronskoj pošti, danas postoji potreba i za pristupom specifičnim poslovnim aplikacijama. Uvođenje mobilnih uređaja je preduslov za smanjenje troškova poslovanja. Izuzetna prednost da zaposleni mogu sa bilo koje lokacije da obavljaju svoje poslovne zadatke pristupom centralnoj lokaciji.

Korisnici preko mobilnih uređaja sve više pristupaju aplikacijama instaliranim na virtuelnoj serverskoj infrastrukturi (klaudu iliti oblaku) servis provajdera. Na takav način se, na primer, zaposlenima u kompaniji koja je

Tamara J. Sević, Skadarska 31, Beograd, Srbija; (e-mail: tamara_sevic@yahoo.com).
dr Dušan Vujošević. Računarski fakultet, Beograd, Srbija (e-mail: dvujosevic@raf.edu.rs)

korisnik klada omogućava da u svakom trenutku i na svakom mestu obavljaju poslovne zadatke – šalju i primaju elektronsku poštu, pristupaju dokumentima koji se nalaze na virtuelnom serveru, koriste aplikacije vezane za poslovanje kompanije. Mobilni pristup kladu omogućava i da se sva obrada podataka koji se prikupljaju mobilnim uređajima vrši na virtuelnom serveru servis provajdera.

Glavni servisni modeli u kladu su infrastruktura, hardver i softver [1]:

- (*SaaS*) *Software as a service* – Softver kao servis
- (*PaaS*) *Platform as a service* - Platforma kao servis
- (*IaaS*) *Infrastructure as a service* – Infrastruktura kao servis

U okviru SaaS korisniku je dozvoljeno da, najčešće preko veb brauzera, koristi aplikacije servis provajdera koje rade na klad infrastrukturi. Korisnik nema prava da upravlja ili kontroliše klad infrastrukturu uključujući mrežu, servere, operativne sisteme i skladišta. Provajder razvija funkcionalnosti, vrši hostovanje, a korisnik ih samo koristi.

U okviru PaaS korisniku je dozvoljeno da kreira i upravlja aplikacijama koristeći alate i programske jezike koji su podržani od samog servis provajdera. Korisniku nije dozvoljeno da upravlja ili kontroliše klad infrastrukturu. Korisnik može da razvija, ali sa unapred predefinisanim skupom servisa. Takođe može da vrši hosting.

U okviru IaaS korisniku je dozvoljena kontrola nad procesima, skladištenje, pokretanje proizvoljnog softvera, što može uključivati operativne sisteme i aplikacije i eventualno ograničenu kontrolu mrežnih komponenti.

U nastavku rada se ističe značaj planiranja resursa i virtuelizacije za korisnika klada. Zatim se izlaže jedna moguća realizacija mobilnog pristupa kladu i analiziraju se njegovi tehnološki, infrastrukturni, bezbedonosni i telekomunikacioni aspekti. Na posletku se prikazuju mogućnosti mobilnog pristupa kladu sa stanovišta korporativnog korisnika na jednom primeru koji je osmišljen za potrebe ovog rada.

II. PLANIRANJE RESURSA I VIRTUELIZACIJA

Sa aspekta korisnika najbitnije je da odredi koliki mu je kapacitet potreban da odgovori na njegove zahteve, tj. zahteve njegove firme. Potrebno je uzeti u obzir trenutne kapacitete sistema, uzeti u obzir zahteve i predvideti buduću potražnju. Korisnik mora da izdvoji određena sredstva kako bi zakupio

resurse i odgovorio na potražnju. Ako je potražnja veća, moraju se alocirati dodatni resursi i obezbediti dodatna sredstva. Ako se potražnja smanjuje, mora se smanjiti obim resursa koji su trenutno na snazi [2].

Klaud koristeći virtuelne resurse može nuditi način da se fleksibilno odgovori na nove zahteve i izazove. Planiranje kapaciteta treba da odgovori na njih raspoloživim resursima, ispita šta trenutno postoji na sistemu, meri njegov rad i pravi sliku stanja koje je u upotrebi, a koja će omogućiti da se isplanira i predvidi potražnja. Cilj planiranja kapaciteta jeste da odgovori na opterećenje i da zadovolji zahteve koji uključuju procesor, memoriju, skladištenje i kapacitet mreže. Svaki od ovih resursa ima stopu iskorišćenosti. Mora se voditi računa da se njihove performanse očuvaju. Proizvođači nude različite alate pomoću kojih je moguće uraditi proračun koji će nam odgovoriti koji kapacitet nam je potreban.

Osim što se virtuelizuju serveri, u svetu se već neko vreme sve više virtuelizuju skladišta, podaci i drugi aspekti informatičkih tehnologija. Kada, primera radi, otvorimo nalog na nekom od popularnih imejl servera, dobijamo, recimo, 15 GB prostora za naše virtuelno sanduče. Ovako veliki dozvoljen limit moguć je upravo zahvaljujući mudrom upravljanju resursima po konceptu virtuelizacije. Naime, dobijen prostor dobijen je virtuelno, a ne fizički. Fizički dobijen prostor je znatno manji, ali će, u onim slučajevima kad bude iskorišćen, ako aplikacija zatraži još prostora, prostor biti dodeljen neosetno za krajnjeg korisnika. Time se, naravno, izbegava blokiranje neiskorišćenog prostora na serveru.

Balansiranje resursima je jedna od ključnih prednosti virtuelizacije. U slučaju, primera radi, pada jednog fizičkog hosta, virtuelne mašine prelaze na druge hostove. U EMC-evom *VMware-u*, na primer, to omogućava tehnologija *VMotion*. Interesantno je da, kao što to pokazuje statistika, više virtuelnih mašina danas u jednom trenutku preleće s jednog servera na drugi, nego što u tom istom trenutku ima aviona koji preleću po nebu.

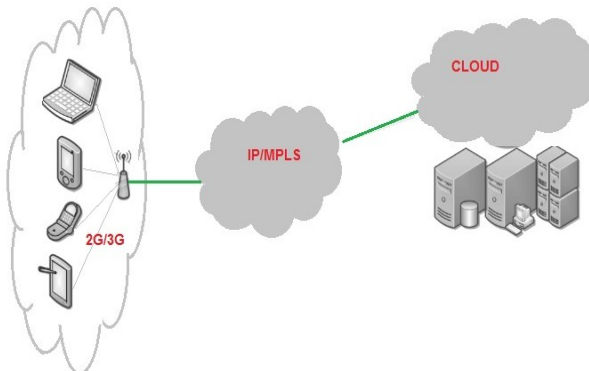
Automatsko balansiranje opterećenjem podrazumeva i da se virtuelne mašine prebacuju sa preopterećenih na manje zasićene hostove. Van špica korišćenja, na primer posle 17h radnim danima, rasterećeni hostovi se mogu automatski isključivati ne bi li se štedela struja. Tako je, na primer, po tvrdnji kompanije EMC, jedna češka telekomunikaciona kompanija na osnovu uštede struje u svom dejta centru kupila šest novih Škoda. Naizgled periferan problem energetske efikasnosti informacionog sistema u stvari je sve značajniji kako se stepen informatizacije društva povećava. Postoji više proizvođača tehnologija virtuelizacije kao što su: *VMware*, *Microsoft*, *Citrix*, i *Oracle*. Vodeći proizvođač tehnologija virtuelizacije je *VMware*, čiji glavni proizvod je trenutno *ESXi*. U svetu 80 procenata virtuelnih mašina

funkcioniše u VMware-u. VMware, koji ima prihod od šest milijardi dolara godišnje i u kome radi 15 hiljada zaposlenih, od 2004. godine je u vlasništvu informatičke korporacije ECM. Među proizvođačima tehnologija virtualizacije je i Microsoft, čiji glavni proizvod se trenutno zove Hyper-V. Poznate su i tehnologije RedHot-KVM i Oracle VM, koje vode poreklo od Xen Server-a.

VMware je kompanija koja se bavi izradom softvera za virtuelne mašine bazirane na Intel-ovim procesorima x86. VMware softver pruža mogućnost korisnicima da kreiraju neograničen broj virtuelnih mašina na računarima sa x86 procesorima. Svaka virtuelna mašina može imati svoj „gostujući“ operativni sistem (OS). *VMware vSphere* upravlja infrastrukturom virtuelnog sistema, skladištenja i umrežavanje hardvera kao osnovom postojanja klada. Kao moćna tehnologija *vSphere* pruža set usluga koje aplikacije mogu da koriste za pristup klada. *VMware* softver je pisan za Windows i Linux okruženja.

III. PRIKAZ MOGUĆE REALIZACIJE PRISTUPA

U narednom tekstu predstavlja se jedan predlog realizacije mobilnog pristupa klada. Pristup se bazira na iskustvu autora stečenom uvidom u odgovarajuća rešenja u privredi, kojima se kritički prilazi i predlažu se, na osnovu uočenih nedostataka i praćenjem stanja u literaturi, mogućnosti za njihovo poboljšanje. Preko mobilne mreže servis provajdera, 2G ili 3G pristupne tehnologije, realizuje se pristup mobilnih uređaja oblaku. Virtuelna



Sl. 1. Mobilni pristup klada

serverska infrastruktura se realizuje posredstvom tehnologije virtualizacije *VMware*, implementirane na serverima dejcentra unutar mreže servis

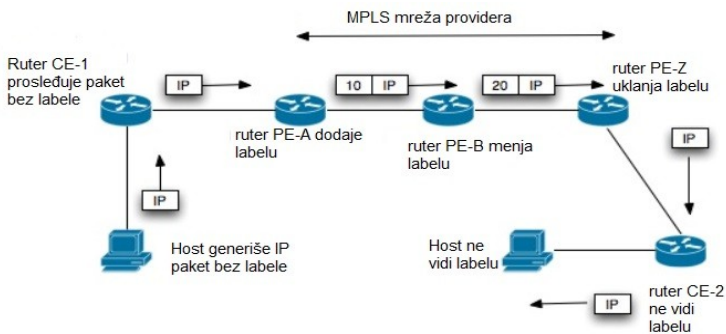
provajdera. Dejtacentar predstavlja skup servera sa sadržajima kao što su baze podataka i bekap sistemi. Serveri se nalaze u posebnoj prostoriji koja mora da zadovolji fizičke i bezbednosne karakteristike. Na Sl. 1 predstavljen je mobilni pristup kladu.

III/1 TEHNOLOGIJA VIŠEPROTOKOLNOG KOMUTIRANJA LABELA

MPLS(*Multiprotocol label switching*) ili višeprotokolno komutiranje labela je mehanizam kojim se postiže razdvajanje saobraćaja od ostatka mreže. MPLS se primenjuje na transportnoj ravni. MPLS je svičing tehnologija koja omogućava enkapsuliranje bilo kog protokola [3]. U ovom slučaju prenosi IP, ali može da vrši transport bilo kog protokola. MPLS labela ima 3 bita kojima može da tretira pakete .

Kada paket ulazi u IP/MPLS mrežu na ulaznom ruteru dodeljuje mu se određena labela. Paket se pomoću labela komutira po unapred određenoj putanji do izlaznog rutera gde mu se skida labela, posle toga se razmatra određena IP adresa [4]. U našem slučaju IP adresa servera na koju paket treba da bude prosleđen. Ruteri u MPLS mreži prosleđuju paket samo na osnovu njegove labela i ne analiziraju sadržaj zaglavlja paketa dok ne dođe do rutera gde izlazi iz IP/MPLS mreže. U zavisnosti na kom se nivou OSI modela vrši enkapsulacija razlikovaćemo L2 ili L3 VPN model. Ruteri između ulaznog i izlaznog rutera ne vide korisnikove IP rute, već ih samo prenose do kraja mreže na osnovu labela. Na Sl.2 predstavljena je enkapsulacija u MPLS tehnologiji.

IV. III/2 VIRTUELNA SERVERSKA INFRASTRUKTURA



Sl. 2. Enkapsulacija u MPLS tehnologiji

Na virtuelnom serveru je moguće izvršavati programe i instalirati operativni sistem na isti način kao i na fizičkom serveru jer on upravo predstavlja njegovu softversku implementaciju[5]. Virtualni serveri su potpuno nezavisni od fizičkog hardvera. Zauzimaju određeni procenat resursa fizičkog servera (*hosta*) na kome se nalaze - procesor, memoriju, pristup skladištu i mrežnu konekciju.

Dele fizičke hardverske resurse po potrebi. Svaki virtualni server koji je pokrenut na jednom fizičkom procesu imaće sopstveni virtualni procesor. Virtualni server radi bez prekida u slučaju da se prebacuje sa jednog na drugi fizički server zato što se mapiranje između virtualnog i fizičkog servera obavlja automatski. Više virtualnih servera se može konfigurisati na jednom fizičkom serveru, a da su međusobno potpuno izolovani. Virtualna infrastruktura podrazumeva sledeće komponente:

- klaster fizičkih servera
- virtualnu i fizičku mrežnu infrastrukturu
- skladišta gde se čuvaju korisnički podaci

VMware ESX serveri mogu da predstavljaju osnovne elemente za izgradnju virtualne infrastrukture data centra kojima korisnici treba da pristupe. Virtualizacija se radi na fizičkim serverima koji apstrahuju procesor, memoriju, skladištenje i resurse u više virtualnih mašina. Dostupne su dve verzije: *VMware ESX: VMware ESX 4.0*, koji sadrži ugrađenu servisnu konzolu, i *VMware ESXi 4.0*, koja ne sadrži servisnu konzolu.

Minimalno vreme otkaza virtualnog servera i visok nivo raspoloživosti omogućeno je *VMware High Availability* funkcionalnošću. Virtualni serveri se automatski restartuju na drugom fizičkom serveru koji se nalazi u klasteru, ako je došlo do otkaza fizičkog servera na kome se nalazi. Virtualna mašina nije striktno vezana za određeni fizički server u klasteru.

Svacom virtualnom serveru se dodeljuje javna IP adresa kako bi bio dostupan sa interneta da bi korisnici mogli da ostvare pristup. Korisnicima se dodeljuju administratorska prava kako bi im se omogućila instalacija dodatnog softvera na virtualnoj mašini.

Prilikom pristupa virtualnom serveru na fajervolu se ova javna IP adresa prevodi pomoću funkcionalnosti VRF (*Virtual routing and Forwarding*) u IP/MPLS mreži, tako da svaka virtualna mašina dobija jedinstvenu IP adresu iz određenog opsega privatnih adresa servis providera (10.x.x.x/24). ISP ruter posredstvom eBGP (*extended Border Gateway Protocol*) protokola oglašava ovu adresu PE (*Provider Edge*) ruterima.

Kreiranje virtualnog servera na *VMWare* platformi podrazumeva:

- Kreiranje virtualne mašine u *VMware* okruženju

- Instalaciju operativnog sistema (*Windows* ili *Linux*)
- Instalaciju dodatnog softvera (npr. *Microsoft SQL server*)
- Alokaciju IP adrese i podešavanje mrežnih parametara (*IP mreža, VLAN*).
- Podešavanje access listi na fajervolu za odgovarajući pristup virtuelnoj mašini

Izbor operativnog sistema je na korisniku *Linux* ili *Windows* servera i samim tim se određuje način pristupa SSH (*Secure Shell*) za *Linux* ili RDP (*Remote Desktop*) za pristup *Windows* serverima. Sigurnost, u smislu ko sme da pristupi virtuelnom serveru, obezbeđena je na fajervol uređaju. ACL (*Access control list*) su konfigurisane da propštaju samo poznate IP adrese sa kojih korisnik pristupa po određenom TCP portu 22 za SSH (*Secure Shell*). SSH je mrežni protokol koji korisnicima omogućava uspostavljanje sigurnog komunikacionog kanala između dva računara. *Access listom* dozvoljavamo ili zabranjujemo određenim korisnicima i protokolima da pridu određenim mrežnim servisima.

U slučaju da korisnik pristupa sa proizvoljne lokacije i da je IP adresa internet konekcije promenljiva, sesija mora biti zaštićena, a podaci kriptovani. U tom slučaju klijent od VPN koncentratora dobija IP adresu i ostale parametre za konekciju. Opseg koji se dodeljuje SIM/USIM karticama korisnika je predefinisani i propušten na fajervol uređajima ka IP adresi virtuelnog servera.

V. III/3 BEZBEDNOST PODATAKA

Kako je klaud virtuelna tehnologija potencijalna nesigurnost po sistem dolazi od samih korisnika. Percepcija korisnika o bezbednosti postaje jednako važna kao i sam kvalitet usluge. Glavne teme bezbednosti na osnovu socijalnog stanovišta u klaudu su [6]:

1. Postoje dve ili više zainteresovane strane. U principu razne usluge su obezbeđene i distribuiraju se u klaudu. Da bi se koristila, usluga informacija o identitetu mora biti prikazana. Postoji kriterijum da se odredi značaj različitih vrsta informacija o identitetu. Ako informacija o identitetu nije bezbedna, mogu se obezbediti samo nevažne usluge. Za viši nivo korišćenja usluge potrebno je obezbediti detaljnije informacije o identitetu.

2. Sigurnost garantuje okruženje. Korisnici ne znaju kako se upravlja njihovim ličnim podacima u klaudu. Nisu u potpunosti istraženi rizici o bezbednosti ličnih podataka u smislu dostupnosti i njihovom skladištenju.

3. Postoji problem kritičnih podataka. Korisnici ne veruju u potpunosti u

sigurnost klad servisa i nisu voljni da povere svoje podatke. Mnoge obrazovne institucije grade privatne klade, ali je za to potrebno puno novca i iziskuje stručno znanje. Dolazimo do zaključka da je potrebno da se sigurnost u kladu podigne na najviši mogući nivo kako bi korisnici sa sigurnošću poveravali svoje podatke.

Sa druge strane, treba postaviti ravnotežu između bezbednosti i udobnosti. Klad se sastoji iz različitih lokalnih sistema i uključuje korisnike iz više okruženja, pa je obezbediti bezbednost u kladu komplikovano. Sigurnosni mehanizam treba da obezbedi garancijije, ali ne bi trebalo da bude previše složen, odnosno ne bi trebalo da korisnicima bude previše komplikovan. Važan faktor usvajanja popularnih komercijalnih operativnih sistema i računara je njihova otvorenost i fleksibilnost. Međutim, ovo može da bude mač sa dve oštrice, jer donosi složenost, smanjuje poverenje u bezbednost i pretnju sigurnosti. Dakle treba da postoji ravnoteža između bezbednosti i udobnosti [7].

Klad ne obezbeđuje samo poverljivost i bezbednost podataka već i njihovu pouzdanost, dostupnost, sigurnost i integritet. Da bi klad bio u službi bezbednosti, u cilju arhivske bezbednosti korišćene su tehnologije za izgradnju sigurnosnih mehanizama. U PaaS modelu, bezbednosni nivo se obično nalazi u okviru aplikacije i platforme što znači da određeni nivo odgovornosti imaju i korisnik i provajder [8].

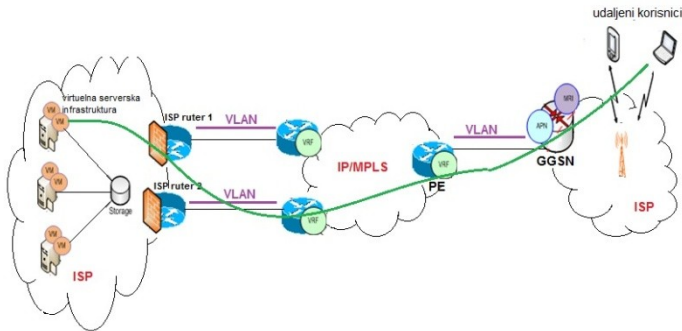
U našoj zemlji postoje odgovarajuće zakonske regulative od značaja za bezbednost podataka u kladu. S obzirom da korisnik dobija administratorska prava i sam instalira odgovarajuće aplikacije na virtuelnom serveru, on mora poštovati Zakon o privatnosti podataka i Zakon o potvrđivanju konvencije o visokotehnološkom kriminalu. Korisnici se obavezuju da neće namerno uneti maliciozni kod u mrežu servis provajdera ili Internet, napadati druge korisnike, niti ugroziti privatnost podataka.

III/4 2G/3G PRISTUP

Za svakog korisnika kreira se poseban APN (*Access Point Name*) u mobilnoj mreži kako bi se povezao sa virtuelnim serverom koji se nalazi u IP/MPLS mreži servis provajdera. IP/MPLS mreža predstavlja jezgro mreže i kroz nju prolazi sav saobraćaj servis provajdera.

Preko GPRS/EDGE/HSDPA pristupne tehnologije mobilni uređaj se povezuje na GGSN (*Gateway GPRS Support Node*) uređaj mreže mobilne telefonije. GPRS (*General packet radio service*) mreže koriste za prenos podataka brzinom od 56 do 114kbit/sec. EDGE (*Enhanced data rate for GSM*

evolution) mreža je klasifikovana kao 3G standard zato što može da obezbedi brzinu do 473,6 kbit/sec, ali je obično ograničen na 70 – 130kbit/sec. Poznata i kao napredna GPRS tehnologija. HSDPA (*High-Speed Downlink Packet Access*) tehnologija koja može da obezbedi brzinu od 7,2 Mbit/sec, ali u



Sl. 3. Pristup mobilnih korisnika virtuelnom serveru preko IP/MPLS tehnologije
stvarnosti najveća brzina je 3 Mbit/sec[9] [10].

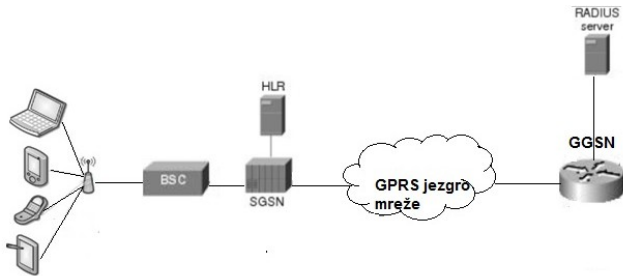
GGSN je osnovna komponenta u GSM/GPRS mreži. GGSN traga za GPRS sesijama, povezujući mobilnog pretplatnika sa odgovarajućim SGSN (*Serving GPRS Support Node*) čvorom, generišući podatke za tarifiranje i prosleđuje IP pakete između mobilnog korisnika i spoljašnje mreže. SGSN prosleđuje IP pakete od ili ka mobilnom pretplatniku u okviru svoje servisne oblasti između GGSN i BSC (*Base Station Controller*) [11]. Preko MPLS VPN tehnologije prenosi se saobraćaj od mobilne mreže do mreže ISP gde se nalazi virtuelna serverska infrastruktura. VLAN koji je kreiran za svakog korisnika predstavlja vezu između GGSN-a i PE rutera IP/MPLS mreže. Kako bi se obezbedila redundansa ISP mreža je preko svoja dva rutera na obodu mreže povezana na dva PE rutera IP/MPLS mreže. Za svakog korisnika se realizuje poseban VLAN-a na oba redundantna linka. Na Sl. 3 predstavljen je pristup mobilnih korisnika virtuelnom serveru.

Isti VLAN treba propustiti na odgovarajućem logičkom interfejsu na PE ruteru i na GGSN-u. Na PE ruteru je definisan i odgovarajući VRF. Interfejs VLAN na PE ruteru ima IP adresu iz iste podmreže kao odgovarajući interfejs VLAN na GGSN-u.

Za svakog korisnika na PE ruteru konfigurise se poseban VRF koji rutira korisnički saobraćaj unutar L3 VPN-a. Svaki VRF korisnika na PE ruteru sadrži statičku rutu ka opsegu IP adresa dodeljenih SIM/USIM karticama čiji

je next-hop IP adresa virtualnog interfejsa (VLAN-a) na GGSN-u. SIM (*Subscriber Identity Modul*) je modul za identifikaciju pretplatnika. Integrisan čip koji bezbedno čuva *International Mobile Subscriber Identity* (IMSI) broj koji se koristi za identifikaciju i potvrdu autentičnosti pretplatnika na mobilnim uređajima.

Oprema kod korisnika je terminalna oprema - mobilni telefon, PDA uređaj, GPRS modem ili bilo koji uređaj u koji je moguće ugraditi SIM/USIM karticu. Preko SIM/USIM korisnik se povezuje u jedinstvenu VPN mrežu na GGSN uređaju. Kreiranje posebnog APN-a (*Acces Point Network*) po korisniku jednoznačno identifikuje korisnika. Kada korisnički uređaj sa svoje SIM/USIM želi da ostvari logičku IP konekciju sa virtuelnim serverom, on



Sl. 4. Prijava mobilnih korisnika u mobilnu mrežu

najpre obavlja procedure prijave na 2G/3G mrežu. Za svakog korisnika postoji korisnički profil koji sadrži podatke za autentifikaciju i listu APN-ova koji su mu dodeljeni. Korisnički profili su smešteni u bazi korisnika HLR (*Home Location Registrar*). Kada korisnik pristupa preko svoje SIM/USIM kartice dodeljuje mu se APN od strane GGSN-a kojim se definišu servis i parametri za pristup. Korisnik mora da se autentifikuje i autorizuje na RADIUS (*Remote Authentication Dial-In User Service*) serveru. RADIUS je protokol između mrežnih elemenata i servera za autentifikaciju. Koristi se za autentifikaciju i autorizaciju korisnika na mrežne resurse. Važnu ulogu ima i u tarifiranju saobraćaja dobijajući informacije o trajanju sesije, korisniku i saobraćaju. Na Sl. 4 Prijava mobilnih korisnika u mobilnu mrežu.

U okviru mobilne mreže ne sme biti preklapanja IP adresa koje se dodeljuju statički ili dinamički. U oba slučaja na GGSN-u se definiše adresni opseg koji pripada mobilnoj mreži. Ako se dodeljuju dinamički koristi se funkcionalnost DHCP-a (*Dynamic Host Configuration Protocol*) koji dinamički dodeljuje adrese iz unapred definisanog pool-a adresa. U suprotnom statički na HLR-u se dodeljuje IP adresa svakoj SIM/USIM

kartici. Postoje dve različite faze u procesu povezivanja mobilnog korisnika na mobilnu mrežu:

- GPRS *attach* procedura
- aktivacija, deaktivacija i modifikacija PDP konteksta

U okviru GPRS *attach* procedure obavljaju se autentifikacija, šifrovanje i uspostavlja se logički link između mobilnog uređaja i SGSN-a. SGSN vodi računa o poziciji MS-a. Pamćenje i ažuriranje pozicije mobilnog korisnika omogućava GPRS mreži da locira MS i da mu prosleđuje pakete sa IP adresom destinacije koja odgovara datom mobilnom uređaju.

SGSN aktivira PDP (*Packet Data Protocol*) kontekst u kom se nalazi informacija o dodeljenom APN-u i zahtevanom QoS (*Quality of Service*). QoS omogućava razdvajanje saobraćaja po prioritetu. Prednost se daje prenosu glasa, jer zakasneli paketi nemaju svoju svrhu. Posle uspešno obavljene prve faze uspostavlja se konekcija između mobilnog korisnika i SGSN-a. PDP kontekst se kreira za svaku sesiju i podaci o njemu se čuvaju u HLR-u, SGSN-u i GGSN-u.

GPRS je osnovni protokol kojim se obavlja prenos IP paketa preko 2G/3G mreže. U osnovi ovog protokola je mogućnost da korisnici kreću a da pri tom ostanu povezani na jedinstven GGSN uređaj. Trenutni podaci o korisniku se prenose kroz tunel između GGSN-a koji je odgovoran za korisničku sesiju i SGSN-a koji trenutno opslužuje korisnika. Kako bi se postugla odvojenost saobraćaja o kome govorimo od ostalih servisa u okviru IP/MPLS mreži sve virtuelne mašine nalaze u jedinstvenoj VRF ruting tabeli.

IV ZNAČAJ UPOTREBE MOBILNOG PRISTUPA KLAUDU U ORGANIZACIJAMA

Upotreba mobilnog pristupa klauđu donosi značajne prednosti organizacijama. Omogućava im da umrežavaju zaposlene, što je naročito od značaja za one organizacije u kojima su poslovni procesi takvi da zaposleni deo radnog vremena provode van svojih kancelarija.

Primena mobilnog pristupa klauđu biće opisana, na primeru održavanja higijene u jednom hotelu. Realno bi bilo potrebno da za zaposlenu osobu koja održava, to jest posprema hotel poslodavac obezbedi kancelariju koja podrazumeva troškove održavanja, IT infrastrukturu, stručno osoblje za održavanje mreže. Vreme koje poslodavac izdvaja da koordinira svim procesima oko održavanja prostora, organizovanja zaposlenih, obračuna zarade je ogromno. Ako bi to vreme smanjili na minimum poslodavcu ostaje dovoljno novca i vremena za drugi posao ili odmor.

Razmišljajmo sada u ovom pravcu: Sve aplikacije su smeštene u kladu, oslobodamo se brige oko održavanja opreme kao i brige oko selekcije kadra, da li je kadar profesionalan i poseduje dovoljan nivo znanja. U ovom slučaju nam servis provajder garantuje da dobijamo najbolji tim koji se brine o sigurnosti naših aplikacija. Nije mala stvar voditi računa o bekap podacima. U slučaju da se desi poplava firma bi imala potpun gubitak podataka. U velikim sistemima mora da postoji tehnologija oporavka od havarija (disaster recovery), koji se obično nalazi na nekoj drugoj geografskoj lokaciji. Smanjujemo trošak koji je potreban da kupimo nekretninu gde bi se nalazilo sedište firme, ili da je iznajmimo na mesečnom nivou. Najzad dolazimo do zaključka da cela kancelarija, sva oprema i osoba koja je održava može da stane u jedan mobilni uređaj. Kako u ovom slučaju izgleda poslovni proces?

Osoba koja posprema nalazi se ispred hotela. Niko ne treba da vodi računa o tome kada je došla na posao. Provlači karticu i tada njeno radno vreme počinje. Preko GPRS-a dobija obaveštenje na svom uređaju da dođe do apartmana 17. Ponovo provlači karticu i pored započetog sata kada je krenulo čišćenje dobija obaveštenje da za apartman broj 17 ima 45 minuta da ga pospremi. Preko aplikacije dobija zadatke, recimo: promena posteljine, pranje prozora jer su oni na redu svake druge nedelje, usisavanje, promena peškira. Prikazuje joj se i lista posebnih želja, ako ih je gost izrazio.

Po završetku, zaposlena ponovo provlači karticu. Sada znamo koliko je radila, šta je radila i koliko ju je za svaki stavku potrebno platiti. Ovde se postiže dodatna sigurnost za goste, jer se zna kada i u koje vreme je osoblje boravilo u sobi. I na kraju, naravno, plaćanje se može izvesti elektronski – na račun se dobija novac i radni dan je gotov. Zaposlena sada možete da se opusti i druži. Naravno tu je opet potrebna pomoć mobilnog uređaja, ali u ovom slučaju ličnog, jer, recimo, poslovni ne sme da se koristi u privatne svrhe, zato što je predefinisano vreme kada može da se uključi i šta sa njega možete da se radi. Sada je zaposlena srećna što preko GPRS-a niko više ne zna gde je i može da sa svojim prijateljima da četuje koliko želi.

V ZAKLJUČAK

Dolazimo do zaključka da je sprega mobilnog pristupa i klada danas izvodljiva i veoma važna. Ona omogućava neverovatnu brzinu u poslovanju. Potreba za velikim brzinama protoka podataka, globalni roming i servisi koji zahtevaju odgovarajući kvalitet najvažniji su razlog za prelaz ka narednoj generaciji mobilnih sistema, uporedo sa ekspanzijom socijalnih mreža i

drugih potreba za kladom. Ukratko razvoj teži ka idealu: Pristup bilo odakle bilo čemu.

Dalja istraživanja mogu se bazirati i na praćenju razvoja bežičnih komunikacija koje nam nude veće brzine kao i mogućnost da lakše koristimo sve što klad može da ponudi. Konkretnije, uvođenje LTE (*Long Term Evolution*) ili 4G u mobilnim mrežama zahteva prilagodavanje pristupa prikazanog u ovom radu.

ZAHVALNICA

Zahvaljujem svojoj porodici koja je imala dovoljno strpljenja i razumevanja za vreme koje sam izdvojila kako bi ovaj rad završila.

LITERATURA

- [1] Mell, P., & Grance, T., "NIST definition of Cloud Computing," , 2011 Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
- [2] Barrie Sosinsky, "Cloud Computing Bible", Published by Wiley Publishing, Inc. ISBN: 978-0-470-90356-8
- [3] RFC 3031, "Multiprotocol Label Switching Architecture", January 2001.
- [4] RFC 3023, "MPLS Label Stack Encoding", January 2001.
- [5] Dan C. Marinescu, "Cloud Computing," 1st Edition, Theory and Practise, 2013. ISBN 9780124046276
- [6] Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H., & Kanai, A., "Risk Management on the Security Problem in Cloud Computing", 2011
- [7] Farzad, S., "Cloud computing security threats and responses," 2011. Paper presented at IEEE 3rd International Conference on Communication Software and Networks (ICCSN). IEEE Xplore doi: 10.1109/ICCSN.2011.6014715
- [8] Ren, K., Wang, C., & Wang, Q., "Security Challenges for the Public Cloud" , 2012, IEEE Internet Computing, IEEE. ISSN :1089-7801
- [9] Qadeer, M.A., Habeeb, A.A. ; Ahmad, S., "Voice over Data over GPRS/ EDGE Networks," 2009. ISBN: 978-1-4244-3334-6
- [10] D. Rouffet, S. Kerboeuf, L. Cai, V. Capdevielle, "4G MOBILE," Alcatel Telecommunications Review, 2005.
- [11] Chris Hellberg, Dylan Greene, and Truman Boyes, "Broadband Network Architectures", *Designing and Deploying Triple-Play Services*, 2007. ISBN 0-13-230057-5

ABSTRACT

This paper presents one approach to the cloud via mobile devices. It analyzes the benefits of the cloud, virtualization and balancing resources in the context of mobile access. Describes one possible server infrastructures that support this approach. We have discussed the challenges placed before decision establishes the need to ensure data security. Examines the potential use of mobile access to the cloud brings organizations. The proposed directions for further research.

**MOBILE ACCESS TO THE CLOUD USING THE MECHANISM
*MULTIPROTOCOL LABEL SWITCHING***

Tamara Sević
dr. Dušan Vujošević