TELEKOMUNIKACIJE
NAUČNO-STRUČNI ČASOPIS ZA TELEKOMUNIKACIONE TEHNOLOGIJE
ACADEMIC AND PROFESSIONAL TELECOMMUNICATIONS TECHNOLOGIES JOURNAL
ISSN 1512-8318

God. 8., br. 25., 2009. **Vol 8, No 25, 2009**

Časopis je namijenjen stručnjacima, inžinjerima, studentima i izlazi kvartalno. Svrha časopisa je izvještavanje o istraživanju, naučnom razvoju, proizvodima i novostima iz svijeta telekomunikacija.

BOSANSKOHERCEGOVAČKO
UDRUŽENJE ZA TELEKOMUNIKACIJE
SARAJEVO

Izdavač/Publisher
Bosanskohercegovačko udruženje
za telekomunikacije

Štampa/Printed by
SaVart

Časopis je evidentiran u evidenciji javnih glasila pri Ministarstvu obrazovanja, nauke i informisanja Kantona Sarajevo pod brojem NKM 42/02.

Časopis *TELEKOMUNIKACIJE* u pravilu izlazi četiri puta godišnje.
Cijena časopisa je 5 KM, za pravna lica 10 KM i za inostranstvo 5 EUR.
Račun broj: 1610000031970047 kod Raiffeisen bank d.d. Sarajevo

Adresa Uredništva
Bosanskohercegovačko udruženje
za telekomunikacije
Zmaja od Bosne 88
71000 Sarajevo
web: www.bhtel.ba
E_mail: bhtel@bih.net.ba
Tel.: 033 205–602

SADRŽAJ / CONTENTS

Zaštita djece u cyber prostoru

Cyber prostor je odgajalište za mlade umove da rastu i proširuju svoje horizonte. To je izvor znanja i informacija u digitalnom dobu i inkubator svježih ideja i inovacija, te također izobilje svega što je dobro i divno u virtuelnom svijetu zabave, gdje svako može dozvati, gotovo sa magičnom lahkoćom, sve što um želi jednim klikom prsta. Njegov meni nudi beskrajan mozaik kultura, jezika, literature, nauke i tehnologije, muzike i pozorišta, igara i sportova — i mnogo više. Ipak, cyber prostor ima svoje izazove. Kako djeca i tinejdžeri ulaze u široko otvoreni svijet cyber prostora, surfajući Internetom, upijajući njegovu enciklopedijsku širinu sadržaja, pristupajući video bibliotekama, ulazeći u „sobe za chat" i izgrađujući društvene mreže, oni su izloženi određenim elementima društva kojih bismo se klonili u stvarnom svijetu. Troje od četvero djece su voljni da online dijele lične informacije o sebi i svojoj familiji u razmjenu za robe i usluge. Jedno od petero djece je meta nasilnika ili pedofila svake godine.

Zaštita djece u cyber prostoru je, jasno, naša dužnost. Zato smo lansirali Child Online Protection (COP) inicijativu — integralni dio ITU-ove Globalne agende o cyber sigurnosti. Ona je u skladu sa našim mandatom da pojačamo cyber sigurnost i da uspostavimo osnove za siguran i zaštićen cyber svijet za buduće generacije. Mi u ITU ovo shvatamo veoma ozbiljno, i ove godine tema Svjetskog dana telekomunikacija i informacionog društva je **Zaštita djece u cyber prostoru**. Ona će utjecati na naš rad ne samo toga dana, nego i tokom cijele godine, te, također, i u budućnosti. Internet i rastuća konvergencija u online aplikacijama i mobilnim uređajima su globalni resursi kojima se mora dozvoliti da napreduju za opće dobro. Moramo nastojati da učinimo cyber prostor sigurnim, zdravim i produktivnim okruženjem za našu djecu. Moramo kreirati globalnu mrežu da zaštitimo našu djecu online propisivanjem nacionalne legislative, jačanjem izgradnje kapaciteta, podizanjem javne svijesti i unapređenjem nacionalne cyber reaktivnosti. Samo tada možemo reći da smo kreirali univerzalno pristupačno informaciono društvo, gdje se ljudsko dostojanstvo poštuje i gdje svako – naročito djeca – može imati koristi od mogućanosti koje pružaju ICT da se postignu viši nivoi razvoja. Proslavljamo Svjetski dan telekomunikacija i informacionog društva 2009. sa znanjem da smo iznijeli jaku inicijativu da učinimo cyber prostor sigurnim mjestom za našu djecu, gdje svako dijete može iskoristiti puni potencijal ICT-a, i gdje svaki građanin na ovoj planeti može iskusiti pravo da pristupi, koristi, kreira i dijeli informacije. Odlučimo, zato, da zaštitimo našu djecu u cyber prostoru i promovirajmo njihova neotuđiva prava da pristupe informacijama i znanju u sigurnom i zaštićenom okruženju.

Hamadoun I. Touré
Generalni sekretar ITU

mr. Nedžad Rešidbegović, dipl. ing. el.

Upravljanje mrežama i servisima sa inteligentnim sistemima automatskog odlučivanja i poslovnim procesima

Managing Networks and Services with Intelligent Systems Automating decisions and business processes

Sažetak

Visoki troškovi poslovanja u današnjem promjenjivom telekomunikacijskom tržištu tjeraju davaoce servisa da ih moraju postići, sa odabranim resursima, brzim prilagođavanjima na nove tehnologije, te upravljati mnoge procese većim premoštenjem kontrole. Da bi se ispunili ovi zahtjevi i trenutno zaštitio profit i visok kvalitet servisa (QoS), provajderi trebaju upravljanje sistemima čija im snaga ugrađene inteligencije omogućava da automatiziraju njihove mrežne operacije i poslovne procese. Takozvani inteligentni sistemi mogu biti korišteni da preuzmu ljudsku ekspertizu, korištenjem softverskih kodova poznatih kao pravila, koja su bazirana na dizajnu ekspertnih sistema. Takvi sistemi ne samo da mogu automatizirati poslovne procese, već također analizirati mrežne probleme za određivanje njihovog uzroka slučaja i provesti analizu predviđanja. Postoji potreba za jedinstvenim pristupom za troškovno efektivni put ka inteligentnim, automatiziranim mrežama i upravljanju servisima.

Ključne riječi: Kvalitet servisa QoS, Inteligentni sistemi, Poslovni procesi

Abstract

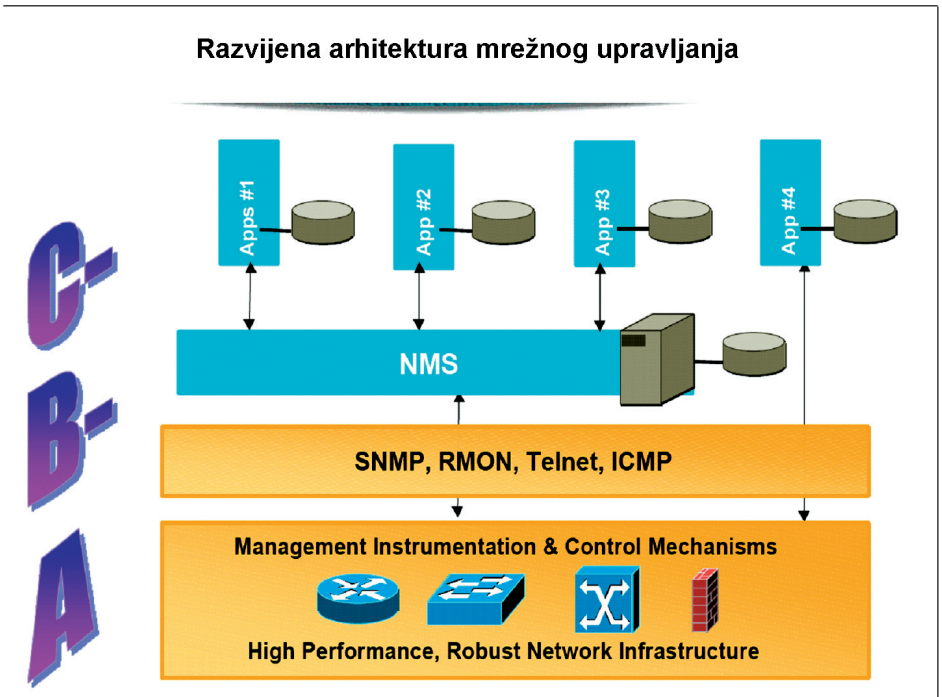
The high cost of business in today's swiftly changing communications markets, service providers must achieve more with fewer resources, adapt rapidly to new technologies, and manage many more processes across a larger span of control. To meet these requirements and simultaneously preserve profits and high quality of service (QoS), providers need management systems whose powerful built-in intelligence enables them to automate their network operations and business processes. So-called intelligent systems can be used to capture human expertise, using software code known as rules, which are based on expert system design. Such systems can not only automate business processes, but also analyze network problems to determine their root cause and perform predictive analysis. There is a need to have a unified approach to cost-effective route to intelligent, automated network and service management.

Key words: Quality of Service, Intelligent Systems, Business Processes

UVOD

Davaoci usluga komunikacija, operirajući u post-regulatornom svijetu, imaju potrebu da upravljaju poslovanjem mnogo efikasnije nego prije. Suočene s visokorazvijenom konkurencijom, nedostatkom stručnog osoblja, mnogo ponavljanim zadacima upravljanja te porastom novih tehnologija koje treba usvojiti, kompanije su primorane da stalno smanjuju vrijeme i cijenu razvoja i upravljanja novim servisima. [1] U toku prošlih godina davaoci usluga širom svijeta su agresivno otvarali nova tržišta, tehnologije i poslovanje. Bez prethodne regulatorne kontrole i usmjereni na udio u tržištu, oni investiraju nepredviđen iznos kapitala i resursa. Tako, provajderi moraju naći način da konsolidiraju upravljanje višestrukih mrežnih elemenata i sistem upravljanja elementima – element management systems (EMS), kako bi se ostvarila prednost naprednih mrežnih funkcija, tako da se mogu usmjeriti više na upravljanje uslugama. Također, davaoci usluga imaju potrebu da smanje brzinu vremena isporuke: mean-time-to provision (MTTP) za nove usluge putem različitih mrežnih tehnologija. Ultimativno, za uspješno natjecanje, moraju se sniziti brzine srednjeg vremena obnove: mean-time-to-repair (MTTR), ubrzavajući korekciju mrežnih grešaka i ciklusa rekonfiguracije integrirajući upravljanje procesima isporuke servisa i razne procese mrežne greške i izvedbe. Takvo unapređenje je sve više potrebno u vremenu pada ekonomičnosti. Da bi se ostalo u konkurenciji, provajderi komunikacija treba da rade, ne više, već pametnije, da osiguraju koristi porasta kroz visoki obrt povrata investiranja – (ROI) u mrežnu infrastrukturu.

Automatizacija je sada prihvaćena kao ključ za održanje pozicije sa konkurencijom i polagano mijenjanje tržišta i tehnologija. Dok davaoci servisa vide automatizaciju kao ključ u rješavanju mnogih izazova sa kojim se suočavaju, samo mali broj ima stvarno iskustvo u iskorištenju njihove snage na praktičan i razumljiv način. Samostalne aplikacije mogu automatizirati pojedine mrežne funkcije, ali razumljiv sistem je još san, a ne realnost. Razočarenja sa dugim i skupim projektima automatizacije čine davoce usluga zabrinutim i mnogi su skeptični u vezi s korištenjem automatizacije procesa za ostvarenje napretka više na globalnom nivou, gdje je potreba, ustvari, najveća.



Slika 1.
Razvijena arhitektura mrežnog upravljanja

IZAZOVI

Šta znači upravljanje mrežama?

Primarna uloga upravljanja mrežama je:

- Vrednovanje korisničkog iskustva (konektivnost, odgovor servisa na vrijeme itd.);
- Prihvatanje promjena u mreži (greške, korisnička mobilnost, nove on-line aplikacije);
- Primjena prilagođavanja korporativnoj politici (provjera/kontrola kod korisnika, diferencijacija korisnik/aplikacija);
- Nalaženje izvještaja za upravljanje (ko nije zadovoljan, šta je moj ROI);
- Identificiranje kako pomoći mreži kao dobit (marketing).

Mrežno upravljanje mora rasti nasuprot trendovima umrežavanja:

- *Korisnici* (više mobilni, zahtjevni i sa vještinama za potvrdu korporativne politike, naprimjer, URL blokada);
- *Aplikacije* (manje osjetljive na kašnjenje, tražnja za širokopojasnošću, multimedija, nepodržavane aplikacije od mreže, naprimjer DOOM);
- Oboje, i korisnici i aplikacije (imaju povećanu ovisnost od mrežnog zahtijevanog definiranja servisnog nivoa);
- Novi mrežni dizajni (intranet, extranet, VPN);
- Saobraćajni uzorci, naprimjer, neočekivane tačke zagušenja (povećanje kratkog vijeka „toka“, naprimjer, WEB, dinamički portovi, enkripcija, n-ta arhitektura.

Na Slici 1. data je razvijena shema upravljanja koja povezuje navedene tri odvojene cjeline. [2]

Šta će se dogoditi sa davaocima usluga?

- SNMP (Simple Network Management Protocol) će, prema stručnjacima CISCO-a, ostati kao dobar mehanizam za prikupljanje podataka (može se upravljati uređajem sa SNMP-om, ne mrežom)
- NMS (Network Management System) okviri postaju čvorovi na upravljanju intranetom.

„...arhitektura ranijih generacija produkata upravljanja nije vjerovatno da će dominirati tržištem u sljedećih pet godina” [3].

Kao najprihvatljivije rješenje (Slika 2.) danas se nameće WBEM (Web) arhitektura mrežnog upravljanja:

WBEM izgrađen na DMTF-ovom CIM

- WBMEM initiative 1996 Cisco, Compaq, Microsoft, Intel, MBMC su:
  1. izgradili zajednički informacioni model CIM (Comon Information Model) za upravljanje i
  2. iskoristili snagu Weba za upravljanje interoperabilnošću => CIM &XML čine WEBM osnovnu tehnologiju

Dakle, šta je to CIM:

- *CIM, zajednički informacioni model* – definira sheme koje se koriste da predstave realni svijet objekata koji se upravljaju. CIM koristi objektno-orijentiran obrazac, gdje upravljivi objekti i njihove međusobne relacije se modeliraju korištenjem koncepta

i klasa i instanci. Vendori proširuju standardne klase da predstave jedinstvene buduće/funkcije. Moglo bi biti korisno razmisliti o CIM-u kao standardu i proširenim MIB-ovima, koji također uključuju odnose i definicije.

- *Objektno orijentirani informacioni model* – konceptualni okvir u kojem se svaki informacioni sistem može modelirati. Nezavisan repository i implementacija standardizacija podataka i redukcija njihove složenosti. Podržava široko korporativno upravljanje podacima, naprimjer, nasuprot node-centricu. Dopušta integraciju upravljanja informacijama sa raznih izvora i sa raznim sintaksama.
- *Osnovni model* – preuzima informacije koje su aplikativne za sve domene znanja.
- *Zajednički model* – standard. Informacijski korporativno upravljanje određenim oblastima, ali nezavisno od pojedine tehnologije ili implementacije. Uključuje sisteme, aplikacije, mreže, baze podataka i događaje.
- *Prošireni modeli* – predstavljaju dobavljača za prošireni produkt koji je često ovisan od određene platforme ili okruženja.

Pitanje je zašto objektno orijentiran, a ne jednostavno samo shema?

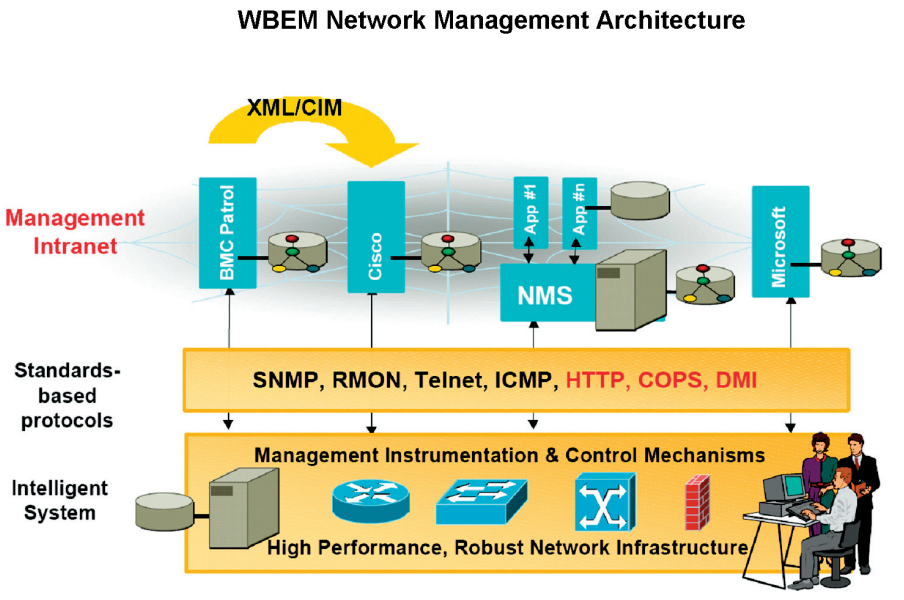
- Mrežni elementi i servisi se razlikuju od drugih objekata direktorija. Standardni objekti su jednostavni i postoje unutar statičkih granica, kao korisnik je uvijek korisnik. Mrežni elementi i servisi su kompleksni objekti i postoje u konstantno promjenljivom okruženju, kao modularni switch može mijenjati funkcije.

Model mora djelovati unutar mrežnih elemenata, mrežnih servisa, mreže i klijenata mreže.

Elementi CIM-a:

CIM objektno orijentirani gradivi blokovi:

– klase objekata (tipovi),
– naslijeđe (ponovno korištenje, proširenje vendora),
– pridruživanje i agregacija (odnos između objekata),



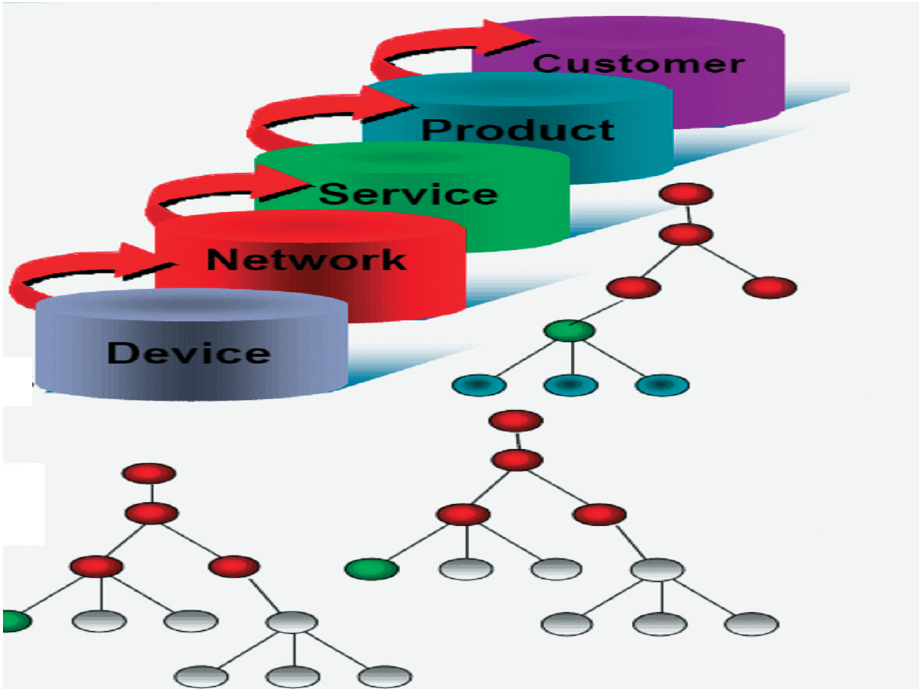
Slika 2.
WBEM arhitektura mrežnog upravljanja

– glavnina (broj komponenti koje učestvuju u svakoj strani odnosa),
– ograničenja i meta-podaci (kako se jedan objekt ili relacija koristi).

„Možda CIM, najvažniji diferencijator od ranijih standarda ima njihovu sposobnost da pokaže relacije između raznih elemenata i komponenti koje čine kompjuterski sistem ili korporativnu mrežu“, prema Elisabet Horwitt.

Izgradnja blokova za CIM i upravljivi objekti u CIM-u:

- fizički i logički elementi
– ranija sposobnost za sažimanje kompleksnih objekata (kao što je ruter) u njihove fizičke i logičke aspekte;
– širok dijapazon aplikacija (od žica i čipova kroz rutere, komutacije, kompjuterske desktopove i sisteme).
- pridruživanje i agregacija – objedinjavanje
– opis relacija između dviju klasa i karakteristike odnosa;
– primjer: servis (OSPF) radi unutar fizičkog elementa (ruter) i u zajednici je korišten za opis i odnose.



Slika 3.
Objektno orijentirani informacioni model

IZBOR AUTOMATIZACIJE DANAS

Razmotrimo današnje opcije za automatizaciju sistema mrežnog upravljanja:

Vlastiti razvoj (In-house development) — korištenje uobičajenih softverskih programa, kreiranih od vlastitih programera ili konsultanata za automatizaciju upravljanja isporukom servisa, osiguranje i korištenje je dugotrajno i skupo. Ovakav pristup je, također, nepraktičan u današnjem stalno promjenljivom tržištu, zato što zahtijeva dugi ciklus razvoja za kreiranje aplikacija koje nije lako poboljšavati ili mijenjati. Vlastiti razvoj čini kompaniju zavisnom od stalnog pristupa programskim ekspertizama, dodajući besmislen rizik od automatizacije projekta.

Paketirana rješenja (Packaged point solutions) — Korištenje paketiranih rješenja za automatizaciju upravljanja specifičnih funkcija, kao što su fault i performance, rijetko unapređuje ukupnu efikasnost zato što se takve aplikacije teško mijenjaju ili proširuju iznad njihove originalne cjeline. Tipično, nedostatak sposobnosti da se dijele podaci ili procesi sa drugim aplikacijama upravljanja rezultiraju duplikacijom i prelaskom u područja kao što su trening, održavanje, podrška, a da ne spominjemo potrebu da se djeluje sa višestrukim vendorima i protokolima. Sve ovo čini pojedina rješenja manje efikasnim i vrijednim za kompanijske poslovne napore.

Inteligentni sistemi – Oni uključuju korištenje:

– ekspertnih sistema,
– upravljanja baziranog na politici,
– automatizacije procesa upravljanja.

Takvi inteligentni sistemi će se razmotriti u ovom dijelu uz primjenu na NGOSS upravljanja, posebno za osiguranje i isporuku servisa [6].

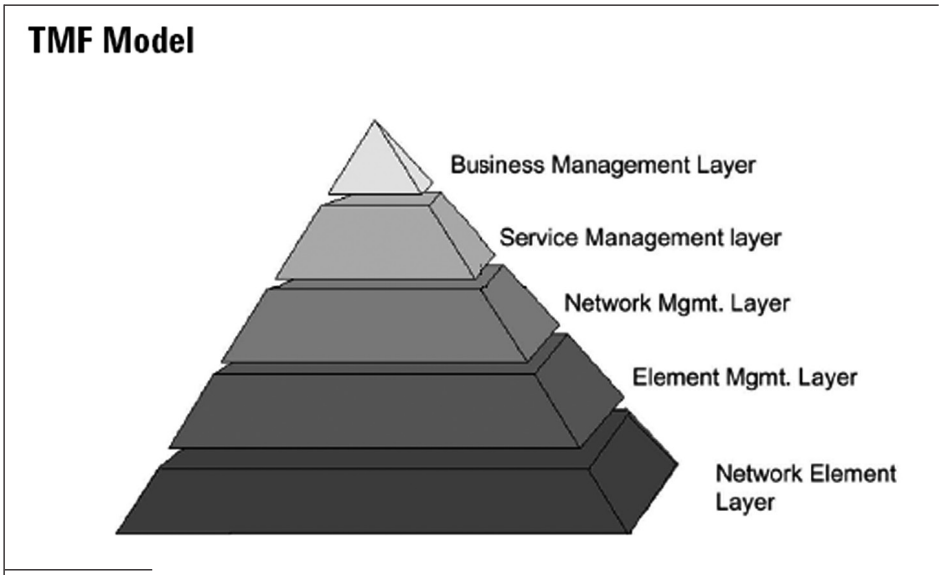
INTELIGENTNI SISTEMI

U akademskom polju nastalo je za umjetnu inteligenciju – artificial intelligence (AI) – nekoliko različitih pristupa kako bi unaprijedili kompjuterizirane sisteme koji su korišteni za rješavanje komercijalnih problema. Među njima su robotika, computer vision, neuralne mreže i ekspertni sistemi. Ekspertni sistemi su kompjuterski sistemi koji pohranjuju rezultate ljudskih iskustava i mogu djelovati na tako sakupljenom znanju. Ekspertni sistemi podrazumijevaju razne koncepte, procedure i tehnike za dostizanje i ponovno korištenje kompanijske ekspertize u implementiranju rezultata za veću efikasnost, koji prelaze ograničenja konvencionalnog programiranja. Koristeći se programskim jezicima visokog nivoa, takav sistem podrazumijeva pravila bazirana na znanju za procesiranje (obradu) informacija baziranih na pohranjenim iskustvima o tome koje akcije se zahtijevaju u datoj situaciji. Kroz ovakvu sposobnost za predstavljanje ovakvih informacija u lingvističkom i vizuelnom obliku i djelovanje na nju kroz logičke interfejse, sistem baziran na pravilima može uhvatiti smisao predmeta specijalista ekspertize i pohraniti ih u baze podataka za ponovno korištenje u funkcijama upravljanja za automatizaciju mreže. Nasuprot neuralnim mrežama, koje su također prema produktima studija umjet-

ne inteligencije (AI), ekspertni sistemi ne mogu učiti na vlastitom iskustvu. Takav sistem je onoliko pametan koliko i osoba koja piše pravila na kojima je sistem baziran. To su inžinjeri znanja koji su stručni u pretresanju specijalističkih tema i koji ih prevode u pravila programskog jezika visokog nivoa. Ova pravila se zatim pohranjuju u mašinu za pravila rada ili bazu znanja.

UPRAVLJANJE BAZIRANO NA ZNANJU

Znanje (*knowledge base)* je dio ekspertnog sistema koji sadrži činjenice i heurističko učenje *(bazirano na učenju, otkrivajući činjenice iz vlastistog iskustva)* u određenom domenu. Takvo znanje može biti u formi modela podataka, pravila međusobnih odnosa i dijaloga. Praveći poređenje i uzroke bazirane na znanju pohranjenom u pravilima, ovakav tip sistema obrade informacija i izvedenih funkcija sličnih akcijama koje bi stručno lice koristilo, baziran je na dizajnu ekspertnog sistema, koji koristi softver za simulaciju ljudskih akcija i odluka. Sistem baziran na pravilima može također poslužiti kao osnova za automatsko procesiranje visokog nivoa. Takav sistem može čak biti razvijen da uči automatski kako se mijenja status mreže, koristeći samootkrivanje i druge tehnike automatskog učenja. Izvedeno na osnovu istraživanja iz AI, ekspertni sistemi kao ovi postali su interesantni telekom-industriji tokom 1980-ih. Jednu deceniju poslije, domeni specifičnih eksperata ili sistema baziranih na pravilima bili su razvijeni da tokove diskretnih funkcija, kao što su mrežni alarmi kod nadzora i organizacije, počinju razvijati standarde za modeliranje podataka koje se odnose na mreže. Od tada mnogi veliki operatori su izabrali ovakav put za brže pružanje usluga na tržište. Softver baziran na pravilima također se može koristiti da se dostigne informacija specifične aplikacije i njihovo pohranjivanje sa drugim informacijama baziranim na znanju, omogućavajući servis provajderu da kreira sistem upravljanja koji imitira ljudsko rješavanje problema. Potican potrebom za boljim načinom



Slika 4.
TMF model upravljanja mrežama i servisima

automatskog upravljanja kompleksnim NGN mrežama, neki dobavljači koriste ekspertne sisteme projektirane da unaprijede inteligenciju operatorovog softverskog OSS sistema podrške.

Za kompletniju sliku, pregledajmo zahtijevane komponente za jedan ekspertski pravilima baziran sistem:

- Domen takvog sistema je upravljanje mrežnom infrastrukturom, fiksne, mobilne i podatkovne IP [uključivo voice-over-packet (VoP) i treće generacije (3G) bežični pristup].
- Predmet eksperta čije znanje se mora pribaviti jeste tipično za menadžera mrežnog operatora, inžinjera, elementa dobavljača ili tehničara lociranog na udaljenom mjestu.
- Sistem korisnika baziran na pravilima su osoblje centara mrežnih operatora (NOC) koji moraju tražiti razne komponente sistema za osnovne podatke o tome kako mreža ili servisi funkcioniraju.
- Inžinjer znalac ili pisac pravila (procesa) jeste kompjuterski pismena osoba koja sakuplja intervjuirajući ekspertni predmet i pregleda ekspertnu dokumentaciju o mrežnom domenu.
- Mašina znanja – ponekad zvana u uzročna mašina, jeste server koji precesuira pravila kad se povuku sa vanj-

skim poticajima od ljudi, mrežnih elemenata ili vanjskog OSS sistema podrške.

- Konačno, ekspertni sistem baziran na znanju jeste upravljanje bazirano na informaciji (MIB) za domen pohranjivanja podataka i relacija izvedenih sa elemenata, mreža, servisa i poslovnih ciljeva. Ovo omogućava osnovu za mrežno dizajniranje i pridruživanje, korelaciju izvora uzroka, utjecaja na analizu i drugih ključnih funkcija mrežnog upravljanja.

UPRAVLJANJE BAZIRANO NA POLITICI (POLICY-BASED MANAGEMENT)

Vrijednost kao što je sistem baziran na pravilu može biti kao prvi korak u zadovoljenju današnje urgentne potrebe za automatiziranjem donošenja odluke u komunikacijskom okruženju. Potreba za upravljanjem mnogim novim servisima i usvajanjem novih tehnologija i protokola koji traže pametniji sistem upravljanja u težnji za efikasnošću koji kombinira snagu sistema baziranog na pravilima sa ponovnim korištenjem politike i automatiziranih procesa.

U nedostatku načina za postizanje opće kontrole mreža i usluga, provajderi moraju sakupiti odvojene sisteme koji rade u više različitih dijelova njegove organizacije i pokušati koordinirati rezultate. Ironijom, jedna komplikacija ove dileme je da kako tehnologija postaje jeftinija i vrijednija, veći zahtjev se postavlja pred stručnjake koji nedostaju i sakupljaju. Ovaj pristup resursima, uporedo sa potrebom za upravljanjem preraslim brojem procesa, napravio je ponovno korištenje, ugrađeno u inteligenciju i automatizaciju sa velikim prioritetom za sisteme upravljanja.

Upravljanje bazirano na politici, mnogo efikasniji način za postavljanje ekspertnih pravila, dalje unapređenje provajderove sposobnosti da modificira i mijenja način na koji je mreža upravljana. Kako je ekspertiza stvorena i modelirana, rezultiraju pravila koja se mogu grupirati da kreiraju politiku kako bi ih provajder mogao ponovo koristiti da automatizira upravljanje mrežama i servisima. Na osnovu poznatog ponašanja mreže, takva politika se pakuje po pravilu da mogu automatski izvesti upravljanje osiguranjem servisa, isporukom i funkcijama korištenja.

Politika igra važnu ulogu u današnjim sistemima upravljanja baziranim na znanju. Uzmimo trenutak da razumijemo kako je uključeno korištenje politike u takvim sistemima. Razmotrimo model TeleManagement Forum's (TMF) [5] široko prihvaćen standard za upravljanje mrežama i servisima. Svaki sloj gradi sljedeći blok, polazeći od sloja upravljanja elementima – element management layer (EML) i dalje nastavljajući prema sloju mrežnog upravljanja – the network management layer (NML) i slojevima za upravljanje servisima i poslovanjem (Service & Business Management Layers – SML & BML)).

PROCES IDENTIFIKACIJE POJEDINAČNIH UZROKA GREŠAKA MREŽE

Predstavlja „Sveti Gral" u osiguranju isporuke servisa. Proces identifikacije pojedinačnih uzroka greške mreže je drugi način vrednovanja unapređivanja inteligencije softverskog upravljanja i posebno sistema za osiguranje usluga – servisa. Sofisticirani softver uzroka događaja može pružiti mnogo inteligentniji osnov za automatsku korekciju mrežnih grešaka kroz mreže, sisteme i aplikacije pomoću tehnika kao što su korelacija događaja, ograničavanje i odbacivanje sadržaja.

Neki OSS provajderi koriste pogon korelacije baziran na pravilu kao pomoć u pružanju tih funkcija. Drugi imaju kontrolirana pravila sa politikom i neki imaju također uključenu statističku analizu poznatu i kao SPC – statistical process control. Kako provajderi treba da primijene takve tehnike za nadzor većeg, mnogo globalnijeg okruženja, automatizacija postaje čak mnogo kritičnija za dijagnosticiranje i korekciju mrežnih i servisnih problema. Studija o tome kako je problem

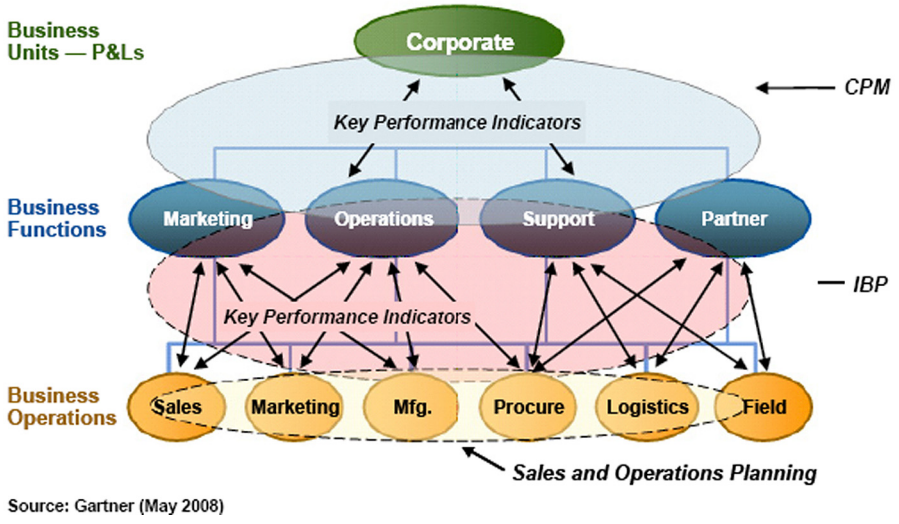
utjecao na korisnike i servise izgrađena je na analizi uzroka događaja, korištenjem naprednih korelacija događaja za podudaranjem izvjesnih mrežnih događaja sa servisima koji su potencijalno afektirani od njih. Uspjeh ovakvih tehnika ovisi o tome da OSS ima model popravke mrežnih resursa za indikaciju gdje su problemi nastali kroz domene, mrežni i servisni sloj ili čak komponente.

Analiza uzroka događaja i politika

Za ostvarenje koristi od analize uzroka događaja, kompanije počinju da primjenjuju politiku na kompleksnu korelaciju i scenarija ograničenja. Korelacija i ograničavanje mogu biti definirani kao posebne tehnike za smanjenje srodnih uzbuna u upravljanju mrežnim greškama. Cilj politike korelacije je da preuzme uzbune primljene sa višestrukih mrežnih elemenata i korelira ih sa Izvorom događaja kao što je neraspoloživost mrežnog elementa, prekida optike ili loše mrežne komponente – naprimjer, elektronska ploča, završna tačka ili port. To pokreće da su sve uzbune skinute i/ili zaustavljene i nove uzbune se generiraju da odrede pojedine uzroke događaja. Cilj politike blokiranja-suppresije u drugu ruku je da identificira uzrok događaja kako se glavna uzbuna širi, dok su sve druge uzbune neselektivno i u izraženoj mjeri zaustavljene. Naprimjer, kad padne ruter IP mreže, svi daljnji alarmi rutera su zaustavljeni kako ne želе da uzbude NOC osoblje. Slično u kablovskoj strukturi – ako glavni pojačivač ispadne dobro, konstruirana politika može osigurati supresiju svih daljnjih uzbuna vanjske kablovske strukture. Drugi primjer uključuje prigušenje svih uzbuna sadržanih na polici mrežnog elementa, u skladu sa višim nivoom greške na fiksnoj komutaciji i u bežičnom domenu, naprimjer, može uključiti blokiranje svih daljih uzbuna pojedinih ćelija, slijedeći obuhvat kontrolora baznih stanica.

Nastanak integriranog poslovnog planiranja

Mnogi operativni procesi i prodaja (S&OP-Sales & Operation Planing) nemaju stratešku dimenziju koja povezuje najviši nivo kompanije do samog dna. [7]



Slika 5.
Relacije između CPM, IBP i S&OP

Kako bi se popunila ova praznina, sljedeća generacija S&OP je počela da objedinjuje što „Gartner“ naziva IBP – integrirano poslovno planiranje. IBP pruža stratešku vezu da S&OP je uvijek u funkciji da bude, što je povezivanje „mreža“ između strategije i operative. U praksi, IBP treba postaviti kao dodatni sloj procesa preko vrha operativnog S&OP procesa. Sada se IBP vidi kao predstavnik kasnijeg stadija zrelosti poduzećkog S&OP razvoja. Također, IBP proces zahtijeva rijetko različite tehnološke podrške od S&OP. Ključni zahtjevi za IBP sposobnost uključuju:

- *Eksplicitni proces mapiranja*: IBP treba da bude podržan sposobnošću da eksplicitno definira proces koji je bio modeliran i da bude u stanju lako mijenjati ovaj model procesa kako su zahtijevane različite evaluacije.
- *Jako finansijsko modeliranje*: IBP treba da bude podržan sposobnošću da efektivno modelira finansijski učinak ranije razvijenih različitih operativnih strategija. To uključuje efektivni povrat investicija isto kao i učinak na profit i gubitak preduzeća (P&L), bilans stanja i protok novca. Sposobnost da se pruži razumljiva analiza profitabilnosi produkta/kupca koja će biti vrednovana.
- *Holističan pogled na lanac snabdijevanja:* IBP treba da se podrži sposob-

LITERATURA

[1] – Raymond W. Smith, *Annual Review of Communications*, IEC-1994/5

[2] – John Thomas; *Upravljanje mrežama i aplikacijama u novom milenijumu*, www.cisco.com, 2007.

[3] – Susan Aldrich &James Herman, *Intelligent Systems & Automating decisions for business processes*, Northeast Consulting Resources, 2008.

[4] – Rob Mattison: *Data Warehousing & Data Mining for Telecommunications*, Artech House - Boston [1997]

[5] – WWW/telemanagement.forum.com [2005]

[6] – Kurt Schlegel, Bhavish Sood, *Business Intelligence Platform Capability Matrix*, Gartner, 23 April 2007

[7] – "*Integrated Business Planning Is the New Sales and Operations Planning*" and "*Hype Cycle for Supply Chain Management and Procurement"*, 2007.

[8] – Michael Smith, Bill Gassman, John E. Van Decker, *Using Key Performance Indicators to Facilitate Business Process Improvement*, Gartner, June 2008.

nošću da modelira kompletne procese lanca snabdijevanja, ukuljučujući, ako je odgovarajuće, procese koji se proširuju u baze korisnika i dobavljača. Ključno ograničenje lanca snabdijevanja treba da bude predstavljeno u modelima koji daju realističnu procjenu alternativnih strategija.

- *Ekstenzivna optimizacija i sposobnost poslovnih pravila:* IBP treba da se podrži sposobnošću značajnom optimizacijom, simulacijom sposobnošću poslovnih pravila za podršku rješavanju kompleksnih interakcija kroz procese. Dodatno rješavanju kompleksnih problema optimizacije sa razumnom brzinom, IBP će biti ključ razvoja odgovarajućeg broja alternativnih strategija na neophodnom nivou detalja.
- *Saradnja:* IBP treba da se podrži sposobnošću saradnje koja omogućava dijeljenje i širenje evaluiranih strategija i podruštvljava razne pretpostavke, podupirući one „šta ako".
- *Jake veze u S&OP:* imajući izvedene optimalne strategije za praćenje ovih potreba, koje treba da se prenesu natrag kroz S&OP, kako bi bio konvertiran u politiku operativnih planova, izvršen putem operativnog planiranja i izvršenja procesa i nadziran u smislu udovoljenja..
- *Pristup za analitike podržavanja,* kao što je upravljanje radom produkta, koji prati rad produkta kroz lanac snabdijevanja i prenosi natrag u proces strategijske evaluacije.

Da se dostigne upravljanje radom produkta, jedinstven pogled na osnovne podatke kroz potrebe preduzeća da budu raspoložive procesima planiranja. Dodatno, povezivanje analitičke sposobnosti tijesno povezane sa modeliranjem procesa (konvergencija BI i poslovnih aplikacija) jeste preduvjet.

Slika 1. pokazuje tri nivoa upravljanja radom kao i veze između IBP i S&OP i odgovarajući fokus i dodirne tačke za ove poslovne procese. [8]

IBP je strateško planiranje i okvir konzistencije koji ujedinjava planove kroz funkcije poslovanja i integrira ove planove u razumljive ključne indikatore rada. Jedan od njegovih ključnih rezultata jeste da konvertira strategijske planove u značajne finansijske planove koji pokazuju učinak visokog nivoa strategija na ključne finansijske izvještaje organizacije. IBP, međutim, ima vrlo jaku vezu između kompanijske CPM strategije i procesa. S&OP proces stoji ispod sloja IBP i povezuje integrirane i finansijski potvrđene, strategijske planove (kao rezultat IBP procesa) sa operativnim planovima na funkcionalnom/poslovnom nivou operacija u kompaniji. Imajući ova tri sloja (CPM, IBP and S&OP) na mjestu koje pruža i integrira od vrha do dna upravljanje radom i okruženjem planiranja, značajno će se unaprijediti sveukupni rad lanca snabdijevanja preduzeća kroz zajedničke mjere, strategijsko „šta ako", evaluaciju, povezivanje i integriranje operativnog planiranja.

ZAKLJUČAK

Današnje upravljanje radom davalaca servisa je usko povezano sa kvalitetnim planiranjem. S druge strane, kvalitetno planiranje ne obuhvata strategijsko, poslovno i operativno planiranje. Jasno je da se ono provodi u dinamički promjenjivom okruženju. Iz tog razloga nužno je uvesti i izgraditi takve sisteme automatizacije i inteligencije, kako bi se brzo odgovorilo na postavljene izazove. Tek tako kompleksno uspostavljen sistem rada tehnologija ljudi i procesa dat će prave efekte i pomoć kompanijama da na vrijeme i ispravno reagiraju.

KEYMILE
access to the world

»Kada da očekujem Triple Play uslugu u svom domu?«

MileG@te

Glas, Širokopojasni Internet i Televizija preko jedne linije, preko jedinstvenog sustava.

Milegate NGN Access Nod, uređaj slijedeće generacije će korisniku dati bezgraničano "Triple Play" iskustvo. Integracija glasa, Širokopojasnog Interneta i Televizije postaje realnost. Brzina: neblokirajuća arhitektura, omogućava preko 20 Mbs prema svakom korisniku istovremeno. Realizacija: MileGate obitelji, sa izvedbom od 1-8 U daje visoku gustinu sučelja sposobnu da se integrira u bilo koju mrežnu topologiju - Bez obzira da li se planira centralizirana arhitektura ili distribuirana arhitektura sustava sa vanjskim instalacijama.
MileGate - Vaša vrata za pristup budućnosti.

www.keymile.com

Za KEYMILE program, molimo vas da kontaktirate UNIS Telekom d.d.

UNIS Telekom d.d.

Dr. Ante Starcevca 50
88000 Mostar, BiH
Telefon: (036) 314-407
Fax: (036) 314-408
www.unistelekom.ba

SUPER BRZI INTERNET

Ako Vas uspavljuje čekanje da se nešto skine s Interneta, sigurno će Vas razbuditi nova ponuda super brzog Interneta!

ADSL START	512/128 kbit/s
ADSL MEDIUM	1024/192 kbit/s
ADSL PROFI	2048/256 kbit/s

HTMOSTAR

Besplatni info telefon: 0800 888 88
www.ht.ba

mr. Hakija Grabovica, dipl. ing. el.

Menadžment radio resursa u UMTS-u
Radio resource management in UMTS

Sažetak
Nedostatak raspoloživog spektra, što se posebno vidjelo na aukcijama koje su prethodile konačnoj raspodjeli licenci za UMTS operatore, ukazao je na veliku važnost efikasnog korištenja spektra. Radio pristupne mreže poput UTRAN u UMTS-u sasvim sigurno koriste spektar efikasnije od 1G i 2G sistema upotrebom unaprijeđenih tehnika kodiranja, višestrukog pristupa, diverziti shema itd. S druge strane, WCDMA tehnika usvojena u UTRAN-u čini preciznu kontrolu interferencije generisane ovim pristupom ključnim problemom za pouzdan rad sistema. Uz to, fleksibilnost i velike bitske brzine u UMTS-u čine kontrolu interferencije još težom. Zato, proizvođači moraju uvesti, svaki na svoj način, mnogo veću upotrebu strategija menadžmenta radio resursa nego što je to bio slučaj u prošlosti, kako bi se postiglo efikasno korištenje raspoloživog spektra uz istovremeno očuvanje QoS-a po servisu na utvrđenim vrijednostima.
Ključne riječi: 3G, CRRM, RRM, RRU, QoS, UMTS, UTRAN;

Abstract
The scarcity of available spectrum, particularly as seen in the auctions that preceded the final licences allocation for UMTS operators, has draw attention to a large importance of using the spectrum efficiently. Radio access networks such as UTRAN in UMTS certainly exploit spectrum more efficiently than 1G and 2G by using advanced coding technics, multiple access, diversity schemes, etc. On the other hand, the WCDMA technique adopted in UTRAN makes the accurate control of the interference generated by this access a key issue for reliabile function of the system. In addition, the flexibility and high bit rates in UMTS makes interference control even more difficult. Therefore, manufacturers have to introduce, on a proprietary basis, much more utilization of Radio Resource Management strategies than in the past, so that an efficient use of the available spectrum can be achieved but in the same time retention of the QoS per service at the agreed values.
Key words: 3G, CRRM, RRM, RRU, QoS, UMTS, UTRAN;

INDEKS POJMOVA I SKRAĆENICA

3G (*3 Generation*), treća generacija bežičnih mobilnih ćelijskih sistema
3GPP (*3G Partnership Program*), ugovor o saradnji između ETSI (Evropa), ARIB/TTC (Japan), CCSA (Kina), ATIS (Sj. Amerika) i TTA (Južna Koreja), čiji je zadatak da specificira standarde 3G telefonije, u okviru ITU projekta IMT-2000
4G (*Fourth Generation*), četvrta generacija mobilnih komunikacija
AAA (*Authentication, Authorisation & Accounting*), autentifikacija, autorizacija i obračun
APC (*Access Point Controller*), kontroler pristupne tačke
BSC (*Base Station Controller*), kontroler bazne stanice

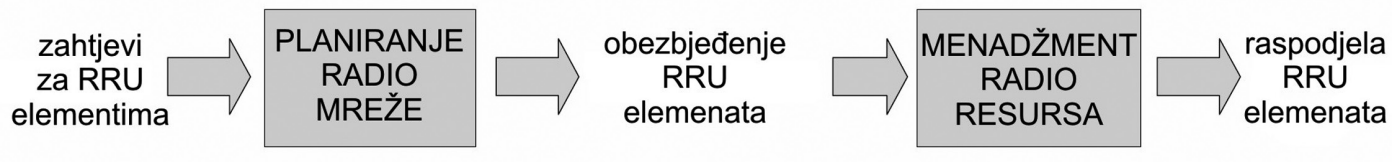
1. UVOD

Nedostatak raspoloživog spektra, što je bilo očito tokom aukcija koje su prethodile konačnoj raspodjeli licenci za UMTS operatore, ukazao je na veliku važnost efikasnog korištenja spektra. Premda UMTS različitim naprednijim tehnikama efikasnije koristi spektar nego prijašnji sistemi, precizna kontrola interferencije inherentne WCDMA pristupu jeste ključna za dobar rad sistema. Osim toga, fleksibilnost UMTS radio interfejsa i veće bitske brzine dodatno otežavaju kontrolu interferencije. Zato, proizvođači moraju, svaki na svoj način, posvetiti mnogo više pažnje strategijama menadžmenta radio resursa nego do sada, da bi se raspoloživi spektar što bolje iskoristio. RRM (*Radio Resource Management*) tehnike u cjelini moraju očuvati QoS po servisu na utvrđenim vrijednostima na temelju kompromisa.

2. KONCEPT RADIO RESURSA

Na početku je neophodno uvesti koncept radio resursa, koji se oslanja na element radio resursa (RRU). RRU (*Radio Resource Unit*) element određen je skupom osnovnih fizičkih parametara prijenosa neophodnih za podršku valnog oblika signala koji prenosi informacije krajnjeg korisnika u skladu sa referentnim servisom. Tako kod FDMA, RRU element odgovara određenom propusnom opsegu unutar date noseće frekvencije. Kod TDMA, RRU element odgovara nosećoj frekvenciji i vremenskom slotu.

Kod CDMA, RRU element je određen nosećom frekvencijom, kodnom sekvencom i nivoom snage. Osnovna razlika u odnosu na spomenute tehnike jeste da kod CDMA potrebni nivo emitovane snage neophodan za održavanje veze nije fiksan već ovisi o nivou interferencije [1]. Na primjer, za pružanje datog servisa u UTRAN FDD koristi se 5 MHz dio u opsegu od 2 GHz, te ortogonalni OVSF (*Orthogonal Variable Spreading Factor*) i skrembling kodovi. Unatoč tome, iznos emitovane snage mijenjat će se u vremenu u ovisnosti o više elemenata, kao što



Slika 1.
Veza između planiranja radio mreže i menadžmenta radio resursa

INDEKS POJMOVA I SKRAĆENICA

CN (*Core Network*), jezgro mreže
CRRM (*Common Radio Resource Management*), zajednički menadžment radio resursa
CS (*Circuit-Switched*), kanalna komutacija
FDD (*Frequency Division Duplex*), dupleks s frekvencijskom raspodjelom za uplink i downlink smjer signala u isto vrijeme
GERAN (*GSM/EDGE Radio Access Network*), GSM/EDGE radio pristupna mreža
GGSN (*Gateway GPRS Support Node*), čvor za podršku GPRS gejtveja
GPRS (*General Packet Radio Service*), opći mobilni paketski radio servis
HSS (*Home Subscriber Server*), domaći pretplatnički server
IEEE (*Institute of Electrical and Electronics Engineers*), međunarodna neprofitabilna organizacija; udruženje inžinjera, naučnika i studenata iz oblasti elektrotehnike i elektronike
IMS (*IP Multimedia Subsystem*), IP multimedijski podsistem
PS (*Packet Switched*), paketska komutacija
QoS (*Quality of Service*), kvalitet servisa
RAN (*Radio Access Network*), radio pristupna mreža

su propagacioni uvjeti, interferencija, nivo opterećenja ćelije, itd.

Osim toga, u situaciji s višestrukim servisima, svaki servis može trebati različite iznose RRU elemenata. Naprimjer, servisi s višom bitskom brzinom će zahtijevati više RRU elemenata. Bit će potreban dodatni opseg kod FDMA, dodatni vremenski slotovi kod TDMA ili dodatne kodne sekvence zajedno sa višim nivoima emitovane snage kod CDMA.

3. PLANIRANJE RADIO MREŽE

Cilj mrežnog operatora jeste implementacija mreže koja može podržati njegove korisnike sa zahtijevanim QoS u ciljanom području pokrivanja. U tom smislu, u cijeloj mreži treba riješiti nekoliko problema: dizajn radio mreže, prijenosne mreže i jezgra mreže. Kad je u pitanju radio segment, problem je obezbijediti dovoljno RRU elemenata u cijelom servisnom području s dovoljnim kvalitetom.

Ulaganje u infrastrukturu radio mreže je proporcionalno broju korištenih baznih stanica ili Node B [2], što raste sa:

- brojem korisnika koje treba podržati;
- servisnim područjem;
- prosječnom brzinom prijenosa korisnika;
- traženim QoS nivoom.

Troškovni element povezan sa pružanjem QoS igra ključnu ulogu. Najlakši način za garantovanje QoS jeste predimenzioniranje mreže i obezbjeđivanje veoma velikih radio resursa. Jasno, izazov je pružiti traženi QoS nivo s minimalnim resursima, te tako minimizirati ulaganja operatora uz ispunjenje zahtjeva dizajna mrežne. Osim toga, 3G mreže moraju podržati raznolike servise, uključujući one koji su sada dobro znani, kao i one koji će se pojaviti u budućnosti. Zato, QoS koncept za 3G radio interfejs treba biti fleksibilan i praktičan, tj. treba biti jednostavan za implementaciju i imati mali obim kontrolne signalizacije.

Planiranje radio mreže ima kao posljedicu obezbjeđenje RRU elemenata u čitavom servisnom području putem određene topologije radio mreže i date konfiguracije ćelijskih lokacija. Treba istaći da, sve dok su aspekti poput uvođenja novih servisa i upotrebe servisa promjenljivi u vremenu i prostoru, iznos RRU elemenata koje treba obezbijediti također je promjenljiv vremenski i prostorno. Shodno tome, planiranje radio mreže jeste proces koji stalno evoluira.

4. MENADŽMENT RADIO RESURSA

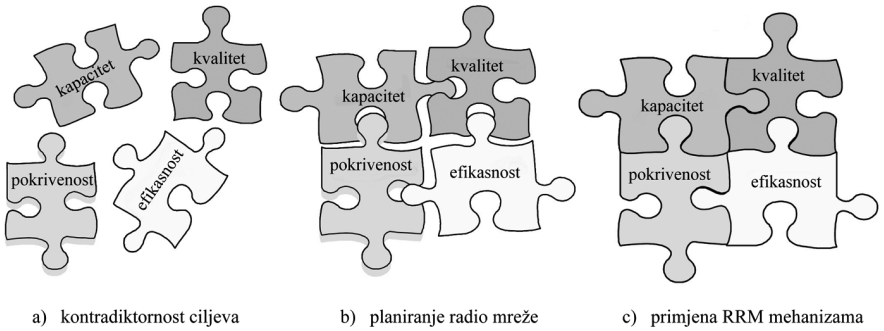
Pokretanje komercijalne radio mreže očituje se skupom zahtjeva za RRU elementima, tako što je dati iznos RRU elemenata obezbijeđen u cijelom servisnom području u određenom vremenu [1]. Zato je potrebna odgovarajuća raspodjela RRU elemenata različitim korisnicima u mreži, u skladu s njihovim zahtjevima za servisima i kretanjem u mreži. Za raspodjelu i upravljanje RRU elementima zadužene su RRM funkcije (Slika 1.).

Mobilne ćelijske komunikacije su po prirodi dinamične. Ta dinamičnost se ispoljava u više dimenzija. Broj korisnika se mijenja ne samo kao posljedica rasta penetracije servisa, već i kao posljedica prostornih varijacija saobraćaja. Karakteristike generisanog saobraćaja ovise o vrsti aplikacije koju korisnici pokreću, što opet ovisi o broju istovremenih korisnika. Svi se korisnici kreću po ćeliji/mreži, pa se i uvjeti propagacije mijenjaju u vre-

menu: korisnici mijenjaju udaljenost od bazne stanice, što mijenja vrijednost gubitka putanje, različite prepreke izazivaju spori feding, u zatvorenim ambijentima nastaje brzi feding, a brzina kretanja korisnika dodatno utječe na dinamizam. U sistemima ograničenim interferencijom, kakav je UMTS, svaki novi korisnik povećava interferenciju, pa svaki korisnik treba vršiti prijenos sa optimalnim nivoom snage. Zato kod UMTS FDD sistema tehnički dizajn igra ključnu ulogu u krajnjim performansama kvaliteta i kapaciteta [3].

Dakle, dinamičnost mreže zahtijeva dinamičan menadžment radio resursa putem RRM mehanizama sa velikim brojem parametara koje treba izabrati, izmjeriti, analizirati i optimizirati.

Funkcije menadžmenta radio resursa i QoS-a su važne kod 3G sistema s obzirom na to da se sistem na njih oslanja da bi garantovao određeni ciljani QoS, očuvao planirano područje pokrivanja i pružio velik kapacitet. RRM funkcije su vrlo bitne za garantovanje određenog kvaliteta, i pružanje planirane pokrivenosti i kapaciteta. Takvi su ciljevi u biti kontradiktorni i zahtijevaju ustupke (npr., veći kapacitet na račun manje pokrivenosti i QoS, ali bez odbacivanja poziva). Planiranje UTRAN je prvi korak, dok RRM može izvršiti konačno optimiziranje (Slika 2.).



Slika 2.
Optimizacija kapaciteta, kvaliteta, pokrivanja i efikasnosti

Kod WCDMA, korisnici emituju signale u isto vrijeme i na istoj frekvenciji, koristeći različite kodne sekvence za širenje signala, koje u većini slučajeva nisu savršeno ortogonalne. Shodno tome, postoji sprega među različitim korisnicima, što čini performanse date veze mnogo više ovisnim o ponašanju ostatka korisnika koji dijele radio interfejs. U tom kontekstu, RRM funkcije su od presudnog značaja kod WCDMA, jer ne postoji stalan maksimalno raspoloživ kapacitet zbog stalno prisutne interferencije. Također, RRM može smanjiti potrebu čestog replaniranja radio mreže u uvjetima iznenadnog i kratkotrajnog porasta saobraćaja. Tako je RRM odgovoran za efikasno korištenje UTRAN radio interfejsa.

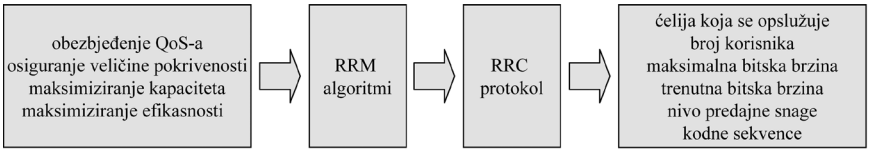
RRM funkcije se mogu primijeniti kroz više različitih algoritama, a to utječe na cjelokupnu efikasnost sistema i na cijenu infrastrukture. Bez sumnje, RRM strategije imaju važnu ulogu u zrelom UMTS scenariju. Uz to, RRM strategije nisu predmet standardizacije, te su moguća različita rješenja među proizvođačima i operatorima.

RRM algoritmi mogu biti centralizovani i smješteni u mrežnom entitetu poput RNC, ili distribuisani i smješteni u svakom mobilnom uređaju. Downlink koristi centralizovano rješenje, jer je mnogo više informacija o svim korisnicima potrebnih za RRM smješteno u RNC. Uplink koristi kombinovano rješenje da bi se smanjio iznos kontrolne signalizacije.

Slika 3. prikazuje funkciju RRM strategija, kao i koncept njihovog provođenja. Kako se vidi, ciljevi RRM mehanizama su obezbjeđenje traženog nivoa QoS-a i osiguranje ciljane veličine područja pokrivanja, uz istovremeno maksimiziranje kapaciteta i efikasnosti radio mreže. S tim ciljem RRM tehnike uglavnom kontrolišu skup radio parametara, kao što je maksimalna i trenutna bitska brzina, predajna snaga, itd., koji imaju cilj raspodjelu neophodnih RRU elemenata u mreži kako bi se postigli takvi ciljevi. Da bi se postavile odgovarajuće vrijednosti ovih parametara, potrebna je podrška RRC (*Radio Resource Control*) protokola [1]. Putem poruka RRC protokola, mreža (tj. RNC) ima mogućnost koordinacije i upravljanja raspodjelom RRU elemenata do svakog mobilnog uređaja.

INDEKS POJMOVA I SKRAĆENICA

RAT (*Radio Access Technology*), radio pristupna tehnologija
RNC (*Radio Network Controller*), kontroler radio mreže
RRM (*Radio Resource Management*), menadžment radio resursa
RRU (*Radio Resource Unit*), element radio resursa
SGSN (*Serving GPRS Support Node*), čvor za podršku GPRS servisa
UTRAN (*Universal Terrestrial Radio Access Network*), univerzalna zemaljska radio pristupna mreža
WCDMA (*Wideband Code Division Multiple Access*), širokopojasni višestruki pristup na temelju kodne raspodjele
Wi-Fi (*Wireless Fidelity*), oznaka za skup standarda IEEE 802.11x
WiMAX (*Worldwide Interoperability for Microwave Access*), svjetska interoperabilnost za mikrotalasni pristup. Često sinonim za standard IEEE 802.16



Slika 3.
Ciljevi RRM algoritama, potrebni protokol i kontrolisani parametri

Funkcija menadžmenta kodova kontroliše upotrebu OVSF kodova u downlinku koji su ortogonalni, te time otporniji na interferenciju. Njihov je broj ograničen, i potrebno ih je efikasno koristiti, čuvajući maksimalan broj kodova za velike brzine.

Algoritmi raspoređivanja paketa koriste slobodne resurse za NRT (*Non Real Time*) saobraćaj. Kako NRT podaci ne postavljaju stroge zahtjeve o pitanju kašnjenja, ovaj se saobraćaj raspoređuje prema relativnom prioritetu. Ako RT (*Real Time*) saobraćaj treba više resursa, NRT podaci će biti preraspoređeni u svakom vremenskom intervalu prijenosa [1].

5. RRM FUNKCIJE

RRM funkcije su odgovorne za postavke različitih parametara koji utječu na ponašanje radio iterfejsa u uplinku i downlinku, a sve su zadužene za optimizaciju UTRAN te su zato jako međusobno povezane. RRM funkcije obuhvataju: kontrolu pristupa AC (*Admission Control*), kontrolu opterećenja LC (*Load Control*), menadžment kodova, raspoređivanje paketa (*Packet Scheduling*), handover, i kontrolu snage.

Algoritmi kontrole pristupa i opterećenja se nalaze u RNC i sprečavaju preopterećenje radio interfejsa koje može izazvati odbijanje poziva, manji QoS i sl. Zadatak AC je da prihvati/odbije pristup korisniku u mrežu na temelju trenutnog stanja radio interfejsa i traženog servisa, dok se LC aktivira po preopterećenju i smanjuje ga na nivo definisan planiranjem mreže. LC mora djelovati brzo da bi očuvao traženi QoS, voditi računa o smislu akcije i trenutno aktivnih servisa, ili u krajnjem slučaju odbaciti aktivni poziv.

Iako je handover inherentan ćelijskim sistemima, UMTS ima više opcija ako mobilni uređaj krajnjeg korisnika može biti istovremeno povezan sa više ćelija, i ako ove ćelije koriste isti frekvencijski opseg. Premda je koncept handovera jednostavan, njegova praktična realizacija je kompleksna jer predstavlja višedimenzionalni problem sa velikim brojem parametara. Štaviše, podesnost odluka o handoveru i vremena pokretanja odluke jako utječe na cjelokupne performanse UTRAN mreže, što handover čini ključnom procedurom.

Algoritmi kontrole snage trebaju u promjenljivim uvjetima rada optimizirati predajnu snagu mobilnog uređaja krajnjeg korisnika (uplink) i predajnu snagu bazne stanice Node B (downlink).

6. UZAJAMNI RAD I POVEZIVANJE IZMEĐU RADIO PRISTUPNIH MREŽA

S obzirom na paralelno postojanje više suštinski različitih RAT (*Radio Access Technology*) tehnologija, a čiji razvoj nadziru različita telekomunikacijska udruženja željna dominiranja TK sektorom, veoma važno pitanje je menadžment radio resursa u takvom heterogenom mrežnom scenariju, u kojem bi različite RAT trebale usklađeno koegzistirati i raditi. Takvi se scenariji opisuju kao sistemi "poslije 3G" i formiraju osnovu ka četvrtoj generaciji mobilnih mreža. Kada zajedno posmatramo različite RAT, moguće je postići mnogo efikasniju upotrebu raspoloživih radio resursa uvođenjem CRRM (*Common Radio Resource Management*) algoritama koji uzimaju u obzir cjelokupne resurse u svim raspoloživim RAT.

Uzajamni rad različitih RAT u heterogenim bežičnim mrežama može se realizirati sa različitim stupnjevima povezivanja. Oni ovise o načinu povezivanja radio pristupnih mreža i načina realizacije različitih aspekata poput zajedničkih radnih procesa ili razmjena mjerenja da bi se postigla zajednička kontrola nad radio pristupnim mrežama. Na taj način bi se postiglo efikasno korištenje svih resursa kojima operator raspolaže, a istovremeno

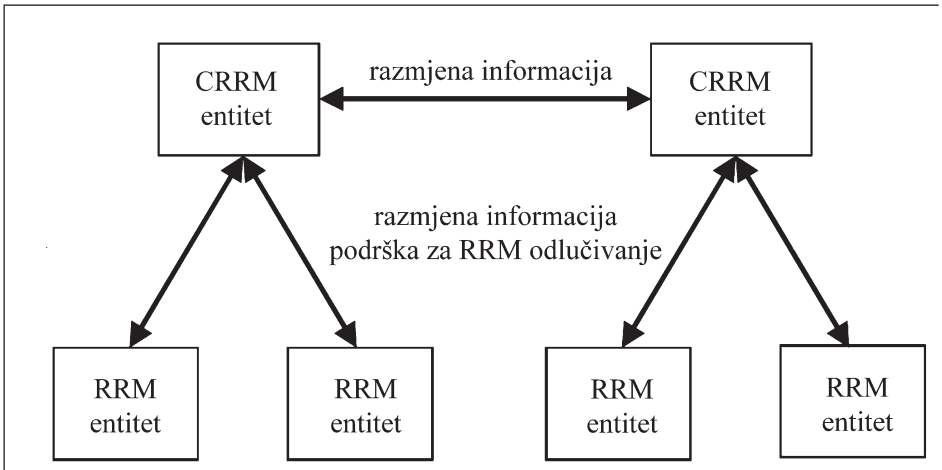
poboljšao kontinuitet servisa za krajnjeg korisnika. Ovdje su kratko predstavljeni aspekti povezivanja aktuelnih UTRAN, GERAN, WLAN i WiMAX mreža. CRRM je uveden u 6.1 odjeljku, s obzirom na to da je, u ovom trenutku, stupanj povezivanja najveći između UTRAN i GERAN tehnologija, te su shodno tome i mogućnosti iskorištenja resursa ovdje najveće.

6.1. UZAJAMNI RAD I POVEZIVANJE UTRAN I GERAN TEHNOLOGIJA

Osnovna UMTS arhitektura koristi iste osnovne elemente CS i PS domena jezgra GSM/GPRS sistema. Naredna izdanja uvode IP protokol u CN elemente oba domena, čime nastaje specifično 3G jezgro. U Release '99 su RNS i CN vezani Iu interfejsom, dok je GERAN sa 2G jezgrom vezan A i Gb interfejsima za CN i PS servise. Release 5 u GERAN uvodi podršku za Iu interfejs, te tako omogućava konverzacijske i streaming servise u GPRS mrežama (osim interaktivnih i background servisa podržanih sa Gb), i omogućava multimodnim terminalima (UMTS/GSM/GPRS) da koriste isti tip servisa neovisno o pristupnoj mreži.

Zato je uzajamni rad UTRAN i GERAN realizovan povezivanjem RNC i BSC na isto 3G jezgro mreže putem Iu interfejsa, čime se postiže čvrsta veza između obje pristupne mreže i omogućava upotreba strategija zajedničkog menadžmenta radio resursa (CRRM) za optimiziranje rada mreže. Moguće je i povezivanje putem Iur-g interfejsa za još jače povezivanje i provođenje CRRM strategija direktno između RAT kontrolera, bez oslanjanja na komunikaciju sa CN entitetima.

CRRM strategije imaju kao cilj efikasno iskorištenje radio resursa u heterogenim mrežama koordiniranjem raspoloživih resursa u postojećim RAT. Zato je CRRM opći koncept koji se može primijeniti na bilo koju RAT kombinaciju, premda su specifičnosti implementacije i stupanj koordinacije veoma ovisni o stupnju povezivanja koje postoji između određenih radio pristupnih mreža.

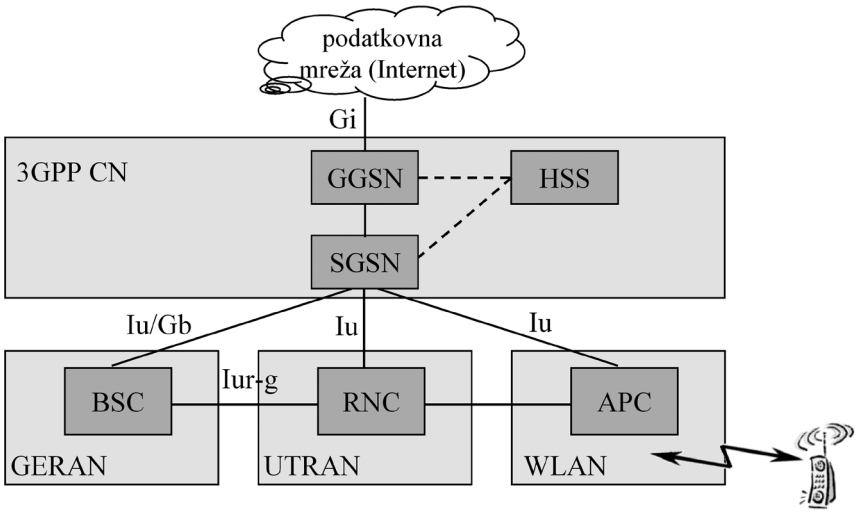


Slika 4.
CRRM funkcionalni model

3GPP funkcionalni model za CRRM rad (Slika 4.) uzima u obzir ukupan iznos resursa koji je raspoloživ operatoru i podijeljen je na fondove radio resursa. Svaki se fond sastoji od resursa raspoloživih u skupu ćelija, obično pod kontrolom RNC ili BSC, sa dva tipa entiteta za menadžment fondova, RRM entitet i CRRM entitet. RRM entitet je zadužen za menadžment resursa u jednom fondu određene radio pristupne mreže. CRRM entitet provodi koordinirani menadžment fondova koje kontrolišu različiti RRM entiteti, obezbjeđujući da odluke ovih RRM entiteta uzimaju u obzir raspoloživost resursa i u drugim RRM entitetima, a može komunicirati i sa drugim CRRM, prikupljajući informacije o ostalim RRM entitetima koji nisu pod njegovom direktnom kontrolom.

6.2. UZAJAMNI RAD I POVEZIVANJE UTRAN I WLAN TEHNOLOGIJA

Uzajamni rad i povezivanje UTRAN i WLAN tehnologija su osmišljeni drugačije nego kod UTRAN i GERAN. Osnovni je razlog što WLAN u općem slučaju razvijaju grupacije (proizvođači i standardizacijska tijela) koje ne pripadaju 3GPP, i shodno tome oni se ne pridržavaju mrežnih arhitektura 3GPP sistema. Osim toga, veći broj različitih WLAN



Slika 5.
Najviši stupanj povezivanja UMTS i WLAN

standarda otežava razvoj općih mehanizama za uzajamni rad.

Uprkos preprekama, uspješna primjena WLAN na globalnom nivou i velike brzine prijenosa podataka koje nude čini ih privlačnom alternativom za proširenje područja pokrivanja ćelijskih sistema na "hotspot" lokacije. Iz tog razloga čine se određeni napori u okviru standardizacijskih tijela kako bi se postigla integracija 3GPP i WLAN tehnologije.

Uzajamni rad UTRAN i WLAN mora uzeti u obzir tehničke ali i ostale aspekte, s obzirom na to da okruženja u kojima sistemi koegzistiraju (javna, poslovna, ili stambena) mogu obuhvatiti različita administrativna područja i različite vlasnike WLAN mreža, što vodi, naprimjer, različito definisanim zahtjevima za sigurnost, naplatu i/ili autentifikaciju.

U okviru 3GPP standardizacije postoji šest različitih scenarija povezivanja UTRAN i WLAN mreža [4]. Cilj je omogućiti postupnu integraciju, pa svaki scenarij obuhvata prethodna svojstva i predstavlja naredni korak u procesu integracije.

Ovi su scenariji poopćeni o pitanju posjedovanja mreža i ne pretpostavljaju bilo kakvu vezu između 3GPP operatora i WLAN vlasnika, koji može biti 3GPP ili neki drugi entitet koji pruža WLAN pristup u datom području (hotel, aerodrom i sl.) [1].

Navedeni scenariji uzajamnog rada UTRAN i WLAN omogućavaju različite stupnjeve povezivanja 3GPP i WLAN. Najjednostavniji je labava sprega u kojoj se koriste dvije različite pristupne i transportne mreže za UMTS i WLAN, a ne zahtijeva nove elemente. Sljedeća mogućnost za povezivanje je korištenje Gi interfejsa. U ovom su slučaju potrebni dodatni 3GPP CN elementi (*3GPP AAA server*, *Packet Data Gateway*, *WLAN Access Gateway*) za obradu kontrolnih informacija i podataka iz WLAN, jer se moraju potraživati autentifikacijske informacije i profil korisnika iz HSS-a 3GPP mreže.

Krajnji je cilj da WLAN bude dodatna RAN poput GERAN ili UTRAN (Slika 5.). Tako jako povezivanje zahtijeva da se WLAN poveže na UMTS jezgro mreže putem Iu interfejsa, što bi omogućilo uvođenje u WLAN već predviđenih RRM i CRRM funkcija između GERAN i UTRAN. Za to je potreban novi element u WLAN sa funkcijama sličnim RNC u UTRAN ili BSC u GERAN [1]. To je APC (*Access Point Controller*) koji bi bio zadužen za kontrolu radio resursa pristupnih AP tačaka. Najviši stupanj povezivanja obezbjeđuje dodatni interfejs između RNC i APC, sličan Iur-g interfejsu. Neprekinutost rada PS i CS servisa ovisi o RRM i CRRM funkcionalnostima, kao i mogućnosti mapiranja UMTS nositelja servisa na odgovarajuće WLAN parametre.

6.3. UZAJAMNI RAD I POVEZIVANJE UTRAN I WiMAX TEHNOLOGIJA

U kontekstu 3GPP standardizacije, WiMAX nije još aktivno uključen u proces standardizacije uzajamnog rada sa UMTS. Određeni napori se, ipak, čine, što se vidi iz aktivnosti 3GPP TSG SA grupe tokom radnog sastanka iz marta 2007. godine. Naime, 3GPP trenutno u okviru Release 8 radi na LTE studiji i evoluciji arhitekture. Važni zadaci ove studije obuhvataju smanjenje kašnjenja, poboljšanje mogućnosti sistema, sma-

njenje cijene po bitu i veće brzine prijenosa podataka. Sastavni dio studije čine razmatranja mogućnosti pružanja IP-temeljenih 3GPP servisa putem različitih ne-3GPP pristupnih tehnologija. U tom smislu, 3GPP TSG SA grupa uputila je poziv WiMAX forumu i IEEE 802.16 da aktivno učestvuju u definisanju mogućih scenarija uzajamnog rada i zahtjeva pri mobilnosti između 3GPP i WiMAX sistema.

Polazeći od već spomenutih scenarija povezivanja UTRAN i WLAN, raspoloživi se rezultati mogu iskoristiti i za povezivanje UTRAN i WiMAX, uključujući različite stupnjeve povezivanja. Trenutno aktuelna rješenja povezivanja se zasnivaju na korištenju IMS VCC (*Voice Call Continuity*) funkcionalnosti koja omogućava korisnicima prelazak između različitih tipova mreža. Koristeći IMS postiže se rješenje u skladu s 3GPP i podržava svojstvo kontinuiteta govorne veze za neprekinuti dvosmjerni handover između IMS i CS domena. Također, prelaz između WLAN/WiMAX "hotspotova" i UTRAN /GERAN ćelija zahtijeva multi-modne terminale.

Raznolikost i nekonzistentnost rješenja ne iznenađuje s obzirom na to da originalni WiMAX standard iz 2001. godine, ali i standard iz 2004. godine, očigledno, nisu dovoljno dorađeni i očekivane su nove verzije. Nastali standard za fiksni WiMAX nije uspio postati globalno zastupljen kao Wi-Fi. Standard za mobilni WiMAX s kraja 2005. godine relativno je nov i tek se očekuje njegova veća praktična primjena. Ovisno o uspjehu, pojavit će se ili izostati zainteresovanost za integraciju sa UMTS na nivou na kojem je to uspio Wi-Fi.

7. ZAKLJUČAK

Iz ovog kratkog pregleda UMTS RRM strategija i funkcija, može se zaključiti dosta toga.

Spektar je oduvijek bio na cijeni, a i ostat će takav još dugo vremena. Zato je potrebno koristiti sve moguće načine za njegovo efikasno korištenje.

Efikasna upotreba spektra omogućava pouzdan rad sistema i zadovoljstvo korisnika pruženim servisom, uz istovremeno zadovoljstvo operatera izraženo kroz optimalno ulaganje sredstava u radio pristupni segment mreže, kao najskuplji i najzahtjevniji dio svake mreže.

Bez obzira na dominaciju bilo koje grupacije, evidentno je da će mnoge tehnologije egzistirati još dugo u budućnosti. Ovdje spomenute (UMTS, WLAN, WiMAX) najzastupljenije su i dobra su osnova za 4G sisteme (ili sisteme poslije 3G). Kao takve, one čine heterogeno okruženje. Svaki operater može uvesti svaku od tehnologija, ali je bitno da pritom omogući kontinuitet servisa.

Štaviše, od presudnog je značaja za komercijalni uspjeh bilo kog operatera da efikasno upotrijebi fizičke resurse u svim svojim mrežama. To bi mu omogućilo privlačenje većeg broja korisnika, sa različitim terminalima i kroz pristup većem broju servisa, s različitim brzinama i QoS zahtjevima, a po nižim cijenama.

LITERATURA

[1] Jordi Perez Romero, Oriol Sallent, Ramon Agusti and Miguel Angel Diaz-Guerra, "*Radio Resource Management Strategies In UMTS*", John Wiley & Sons, 2005

[2] 3GPP TR 25.881 v5.0.0 "*Improvement of RRM across RNS and RNS/BSS*"

[3] Jonathan P. Castro, "*The UMTS Network and Radio Access Technology: Air Interface Techniques for Future Mobile Systems*", John Wiley & Sons, 2001

[4] 3GPP TR 22.934 v6.2.0 "*Feasibility study on 3GPP System to Wireless Local Area Network (WLAN) interworking*"

[5] Hakija Grabovica, magistarski rad "*Uticaj tehnološko-ekonomskih kriterija na izbor pristupnih tehnologija kod mobilnih operatora*", Univerzitet u Sarajevu – ETF Sarajevo, maj 2008.

[6] Ajay R. Mishra, "*Fundamentals of Cellular Network Planning and Optimisation: 2G/2.5G/3G... Evolution to 4G"*, John Wiley & Sons, 2004

[7] 3GPP 25.922 v6.0.1, "*Radio resource management strategies (release 6)*"

Ericsson je vodeći svjetski isporučitelj tehnologije i usluga telekomunikacijskim operatorima. Kao tržišni lider u mobilnim tehnologijama 2G i 3G, Ericsson isporučuje komunikacijske usluge i upravlja mrežama koje poslužuju više od 250 milijuna pretplatnika. Lista proizvoda i usluga kompanije sadrži infrastrukturu mobilne i fiksne mreže te širokopojasna i multimedijska rješenja za operatore, preduzeća i kompanije koje se bave razvojem. Zajednička kompanija Sony Ericsson isporučuje krajnjim korisnicima personalizirane mobilne uređaje sa velikim mogućnostima.

Ericsson unapređuje svoju viziju “komunikacije za sve” inovacijama, tehnologijom, te održivim poslovnim rješenjima. Prisutan je u 175 zemalja, a više od 70 000 zaposlenika stvorilo je 2008. prihod od 27 milijardi US dolara (209 milijardi SEK). Utemeljen 1876. i sa sjedištem u Stockholmu, Švedska, Ericsson je uvršten u kotacije na berzi OMX Nordic u Stockholmu te u sistemu NASDAQ.

Ericsson d.o.o.
Fra Anđela Zvizdovića 1/X
71 000 Sarajevo, Bosna i Hercegovina
Tel.: +387 33 252 260
Fax: +387 33 209 419
www.ericsson.com/ba

Za više informacija posjetite
www.ericsson.com ili www.ericsson.mobi

ERICSSON
TAKING YOU FORWARD

mr. Halil Šabanović, dipl. ing. el.

Integracija GPRS i WLAN pristupnih mreža
Integration of WLAN and GPRS networks

Sažetak

Kako se bežične komunikacione tehnologije razvijaju i postaju sve rasprostranjenije, granice bežičnih aplikacija se pomjeraju sve dalje. Bežične tehnologije koje su se pozicionirale u primjeni za specifične aplikacije, danas su u mogućnosti obezbijediti neke sasvim nove servise. Osim toga, postoji i stalna potreba za unapređenjem mobilnosti i pokrivanja signalom WiFi mreža, te povećanjem kapaciteta podatkovnih servisa kod mobilnih mreža. WiFi nudi bržu konekciju i znatno niže cijene servisa u odnosu na 2.5G mobilne mreže, kao što su GPRS mobilne mreže. Mobilne mreže, sa druge strane, obezbjeđuju znatno šire pokrivanje signalom od WiFi mreža. Mnogi operatori koji pružaju GPRS servise razmatraju, ili su već obezbijedili, pružanje i WiFi servisa s ciljem povećanja kapaciteta svojih mreža, te smanjenja sve većih zagušenja na svojim GPRS mrežama. Kao rezultat toga, osnovna prednost postignuta integracijom GPRS i WLAN tehnologija je cjenovna efikasnost korištenja servisa obiju mreža. Na taj način, telekom operator može postići znatne prednosti u cijenama korištenja servisa na objema mrežnim tehnologijama. Mobilni operatori imaju opciju da integracijom svojih mobilnih mreža sa WiFi hotspotovima obezbijede korisnicima svojih usluga jedinstven sistem naplate korištenja uz cjenovno efikasnije podatkovne servise na WiFi mrežama u odnosu na iste na mobilnim mrežama. Ovaj rad prezentira osnovne probleme i najpoznatija rješenja integracije GPRS i WiFi mreža.

Ključne riječi: WLAN, WiFi, GPRS, GSM, MobileIP, SS7

Abstract

As wireless technologies have been emerging and improving, there is a trend of moving the boundaries of their applications. The wireless technologies very usable for their specific set of applications are able to provide some very new services. There is also an oportunity for improvement in mobility and coverage of WiFi and the increasing capacity of data services in cellular networks. WiFi offers fast connectivity and relatively much cheaper services compared to 2.5G cellular networks, such as General Packet Radio Service (GPRS). Cellular networks provides much larger coverage than WiFi networks. Many cellular operators consider providing WiFi services along with their networks in order to improve their networks' capacity and reduce increasing congestions in their GPRS networks. That way they can achieve better pricing potential of services in both networks. Cellular operators have an option to integrate their networks with the WiFi hotspots and provide a common billing to their customers with improved and cost effective data access over WiFi compared to cellular networks. This work presents the main issues and the best known solutions for the integration of WiFi and GPRS networks.

Keywords: WLAN, WiFi, GPRS, GSM, MobileIP, SS7

INDEKS POJMOVA I SKRAĆENICA

AuC – Authentication Center
EAP – Extensible Authentication Protocol
GSM – Global System for Mobile
GPRS – General Packet Radio Service
Handover – tehnološki koncept celularnih mreža za prelazak izmedu mrežnih ćelija
HLR – Home Location Register

PREGLED ARHITEKTURA INTEGRACIJE WIFI I GPRS MREŽA

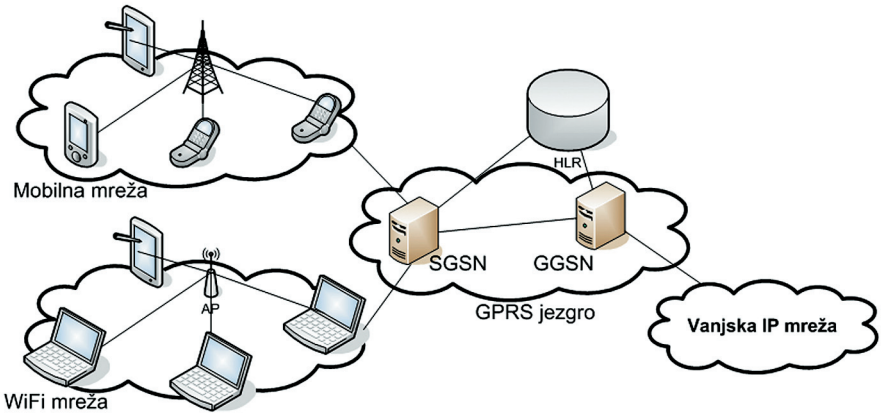
Integracija GPRS i WiFi mreža obezbjeđuje široko pokrivanje i širokopojasni pristup na određenim lokacijama (škole, poslovni objekti, aerodromi, hoteli, kafei i druga javna mjesta). Osim toga, integracijom WiFi i GPRS mreža, operatori su u mogućnosti pružiti servise specifične za 3G mreže. Poznata su dva tipa integracijske arhitekture: čvrsta integracija (tight coupling) i slaba integracija (loose coupling). Osnovna prednost koja se postiže integracijom GPRS i WLAN mreža je mogućnost korištenja najboljih osobina obiju tehnologija. Visoka propusnost WLAN mreža iskoristiva je za brzi transfer podataka i aplikacije koje rade u realnom vremenu, dok se GPRS mreža koristi u području koje nije pokriveno WLAN mrežom, ali sa ograničenim mogućnostima. WLAN i GPRS bi trebali biti u mogućnosti dopunjavati se svojim osobinama, a da pritom ne smetaju jedno drugom za iste korisnike.

ČVRSTA INTEGRACIJA

Kod ovog tipa arhitekture, WiFi je povezan na jezgro GPRS mreže kao alternativnu radio pristupnu mrežu. Hotspotovi koriste GPRS infrastrukturu kao svoje mrežne resurse, uključujući korisničke profile i biling rješenja. Mobilni korisnici su u mogućnosti izabrati preferiranu pristupnu mrežu i odgovarajuću brzinu prijenosa. Slika 1. ilustrira arhitekturu čvrste integracije.

SLABA INTEGRACIJA

Hotspotovi se povezuju sa GPRS mrežom u okviru IP mreže operatora. Na taj način saobraćaj sa WiFi mreže usmjerava se direktno na IP mrežu operatora, umjesto prema GPRS jezgru mreže. Prema tom principu, WiFi i mobilna mreža nastavljaju funkcionirati samostalno uz zajedničku AAA platformu. Hotspotovi mogu biti u vlasništvu trećeg operatora sa uspostavljenim roaming funkcijama putem dedicirane konekcije između mobilnog operatora i WiFi operatora. Slika



Slika 1.
Arhitektura čvrste integracije GPRS/WLAN mreža

INDEKS POJMOVA I SKRAĆENICA

IEEE – Institute of Electrical and Electronics Engineers
IETF – Internet Engineering Task Force
IP – Internet Protocol
MobileIP – Mobile Internet Protokol
PDA – Personal Digital Assitant
QoS – Quality of Service
SIGTRAN
SIP – Session Initiation Protocol
SS7 – Signaling System #7
TCP – Transmission Control Protocol
UDP – User Datagram Protocol
UMA – Unlicensed Mobile Access
VoIP – Voice over Internet Protocol
WiFi – Wireless Fidelity, IEEE 802.11
WLAN – Wireless Local Area Network

br. 2 – prikazuje arhitekturu slabe integracije GPRS/WLAN mreža.

Pretpostavimo da korisnik ima potrebu obaviti transfer podataka, a trenutno je konektovan na GPRS mrežu. Korisnik je pretplaćen i na GPRS kao i na WiFi pristup. Neophodno je postojanje jedinstvenog AAA servera i biling sistema u vlasništvu mobilnog operatora. Ovaj sistem će funkcionirati za sve uvezane hotspotove. U takvom okruženju korisnik može izabrati jednu od opcija:

- Nastaviti transfer podataka putem GPRS mreže po cijeni za ovaj vid pristupa ili
- Potražiti dostupne WiFi hotspotove za uspostavu nove konekcije.

Jednom kada korisnik ima na raspolaganju pristup hotspotu, prije uspostave konekcije na WiFi mrežu određuje se da li korisnik treba platiti i roaming uslugu (hotspot stranog operatora) ili se nalazi u zoni pokrivanja svog operatora. Integracijom dviju pristupnih tehnologija operatori su u mogućnosti pridobiti nove korisnike ponudom servisa sa dodanom vrijednošću. Osim toga, GSM/GPRS mobilni operatori mogu graditi svoje 3G mreže sa mnogo manje žurbe, tako što će ponuditi korisnicima servise slične onima kod 3G tehnologija.

Autentifikacija mobilnog korisnika može se izvesti na resursima GPRS mreže (HLR/AuC), bilo putem SS7 linka ili korištenjem SIGTRAN protokola na SCTP elementu. SIGTRAN rješenje posjeduje mogućnost spajanja WLAN mreža sa SS7 resursima, gdje se SS7 siganlizacioni saobraćaj za autentifikaciju prenosi putem IP mreža do SGW (Signalling Gateway) elementa, koji djeluje kao logički interfejs ka SS7 mrežama.

ROAMING I MOBILNOST

Veoma važna funkcionalnost WLAN – GPRS integracije predstavlja mobilnost korisnika, odnosno mogućnost da korisnik slobodno putuje između pristupnih tačaka i mobilnih mreža. Postoji više rješenja za mobilnost, a njihova realizacija se može izvesti na različitim mrežnim slojevima. Jedan od načina realizacije mobilnosti je i implementacija protokola između aplikacija i transportnog nivoa. Osim toga, moguće je rješenje na transportnom nivou uz pomoć proxy elementa, postavljenog između mobilne jedinice i servera. Proxy će prihvatati pakete od servera i prosljeđivati ih ka mobilnom uređaju, a isto vrijedi za saobraćaj u obrnutom smjeru.

MobileIP predstavlja jednu od implementacija koja se realizira na mrežnom nivou. Ovaj protokol je uobičajeno rješenje za mobilnost korisnika u heterogenim mrežama, budući da je besplatan i ne zahtijeva velika ulaganja u hardver. MobileIP radi trenutno na IPv4 mrežnom protokolu, a također postoje opcije i za IPv6.

AAA FUNKCIONALNOST

Integracija WLAN i GPRS mreža otvara pitanje korištenja jedinstvenog rješenja za AAA funkcionalnost (Autentifikacija, Autorizacija i obračun-Accounting) za oba sistema ili možda zasebnih rješenja za svaku mrežu. AAA server za GPRS mrežu se razlikuje od onog za WLAN mreže. Kombinirani server koji je u mogućnosti obrađivati zahtjeve različitih vrsta korisnika, predstavlja moguće rješenje za integraciju.

Zahtjevi koji se postavljaju pred AAA server bi bili:

- Autentifikacija

Proces verifikacije da je korisnik ovlašten za pristup mreži.

- Autorizacija

Funkcija koja obezbjeđuje dodjelu resursa i različitih nivoa korištenja aplikacija za pojedine korisnike.

- Obračun

Obračunski server mora prikupljati zapise o korištenju svih mrežnih resursa na odgovarajući način. Sistem bilinga može se bazirati na vremenu konekcije korisnika ili količini prenesenih podataka. Jedna od prednosti obračunskog servera je njegova mogućnost razlučivanja saobraćaja, govora i sadržaja, prema posebnostima u načinu naplate korištenja. Zapisi o različitim korištenim resursima omogućavaju naplatu servisa na različitim osnovama.

- Dodjela IP adresa i upravljanje mobilnošću klijenata

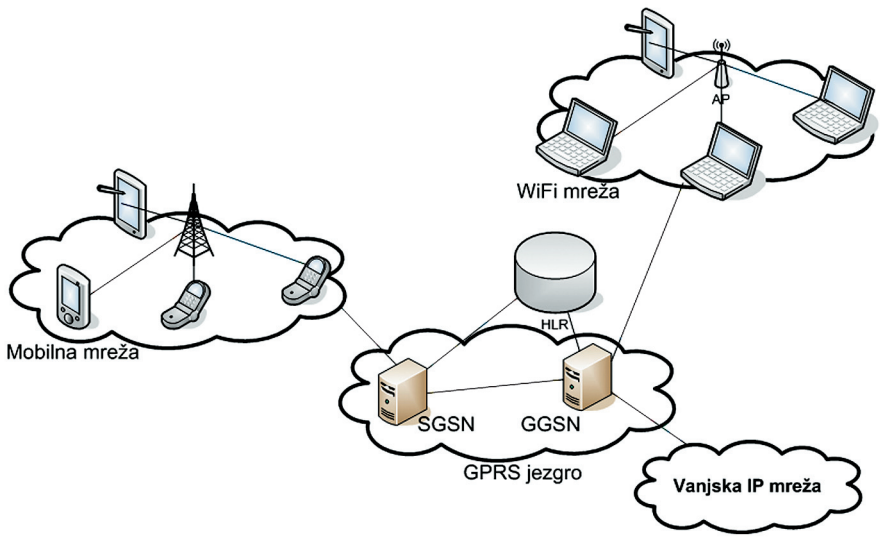
Kada se korisnik autentificira, AAA server dodjeljuje korisnikovom uređaju odgovarajuću IP adresu.

- Nivo servisa

GPRS AAA server mora čuvati zapise o nivou servisa obezbijeđenom svakom od korisnika, dok kod WLAN mreža ovu funkciju obavlja NAS element.

- Biling

Generiranje biling informacija iz obračunskih zapisa.



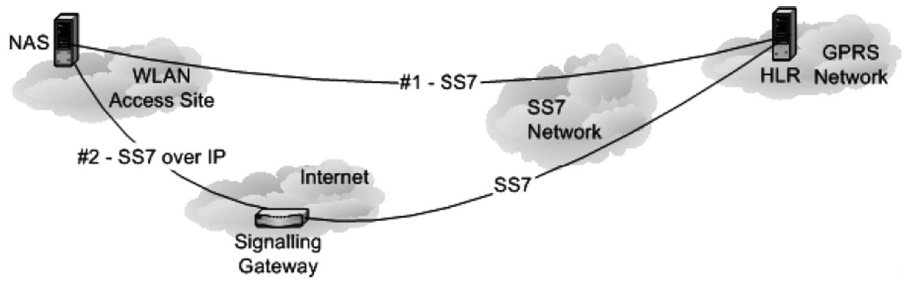
Slika 2.
Arhitektura slabe integracije WLAN/GPRS mreža

SIM-HLR RJEŠENJE

Jedno od najčešće korištenih rješenja integracije GPRS i WLAN mreža, bazira se autentifikacijskim podacima SIM kartice mobilnog korisnika. SIM kartica na jedinstven način identificira pojedinog korisnika, te povezuje korisnika sa biling računom i servisima koje je izabrao da koristi. U telekomunikacijskoj industriji, SIM modul je razvijen u svrhu pohranjivanja autentifikacijskih i zaštitnih informacija. Ove informacije se koriste za poređenje sa centraliziranom korisničkom bazom, koja se kod mobilnih mreža naziva Home Location Register (HLR). HLR se funkcijski kombinira sa autentifikacijskim centrom (Authentication Central – AuC), a koji sadrži duplikatne vrijednosti ključeva i autentifikacijskih algoritama. Navedene informacije omogućavaju mrežnu autentifikaciju mobilnog korisnika na bazi odgovora dobijenih od SIM kartice.

Jedan od glavnih problema autentifikacijske tehnike bazirane na SIM karticama i provjeri sa informacijama pohranjenim na HLR-u je potreba za SS7 linkovima prema GPRS mreži. Tehnologija koja bi se koristila za ovu vrstu autentifikacije za potrebe manjih WLAN operatora, morala bi biti laka za postavljanje i cjenovno isplativa. U skladu sa ovim zahtjevima, nameće se potreba korištenja Interneta umjesto skupih SS7 dediciranih linkova. Mnogi od današnjih servisa koji koriste SS7 mreže, sve više prelaze na IP tehnologije, iz razloga što operativni troškovi postaju znatno manji nego sa SS7 uređajima. Praktičan primjer za ovaj trend su VoIP rješenja, koja omogućavaju rutiranje govornih poziva putem IP mreža.

Tehnologija dizajnirana za jednostavno korištenje, lakše se sa uspjehom implementira, što bi mogao biti slučaj i sa WLAN mrežama u slučaju mobilnih korisnika. To bi značilo da je neophodno učiniti prijelaz, mobilnost i roaming između različitih mrežnih tehnologija



Slika 3.
IP-SS7 interworking scenarij

što jednostavnijim za korisnike mobilnih mreža. SIM kartice su pravi izbor na putu obezbjeđenja transparentnog i jednostavnog mrežnog pristupa za uobičajenog korisnika, bez obzira na mrežnu tehnologiju.

GPRS korisnici su u mogućnosti koristiti roaming u mrežama drugih telekom operatora, a također korisnici WLAN servisa mogu uraditi isto u drugim WLAN mrežama. Ono što nedostaje jeste mogućnost da GPRS korisnici slobodno koriste roaming u WLAN mrežama, ali i obratno. Postojeća autentifikacijska infrastruktura je građena na RADIUS serverima, što logički zahtijeva korištenje ove tehnologije u GPRS mrežama. Uvezivanje RADIUS servera sa GPRS jezgrom bi trebalo obezbijediti transparentan autentifikacijski interfejs za roaming scenarij u WLAN mrežama.

WLAN-GPRS FIZIČKI INTERFEJS

Komunikacijski interfejsi prema SS7 baziranim elementima su uobičajeno skuplji i kompleksniji od IP baziranih rješenja. Više razloga je za tu činjenicu, a osnovni je to da SS7 mreže zahtijevaju redudancu u komunikacijskim linkovima kako bi se kompenzirao eventualni gubitak linka. Zahtjev za redudansom u linkovima omogućava SS7 mrežama visoku pouzdanost za signalni saobraćaj pri uspostavi poziva ili mrežnoj signalizaciji.

IETF je razvio standardizirani transportni protokol za SS7 baziranu signalizaciju, koja omogućava da SS7 paketi mogu biti transportirani putem IP baziranih mreža. Standard je nazvan SIGTRAN, a definira korisnički adaptacijski sloj koji omogućava transport SS7 baziranog signalnog saobraćaja putem IP mreža, poput Interneta naprimjer.

IP mreže danas još imaju problema u obezbjeđenju sigurnih i pouzdanih servisa koji bi bili uporedivi sa istima na SS7 mrežama. Osnovni razlog za to leži u nedostacima postignutih QoS servisa u postojećim IPv4 mrežama. Zbog toga je i najteži zadatak pri prijelazu na IP tehnologije, postizanje striktnih zahtjeva SS7 mreža. Osim toga, visoka zahtijevana redudansa za linkove kod SS7 mreža mora biti ispoštovana i kod IP mreža. Zbog toga je bilo neophodno na transportnom sloju zamijeniti UDP i TCP protokole sa drugim standardom, koji bi mogao obezbijediti perfomanse koje odgovaraju SS7 signalizaciji. Tako je nastao SCTP. SCTP radi na IP sloju, obezbjeđujući SIGTRAN konceptom višestrukih tokova analognih redudantnim komunikacijskim linkovima kod SS7 mreža.

Kreiranje analogne SS7 mrežne arhitekture na IP mrežama omogućava jedno sasvim novo područje aplikacija, počevši od VoIP baziranih pa do evolucije konvergiranih mreža poput WLAN i GPRS.

IP-SS7 INTER-NETWORKING

HLR i AuC su locirani na SS7 baziranoj mreži, što znači da IP bazirane mreže, poput Interneta, nisu u mogućnosti direktno doseći ove elemente. Da bi ovi elementi bili dostupni sa IP mreža, neophodno je koristiti neku vrstu SS7/IP gatewaya ili direktne SS7 linkove. Osnovni principi SS7/IP interworkinga predstavljeni su Slikom 3.

1. Direktna komunikacija putem SS7 linkova
   Direktni SS7 komunikacijski linkovi prema GPRS mreži, omogućavaju WLAN operatorima verifikaciju prava konektovanih korisnika, na osnovu autentifikacijskih podataka pohranjenih na GPRS mreži. Ovo rješenje koristi strandardizirani Gr GPRS interfejs, što znači da se autentifikacijski saobraćaj obavlja putem Mobile Application Part (MAP) protokola na SS7 mreži i HLR/AuC elementima.

2. Tuneliranje SS7 signalizacije putem IP protokola uz pomoć IP-SS7 signalizacijskog Gatewaya
   Prednost ovog rješenja je u tome što pojedini WLAN operatori ne trebaju investirati u specifične SS7 bazirane uređaje, već su u mogućnosti koristiti tunelirani SS7 saobraćaj kroz javne ili privatne IP mreže ka IPSS7 signalizacionom Gatewayu, koji vrši transformaciju IP paketa u standardni SS7 mrežni saobraćaj. Kao kod prethodnog primjera, SS7 putem IP signalizacija koristi GPRS Gr interfejs kroz komunikaciju putem MAP protokola.

SIGNALIZACIONI GATEWAY (SG)

Obezbjeđenje atraktivne platforme za pristup SS7 mrežama za autentifikacijski saobraćaj sa WLAN mreža, uobičajeno uključuje neku vrstu signalizacionog gatewaya ili AAA brokerski servis. WLAN operatori koji ne posjeduju mogućnost komunikacije sa SS7 mrežama mogu koristiti komercijalne servise za autentifikaciju od operatora koji pružaju iste. Omogućavanje ovakvih servisa bi se moglo obezbijediti kroz AAA proxy servis za autentifikacijski saobraćaj uz pomoć AAA protokola, ili uz pomoć SS7/IP interfejs gatewaya za WLAN operatore. Postoji veći broj mogućih arhitektura za autentifikaciju, zavisno od tipa postojećih relacija povjerenja između operatora i AAA brokera.

Obezbjeđenje signalizacionog gatewaya bi moglo biti skupo, uz skup različitih problema koje je potrebno riješiti. Tehnološko rješenje zahtijeva od WLAN operatora podršku za SIGTRAN protokol i internetski pristup.

Troškovi ulaganja u signalizacioni gateway zavise i od obima korištenih funkcionalnosti koje će se obrađivati u hardveru. Osim komercijalnih, postoje i besplatni open source SS7 i SIGTRAN softveri, poput OpenSS7 rješenja naprimjer. Besplatna rješenja mogu znatno smanjiti troškove ulaganja.

SS7/IP RJEŠENJA

Postoji više rješenja za transport SS7 signalizacije putem IP mreža. SIGTRAN obezbjeđuje nekoliko korisničkih adaptacijskih slojeva, a neki od njih su M3UA, SUA i TUA. Zavisno od obima korištenih SS7 funkcionalnosti moguće je postići SS7 transport sa jednog od slojeva MTP3 do TCAP.

GPRS-WLAN MOBILNOST

Integracija GPRS i WLAN mreža može se postići na bazi različitih aspekata, kao što su, naprimjer, iskustveni aspekt krajnjeg korisnika i aspekt korištene AAA infrastrukture. Uspostavljanje mrežne platforme u kojoj mobilni korisnik može koristiti roaming u vezi je rješenjem problema stalne mrežne povezanosti. Rješenje ovog problema naziva se mobilnost.

Drugi problem koji je potrebno riješiti je u vezi s mogućnošću AAA infrastrukture da izvrši autentifikaciju, autorizaciju i obračun za različite grupe mobilnih korisnika na različitim pristupnim mrežama i mrežnim platformama.

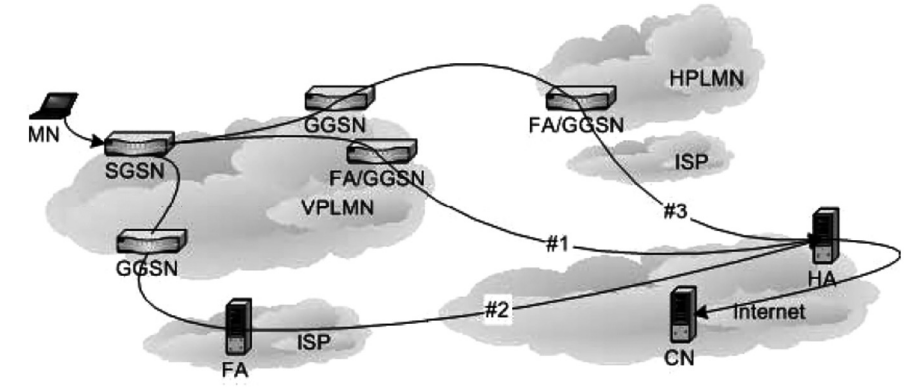
Navedena dva problema su međusobno povezana iz razloga što AAA infrastruktura može kontrolirati korisnikovu mobilnost kroz definirane autentifikacijske procedure pri konekciji na novu mrežu.

Handover je jedan od važnih procesa usko u vezi sa perfomansima i efektivnosti mobilnosti jedne integrirajuće platforme.

MOBILEIP U WLAN/GPRS INTER-NETWORKINGU

Integracija WLAN-GPRS mreža na IP nivou za sada je najatraktivnije rješenje mobilnosti i jednostavne integracije ovih heterogenih mreža. Integracija servisa mobilnosti u GPRS mrežama može se implementirati na različite načine.

Za uspostavljanje MobileIP funkcionalnosti u IPv4 mrežama, neophodna je funkcija stranog agenta (Foreign Agent – FA). Osnovni razlog za implementaciju FA je u vezi sa problemom adresnog IPv4 prostora. Zbog toga se mobilnost u IPv4 mrežama oslanja na korištenje roaming adrese (Care of Addresse – CoAs). Koncept CoA omogućava FA elementu da opslužuje više mobilnih klijenata sa jednom CoA, funkcijski slično NAT



Slika 4.
MobileIP-GPRS interworking, scenarij 1

translaciji. Efikasno MobileIP rješenje bi moglo biti sagrađeno na IPv6 protokolu, gdje ne postoji manjak adresa, a CoA adresa mobilnog klijenta se koristi za direktno rutiranje informacija od domaćeg agenta (Home Agent – HA) do mobilnog klijenta (Mobile Node – MN) putem zaštićenog tunela.

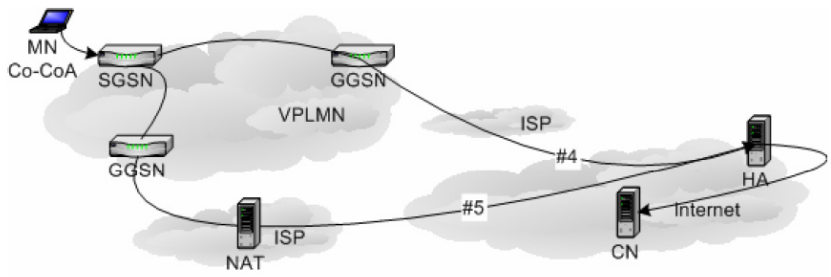
Implementacija podrške za mobilnost GPRS mreža u IPv4 okruženju podrazumijeva više metoda. Jedna od metoda se sastoji u integraciji FA funkcija u okviru GGSN noda. Drugi metod zahtijeva zaseban vanjski FA nod. Integracija FA unutar GGSN-a (nazovimo ga scenarij 1 – Slika 4.) izgleda kao logičan izbor zbog svoje jednostavnosti. GPRS mreže uobičajeno koriste GTP tunele kako bi rutirali IP pakete interno između SGSN i GGSN nodova. Svaki od GTP tunela posjeduje jedinstven TID (Tunnel ID) identifikator povezan sa određenim mobilnim nodom. Jedina funkcija FA bi bila rutiranje dolaznih paketa sa CoA adresom, od HA do asociranog MN GPRS tunela. Osim rutiranja, FA izvršava i funkciju de-enkapsulacije MobileIP paketa.

Scenarij 1 zahtijeva, dakle, modifikaciju postojećih GPRS mrežnih elemenata. Da bi se izbjegla navedena izmjena GPRS mreže, FA se uspostavlja kao zaseban nod (nazovimo to scenarij 2 – Slika 5.). Lociranje zasebnog FA noda koji pripada GPRS PLMN arhitekturi, ne zahtijeva modifikacije na elementima mreže.

Osnovni problem kod MobileIP protokola je korištenje zaštićenih tunela, što uzrokuje dodatno opterećenje saobraćajem na mreži, a samim tim se smanjuje ukupna efikasnost transporta putem GPRS radio interfejsa. Zaštićeni tuneli također zahtijevaju da uređaj mobilnog klijenta bude sposoban enkapsulirati/dekapsulirati pakete saobraćaja sa HA, što opterećuje resurse mobilnih uređaja. Zbog toga bi bolje rješenje bilo kada bi FA rješavao taj posao umjesto mobilnih uređaja korisnika. Kako bi se smanjilo saobraćajno opterećenje na GPRS mreži, enkapsulacija i dekapsulacija se obavlja na FA nodu.

Dodatna prednost korištenja zasebnog FA noda je i mogućnost dodjeljivanja jedne IPv4 adrese za više mobilnih klijenata, čime se smanjuje potreban opseg javnih IP adresa za GPRS mrežu.

MobileIP mobilni klijent koji traži podršku za roaming u nekoj mreži, može doći u situaciju da u toj mreži nije obezbjeđena FA funkcija. Ovaj slučaj je čest kod mreža baziranih na IPv4 sa podrškom za mobilnost. Alternativno rješenje za ovu situaciju je pokušaj pronalaska FA noda u drugim mrežnim domenama koje bi mogle sadržavati FA. Kod GPRS mreža to bi značilo korištenje međuoperatorskog PLMN roaminga do mreže koja bi mogla obezbijediti funkcije FA noda za datog mobilnog klijenta.



Figur 4.8-2 Scenarios 4 and 5

Slika 5.
MobileIP-GPRS interworking, scenarij 2

MOBILEIP AAA I GPRS AAA INTEGRACIJA

Da bi se omogućila konekcija većem broju korisnika na WLAN mrežu, neop-

hodno je obezbijediti jednostavnost procedure konekcije. Registrirani korisnik GPRS mreže se autentificira kod svoje matične GPRS mreže, što se svakako može koristiti za pristup WLAN mreži. Jedno od rješenja je mogućnost implementacije jedinstvenog AAA servera za servisiranje na obje mreže (GPRS i WLAN). Drugo rješenje obuhvata uspostavu lokalnog obračunskog servera na strani WLAN mreže, a koji bi prosljeđivao obračunske informacije matičnoj GPRS mreži. Ovo drugo rješenje zahtijeva znatno manje modifikacija postojećih sistema.

AAA RJEŠENJE SA DIAMETER PROTOKOLOM

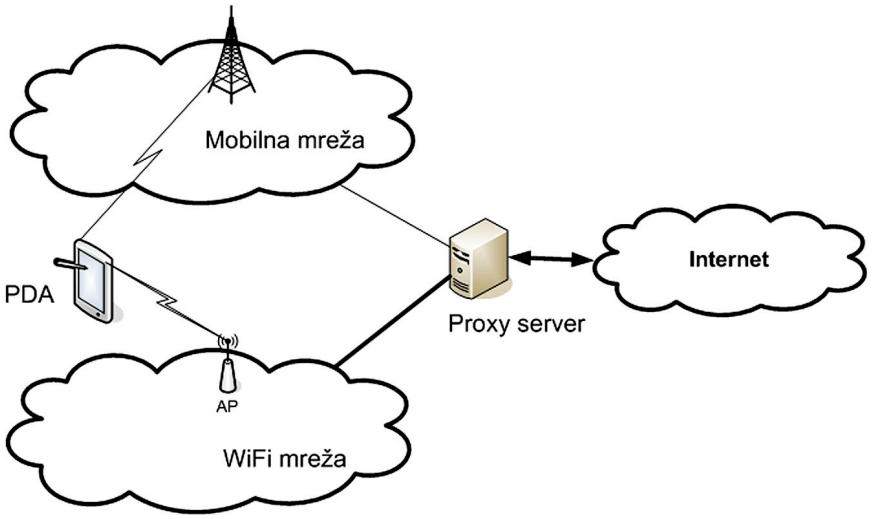
Rješenje integracijske AAA funkcionalnosti uz pomoć DIAMETER protokola nije najjednostavnije iz razloga što ne postoji besplatna (open source) DIAMETER implementacija. Osim toga, postoji problem neophodnosti ponovne prijave (logiranja), svaki put kada se mijenja mreža. Ovaj problem se može riješiti onemogućavanjem WLAN autentifikacije, što, s druge strane, dovodi sigurnost sistema u pitanje.

KOMBINACIJA IEEE802.1X AUTENTIFIKACIJE I MOBILEIP

Koristeći IEEE802.1X standardnu autentifikaciju, postaje nepotrebna AAA funkcionalnost za MobileIP registraciju, zbog čega će na kraju MobileIP servisi biti znatno jednostavniji. Prvo se mobilni klijent autentificira od pristupne tačke. Nakon toga, izvršava se MobileIP registracija.

HANDOVER PROCES IZMEĐU WLAN I GPRS MREŽA

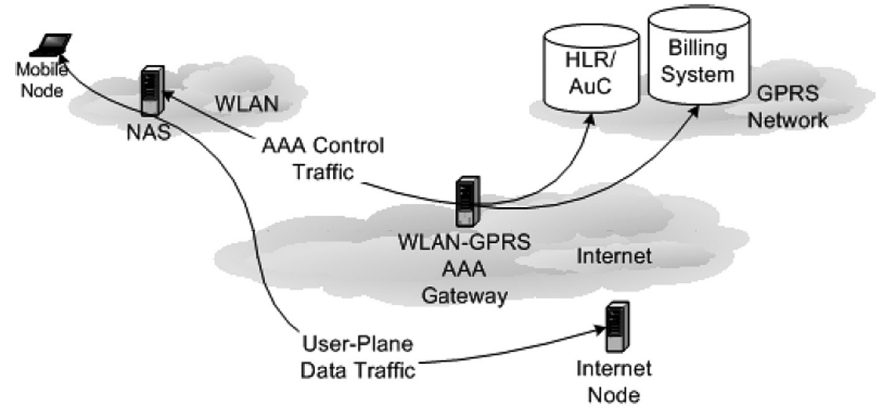
Komplementarne mogućnosti WLAN i GPRS mreža obezbjeđuju efikasnu pristupnu infrastrukturu koja je široko rasprostranjena i na pojedinim područjima širokopojasna. Dok su WLAN mreže ograničene u pokrivanju područja, GPRS je ograničen u propusnoj moći. Zbog svega toga, neophodan je kompromis kada se koriste obje mreže.



Slika 6.
Vertikalni handover proces između WLAN i GSM mreža

Troškovi konekcije su važan faktor koji diktira način korištenja pristupnih tehnologija. Za firme sa velikim brojem pokretnih zaposlenika (održavanje, elektro i telefonski servisi), značajna je i cijena terminalnog uređaja.

Slika 6. djelomično ilustrira rješenje sa implementiranim posredničkim proxy serverom. Svakoj od dvije mreže (WLAN i GPRS) pristupa se posredstvom proxy servera. Tako naprimjer, kada korisnik PDA uređaja želi pristup Internetu, proxy server određuje tip korištenog mrežnog pristupa, da bi mogao prilagoditi zahtijevane sadržaje mogućnostima korisnikovog terminalnog uređaja, ali i pristupne mreže. Djelovanje proxy servera usmjereno je na smanjenje udaljenosti i vremena za dohvat traženih sadržaja, umanjujući na taj način troškove konekcije. PDA uređaj će uvijek biti konektovan na GPRS mrežu, dok će koristiti konekciju na WLAN kad god se nađe u zoni pokrivanja ove mreže. Kada se koristi WLAN za mrežni pristup, naplaćuje se samo korištenje WLAN pristupa. WLAN cijene konekcije su znatno manje nego kod GPRS mreže, zbog čega se WLAN preferira nad GPRS pristupom, kad god je to moguće.



Slika 7.
Princip slabe WLAN-GPRS integracije

Problem nastaje kada je uspostavljen link na sadržaje putem GPRS mreže, a istovremeno PDA dolazi u zonu pokrivenosti WLAN mrežom. Mrežni pristup bi se trebao promijeniti sa GPRS na WLAN, ali to zahtijeva prekid linka ka Internetu. U tom slučaju, neophodan je mehanizam za vertikalni handover (Vertical Handover), koji bi omogućio nastavak aktivne konekcije bez prekida.

PDA će uočiti prisutnost WLAN signala prilikom ulaska u zonu pokrivanja WLAN mreže. Na osnovu uočenog RF signala WLAN mreže, može se odrediti da li je dozvoljena promjena sa GPRS na WLAN pristup. Proxy serveru se šalje poruka (potvrda WLAN mreže) putem aktivne GPRS konekcije, tako da proxy server može započeti uspostavljanje WLAN konekcije između PDA i sebe samog. Poruka poslana proxy serveru funkcionira na isti način kao i TCP/IP sa trostrukim dogovorom (three-way handshake).

Ako je kvalitet WLAN signala zadovoljavajući, PDA otvara konekciju putem WLAN mreže za prijenos podataka između PDA i proxy servera.

Nakon potvrda i završetka autentifikacijskih procesa između PDA i proxy servera za WLAN konekciju, proxy server mijenja rutu IP paketa sa GPRS na WLAN konekciju. PDA nakon toga zna da mora koristiti uspostavljenu WLAN konekciju umjesto ranije aktivne GPRS konekcije.

Nakon uspostave WLAN konekcije, GPRS transfer podataka se zaustavlja dok se uspostavlja WLAN transfer podataka, bez prekida aktivne konekcije korisnika prema Internetu. Promjena mrežnog pristupa može se primijetiti sa strane korisnika samo po brzini prijenosa, budući da WLAN omogućava znatno veću propusnu moć od GPRS mreže.

Kako je WLAN potpuno drugačija mreža od GPRS mreže, neophodno je obezbijediti drugu IP adresu za korisnički PDA. Ovo vrijedi i za slučajeve prelaska korisnika sa jednog na drugi segment WLAN mreže. IP adresa se mijenja iz razloga promjene identiteta korisnika na različitim mrežama. Sa strane mreže to su sve različiti korisnici, zato što se različite IP adrese dodjeljuju PDA uređaju pri svakoj promjeni. MobileIP standard razvijen od Internet Engineering Task Force (IETF) 1992. godine, nudi jedno efikasnije rješenje problema.

MobileIP omogućava transparentan roaming između IP mreža i pristupnih tehnologija. MobileIP rješava transparentnost na sloju iznad IP sloja, upravljajući operacijama nad TCP i UDP paketima.

Kada kvalitet WLAN signala padne ispod prihvatljive vrijednosti date QoS standardom, PDA će upozoriti proxy server o degradaciji WLAN signala, a zatim će proxy server promijeniti tabelu rutiranja ponovo putem GPRS konekcije.

Ukoliko se WLAN signal ne izgubi kompletno već zadržava neki nivo daleko od optimalnog, korisniku se pruža opcija ručnog izbora zadržavanja WLAN konekcije. Kod prvog rješenja, GPRS mreža upravlja mobilnošću klijenta. WLAN funkcionira kao jedna od GPRS ćelija. Cjelokupni saobraćaj prolazi kroz SGSN ili GGSN node, čak i kada se destinacija nalazi u istom IP mrežnom segmentu. Kod drugog rješenja, mobilnost je upravljana sa WLAN mreže, bazirano na IEEE 802.11 pravilima. Kod trećeg rješenja između dvije mreže ubacuje se poseban element sa nazivom gateway mobilnosti. Ovaj element upravlja rutiranjem saobraćaja na bazi Mobile IP funkcionalnosti i u

principu je proxy server koji se može instalirati bilo na GPRS ili WLAN mreži.

GPRS-WLAN INTEGRACIJA I IZBOR MREŽNE ARHITEKTURE

Integracija GPRS i WLAN mreža uveliko zavisi od izabrane arhitekture WLAN mreže. GPRS mreže slijede postignute standarde dok WLAN mreže često mogu biti dizajnirane na različite načine, kako bi ostvarile operativnost potrebnu za određene specifične potrebe. Zbog toga, integracija WLAN i GPRS mreža može biti otežana problemima sa različitih aspekata.

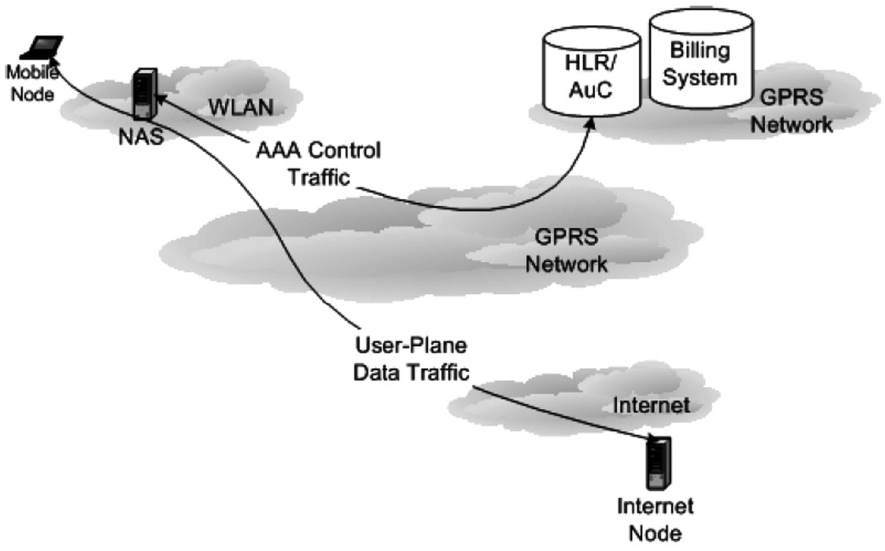
SLABA INTEGRACIJA

Čvrstina integracijskih veza između WLAN i GPRS mreža ovisi o tome koliko su ove tehnologije interoperabilne. Za slabu integraciju, mrežni interworking se uglavnom bazira na dijeljenju korisničkih informacija u svrhu realizacije AAA funkcionalnosti. Slabo integrirana WLAN mreža koristi informacije dobivene od HLR-a o registriranim GPRS mobilnim korisnicima, te određene funkcionalnosti biling sistema operatora kako bi se prenijele informacije za naplatu korištenja resursa (Slika 7.).

Servisi poput mobilnosti (MobileIP npr.), sigurnosti i zaštite (npr. IPSec protokol set), te mehanizmi za handover moraju biti podržani na standardizirane načine. Kod jako integriranih sistema, WLAN mreža će obezbijediti iste funkcionalnosti kroz odgovarajuće GPRS primitive. Slabo integrirani sistemi su jednostavniji za podršku i integraciju, čineći ovo rješenje pogodnijim za ubrzanu evoluciju.

U takvom rješenju, samo AAA baziran saobraćaj će se odvijati prema GPRS mreži za svakog mobilnog korisnika. Drugim riječima, WLAN mreža za roaming GPRS korisnika ne koristi upravljanje mobilnošću niti druge GPRS specifične funkcionalnosti.

WLAN mreža je u mogućnosti da koristi Internet kao transportnu mrežu za prijenos kontrolne signalizacije i podataka o korisničkim profilima. Za lokacije bez IP backbone mreža, ali istovremeno



Slika 8.
Princip jake WLAN-GPRS integracije

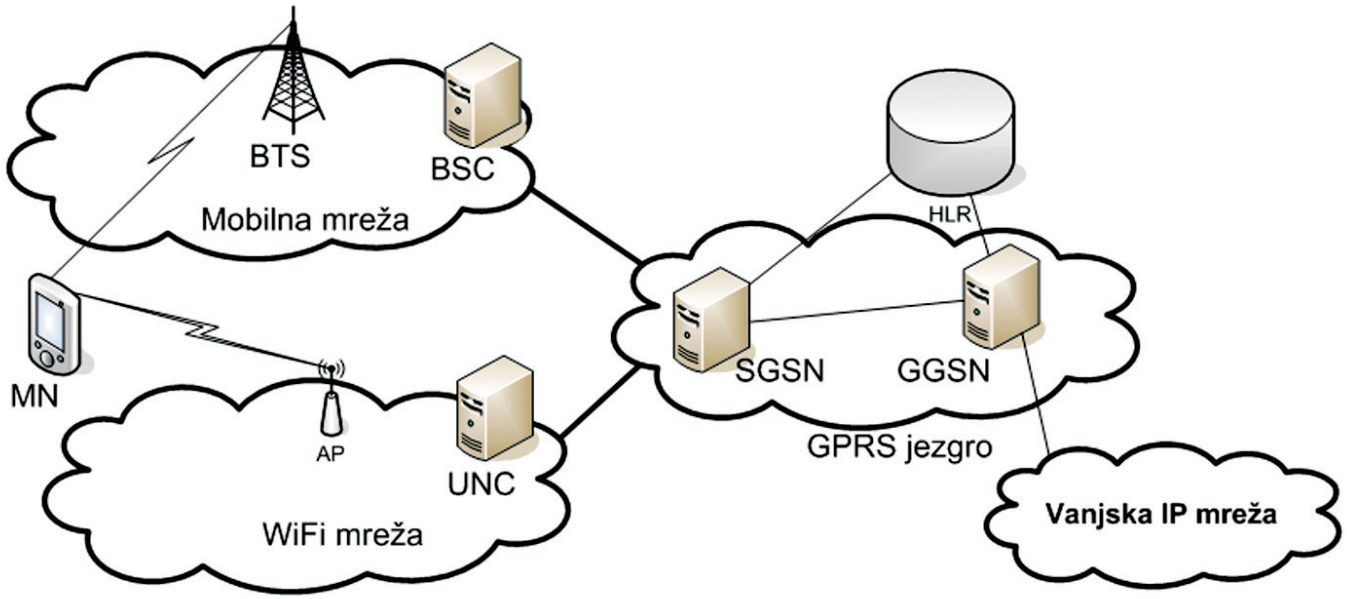
pokrivenih GPRS mrežom, jaka integracija može obezbijediti alternativne metode za servise visoke kvalitete mobilnim korisnicima.

Nekoliko autentifikacijskih mehanizama su standardizirani od IETF-a s ciljem omogućavanja autentifikacijske funkcionalnosti na bazi informacija pohranjenih na SIM kartici mobilnog korisnika i AuC noda GPRS mreže. Ovi mehanizmi su bazirani na EAP protokolu. Za sisteme sa slabom integracijom definirane su EAP-SIM, EAP-AKA i EAP-SIM-GMM varijante. Zbog sigurnosnih zahtjeva, preporučuju se za WLAN-GPRS AAA integraciju EAP-SIM i EAP-AKA varijante.

U osnovi, EAP obezbjeđuje fleksibilnu autentifikacijsku platformu koja omogućava autentifikaciju mobilnih klijenata na više različitih načina.

JAKA INTEGRACIJA

Za razliku od slabe integracije, rješenja sa jakom integracijom dijele mnogo više funkcionalnosti. Kod rješenja jake integracije WLAN-GPRS mreža, WLAN mreža koristi mehanizme autentifikacije, mobilnosti i zaštite realizirane na strani GPRS mreže (Slika 8.). Zbog navedenog, WLAN mreža treba da razumije GPRS



Slika 9.
Funkcionalna shema rada UMA koncepta

LITERATURA

[1] "Convergence Technologies for 3G Networks", John Wiley & Sons, Ltd

[2] "Internet Communications Using SIP", John Wiley & Sons, Ltd

[3] 3GPP website: www.3gpp.org

[4] Ramjee Prasad, Marian Ruggieri: "Technology trends in wireless communications", 2nd edition, Artech House

[5] FMCA. 2006. FMCA Convergence Application Scenarios. http://www.thefmca.com/assets/pdf/FMCA_Convergence_Application_Requirements_Rel_1.0.pdf

[6] Vrdoljak, M., Vrdoljak, S., Skugor, G. 2000. "Fixed-Mobile Convergence Strategy: Technologies and Market Opportunities", IEEE Communications Magazine

[7] Disruptive Analysis Ltd, May 2006 Confidential Enterprise FMC White Paper

primitive, kako bi izvršavala sistemske funkcionalnosti poput bilo koje GPRS mreže. Iako rješenja sa jakom integracijom obezbjeđuju bolje perfomanse mobilnosti i brži handover proces pored ostalog, posao integracije je daleko zahtjevniji od onog pri realizaciji rješenja sa slabom integracijom.

WLAN mreža će koristiti povezivanje na drugom sloju prema interfejsu za GPRS mrežni transportni backbone. I signalni kontrolni saobraćaj povezan sa AAA servisima, kao i podatkovni saobraćaj povezan sa mobilnim korisnikom, proći će kroz GPRS backbone i koristiti postojeće interfejse prema vanjskim paketskim mrežama, kao naprimjer Internetu. IETF je standardizirao nadolazeću EAP-GPRS varijantu za EAP autentifikacijski okvir, koji obezbjeđuje autentifikaciju mobilnih korisnika u rješenju sa jakom integracijom.

Zaštitni mehanizmi prema vanjskim mrežama će se obrađivati sa strane GPRS mreže, tako da ne treba da budu problem u realizaciji za WLAN operatore.

POZNATIJA KOMERCIJALNA WLAN-GPRS RJEŠENJA

Na tržištu postoji više komercijalnih rješenja integracije GPRS i WLAN mreža, od kojih ćemo opisati neka.

WEROAM

Weroam je ponudio tržištu rješenje za lokalne WLAN mreže koje omogućava GPRS korisnicima prijavu na Weroam WLAN mrežu. Saobraćaj počinje kroz WLAN sa pristupne tačke, a zatim do Weroam pristupnog servera. Sva komunikacija između pristupnog servera i različitih izvora autentifikacije obavlja se unutar IP mreže. Neke od specifičnosti Weroam rješenja su:

- Da bi se izvršila autentifikacija, SIM kartica mora biti spojena na računar putem čitača SIM kartica;
- SIM kartica se autentificira uz pomoć HLR-a kojem se pristupa putem IP/SS7 signalizacijskog gatewaya;
- Saobraćaj se može obavljati putem Interneta ili GPRS mreže.

Obračun se obavlja putem RADIUS interfejsa, nakon završetka sesije obračunska informacija se u TAP formatu šalje ka matičnoj GPRS mreži.

TRANSAT

Transat je obezbijedio vlastito rješenje za GPRS-WLAN integraciju. Autentifikacija korisnika se bazira na SIM kartici, na isti način kao kod regularnog GPRS sistema. SIM je spojena na laptop uz pomoć SIM-USB adaptera. Softver za komunikaciju sa SIM karticom i funkcije GPRS protokola izvršavaju se lokalno na laptopu korisnika. Drugi dio Transat rješenja sastoji se od servera koji funkcionira kao SGSN-GGSN povezan sa WLAN mrežom.

Saobraćaj sa laptopa će prolaziti kroz WLAN mrežu, putem IP konekcije prema GPRS mreži. Konekcija prema GPRS sistemu je također po prirodi IP, nije neophodna SS7 konekcija na lokalnoj mreži. Lokalno locirani Transat server generira obračunske informacije u istoj formi kao regularna GPRS mreža, te nakon slanja obračunskih informacija ka matičnom GPRS sistemu, korisnikov račun se opterećuje na isti način kao i kod regularnog GPRS saobraćaja.

UMA (UNLICENSED MOBILE ACCESS)

UMA predstavlja relativno novu tehnologiju razvijenu s ciljem da se postigne set specifikacija za proširenje mogućnosti govornih i podatkovnih GSM/GPRS servisa, na način da se mogu koristiti i na nelicenciranom radio opsegu kao što su Bluetooth i WiFi. Slika 9. prikazuje funkcionalnu shemu rada UMA koncepta. Osnovna ideja UMA koncepta leži u korištenju nelicenciranih mobilnih pristupnih tehnologija, kako bi se ostvario pristup do GSM i GPRS servisa. Umjesto korištenja GSM ili GPRS interfejsa, UMA omogućava pristup resursima GSM i GPRS mreža putem neke od nelicenciranih bežičnih tehnologija, najčešće Bluetooth i WiFi. Da bi se pritom postigla neprekidnost korištenja servisa, dizajniran je poseban mrežni element, koji je nazvan UNC (UMA Network Controller).

Mobilni korisnik UMA tehnologija koristi dual-mode mobilni uređaj koji je u mogućnosti pristupiti na WiFi i na GSM/GPRS mreže. UMA podržani mobilni uređaj uspostavlja vezu sa UNC nodom kada se uspije konektovati na neku od nelicenciranih mreža. Na taj način se putem UNC noda, posredno omogućava mobilnom korisniku pristup do GSM/GPRS jezgra mreže. Svakom konekcijom na neku od WiFi mreža, UMA klijent će pokušati uspostaviti kontakt sa UNC nodom putem IP mreže, a zatim se autorizirati/autentificirati za pristup GSM/GPRS mrežnom jezgru. Kada to uspije, mobilni UMA klijent ažurira svoju novu lokaciju u GSM mreži, tako da se svaki budući saobraćaj u vezi s datim klijentom rutira na UMAN (UMA Network), umjesto na RAN (Radio Access Network). UMA mobilni klijent je u mogućnosti koristiti roaming između mobilnih i bežičnih mreža, bez prekida aktivne govorne sesije prilikom handovera.

UMA je jednostavna za implementaciju s obzirom na to da ne zahtijeva velike izmjene na jezgru mobilne mreže. UMA podržani mobilni uređaj zahtijeva instaliran UMA klijentski software, koji omogućava komunikaciju sa UNC-om.

LITERATURA

[8] Nortel Networks, “Designing converged enterprise networks for IP telephony”, White Paper, www.nortelnetworks.com

[9] Voice over 802.11, Artech House 2004

[10] Mobile IP technologies and applications, Cisco Press 2005

[11] Wireless and mobile All-IP networks, John Wiley & Sons 2006

[12] Network models for converged fixed and mobile telephony, Technical paper Alcatel 2005

[13] Evolution towards converged services and networks, white paper Ericsson April 2005

[14] Unbounded mobilty: Always connected, anywhere; white paper Alcatel October 2005

[15] HiPath – Total business communications, white paper Siemens communications 2005

[16] Rationalizing fixed-mobile convergence, Yanky group report May 2006

[17] Continuity: the fixed-mobile convergence solution, Application brief UTStarcom Inc. USA 2006

mr. Selma Kovačević, dipl. ing. el.

Primjena DWDM tehnologije u radu Disaster Recovery sistema

DWDM technology usage in Disaster Recovery systems

Sažetak

Svjedoci smo neumitnog napretka elektronskih tehnologija koje postepeno zauzimaju sve sfere poslovnog i društvenog života čovječanstva. Fizičke transakcije koje su dosad obavljali ljudi, bivaju potisnute i često u potpunosti zamijenjene novim elektronskim transakcijama, pametnim karticama, te drugim sličnim servisima.

Iako je ovakav trend prisutan u gotovo svim institucijama i kompanijama čije se poslovanje zasniva na određenim podacima, možemo reći kako je finansijski sektor bio taj koji je u najvećoj mjeri pokrenuo revoluciju IT tehnologija.

Novi izazovi stvaraju određenu vrstu pritiska na kompanije da održe zadovoljavajući stepen brzine i integriteta mreže i mrežnih servisa. Instituciije koje svakodnevno rade sa elektronskim transakcijama imaju obavezu da osiguraju privatnost, pouzdanost i dostupnost za veliku količinu strukturiranih i nestrukturiranih podataka. Zahtjevi i očekivanja korisnika su sve veći, tako da korisnici očekuju uslugu koju su platili i u slučaju da se dese nepredviđene havarije, poput zemljotresa, poplava ili požara.

Iz navedenih i brojnih drugih razloga, koncept Disaster Recovery sistema dobija nova značenja. Naime, različite vrste realnih prijetnji sigurnosti poput: terorističkih napada, kompjuterskih virusa i hakerskih napada, industrijskog i socijalnog inžinjeringa, te sve učestalije havarije utjecali su na sve veće interesovanje i ulaganja u ovaj aspekt sigurnosti. Svaka vrsta havarije može ugroziti dostupnost, integritet i povjerljivost kritičnih poslovnih resursa, što može rezultati milionskim gubicima i u konačnici nestankom firme. Da bi se omogućio oporavak sistema od havarije, neophodno je obezbijediti mrežnu infrastrukturu adekvatne propusnosti i pouzdanosti.

Ključne riječi: WDM, DWDM, Disaster Recovery sistemi, Hot standby stanje, primarna i rezervna lokacija

Abstract

We all evidence high-speed progress of electronic technologies which gradually occupy all areas of business and social life. Fisical transactions which until recently were done by people become supressed and often completely replaced by electronic transactions, smart cards and other similar services.

Although this trend has become everyday business for almost every institution and company whose business is based on data and some information, IT technologies are dominating and critical in banking and financial sector in general.

New challenges create some kind of pressure on this companies to maintain satisfying speed and network integrity level. Institutions that work with electronic transactions every day has an obligation to ensure privacy, reliability and availability of structured and unstructured data. User requirements and expectations become bigger meaning that users expect to get service they payed for, regardless of unexpected disasters like earthquake, flood or fire.

Considering all mentioned and many other reasons, Disaster Recovery systems concept is getting new importance in today world. Different types of threats like: terrorism, computer viruses and hacker attacks, industrial and social engineering, and frequent disasters affect increasing investment in security issues. Any kind of disaster can endanger availability, integrity and privacy of critical business resources, which can lead to milions loses. In order to enable system recovery after disaster, it is necessary to have network infrastructure of adequate throughput and reliability.

Key words: WDM, DWDM, Disaster Recovery Systems, Hot standby state, Primary and Backup location

I. UVOD

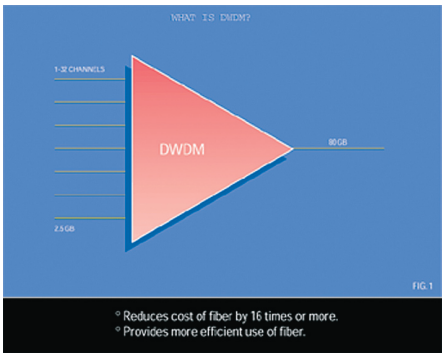
Ne tako davno, sistemi su radili na neuporedivo manjim brzinama nego što je to danas. Standardne tehnologije poput Etherneta, LAN mreža ili modema brzine 9.600 Bps bile su više nego dovoljne da povežu različite tipove uređaja u mreži. Uporedo sa brzim razvojem novih hardverskih uređaja, mrežnih protokola i standarda, došlo je do povećanja broja elektronskih transakcija, procesne moći računarskih jedinica i interfejsa, te razvoja adekvatnih softverskih rješenja. Za razliku od količine podataka koja se procesira i pohranjuje na diskovima PC računara i servera, obim podataka koji se obrađuje u okviru informacionih sistema finansijskih kompanija je neuporedivo veći i zahtijeva posebnu vrstu hardversko-softverskih rješenja za osiguranje konzistentnosti, sigurnosti i dostupnosti. Brzine mrežnih uređaja koji povezuju opremu u datim centrima povećale su se s vremenom, kako bi se ostvarila kompatibilnost sa novim mrežnim tehnologijama i standardima poput Fiber Channela i ESCON-a.

Fiber-optičke mrežne konekcije generalno omogućavaju velike brzine i kvalitet potreban za prijenos velike količine dnevnih transakcija, što, s druge strane, ima i svoju cijenu. Stoga je efikasna upotreba fiber-optičkih mreža od suštinske važnosti. Upravo ovu efikasnost moguće je postići kroz DWDM tehnologiju.

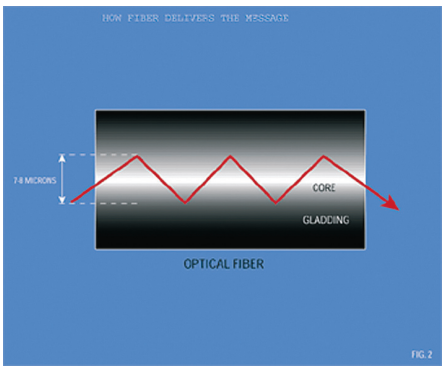
II. OSNOVE DWDM TEHNOLOGIJE

DWDM je tehnologija koja se koristi od mrežnih providera za efektivno povećanje mrežne propusnosti, te u konačnici za povećanje dobiti, a bez dodatnih troškova izgradnje novih fiber linkova. Glavni tržišni pokretač razvoja i primjene DWDM tehnologije bio je eksponencijalni porast internetskog saobraćaja. Naime, nove statistike pokazuju kako je trenutni broj korisnika Interneta u svijetu čak 1.5 milijardi, za razliku od 2000. godine, kada je broj korisnika bio 360.000.

Osim naglog povećanja broja korisnika, pojavile su se nove aplikacije koje zahtijevaju znatno veće kapacitete mrež-



Slika 1.
DWDM tehnologija korištena u prijenosu podataka



Slika 2.
Princip rada fiber kanala u DWDM sistemu

INDEKS POJMOVA I SKRAĆENICA

LAN – Local Area Network
DWDM – Dense Wave Division Multiplexing
SONET – Synchronous Optical Network
ATM – Asynchronous Replication Mode
IP – Internet Protocol
TDM – Time Division Multiplexing
IT – Information Technology
ROADM – Reconfgiurable Optica Add/Drop Multiplexer
MSPP – Multiservice Provisioning Platform
MSTP – Multiservice Transport Platform
MAN – Metrpolitan Area Network

nih linkova poput: TV visoke definicije, video-na-zahtjev, telemedicina, video-konferencija, i slično. Slika 1. prikazuje osnovni koncept rada DWDM tehnologije u prijenosu podataka.

Telekom kompanije su već prešle na DWDM tehnologiju kako bi mogle pratiti zahtjeve svojih korisnika o pitanju performansi. U ovom slučaju se radi o tome da DWDM ima mogućnost da poveća snagu jedne optičke niti i do 100 puta. Ovo se postiže kombiniranjem višestrukih 2.5 Gbps signala na jednom DWDM fiberu. Na ovaj način je moguće dobiti novih 16 ili 32 kanala u DWDM sistemu, što predstavlja idealno rješenje za Disaster Recovery sisteme.

Kompanije koje se nalaze na velikim geografskim udaljenostima prve su počele ulagati u DWDM tehnologije. Zbog svoje efikasnosti DWDM je u značajnoj mjeri implementiran na metro tržištu, a s vremenom su sve navedene reference utjecale da finansijske institucije počnu sve više ulagati u prelazak na DWDM tehnologiju, a sa ciljem dobijanja većih mrežnih kapaciteta.

Za razliku od tradicionalnih fiber-optičkih sistema koji koriste jedan optički kanal na talasnoj dužini od 1550nm ili 1350nm, DWDM multiplicira talasne dužine unutar jednog fibera. Osnovna funkcija DWDM sistema jeste precizna kontrola predajnika fiksnih i varijabilnih talasnih dužina, optičkih miltipleksera (ili filtera), i optičkih prijemnika. S obzirom na to da filtriranje umanjuje snagu i energiju svjetlosnog talasa, neophodno je uvesti faktor optičkog pojačanja koji ima zadatak da anulira gubitke u signalu.

U osnovi DWDM tehnologije je prijenos svjetlosnih signala, kako je prikazano na Slici 2.

Zamislimo dugu u kojoj svaka boja prenosi određenu poruku, na način da je odvojena od ostalih boja. U DWDM sistemu fiber ima sposobnost da simultano prenosi više boja. Upotrebom različitih lasera, DWDM može prenijeti sve signale odjednom, nakon čega se na prijemnoj strani radi filtriranje kanala i distribucija originalne poruke. S obzirom na to da se svaki kanal na prijemnoj strani posebno demultipleksira u izvornu formu, moguć je istovremen prijenos različitih formata podataka na različitim brzinama. Tako je, naprimjer, moguće unutar jednog optičkog fiber prenijeti internetske (IP), SONET i ATM podatke.

Broj optičkih kanala koje je moguće koristiti u DWDM sistemu iznosi 32, po 16 u svakom pravcu. Tako da umjesto standardnog fiber kanala za slanje i kanala za prijem, moguće je dobiti 16 fiber kanala za slanje i 16 kanala za prijem signala. Broj fiber kanala koje je potrebno iznajmiti za prijenos određenog signala na ovaj način je smanjen 32 puta, što garantira uštedu na godišnjem nivou, uz evidentno povećanje brzine prijenosa na 80Gbps.

Nova istraživanja i primjene u praksi pokazuju kako DWDM laseri podržavaju postojanje čak stotina talasnih dužina od kojih svaka može prenijeti 10Gbps. Ovo znači da je moguć prijenos terabita podataka preko jednog optičkog vlakna.

III. HISTORIJA RAZVOJA DWDM TEHNOLOGIJA

DWDM tehnologija počela se razvijati u ranim 80-im godinama prošlog vijeka, kada su se koristile dvije talasne dužine: 1310nm i 1550nm (ili 850nm i 1310nm). Slika 3. prikazuje koncept rada prvog DWDM sistema nazvanog 'wideband' WDM.

U ranim 90-im pojavljuje se druga generacija WDM mreža, nazvana 'narrowband' WDM, u kojoj je korišten veći broj kanala (od dva do osam). Ovi kanali su bili raspoređeni unutar intervala od 400 GHz i na talasnoj dužini od 1550nm. Do sredine 90-ih godina 'dense' WDM (DWDM) već koriste od 16 do čak 40 kanala, na frekvencijama koje se kreću u rangu 100-200 GHz. Krajem 90-ih godina, DWDM sistemi evoluiraju do tačke u kojoj podržavaju rad od 64 do 160 kanala, gusto pakovanih po frekvencijskim intervalima od 50 GHz ili čak 25 GHz.

Slika 4. prikazuje historijski razvoj DWDM tehnologije, praćen povećanjem broja talasnih dužina, te smanjenjem razmaka između njih. Paralelno sa gušćim pakovanjem talasnih dužina unutar jednog fibera, postignut je značajan napre-

dak u fleksibilnosti konfiguracije, te u dodatnim funkcijama nadzora i upravljanja.

Povećanje gustoće kanala rezultiralo je značajnim povećanjem propusnosti fiber mreža. Tako je od 1995. godine, kada je demonstriran prvi sistem sa brzinom od 10 Gbps, zabilježen linearni rast mrežnih kapaciteta od dvostrukog povećanja svakih četiriju godina, do povećanja od četiri puta svake godine, kako je i prikazano na Slici 5.

IV. PRIMJENA DWDM TEHNOLOGIJE U DISASTER RECOVERY SISTEMIMA

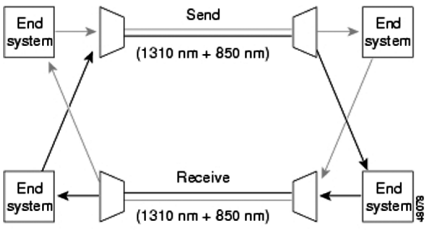
Posljednjih godina koncept Disaster Recovery sistema dobija nova značenja. Naime, različite vrste realnih prijetnji sigurnosti poput: terorističkih napada, kompjuterskih virusa i hakerskih napada, industrijskog i socijalnog inžinjeringa, te sve učestalije havarije utjecali su na sve veće interesovanje i ulaganja u ovaj aspekt sigurnosti. U današnjem svijetu globalizacije, organizacije i IT sistemi su više nego ikada ranije izloženi rizicima i ugrožavanju neprekidnosti poslovanja. Iz svih navedenih razloga, danas niti jedna kompanija čije se poslovanje zasniva na određenim podacima (a sve su takve), ne može sebi dozvoliti da se osloni na jedan sistem za obradu podataka. Bilo koji prekid u pružanju servisa krajnjim korisnicima može rezultirati milionskim gubicima. Ova činjenica dodatno naglašava važnost pouzdanosti u radu mreža nove generacije.

Kako bi izbjegli gubitke uzrokovane nekom havarijom, velika većina banaka, finansijskih institucija i korporacija ima neku vrstu plana za oporavak od havarije. Neki od ovih planova podrazumijevaju postojanje opreme na rezervnoj lokaciji koja je spremna da primi trake sa backupiranim podacima i da se aktivira u slučaju havarije na primarnoj lokaciji. Ovakav scenarij zvuči prihvatljivo, uz napomenu da u ovom slučaju nije moguće vratiti podatke iz trenutka prekida, već u najboljem slučaju podatke stare nekoliko sati. Vraćanje poslovanja na nekoliko sati unazad za neke sisteme može biti prihvatljivo, ali će za većinu banaka uzrokovati velike gubitke, kako u novcu, tako i povjerenju klijenata.

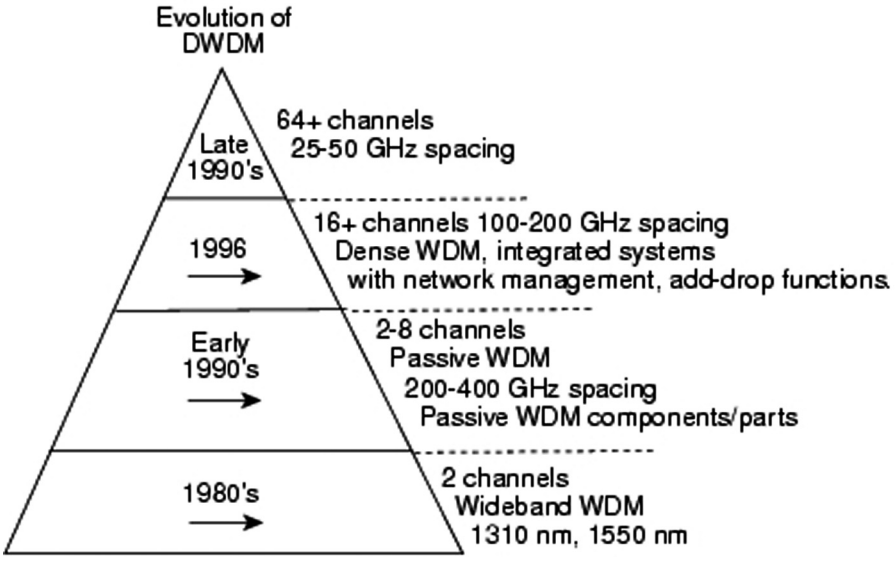
Dakle, backup sistema treba raditi u tzv. 'živom hot standby' stanju. Ovo, konkretno znači da oprema na rezervnoj lokaciji treba sve vrijeme biti aktivna na način da je uključena i da ima sve one podatke koji se u datom trenutku nalaze i na primarnoj lokaciji.

Identične ili slične IT prostorije trebaju, dakle, postojati kako na primarnoj, tako i na rezervnoj lokaciji, koja bi, prema nekim procedurama, za Disaster Recovery sisteme trebala biti udaljena između 15 i 50Km. Primarna i rezervna lokacija trebaju biti povezane brzim mrežnim linkovima i/ili udaljenim periferalima. U danima kada su periferali bili relativno spori, za uspješan Business Continuity koncept bilo je dovoljno posjedovati E1/T1 i E3/T3 TDM Mux opremu.

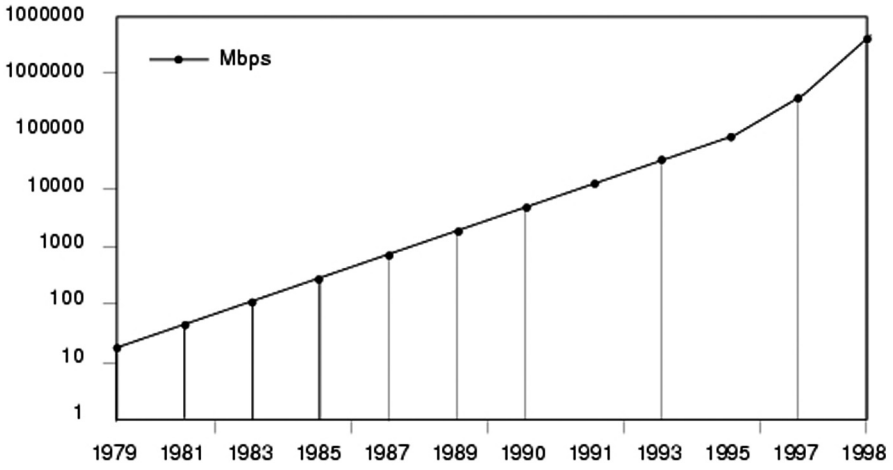
S vremenom, kako su periferali postajali sve brži, a aplikacije dovoljno robusne da podrže on-line replikaciju na serverima, to je i Disaster Recovery počeo činiti revolucionarne iskorake. Tako udaljene lokacije na kojima se nalaze kopije podataka postaju sve bliže, a to se postiže sinhronom replikacijom podataka. Sin-



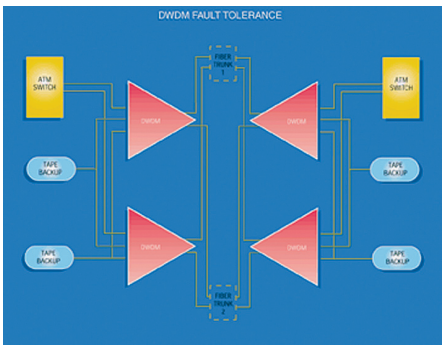
Slika 3.
Princip rada dvokanalne WDM mreže



Slika 4.
Historijski pregled razvoja DWDM tehnologije



Slika 5.
Grafikon linearnog rasta kapaciteta DWDM mreže



Slika 6.
Primjer rada Disaster Recovery sistema sa 10Km udaljenosti i ATM switch-em za backbone saobraćaj

hrona replikacija podataka podrazumijeva da su podaci na udaljenoj lokaciji u svakom tenutku tačni i ažurni u odnosu na primarnu lokaciju. On-line replikacija zahtijeva postojanje dvaju hard diskova identičnih ili sličnih konfiguracija. Podaci se paralelno upisuju na oba diska, tako da ukoliko jedan disk otkaže, drugi automatski preuzima njegovu funkciju, jer ima zapisane identične informacije. Ovaj koncept rada je ključan u transakcijski-baziranim operacijama gdje je neophodno da se backup sistem u slučaju potrebe može brzo aktivirati.

Komunikaciona mreža neophodna za ovakav koncept rada Disaster Recovery sistema sastoji se od brzih fiber optičkih interfejsa koji omogućavaju povezivanje traka i hard diskova do 40Km udaljenosti. U slučaju da se na primarnoj i rezervnoj lokaciji zahtijeva postojanje samo po jednog uređaja, dovoljno je imati jednu fiber paricu. Ukoliko postoji više uređaja, zahtijeva se i veći broj fiber parica. S obzirom na to da je fiber skup za zakup, instaliranje i održavanje, to su DWDM tehnologije pravo rješenje za veću uštedu i efikasnost u prijenosu podataka u Disaster Recovery sistemu. Na Slici 6. prikazan je scenarij kada dvije lokacije udaljene 10Km sadrže: ukupno 4 hosta koja učestvuju u replikaciji podataka, i ATM za povezivanje lokacija.

Jedna od specifičnosti ovog scenarija je mogućnost da se jedan isti signal prenese putem dviju različitih ruta. Ovo je moguće primjenom tzv. 'fault trunk' modula koji omogućava oporavak sistema od prekida, paralelno sa radom servisa.

Drugi scenarij je prikazan na Slici 7. i prikazuje dva računarska centra na udaljenosti od 17Km povezana fiber optičkim linkom. Ovaj model osigurava kontinuiranu on-line replikaciju podataka i oporavak u sekundi.

Zahvaljujući sve većoj upotrebi elektronskog bankarstva, banke imaju sve veću količinu podataka koje trebaju obraditi, poslati ili pohraniti. Gubitak podataka usljed neke havarije može u ovom slučaju uzrokovati milionske gubitke. Banke potencijalne probleme rješavaju na način da osiguravaju postojanje backupiranih podataka na rezervnoj lokaciji. S obzirom na to da su rezervne lokacije na relativno velikoj udaljenosti od primarne lokacije, neophodno je koristiti fiber optičku mrežu za povezivanje opreme na lokacijama. DWDM tehnologija u ovom slučaju omogućava kreiranje tzv.'virtualnihfibera'.

V. DWDM OPREMA ZA DISASTER RECOVERY SISTEME

Kada govorimo o konkretnoj opremi koja se koristi u DWDM mrežama, postoji veliki broj proizvođača opreme za rad DWDM mreža. U nastavku ćemo navesti samo neke od uređaja sa posebnim osvrtom na one karakteristike koje mogu pomoći u radu DWDM mreža.

Cisco ONS 15454 Multiservisna platforma

ONS 15454 predstavlja napredno rješenje za povećanje mrežne efikasnosti, korišteno od strane više od 1000 MSPP i više od 500 MSTP u svijetu. Radi se o trenutno najzastupljenijem DWDM rješenju u metro mrežama i mrežama regionalnog karaktera. Ovo rješenje koristi tzv. RO-ADM tehnologiju koja omogućava multipliciranje talasnih dužina preko cijele mreže, a bez potrebe za dodatnim uređajima za konverziju optičkih u električne

signale, i obrnuto. ONS 15454 omogućava brzine od 40Gbps, a u potpunosti je kompatibilan sa Layer 2, Layer 3 i SAN uređajima. Podržava sve DWDM topologije, i omogućava pružanje svih tipova servisa, na bilo kojoj mrežnoj lokaciji.

Prednosti ROADM i DWDM tehnologija koje dolaze do izražaja na ONS 15454 uređajima su:

- Mogućnost kreiranja različitih mrežnih topologija pomoću adekvatnih softverskih rješenja;
- Automatsko konfiguriranje mreže i mrežnih čvorova;
- Automatizirani monitoring i upravljanje optičkom snagom mreže;
- Jedinstveni IP upravljački interfejs za sve module unutar jednog čvora.

DWDM 2925 platforma

U ovom konkretnom slučaju riječ je o dvosmjernim fiber multiplekserima/demultiplekserima, koji u većini slučajeva dopuštaju multipliciranje na 4, 8, 16 ili 32 kanala po jednom optičkom fiberu talasne dužine 1550nm. Bitne karakteristike ovih uređaja su: zanemarljiv gubitak signala, kao i mali gubitak uzrokovan polarizacijom signala. Uređaji rade na single-mode fiberu, a mogu se konfigurirati za jednosmjernu ili dvosmjernu 4, 8, 16 ili 32-kanalnu transmisiju. Visoka izolacija sprečava interferenciju u dvosmjernoj komunikaciji. DWDM tehnologija uz pomoć adekvatnih uređaja povećava kapacitet fibera, dopušta simultani video, audio i podatkovni prijenos putem jedne fiber parice, pri tome zadržavajući performanse sistema.

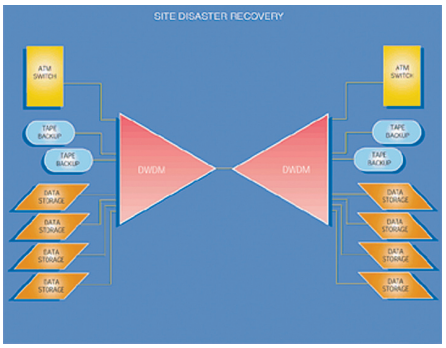
VI. ZAKLJUČAK

DWDM je u vrijeme kada se pojavio predstavljao revolucionarno novu tehnologiju za prijenos podataka putem optičkih mreža, čiji je osnovni cilj rješavanje problema zvanog „nedostatak fiber mreža“. Očekuje se da će upravo ova tehnologija zauzimati centralnu poziciju u optičkim mrežama budućnosti.

Trendovi u razvoju DWDM opreme idu u pravcu uspostave pune kontrole nad pouzdanošću DWDM mreža. Imajući u vidu važnost ovog zahtjeva, proizvođači DWDM opreme kontinuirano rade na poboljšanju kritičnih parametara multipleksera, kao što su: gubital signala, devijacija signala, ometanje signala vanjskim utjecajima, i slično.

Osnovne prednosti DWDM tehnologija koje posebno dolaze do izražaja u radu Disaster Recovery sistema su: značajno povećanje mrežne propusnosti, dodatna fleksibilnost u odnosu na standardne fiber-optičke mreže, pružanje novih servisa, veća skalabilnost, te mogućnost uspostavljanja višestrukih logičkih topologija putem jedne MAN mreže. Iz pobrojanih prednosti, te brojnih primjera iz prakse, možemo zaključiti kako DWDM tehnologija već sada čini okosnicu mrežnog okruženja kako u Disaster Recovery sistemima, tako i u svakodnevnom produkcionom radu korporacijskih sistema.

U budućnosti se očekuje još veća primjena DWDM tehnologija u velikim korporacijskim okruženjima. Riječ je o informacionim sistemima koji zahtijevaju viši stepen centralizacije, te prijenos i replikaciju velike količine podataka u realnom vremenu.



Slika 7.
Disaster Recovery sistem na udaljenosti od 17Km

LITERATURA

[1] http://www.cisco.com/univercd/cc/td/doc/ product/mels/cm1500/dwdm/dwdm_ovr.htm#wp1002608

[2] http://www.drj.com/articles/wint99/gray.htm

mr. Amir Zukanović, dipl. ing. el.

Mrežni menadžment – efektivno upravljanje računarskom mrežom
Network Management – the effective management of a computer network

Sažetak
Mrežni menadžment je ključni faktor u uspješnom radu neke mreže. Kako je biznis postao sve više povezan s mrežnim uslugama, održavanje ovih usluga u funkciji se može ujedno poistovijetiti i sa održavanjem poslova „u životu".
Međutim, bez obzira na svoju važnost, mrežni menadžment još spada u slabo razumljive oblasti u ionako dobro razrađenom svijetu umrežavanja.
Ključne riječi: NMS, FCAPS, SNMP, CMIS, CMIP, TCP, UDP, MIB, SMI, OID, MO, ICMP;

Abstract
Network management is an essential factor in successfully operating a network. As businesses become increasingly dependent on networking services, keeping those services running becomes synonymous with keeping the business running.
Despite its significance, network management is still one of the lesser understood topics in the otherwise well-charted world of networking.
Key words: NMS, FCAPS, SNMP, CMIS, CMIP, TCP, UDP, MIB, SMI, OID, MO, ICMP;

INDEKS POJMOVA I SKRAĆENICA

NMS (Network Management System) – kombinacija hardvera i softvera za monitoring i upravljanje mrežom
ISO (International Organization for Standardization) – internacionalno tijelo za standardizaciju
TCP/IP (Transmission Control Protocol/ Internet Protocol) – protokoli internet steka
SNMP (Simple Network Management Protocol) – protokol koji se koristi u mrežnom menadžmentu za upravljanje mrežom
FCAPS (Fault, Configuration, Accounting, Performanse, Security) referentni model – predstavlja model telekomunikacionog mrežnog menadžmenta. Opisuje kategorije za grešku, konfiguraciju, obračun, performansu i sigurnost, gdje ISO model definira zadatke mrežnog menadžmenta
CMIS (Common Management Information Service) – predstavlja standard u računarskim mrežama za uslugu koju pružaju mrežni elementi u mrežnom menadžmentu
CMIP (Common Management Information Protocol) – predstavlja protokol mrežnog menadžmenta i nudi implementaciju za usluge definirane CMIS-om.

1. UVOD

Ranih 1980-ih došlo je do nagle ekspanzije u umrežavanju. Kada su kompanije uočile smanjenje troškova i porast produktivnosti uvođenjem mrežne tehnologije, onda su počele proširivati postojeće mreže, čak i brže nego što su se uvodile nove mrežne tehnologije i proizvodi. Sredinom 1980-ih određene kompanije su se počele susretati s problemom nekompatibilnosti mrežne opreme od različitih proizvođača.

Problemi u vezi s proširenjem mreže utjecali su na mrežni menadžment i strateško planiranje rasta mreže. Svaka mrežna tehnologija zahtijevala je grupu eksperata. Upravljanje velikim, heterogenim mrežama izazvalo je veliki problem za većinu kompanija. Javila se potreba za automatiziranim mrežnim menadžmentom, integriranim u različita okruženja.

Mrežni menadžment uključuje aktivnosti, metode, procedure i alate koji se odnose na operaciju, administraciju, održavanje i usluživanje umreženih sistema.

Operacija se odnosi na održavanje mreže u funkciji, kao i na servise koje mreža omogućuje. Ona uključuje monitoring mreže, kako bi se otkrili problemi što je ranije moguće.

Administracija obuhvata vođenje evidencije o resursima u mreži i kako se oni dodjeljuju. Ona se odnosi na sve poslove, koji su potrebni da se stvari drže pod kontrolom.

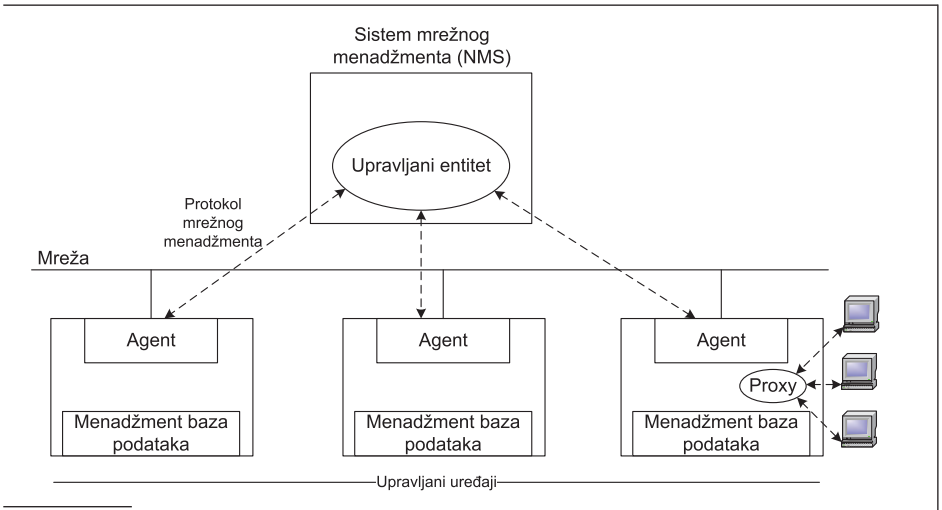
Održavanje je povezano sa izvršavanjem popravki i poboljšanja mrežne opreme. U ovu aktivnost se ubrajaju korektivne i preventivne mjere kao što su podešavanje parametara uređaja i uopće interveniranje, kako bi mreža bolje „radila".

Usluživanje je povezano s konfiguriranjem resursa na mreži u svrhu podrške date usluge. Naprimjer, ovdje može biti uključeno podešavanje mreže tako da novi korisnik može imati pristup VoIP usluzi.[1][2]

2. ARHITEKTURA MREŽNOG MENADŽMENTA

Većina arhitektura mrežnog menadžmenta koristi istu osnovnu strukturu i skup relacija. Upravljani uređaji (managed devices) kao što su računarski sistemi i drugi mrežni uređaji, pokreću softver koji im omogućava da šalju alarme kada se pojave problemi. Upravljani entiteti su programirani da reagiraju na alarme izvršavanjem jedne ili više akcija, uključujući obavještenje operatera, sistemsko gašenje, registriranje događaja i automatske pokušaje popravke sistema.

Menadžment entiteti mogu također pretraživati upravljane uređaje za provjeru vrijednosti određenih varijabli. Pretraživanje može biti automatsko ili ručno (od korisnika), a agenti u upravljanim uređajima odgovaraju na svaki upit. Agenti su softverski moduli koji prvo kompaliraju informaciju o upravljanim uređajima u kojima se nalaze, potom pohranjuju ovu informaciju u menadžment bazu podataka i na kraju je ponude (proaktivno ili reaktivno) menadžment entitetima unutar sistema mrežnog menadžmenta (network management systems – NMS) putem protokola mrežnog menadžmenta. Menadžment proxy je entitet koji nudi menadžment informaciju u korist drugih entiteta (Slika 1.).[1]



Slika 1.
Prikaz arhitekture mrežnog menadžmenta

INDEKS POJMOVA I SKRAĆENICA

SGMP (Simple Gateway Monitoring Protocol) – omogućuje izvršenje komandi na entitetima aplikacionog protokola za postavljanje ili vraćanje vrijednosti u svrhu monitoringa gatewaya, gdje se nalaze entiteti aplikacionog protokola

CMOT (CMIS/CMIP Over TCP/IP) – predstavlja arhitekturu za upravljanje mrežom na daljinu

MIB (Management Information Base) – je konceptualna baza podataka koja se koristi za upravljanje uređajima u komunikacionoj mreži

MO (Managed Object) – predstavlja upravljani objekat, koji se nalazi u MIB-u

SMI (Structure of Management Information) – definira skup srodnih upravljanih objekata u MIB-u

OID (Object Identifier) – predstavlja identifikator koji se koristi da imenuje objekat u MIB-u

ASN.1 (Abstract Syntaxt Notation One) – predstavlja standard koji opisuje strukture podataka za opis, kodiranje, prijenos i dekodiranje podataka

BER (Basic Encoding Rules) – je jedan od formata za kodiranje definiran kao dio ASN.1

IANA (Internet Assigned Numbers Authority) – entitet koji nadgleda globalnu alokaciju IP adresa

3. ISO MODEL MREŽNOG MENADŽMENTA

Za efektivni mrežni menadžment potrebno je razmotriti pet funkcionalnih oblasti, koje su definirane ISO modelom:

– **Menadžment greške (Fault management)**
Cilj ovog menadžmenta je detekcija, logiranje i automatska korekcija mrežnih problema radi djelotvornijeg održavanja mreže u funkciji. Pošto greške mogu prouzrokovati pad ili neprihvatljivu degradaciju mreže, menadžment o grešci je možda najviše implementiran od svih ostalih elemenata ISO mrežnog menadžmenta.
Menadžment greške uključuje prvo utvrđivanje simptoma i izolaciju problema. Potom se problem ispravlja i rješenje se testira na svim važnim podsistemima. Na kraju se evidentira detekcija i ispravka problema.
Postoje dva načina upravljanja greškama: *reaktivni i proaktivni*. Reaktivno znači sačekati da se problem desi i onda ga detektirati i korigirati, a proaktivno podrazumijeva da se odredi da li greške prekoračuju kritične operacione pragove. Ako se desi prekoračenje, proaktivni administrator utvrđuje izvor i smanjuje pojavu greške.[1][2]

– **Menadžment konfiguracije (Configuration management)**
Cilj ovog menadžmenta je monitoring mreže i informacija o sistemskoj konfiguraciji, kako bi se mogli evidentirati i upravljati utjecaji na mrežni rad raznih verzija hardverskih i softverskih elemenata.
Svaki upravljani uređaj ima različite verzije informacija, koje su povezane s njim. Ove informacije se odnose na operativni sistem, Ethernet interfejs, razne softvere povezane sa protokolima (TCP/IP, NetWare, SNMP, ...). Podsistemi menadžmenta konfiguracije pohranjuju ove informacije u bazu podataka. Ukoliko se desi neki problem, ova baza podataka se može pretražiti kako bi se našla rješenja za odgovarajući problem.

– **Menadžment obračuna (Accounting management)**
Cilj menadžmenta obračuna je mjerenje parametara mrežne iskoristivosti, tako da se pojedino ili grupno korištenje mrežnih resursa može na odgovarajući način odrediti. Ovakva regulacija smanjuje mrežne probleme (jer se mrežni resursi na osnovu kapaciteta resursa mogu ravnomjerno rasporediti) i povećavaju pravednost mrežnog pristupa među svim korisnicima.
Prvi korak u menadžmentu obračuna predstavlja mjerenje korištenja svih važnih mrežnih resursa. Analiza rezultata nudi uvid u trenutne uzorke korištenja, a norma korištenja se može postaviti u ovom trenutku. Naravno da se zahtijevaju neke korekcije kako bi se omogućili optimalni pristupi. Od ovog trenutka mjerenjem korištenja resursa moguće je dobiti informacije o naplati kao i informacije koje su potrebne za nastavak pravednog i optimalnog korištenja resursa.

– **Menadžment performanse (Performanse management)**
Cilj ovog menadžmenta je mjerenje i stavljanje na raspolaganje mnogih aspekata mrežne performanse tako da se performansa mreže može održavati na prihvatljivom nivou. Primjeri varijabli performanse uključuju mrežnu

propusnost, vremena odziva korisnika i iskoristivost linka.

Menadžment performanse uključuje tri glavna koraka. Prvi je prikupljanje podataka performanse, koji su od interesa za administratora. Drugi korak je analiza podataka kako bi se odredili normalni nivoi. I na kraju se utvrđuju odgovarajući pragovi performanse za svaku važnu varijablu, tako da prekoračenje ovih pragova ukazuje na mrežni problem na koji se treba obratiti pažnja.

Menadžment entiteti neprestano vrše monitoring varijabli performanse. Kada se dostigne prag performanse, onda se generira alarm i šalje u sistem mrežnog menadžmenta.

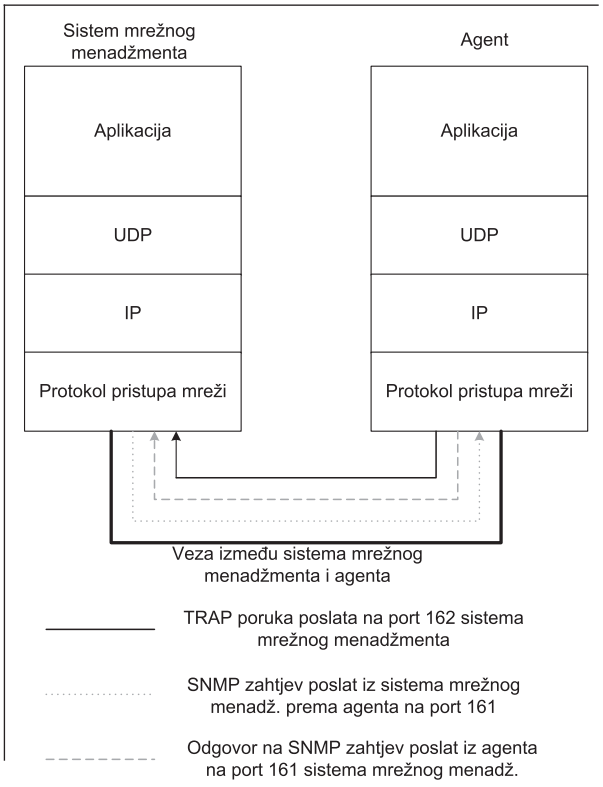
Svaki od prethodno opisanih koraka je dio procesa podešavanja reaktivnog sistema. Kada performansa postane neprihvatljiva, zbog prekoračenja korisnički-definiranog praga, sistem reagira slanjem poruke. Menadžment performanse odobrava, također, proaktivne metode: naprimjer, simulacija mreže se može koristiti kako bi se predvidjeli utjecaji proširenja mreže na performanse.

– **Menadžment sigurnosti (Security management)**

Kod ove vrste menadžmenta vrši se kontrola pristupa mrežnim resursima prema lokalnim smjernicama tako da se mreža ne može sabotirati (namjerno ili nenamjerno), a osjetljivim informacijama se ne može pristupiti bez odgovarajućeg odobrenja. Podsistem menadžmenta sigurnosti može nadgledati korisnike, koji se loguju na mrežne resurse i može odbiti pristup onim koji unesu neodgovarajuću pristupnu šifru.

Podsistemi menadžmenta sigurnosti rade podjelom mrežnih resursa u autorizirane i neautorizirane oblasti. Oni izvršavaju više funkcija, tj. identificiraju osjetljive mrežne resurse (uključujući sisteme, fajlove i druge entitete) i određuju mapiranje između osjetljivih mrežnih resursa i korisničkih skupova. Također, vrše monitoring pristupnih tačaka za osjetljive mrežne resurse i monitoring logova neodgovarajućeg pristupa osjetljivim mrežnim resursima.[1]

Prethodno opisani ISO model je poznat i pod imenom FCAPS model (Fault, Configuration, Accounting, Performanse, Security). Dobar menadžment sistem bi trebao ispuniti sve FCAPS oblasti. Važna činjenica je da su FCAPS oblasti međuovisne. Menadžment greške treba da zna o mrežnoj konfiguraciji kako bi ponudio zadovoljavajuće rezultate. Obračun također ima veze sa postojećom konfiguracijom. Omogućavanje kompletne menadžment funkcionalnosti je veliki izazov, naročito za velike distribuirane mreže koje sadrže mnogo različite opreme.[3]



Slika 2.
Prikaz TCP/IP komunikacionog modela i SNMP-a

4. PROTOKOLI MREŽNOG MENADŽMENTA

Zbog brzog rasta Interneta kasnih 1980-ih pojavila su se tri prijedloga, kako upravljati ekspanzijom Interneta i drugih povezanih mreža:

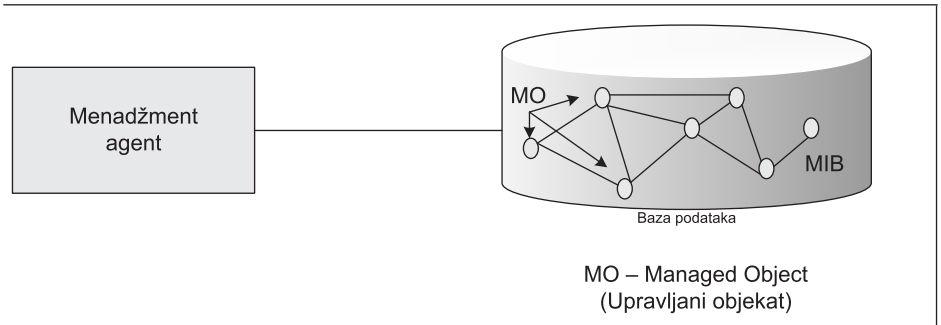
– Visoko-nivojski menadžment sistem (high-level entity management system – HEMS)
– Sistem baziran na OSI modelu, koristeći CMIS i CMIP
– Proširenja postojećeg jednostavnog monitoring protokola gejtveja (Simple Gateway Monitoring Protocol-a – SGMP)

Pristup internetskom menadžmentu sadrži dva koraka. Kratkotrajno rješenje predstavlja proširenja prema SGMP-u, koji je postao poznat kao jednostavni protokol mrežnog menadžmenta (Simple Network Management Protocol – SNMP). Dugotrajno rješenje je bazirano na CMIS/CMIP arhitekturi, a naziva se CMOT (CMIP nad TCP/IP). Međutim, ovo rješenje nije toliko prihvaćeno kao SNMP.

INDEKS POJMOVA I SKRAĆENICA

BGP (Border Gateway Protocol) – predstavlja ključni ruting protokol interneta

CGI (Common Gateway Interface)
– predstavlja standardni protokol za povezivanje eksterne aplikacije sa informacionim serverom, obično web-server



Slika 3.
Prikaz menadžment informacione baze i upravljanih objekata

4.2. Simple Network Management Protocol

Simple Network Management Protocol je kreiran 1988. godine kao kratkotrajno rješenje za upravljanje mrežnim elementima u naglo rastućem Internetu i ostalim mrežama. Međutim, on je ubrzo postao široko prihvaćen u mrežnim menadžment sistemima, kako bi se izvršio monitoring mrežnih uređaja i otkrili uslovi koji zahtijevaju pažnju administratora.

SNMP koristi UDP protokol kao transportni protokol za prebacivanje podataka između menadžera i agenata. UDP je izabran umjesto TCP protokola zbog njegove brzine, međutim, on je nepouzdan protokol, jer ne postoji potvrda izgubljenih paketa na nivou protokola. SNMP aplikacija je ta koja određuje da li su paketi izgubljeni i šalje ih ponovo, ukoliko je to potrebno. Ovo je izvršeno pomoću jednostavnog tajmera. Sistem za mrežni menadžment šalje UDP zahtjev agentu i čeka njegov odgovor. Vrijeme koje sistem za mrežni menadžment čeka, ovisi o tome kako je konfiguriran. Ukoliko vrijeme istekne, a sistem za mrežni menadžment ne dobije odgovor od agenta, on pretpostavi da je paket izgubljen i šalje zahtjev ponovo. Broj pokušaja ponovnog slanja paketa se, također, može konfigurirati.

SNMP koristi UDP port 161 za slanje i primanje zahtjeva, a port 162 se koristi za primanje zamki (trap) od upravljanih uređaja. Svaki uređaj koji implementira SNMP mora koristiti ove brojeve portova kao defaultne, dok neki proizvođači dozvoljavaju promjenu defaultnih portova u konfiguraciji agenta. Ukoliko se promijene defaultne postavke, sistem za mrežni menadžment mora biti svjestan promjena tako da može poslati upit na ispravni port.

Na sljedećoj Slici 2. je prikaz TCP/IP protokol stek, koji je osnova za sve TCP/IP komunikacije. [4]

Kada sistem za mrežni menadžment ili agent želi da izvrši SNMP funkciju (npr. zahtjev ili trap), naredni slijed događaja se odvija u protokol steku:

– Na aplikacionom sloju, SNMP aplikacija odlučuje šta treba da uradi. Naprimjer, ona može da pošalje SNMP zahtjev agentu, može da pošalje odgovor na SNMP zahtjev ili može da pošalje TRAP poruku sistemu za mrežni menadžment. Ovaj sloj nudi usluge krajnjem korisniku.
– Na transportnom sloju, UDP omogućava da dva hosta međusobno komuniciraju. UDP zaglavlje sadrži odredišni port uređaja kojem se šalje zahtjev ili TRAP poruka. Odredišni port je 161 (za upit) ili 162 (za TRAP).
– Na mrežnom sloju, IP pokušava da isporuči SNMP paket na njegovo odredište, što je određeno IP adresom.
– Posljednji korak, koji se mora desiti kako bi SNMP paket dostigao svoje odredište, jeste slanje paketa na fizičku mrežu odakle se on rutira do krajnjeg odredišta. MAC sloj sadrži drajvere uređaja koji prebacuju podatke na fizički dio žice, kao što je mrežna kartica. Ovaj sloj, također, prima pakete iz fizičke mreže i šalje ih prema višim slojevima u protokol steku, kako bi se oni mogli obraditi u aplikacionom sloju (u ovom slučaju SNMP).[4]

4.3. SNMP verzije

SNMPv1

Prvobitni SNMP protokol je danas poznat pod nazivom SNMPv1. Glavna karakteristika ovog protokola je njegova jednostavnost implementacije za agente na upravljanim uređajima, koji imaju ograničeno procesiranje i ograničene memorijske resurse. Međutim, za menadžment aplikaciju ova jednostavnost nije nužno od prednosti. Osim toga, sigurnost nije jača strana ove prve verzije. Autentikacija klijenata izvršava se pomoću community stringa, odnosno lozinka se prenosi kao „čisti“ tekst.

SNMPv1 koristi pet osnovnih podatkovnih jedinica protokola (protocol data unit - PDU), koje su već spomenute ranije: GET REQUEST, GET-NEXT REQUEST, GET RESPONSE, SET REQUEST i TRAP.

SNMPv2

Kada je SNMPv1 dobio široku podršku, ispostavilo se tokom vremena da su određeni aspekti u vezi s njim previše jednostavni. SNMPv1 nije u stanju prihvatiti veliku količinu menadžment informacija. Sigurnost mu je na minimalnom nivou, čineći ga time podobnim i ranjivim za napade. Zbog ovih razloga uvedena je SNMPv2. Najvažniji aspekt SNMPv2 je uvođenje dviju novih menadžment operacija, pored onih iz SNMPv1: GET-BULK REQUEST i INFORM.

GET_BULK operacija omogućava menadžeru da primi veliku količinu menadžemnt informacija sa jednim zahtjevom. Ona radi na sličan način kao i GET-NEXT zahtjev. Međutim, sa GET-BULK zahtjevom menažder nudi dodatan parametar, a to je parametar za maksimalni broj ponavljanja. Ovaj parametar određuje koliko nasljednika bi se trebalo vratiti za dati OID.

INFORM operacija se svodi na obavještenje koje primalac treba da potvrdi. Dok TRAP operacija dozvoljava slanje nepouzdanih obavještenja, INFORM zahtjev nudi mehanizam koji dozvoljava SNMP agentu da šalje pouzdane događaje. Potvrđivanje se obavlja kroz isti PDU, koji se šalje kao odgovor na bilo koji drugi zahtjev.

Implementacija informacija o potvrdi uljučuje mnogo više kompleksnosti nego ona bez potvrda. Razlog ovome je činjenica da je agentu sada potrebno da pamti poruke o obavještenjima koja se emitiraju i da odluči šta uraditi u slučaju da ne primi potvrdu. Prema tome, INFORM zahtjev nije namijenjen za korištenje između agenata baziranih na uređaju i menadžment aplikacija, nego za komunikaciju između menadžment aplikacija, gdje jedna aplikacija privremeno igra ulogu jednog agenta.

SNMPv2 donosi, osim ovih dviju operacija, još prednosti u odnosu na SNMPv1. On redefinira PDU formate tako da se ista PDU struktura može koristiti za bilo koju SNMP operaciju, uključujući zahtjeve i odgovore. Ovo olakšava obrađivanje SNMP poruka.

Postoje varijacija SNMPv2 protokola, koja ima oznaku SNMPv2c. Ova verzija je bazirana na community stringovima, u svrhu praktične upotrebe.

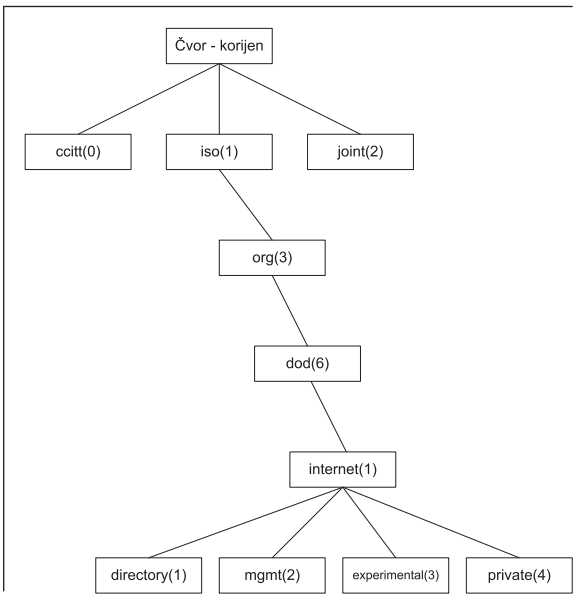
SNMPv3

SNMPv3 je najnovija verzija SNMP protokola. Ova verzija je, zapravo, SNMPv2c zajedno sa sigurnošću. Ona zadržava iste menadžment operacije kao SNMPv2c, ali uvodi dodatke u SNMP poruke za prenošenje pogodnih sigurnosnih parametara koji na kraju čine SNMP sigurnim protokolom. Na ovaj način je omogućena enkripcija menadžment poruka i bolja autentikacija pošiljaoca. Ovako je SNMPv3 manje podložan napadima.

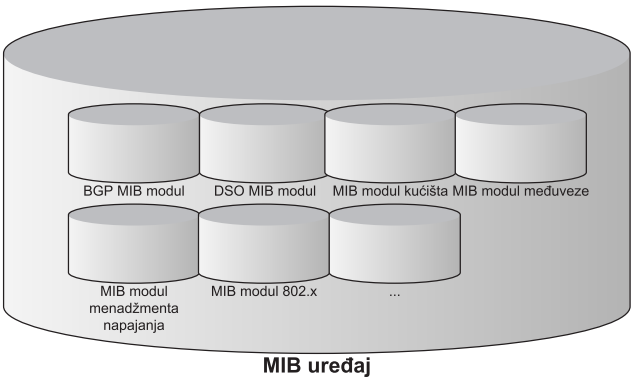
SNMPv3 je postao mnogo moćniji kao i kompleksniji od originalne SNMP specifikacije. Ova verzija je značajno povećala sposobnosti procesiranja agenta i dostupnost moćnijih alata za implementaciju.[2]

SNMP community

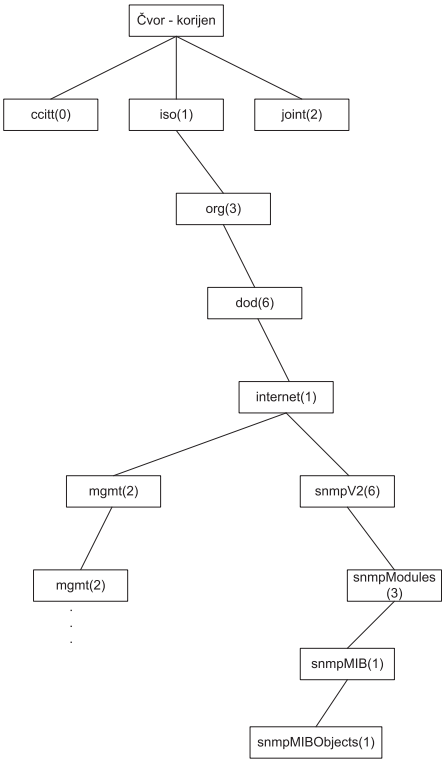
SNMPv1 i SNMPv2 koriste pojam community kako bi uspostavili povjerenje između menadžera i agenata. Agent je konfiguriran sa tri community naziva: *read-only, read-write i trap*. Ova imena su u biti lozinke i ne postoji stvarna razlika između community stringa i lozinke, koja se koristi za pristup korisničkom računu na računaru. Ova tri community stringa kontroliraju različite vrste aktivnosti. Community string „read-only“ dozvoljava čitanje vrijednosti podataka, ali nije omogućena njihova izmjena. Naprimjer, sa ovom vrstom community stringa moguće je samo čitati broj paketa, koji se prenose kroz portove na ruteru, ali nije moguće resetovati brojače. Community string „read-write“ dozvoljava čitanje i izmjenu vrijednosti podataka. Na ovaj način je omogućeno čitati brojače, rese-



Slika 4.
Prikaz stabla identifikatora objekta



Slika 5.
Prikaz jednog MIB-a sa više MIB modula



Slika 6.
Prikaz SMIv2 registracionog stabla za SNMPv2

tovati njihove vrijednosti i čak resetovati interfejse ili napraviti druge promjene koje mijenjaju konfiguraciju rutera. Community string „trap“ dozvoljava prijem TRAP poruka od agenata.

Većina opreme dolazi sa defaultnim postavkama community stringova: *public* za read-only community string i *private* za read-write community string. Kada se podešava SNMP agent, potrebno je konfigurirati njegovo odredište za TRAP poruke. Osim toga, pošto se SNMP community stringovi šalju u izvornom tekstu, može se konfigurirati jedan agent za slanje TRAP poruke o SNMP grešci pri autentikaciji, kada neko pokuša da pretraži uređaj sa pogrešnim community stringom. Ove poruke mogu biti veoma korisne pri otkrivanju potencijalnog napadača, koji pokušava da pristupi mreži.

Postoje načini smanjenja rizika mogućeg napada. Firewall-i i filteri smanjuju šansu da neki napadač putem SNMP-a može nanijeti štetu nekom od uređaja na mreži. Firewall se može konfigurirati da dozvoli da UDP saobraćaj dolazi samo iz poznate liste hostova. Naprimjer, može se dozvoliti da UDP saobraćaj na portu 161 ulazi u mrežu samo ako dolazi iz sistema za mrežni menadžment. Međutim, važno je, također, i napomenuti da ukoliko neko ima read-write pristup nekom SNMP uređaju, on može preuzeti kontrolu nad tim uređajem koristeći SNMP. Ovo može biti vrlo štetno za mrežu, jer je ovim postupkom moguće promijeniti postavke interfejsa rutera, pa čak i tabele rutiranja. Načini zaštite community stringova su korištenje virtuelne privatne mreže ili česta promjena community stringova.[4]

4.4. Menadžment informaciona baza (MIB)

Menadžment agent održava menadžment informaciju uređaja u menadžment informacionoj bazi upravljanog uređaja (Management Information Base - MIB). Menadžment informaciona baza može se posmatrati kao konceptualno skladište podataka. Menadžeri dobivaju menadžment infomacije iz MIB-a, preusmjeravanjem odgovarajućih zahtjeva menadžment agentu, npr. koristeći „get“ operaciju.

Menadžment informaciona baza nije isto kao i baza podataka. MIB ne sadrži informacije o trenutnim upravljanim uređajima u datotečnom sistemu. Umjesto toga, ona je „povezana“ sa realnim svijetom i jednostavno nudi apstrakciju upravljanog uređaja koji se koristi u svrhe upravljanja.

Kada menadžer primi dio informacije iz MIB-a, to predstavlja jedan aspekt uređaja. Kada menadžer manipulira informacijom iz MIB-a, trenutne postavke uređaja se mijenjaju i tako utječu na način kako se uređaj ponaša u stvarnom svijetu. MIB-ovi su jedan od centralnih koncepata u mrežnom menadžmentu i njihova važnost se ne može nadjačati.

MIB-ovi sadrže mnogo individualnih dijelova menadžment informacije o upravljanom entitetu. Ove informacije se odnose na fizičke aspekte kao što su portovi, kao i na logičke aspekte kao što su protokol mašine, softver i osobine pojedinih komunikacionih usluga. Dijelovi menadžment informacije u MIB-u se obično odnose na upravljane objekte (managed objects), koji predstavljaju apstrakcije pojedinih aspekata upravljanog uređaja. Upravljani objekti se ne razlažu dalje u menadžment svrhe nego se tretiraju kao informacioni entitet. Zapravo, ovi aspekti se mogu razmatrati kao predmet menadžment konzervacije između menadžera i agenata. U ovu svrhu se mogu navesti sljedeći primjeri:

- Prijem statističkih informacija o portu, koji se koristi za spajanje opreme na mrežu;
- Kreiranje pravila za kontrolu pristupa, koje firewallu nalaže koje pakete da filtrira;

– Konfiguriranje konekcione krajnje tačke jedne ATM konekcije.

Svaki od ovih aspekata može se predstaviti vlastitim upravljanim objektom.

Na Slici 3. dat je opis MIB-a, koji je povezan s menadžment agentom i koji sadrži nekoliko upravljanih objekata. Upravljani objekti u MIB-u se često prikazuju poredani u konceptualnim strukturama stabla. Razlog ovome je taj, da upravljani objekti imaju međusobne hijerarhijske relacije. Naprimjer, jedan upravljani objekat koji predstavlja komunikacioni interfejs može sadržati drugi upravljani objekat koji predstavlja podinterfejse istog interfejsa.[2]

4.4.1. Struktura menadžment informacije

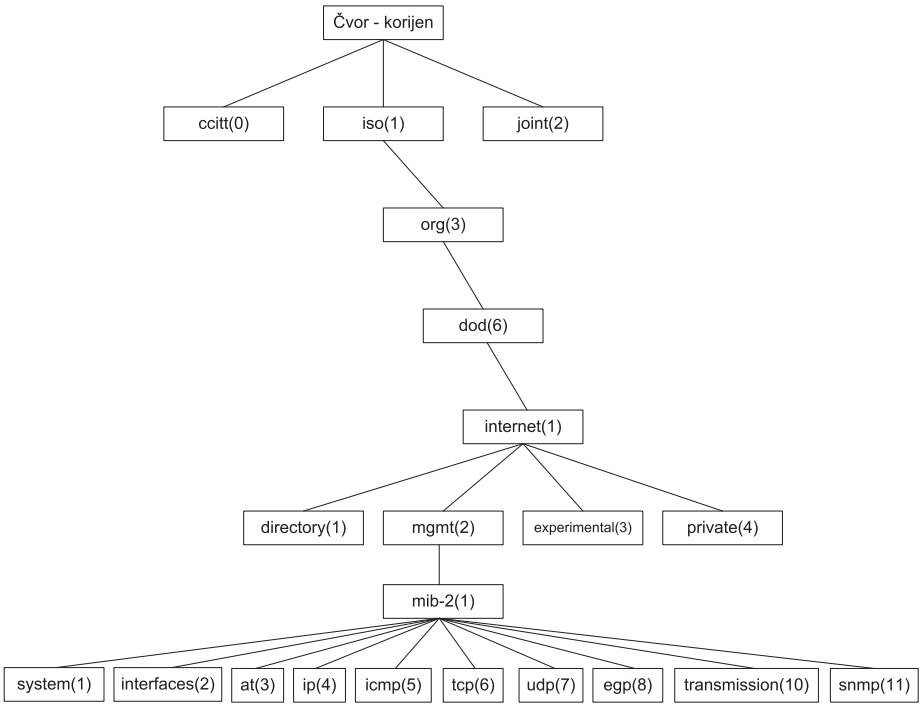
Struktura menadžment informacije (Structure of Management Information – SMI) precizno definira kako se imenuju upravljani objekti i kako se određuju pridruženi tipovi podataka.

Upravljani objekat, koji se može posmatrati kao jedan dio menadžment informacije, sadrži tri atributa:

– **Ime**, ili identifikator objekta (object identifier – OID) jedinstveno definira upravljani objekat. Imena se obično pojavljuju u dva oblika: numerički i oblik razumljiv za čovjeka.
– **Tip i sintaksa**, je definiran koristeći podskup notacije Abstract Syntax Notation One (ASN.1). ASN.1 predstavlja način kako je podatak predstavljen i kako se on prenosi između menadžera i agenata, unutar konteksta SNMP-a. Dobra osobina ASN.1 je da je notacija neovisna o mašini. Ovo znači da računar sa instaliranim Windowsom XP može komunicirati sa Sun Sparc mašinom bez brige o redoslijedu bytea (BIG ENDIAN ili LITTLE ENDIAN).
– **Kodiranje**, jedna instanca upravljanog objekta se kodira u string okteta, koristeći Basic Encoding Rules (BER).

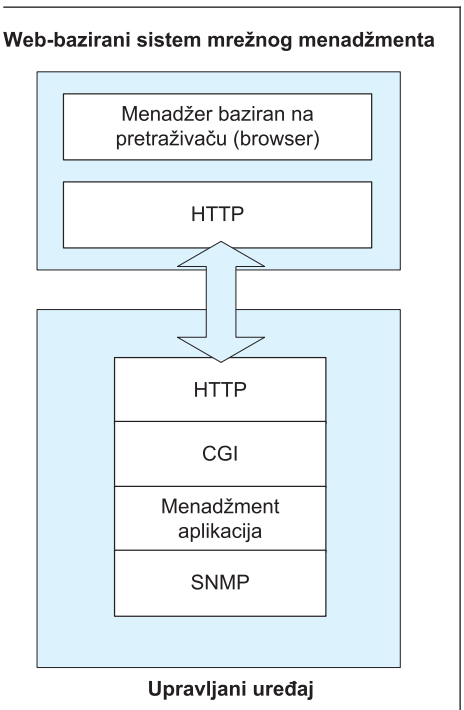
Imenovanje identifikatora objekata

Upravljani objekti su organizirani u hijerarhiji, koja ima oblik stabla. Ova struktura je osnova za SNMP shemu nomenklature. Jedan identifikator objekta je sačinjen od serije integera baziranih na čvorovima u stablu, odvojeni tačkama (.). Prikaz imena u obliku razumljivom čovjeku nije ništa drugo nego niz imena odvojenih tačkama, od kojih svaki predstavlja čvor stabla. Slika 4. prikazuje pojednostavljeno stablo identifikatora objekta.



Slika 7.
Prikaz MIB-II podstabla

Čvor na vrhu stabla se naziva *korijen*, čvor sa djecom se zove *podstablo*, dok čvorovi bez djece se tretiraju kao *listovi*. Naprimjer, na Slici 4. početni čvor se naziva *Korijen-čvor*. Njegovo podstablo čine ccitt(0), iso(1) i joint(2). U ovom slučaju iso(1) je jedini čvor koji sadrži podstablo, ostala dva čvora su listovi; ccitt(0) i joint(2) ne odnose se na SNMP. Podstablo koje uključuje čvorove iso(1). org(3).dod(6).internet(1) se predstavlja u obliku identifikatora objekta (object idebtifier - OID) kao 1.3.6.1 ili kao iso.org. dod.internet. Svaki upravljani objekat ima numerički OID i pridruženi tekstualni naziv. Notacija sa decimalnim tačkama prikazuje kako se upravljani objekat predstavlja unutar jednog agenta. Grana



Slika 8.
Shematski prikaz elemenata web-baziranog sistema mrežnog menadžmenta

LITERATURA

[1] *Internetworking Technologies Handbook*, Cisco Systems, 2000

[2] Network Management Fundamentals, Alexander Clemm, Cisco Systems, 2007

[3] *Network Management, MIBs and MPLS: Principles, Design and Implementation*, Stephen B. Morris, Addison Wesley, 2003

[4] *Essential SNMP*, O'Reilly Media, Douglas R. Mauro and Kevin J. Schmidt, 2005

[5] *Managing Internetworks with SNMP*, IDG Books Worldwide, Mark A. Miller

[6] *Netzwerk- und IT-Sicherheitsmanagement – Eine Einführung*, Universitätsverlag Karsruhe, Jochen Dinger und Hannes Hartenstein, 2008

mgmt definira standardni skup objekata za internetski menadžment. Grana *experimenatal* je rezervirana u svrhe testiranja i istraživanja. Grana *private* je namijenjena da pojedinci i organizacije mogu definirati vlastite objekte. Institucija koja vodi računa o dodijeli brojeva je Internet Assigned Numbers Authority (IANA). Naprimjer, IBM ima broj 2, tako da je bazni OID za njegov privatni prostor definiran kao iso.org.dod.internet.private.enterprises.ibm ili 1.3.6.1.4.1.2.[4]

U strukturi menadžment informacije MIB definicije se određuju kao *MIB moduli*. MIB modul obično služi određenoj svrsi, kao što je definiranje menadžment informacije, koja se odnosi na komunikacione interfejse uređaja. Prema tome, MIB određenog uređaja kreira instance više MIB modula, od kojih svaki predstavlja jedan aspekt upravljanog uređaja. Slika 5. prikazuje ovaj slučaj.

U suštini se jedan SNMP MIB sastoji od skupa upravljanih objekata koji kreiraju instance tipova objekata koji su dio MIB modula. Ovi upravljani objekti nisu objekti u smislu objektno-orijentiran, nego se trebaju posmatrati kao *MIB varijable*.

U jednom MIB modulu definirano je više vrsta informacija:

- **Tipovi objekta**, instance koje sadrže trenutne menadžment informacije – MIB varijable.
- **Obavještenja** koja definiraju informacije koje se mogu prenijeti menadžerima kao dio poruka o događajima, odnosno dobro poznate kao TRAP poruke u SNMP-u.
- **Čvorovi** koji su uvedeni za svrhe grupiranja. Naprimjer, MIB modul za protokol Border Gateway Protocol (BGP) može sadržiti čvor „BGP statistike", pod kojim su grupirani tipovi objekta koji predstavljaju različite vrste statistika o BGP-u.

Što se tiče tipova objekta, dvije kategorije se trebaju razmatrati:

- Tipovi objekta, čija se instanca kreira samo jednom u agentu. Ovo znači da će uvijek postojati tačno jedna instanca tipa objekta u MIB-u, koja se naziva i *skalar*. Primjer ovakvog tipa objekta je serijski broj kućišta.
- Tipovi objekta, čija se instanca kreira više puta. Ovo znači da više objekata istog tipa objekta mogu postojati u MIB-u. Oni se također nazivaju i *objekti kolone*, jer se oni smatraju kao kolona u tabeli koja ima više redova, po jedan za svaku instancu. Primjer ovakvog tipa objekta je onaj koji predstavlja informacije na karticama u kućištu.

Neovisno o kojem tipu objekta se radi, svaki upravljani objekat je jednostavnog tipa podatka, koji je dio SMI i SMIv2 specifikacije jezika. Jednostavni tipovi podataka uključuju stringove i brojeve kao što su integeri, brojači i mjerila. Brojači se koriste za brojanje nečeg, kao što je broj primljenih paketa. Mjerila se koriste, npr., za indikaciju trenutnog korištenja propusnosti. Za razliku od brojača, čija se vrijednost samo povećava, vrijednost mjerila se može smanjivati i povećavati. [2]

4.4.2. Struktura menadžment informacije verzija 2

Struktura menadžment informacije verzija 2 (SMIv2) proširuje SMI stablo objekta, dodavajući internet podstablu SNMPv2-granu, dodavajući nekoliko novih tipova podataka i uvođenjem još nekih promjena. Slika 6. prikazuje SMIv2 stablo objekta za SNMPv2. OID za ovu novu granu je 1.3.6.1.6.3.1.1 ili iso.org.dod.internet.snmpv2.snmpModules.snmpMIB.snmpMIBObjects. [4]

4.5. Menadžment informaciona baza II (MIB-II)

MIB-II predstavlja važnu menadžment grupu, jer svaki uređaj koji podržava SNMP mora, također, podržavati i MIB-II. MIB-II je definiran kao novi čvor, odnosno dijete čvora *mgmt* unutar stabla identifikatora objekta za Internet. On je definiran kao iso.org.dod.internet.mgmt.1 ili kao 1.3.6.1.2.1. Slika 7. prikazuje MIB-II podstablo grane *mgmt*.

Unutar MIB-II podstabla definirano je deset menadžment grupa. Grupa *system* definira listu objekata, koja se odnosi na sistemsku operaciju, kao što je sistemsko ime i sistemsko vrijeme.

Grupa *Interfaces* vodi evidenciju o statusu svakog interfejsa na upravljanom enetitetu. Ova grupa vrši monitoring interfejsa, kako bi utvrdila koji su interfejsi upaljeni i ugašeni, i evidentira stvari kao što su poslani i primljeni okteti, greške itd. Grupa *at*, koja predstavlja prevođenje adresa, koristi se samo u slučaju kompatibilnosti unatrag. *IP* grupa vodi evidenciju o mnogim aspektima IP-a. *ICMP* evidentira ICMP greške, odbacivanja itd. *TCP* vodi evidenciju o stanju TCP konekcije. *UDP* se koristi za evidentiranje UDP statistika, primljenih i poslanih datagrama itd. Grupa *egp* čuva razne statistike o protokolu Exterior Gateway Protocol. Grupa *snmp* mjeri performansu SNMP implementacije na upravljanom entitetu i evidentira broj poslanih i primljenih SNMP paketa. Jedina grupa koja još nema definirane objekte je grupa *transmission*.[4]

5. SISTEMI MREŽNOG MENADŽMENTA

5.1. Web-bazirani mrežni menadžment

Web-bazirani menadžment koristi HyperText Tranfer Protocol (HTTP) i Common Gateway Interface (CGI) za upravljanje mrežnim entitetima. On radi umetanjem web-servera u SNMP-kompatibilni uređaj, zajedno sa CGI-jem kako bi konvertovao zahtjeve slične SNMP-u (iz web-baziranog sistema mrežnog menadžmenta) u stvarne SNMP operacije, i obrnuto. Web-serveri se mogu ugraditi u ovakve uređaje uz vrlo male operativne troškove.

Slika 8. prikazuje pojednostavljen dijagram interakcije između web-baziranog sistema mrežnog menadžmenta i upravljanog uređaja. CGI aplikacija premoštava procjep između menadžment aplikacije i SNMP pogona. U nekim slučajevima menadžment aplikacija može biti kolekcija Java apleta koji se izvršavaju na web-baziranom menadžeru.

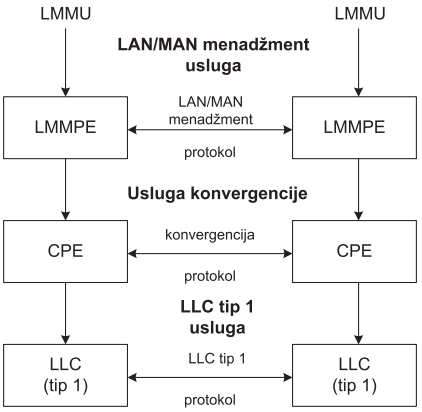
5.2. IEEE mrežna menadžment arhitektura

Ova arhitektura sadrži tri elementa: LAN/MAN menadžment servis (LAN/MAN Management Service – LMMS), LAN/MAN entitet menadžment protokola (LAN/MAN Management Protocol Entity – LMMPE) i entitet konvergencije protokola (Convergence Protocol entity – CPE).

LAN/MAN menadžment servis definira servis koji je dostupan LAN/MAN menadžment korisniku (LAN/MAN Management User – LMMU).

LAN/MAN entitet menadžment protokola prenosi menadžment informaciju putem razmjene protokola. LMMS i LMMPE koriste ISO CMIS i CMIP standarde i omogućuju da dva LMMU razmijene menadžment informacije.

Entitet konvergencije protokola omogućava LAN/MAN menadžment servis preko LAN/MAN okruženja. On dodaje funkcije pouzdanosti i sekvencijalne isporuke podataka nepotvrđenom, nekonekcionom servisu, koji je omogućen preko IEEE 802.1 LLC slojem (Logical Link Control). Ovaj servis je poznat i kao LLC tip 1. Slika 9. prikazuje tri elementa IEEE arhitekture. [5]



Slika 9.
LAN/MAN menadžment komunikaciona arhitektura

6. ZAKLJUČAK

Kompleksnost mreže raste iz dana u dan, što mrežni menadžment stavlja uvijek pred nove izazove. Pojavljivanje raznih zahtjevnih aplikacija (npr. video streaming) dodatno povećava opterećenost mreže i otežava posao mrežnom menadžmentu. Također se mijenjaju i uslovi pod kojima se dešava mrežni menadžment. Ranije je dizajn SNMP-a bio usmjeren na uštedu resursa na strani agenta, međutim, danas to više nije slučaj, jer mrežne komponente posjeduju moćniji hardver i zanemaruje se ovaj problem. Međutim, SNMP je zbog svoje sigurnosne problematike i jednostavnosti ograničen i nepodoban za konfiguriranje parametara mrežnih uređaja. U ove svrhe se uvodi NetConf protokol koji implementira sve ono što SNMP protokolu fali za konfiguriranje.[6]

Budući razvoj mrežnog menadžmenta ne uključuje samo razvoj i promjenu SNMP protokola, nego se razvija također i struktura menadžment informacije. Sve se više teži ka web-baziranom menadžmentu i distribuiranom mrežnom menadžmentu.

UPUTSTVA AUTORIMA

Pored neophodnog kvaliteta i zahtjeva za redovitim izlaženjem, podizanje stručne i tehničke razine časopisa glavna je zadaća svakog izdavača. U skladu sa tim nakanama, te zbog različitosti oblika i formi u kojima su nam do sada pristizali radovi za publikovanje, molimo buduće saradnike i autore priloga da se pridržavaju sljedećih uputstava.

U *Telekomunikacijama* se objavljuju izvorni – još neobjavljeni – naučni i stručni prilozi telekomunikacijskog i informatičkog sadržaja te kraća saopštenja o novostima (stručni susreti, literatura, događaji značajni za struku). Objavljivanjem rukopisa autor svoja autorska prava, u skladu sa Zakonom o autorskim pravima, prenosi na izdavača.

1. Konačna verzija priloga šalje se na adresu Uredništva na CD–u ili e–mailom na adresu uredništva, na kojoj je naznačeno ime autora i datoteke. Grafički prilozi trebaju biti u posebnim datotekama. Zajedno sa CD–om, autor treba poslati i jedan primjerak ispisa na papiru. U slučaju eventualnih razlika, poštovaće se prilog na CD–u.
2. Rukopis mora biti pisan sa proredom (1,5), slovima veličine 12, sa marginama 2,5 cm i tipom slova *Times New Roman*. O konačnom izgledu priloga odlučuje urednički odbor. Naučni i stručni radovi trebaju biti u obimu od oko 4000 riječi (20000 znakova ili do 12 kartica teksta), a saopštenja ne više od 1000 riječi.
3. Naučni i stručni prilog mora imati **rezime** na jezicima naroda BiH (obima do 1000 znakova) i abstract. Rezime mora sadržavati osnovne postavke (nikako samo zaključak ili zgusnuti sadržaj priloga). Na kraju treba dodati ključne riječi (ne više od njih 10). **Abstract** je engleski prijevod rezimea i mora ga obezbijediti autor.
4. **Ilustracije** moraju biti kvalitetne (fotografije dovoljno kontrastne, a crteži i grafikoni jasno odštampani na papiru). Slike i tabele trebaju biti označene arapskim brojevima identično i u prilogu, i pod ilustracijama (npr. "Sl.: ..." odnosno "Fig.: ..." ili "Tabela 1: ..."). Računarske slike moraju se dati na CD–u kao posebne datoteke sa naznakom u kom su programu rađene. Bitmapirane slike moraju biti u formatu tif ili jpg i imati rezoluciju 300–350 dpi (ako su slike u mjerilu 1:1).
5. **Bibliografija** mora biti na kraju priloga i uređena po abecednom redu (počevši od "a"), a ako isti autor ima više radova, onda i po godinama izdanja (od starijih godišta ka mlađim). Autorima se preporučuje da izbjegavaju bilješke pod crtom (fusnote).
   Primjeri pisanja bibliografskih jedinica:
   – za **članak jednog autora**:
   Karić, A., 1992: Razvoj GIS-a u BiH.– PTT novine, XII, 7, 23–35, Sarajevo
   – za **članak više autora:**
   Perić, N. & Bašić, K., 1976: Zamjena koračnih centrala u pošti Sarajevo.– Glasnik inžinjera i tehničara, 12, 44–52, Beograd
   – za **knjigu** (monografiju):
   Laković, J., 1998: *Leksikon GSM-a*.– Svjetlost, str. 232, Sarajevo
6. **Citiranje** u tekstu je obavezno, pri čemu je potrebno navesti samo autora i godinu izdanja citiranog djela: (Karić 1992), a ako je potrebno i stranu: (Karić 1992, 24) ili (Karić 1992, 24–26). Ako je citirano više autora odjednom, treba ih navesti zajedno u zagradi: (Karić 1992, 24; Perić & Bašić 1976).
7. Autori priloga moraju imati dozvolu za objavljivanje sadržaja koji su zaštićeni sa "**copyright**" i ta dozvola mora biti navedena u prilogu.
8. BH TEL ima "**copyright**" za priloge objavljene u *Telekomunikacijama*.

U slučaju nejasnoća ili dvojbi urednik i članovi Redakcije će se sa zadovoljstvom osobno posavjetovati sa autorima.

Urednik