Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00521/2010
Datum: 05.04.2010

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **NIKOLA MILOJEVIĆ**

Naslov: **ZAGOTAVLJANJE VISOKE RAZPOLOŽLJIVOSTI SISTEMOV VOIP**
ENSURING HIGH AVAILABILITY OF VOIP SYSTEMS

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

Tematika naloge:

V nalogi podajte pregled načrtovalskih in izvedbenih korakov, ki so potrebni za zagotavljanje visoke razpoložljivosti računalniških sistemov. Praktične rešitve prikažite na sistemu Cirpak za storitve VoIP.

Mentor:
pred. mag. Igor Škraba

Dekan:
prof. dr. Franc Solina

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Nikola Milojević

Zagotavljanje visoke razpoložljivosti sistemov VoIP

DIPLOMSKO DELO VISOKOŠOLSKEGA STROKOVNEGA ŠTUDIJA

Mentor:
pred.mag. Igor Škraba

Ljubljana, 2010

I Z J A V A O A V T O R S T V U

diplomskega dela

Spodaj podpisani Nikola Milojević,

z vpisno številko 24950383,

sem avtor diplomskega dela z naslovom:

Zagotavljanje visoke razpoložljivosti sistemov VoIP

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom prof.mag. Igor Škraba
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

Ljubljana, junij 2010 Podpis avtorja

Zahvala

Zahvaljujem se vsem, ki so imeli neomajno zaupanje v mene, ter ves ta čas gojili pravo mešanico humorja in vzpodbude glede mojega študija. Omeniti velja tudi Telekom Slovenije in našo kadrovsko službo, ki sta mi trdno stala ob strani v ciljni ravnini.

Seznam uporabljnih kratic in simbolov

bandwith	pasovna širina
BCT	Blade Center – ohišje strežniških rezin
Best Effort	izvedba po najboljših močeh (brez zagotovila kakovosti)
CPE	Customer Premises Equipment – oprema, ki se nahaja pri uporabniku
DB	Database − podatkovna baza
delay	zamuda, zamik
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DPI	Deep Packet Inspection
E.164	mednarodni standard telefonske numeracije
firmware	programska oprema, ki krmili delovanje naprave
FQDN	Fully Qualified Domain Name – popoln domenski naslov
GW	Gateway − prehod (v telefonskem svetu navadno medijski)
HA	High Availability − visoka razpoložljivost
IBM	International Business Machines
IP	Internet Protocol
jitter	tresenje, odmika (neenakomernost) zamude, zamika
LB	Load Balancer − izravnalnik prometa
MGC	Media Gateway Controller − nadzorna enota programskega stikala
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
OSI	Open System Interconnection
P-CSCF	Proxy − Call Session Control Function − posredniški strežnik
peer	klicni zbirnik, logični ekvivalent, "trunk group"
provisioning	funkcija upravljanja z naročniškimi podatki (vpis v baze in naprave)
proxy	posredniški strežnik
RTP	Real-Time Transport Protocol
RTPF	Real-Time Transport Protocol Forwarder − posredovalnik prometa RTP
SBC	Session Border Controler
Single Point Of Failure	posamezna (ena) točka, katere prekinitev povzroči izpad sistema
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SSW	softswitch − Programsko stikalo
TDM	Time Division Multiplexing
WLL AP	Wireless Access Point − brezžična dostopovna točka
VoIP	Voice Over IP
watchdog	nadzorna funkcija, ki preverja delovanje aplikacije

Povzetek

Redki so med nami, ki tekom normalnega delovnega dne ne opravijo vsaj enega telefonskega klica. Črnogledim napovedim navkljub, klasična telefonija še ni (in tudi ni videti, da kmalu bo) izumrla. Trenutno je v obdobju intenzivne tehnološke preobrazbe, saj se spreminja iz prenosnega sistema v storitev. Ključni element te preobrazbe je programsko stikalo (softswitch oz. SSW), ki nadomešča telefonsko centralo.

Namen moje diplomske naloge je celosten pregled načrtovalskih in izvedbenih korakov, katerih cilj je zagotoviti visoko razpoložljivost storitve VoIP, kot jo dojema uporabnik. Pri tem sem se močno oprl na sistem Cirpack, ki v skupini Telekom Slovenije služi kot programsko stikalo VoIP za rezidenčno telefonijo.

Osrednji del naloge je utemeljen na praktičnih izkušnjah, ki smo jih pridobili tekom petih let (uspešnega) delovanja. Predstavljene tehnične rešitve, ki so večinoma uporabljene tudi v praksi, so plod intenzivnega sodelovanja različnih oddelkov v podjetju.

Ključne besede:

telefonija, zanesljivost, razpoložljivost, VoIP, softswitch, Cirpack

Abstract

There are not many amongst us, who do not use telephone on a daily basis. Despite some pretty pessimistic forecasts, wireline telephony does not seem to be dying away. It rather seems it is undergoing a thorough technological transformation, migrating from bearer to service. The key element of this process is softswitch (SSW), a device, aiming to supersede classical telephony switch.

This thesis is intended to be a comprehensive overview of planning and implementation steps, aimed at ensuring a high degree of VoIP service reliability. Most information here is derived from Cirpack telephony platform, which is used as main residential softswitch in Telekom Slovenia network.

The main part of thesis is based on hands-on experience, obtained during five years of uptime. Most of presented technical solutions are in fact used in production environment as well. The developed know-how is a result of intense department cooperation.

Keywords:

telephony, reliability, availability, VoIP, softswitch, Cirpack

Uvod

Pojem visoka razpoložljivost je pogosto zelo različno interpretiran – odvisno predvsem od tega, kdo ga uporabi in kaj želi z njem doseči. Prodajalec opreme (ponavadi sistemski integrator ali kar proizvajalec) zagotavlja t. i. »pet devetk« (99,999 %), ponudnik storitve (v telekomunikacijah navadno operater) se poskuša od ostalih ponudnikov razlikovati z višjo razpoložljivostjo storitve (še posebno za poslovne stranke), medtem ko stranke to kategorijo doživljajo povsem po svoje (pogosto kot delovanje storitve oz. »end-to-end« rešitve). Čeprav to na prvi pogled deluje (vsaj) rahlo nelogično, pa obstaja smiselna razlaga. Navedeni udeleženci telekomunikacijske verige namreč v svojih izračunih oz. opisih razpoložljivosti upoštevajo različno kompleksne sisteme oz. različen nabor naprav/storitev.

Za prodajalca je relevantna izključno samo dotična naprava v najožjem pomenu besede. Okoljski, napajalni in omrežni parametri se razumejo kot predpogoji, ki morajo biti izpolnjeni, da bi proizvajalec sploh pričel meriti oz. ocenjevati zanesljivost delovanja naprave same.

Ker je povsem očitno, da se v realnosti ne da na tak način ocenjevati razpoložljivosti sistemov, telekomunikacijski operaterji v svojih pogodbah o zagotavljanju storitev (SLA – Service Level Agreement) navajajo bistveno manjše vrednosti oz. celo »Best Effort« (kar v prevodu pomeni: »Se bomo potrudili, ne pa tudi zavezali.«). Navadno je zavezujoči SLA namenjen poslovnemu segmentu, ki take zaveze potrebuje, hkrati pa tudi cenovno prenese.

Namen diplomske naloge je kratka predstavitev sistema VoIP in pregled vseh komponent, ki lahko kritično vplivajo na delovanje storitve oz. sistema kot celote. Pri tem se bomo določenih tem sicer zgolj bežno dotaknili, pa vendar verjamem, da bomo vsaj omenili vse točke sistema, ki bi lahko predstavljale t. i. »Single Point of Failure«. Poudarek bo predvsem na programski in arhitekturni redundanci ter njunih omejitvah, saj se pokaže, da je zagotavljanje visoke razpoložljivosti sistema kot celote precej bolj zahtevno kot zagotavljanje razpoložljivosti posameznih komponent istega sistema. Odpornost na napake namreč ni zgolj lastnost posameznih strežnikov, temveč način, kako (so)delujejo kot celota.

»Fail Safe« ne pomeni, da sistem ne more odpovedati – pač pa da bo odpovedal na predviden in kar se da varen način!

1. Sistem Cirpack

V nadaljevanju diplomskega dela se bomo osredotočili na sistem VoIP proizvajalca Tehnicolor s komercialnim nazivom »Cirpack«, zato je prav, da sistem predhodno okvirno spoznamo.

Cirpack sistem je ekvivalent klasičnega telefonskega stikala oz. centrale. Primarni namen je zagotavljanje telefonske storitve uporabnikom, obenem pa tudi ustvarjanje okolja, v katerega je moč vključiti nove, napredne storitve (ki jih stare centrale niso omogočale).

1.1.Strojni del

Fizično je sistem sestavljen iz večjega števila strežnikov IBM, prehodov TDM (namenska strojna oprema) ter Cisco izravnalnikov prometa. Napajanje vseh naprav je 230 V AC, po dva napajalnika na strežnik (razen ohišja strežniških rezin, ki imajo po štiri napajalnike). Sistem je medsebojno povezan z več virtualnimi lokalnimi omrežji, ki se delijo glede na namen in tip prometa (nadzorni promet, signalizacija, govor …). Omrežne povezave so (kjer se le da) podvojene, Gigabit Ethernet, bakreno ožičenje RJ45 , medtem ko se optične vmesnike uporablja za povezavo enega od medijskih prehodov v omrežje TDM (vmesnik STMI) ter za vpetje sistema kot celote v ostanek omrežja.

Na sliki 1 vidimo logično shemo stikala Cirpack. Ključni elementi so MGC (Media Gateway Controller − glavni krmilni strežnik), DB (Database − strežnik s podatkovno bazo), RTPF (RTP Forwarder − vmesnik za promet RTP), TDM GW (medijski prehod), P-CSCF (proxy strežnik), strežnik za prenosljivost številk in LB (izravnalnik prometa).

Vloge posameznih elementov so sledeče:

MGC – glavni strežnik, ki koordinira delo ostalih strežnikov. Na tem mestu se zgodi večina odločitev v sistemu, ki jih nato ostali strežniki izvršijo.

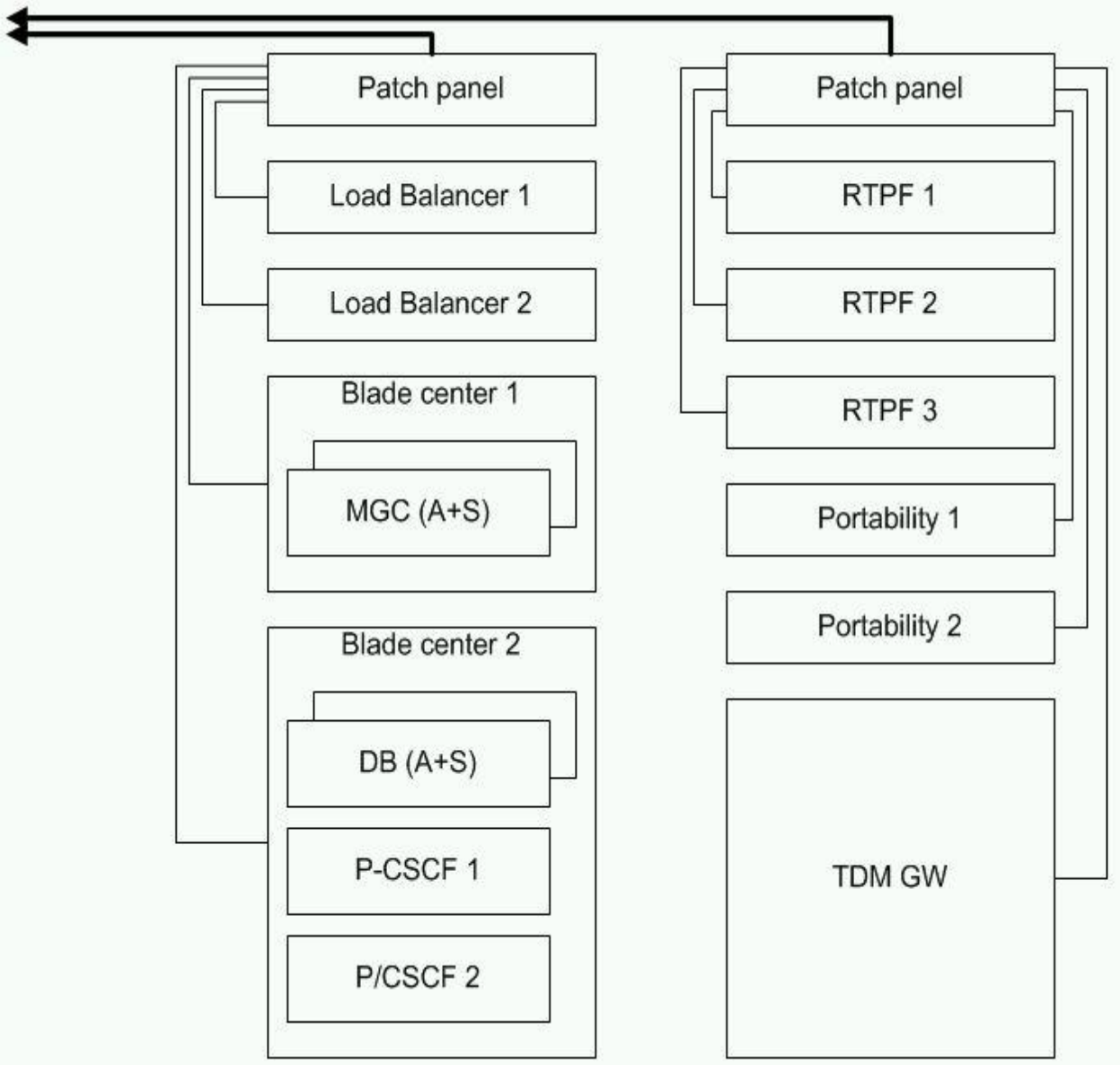
DB – glavna podatkovna baza, na kateri se nahajajo vsi uporabniški podatki. Odločitve MGC strežnika temeljijo predvsem na podatkih, pridobljenih iz strežnika DB.

RTPF – posredovalnik (Real-Time Transport Protocol) prometa RTP oz. proxy za vsebino. Služi tudi za skrivanje topologije omrežja in uporabnikov.

TDM GW – medijski prehod za omrežje TDM. Vsi klici, ki niso znotraj lastnega omrežja, načeloma potujejo skozi medijski prehod (z izjemo interkonekcije IP).
P-CSCF – proxy strežnik za signalizacijo. Stranke v resnici ne vidijo sistema, temveč zgolj te strežnike, ki skrivajo topologijo omrežja in uporabnikov.

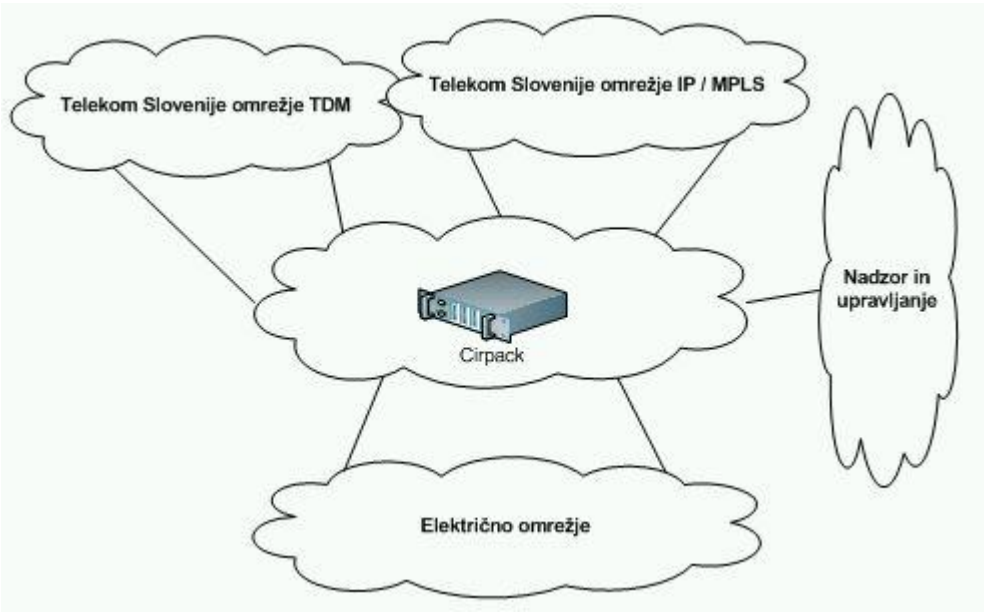
Strežnik za prenosljivost – podatkovna baza vseh prenesenih številk z namenom pravilnega usmerjanja prometa. Ta sistem ni kritičnega pomena, vendar bistveno razbremeni nadrejene centrale.

Izravnalnik prometa (LB - Load Balancer) – ni integralni del programskega stikala, vendar postane pri določeni količini uporabnikov nujen sestavni del. Ta strežnik skrbi za enakomerno porazdelitev zahtevkov klientov na strežnike P-CSCF ter za usmerjanje, če kateri odpove.



Slika 1 – Strojna shema programskega stikala Cirpack.

Slika 2 nam kaže priklop stikala Cirpack v zunanji svet. Povezave lahko razdelimo na električne, komunikacijske (omrežje IP in omrežje TDM) ter nadzorne.



Slika 2 – Priklop stikala Cirpack v zunanje sisteme

1.2.Programski del

Programsko stikalo Cirpack sestavljajo številne aplikacije, ki tečejo na zgoraj navedeni strojni opremi. Kritični, procesorsko zelo obremenjujoči ali kako drugače izjemno pomembni procesi so oblikovani kot samostojne aplikacije, ki medsebojno komunicirajo s pomočjo vrst (»queue«). Posamezne aplikacije je moč nadzirati (log, debug), ponovno pognati (respawn), ponovno naložiti konfiguracijske datoteke (reload) in podobno. Nad aplikacijami se nahaja t. i. »watchdog«, ki nadzira pravilnost delovanja oz. odzivnost aplikacij.

Za brezhibno delovanje storitve, kot jo dojemajo uporabniki, morajo delovati vsi zgoraj navedeni elementi, zato je potrebno poskrbeti za ustrezne mehanizme, ki zagotavljajo pričakovano razpoložljivost. V nadaljevanju bomo natančneje pogledali večino v praksi uporabljenih mehanizmov ter poskušali ugotoviti, kakšen nivo razpoložljivosti nam nudijo.

2. Razpoložljivost v praksi

Razpoložljivost storitve se v praksi pokaže kot precej občutljiva kategorija. Izpad elektrike zaradi nevihte (pri uporabniku doma, kjer oprema ni zaščitena z brezprekinitvenim napajanjem) mimogrede povzroči enourni izpad, programska napaka na modemu ADSL (ki je ne zaznamo takoj) lahko onemogoči storitev tudi za cel dan, težave v omrežju povzročijo nezanesljivo delovanje do nekaj ur in še bi lahko naštevali.

V tabeli 1 vidimo, kolikšen časovni izpad nam še dovoljuje posamezna razpoložljivost, izražena s »številom devetk« [8].

Razpoložljivost, izražena v »devetkah«	Skupni dovoljeni čas izpada storitve na mesec	Skupni dovoljeni čas izpada storitve na leto
99,999 %	0,48 min	5,2 min
99,99 %	4,8 min	52,5 min
99,9 %	43,8 min	525,6 min
99 %	438 min	5256 min

Tabela 1 – Dovoljeni čas izpada storitve v odvisnosti od zahtevane razpoložljivosti.

Povsem očitno je, da že malce resnejši izpad zapečati usodo »petih devetk« (pravzaprav se je s stališča storitve tudi štirih izjemno težko držati). Pa vendar − ali so take vrednosti uporabniku nesprejemljive? Redna mesečna vzdrževalna dela, ki terjajo petminutne prekinitve v časovnem oknu od treh do petih zjutraj, bodo potisnila razpoložljivost sistema na zgolj tri devetke, pa vendar večina uporabnikov tega ne bo nikoli zaznala. Videti je torej, da je razpoložljivost ob pravem času še bolj pomembna kot razpoložljivost sama.

3. Električno napajanje

Kot ena od najnižjih plasti v strukturi zagotavljanja visoke razpoložljivosti sistemov je električno napajanje močno podcenjena kategorija. Povprečen upravitelj sistema se namreč ukvarja s plastmi 4−7 (glede na model OSI [7] – Open System Interconnection) in vse ostale, vključno z napajanjem, jemlje kot samoumevne. To dejstvo nas ne bi smelo pretirano presenetiti, saj je povsem nemogoče biti strokovnjak na vseh področjih in napajalni sistemi so postali tako zapleteni, da zahtevajo specializirane strokovnjake.

Pri zagotavljanju visoke zanesljivosti napajanja se zanašamo na več virov, sistemov napajanja in načinov priklopa napajanja, ki jih bom naštel in na kratko opisal.

3.1.Standardno napajanje

Zagotavlja ga lokalni dobavitelj električne energije in je praktično vedno izmenično. Novodobni strežniški sistemi sicer niso tako »požrešni« kot računalniki preteklosti, vendar jih je neprimerno več. Moderen podatkovni center resnega telekomunikacijskega operaterja vsebuje toliko naprav, da je potrebno ustrezno dimenzionirati priklop na elektroenergetsko omrežje. Naletimo lahko na omejitve, ki so povprečnemu končnemu uporabniku povsem tuje – lokalna razdelilna postaja npr. ni sposobna zagotoviti želene (dodatne) količine energije. Elektroenergetsko podjetje sicer načrtuje razširitev, vendar zaradi pridobivanja gradbenih dovoljenj projekt stoji. Zamude, na katere lahko v tem primeru računamo, so tako velike, da lahko ogrozijo potek celotnega projekta oz. nas prisilijo v selitev na novo lokacijo.

3.2.Brezprekinitveno napajanje

Pri sistemih te velikosti (kot so podatkovni centri) se brezprekinitveno napajanje uporablja predvsem za dva namena:

- premostitev izpada električne energije za čas do vklopa pomožnih (navadno dizelskih) generatorjev in
- zagotavljanje kvalitete električne energije (bremena se vedno napajajo iz baterije ali razsmernika, tako da se izločijo kakršnekoli motnje iz električnega omrežja ali generatorjev).

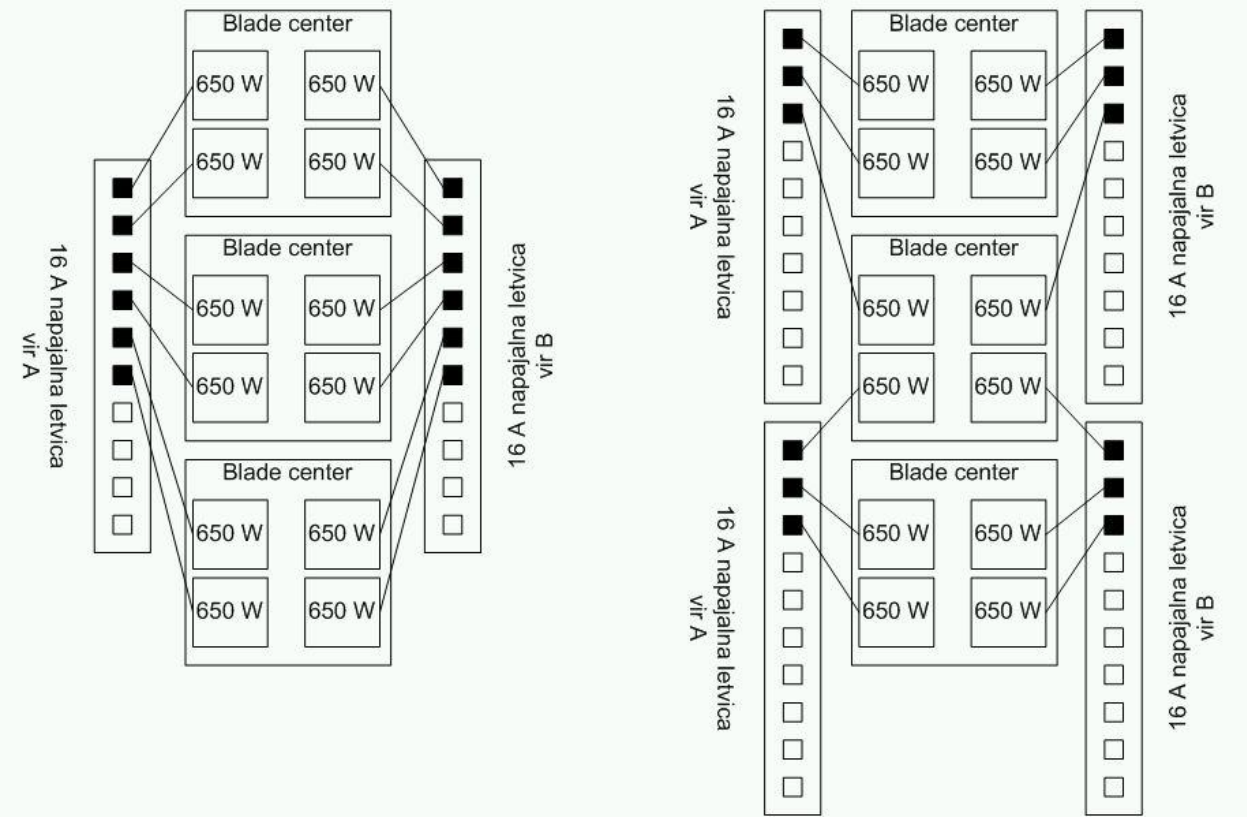
Oblika izvedbe so banke baterij, prilagojenih za tako uporabo (nenehno polnjenje/praznjenje).

3.3.Pomožni generatorji

Tako kot že pri standardnem in brezprekinitvenem napajanju je tudi tukaj ključnega pomena priključna moč naprav, ki naj bi jim generator zagotavljal delovanje. Pri podatkovnih centrih (kot v našem primeru) gre za tako velike porabe, da je tudi velikost generatorjev sorazmerna. Pojavijo se povsem logistične težave dostave in vgradnje, saj je le malokateri prostor zmožen sprejeti tako velike naprave, kot je večstokilovatni agregat. Nenazadnje je potrebno biti pozoren tudi na nosilnost samih tal prostora, kamor opremo vgrajujemo.

Priklop samih naprav v električno omrežje je odvisen od tipa napajalnika (enosmerna/izmenična napetost), je pa vedno izveden večtočkovno – navadno na vir napajanja A in B. Tak način priklopa poleg povečanja zanesljivosti delovanja omogoča tudi praktično brezprekinitvene servisne posege na napajalnem omrežju (nadgradnje, popravila, priklopi novih naprav …). Praksa je, da ima vsaka naprava (ali pa sklop naprav v okviru stojalne omare) svoje varovalke, pogosto ima pa tudi ena sama naprava po več varovalk. S tem se bistveno omeji (morebitni negativni) vpliv posamezne naprave na ostalo omrežje.

Primer slabega načrtovanja, ki lahko (oziroma prej ali slej zagotovo) pripelje do kritične težave, je površen priklop naprav na vir energije A in B znotraj stojalne omare. Ob normalnem delovanju vseh napajalnikov in energetskih virov se namreč poraba energije strežnika enakomerno razporedi na dva vira in s tem tudi na dva električna razdelilca. Ob izpadu posameznih napajalnikov ali pa enega od energetskih virov pa se vsa poraba koncentrira na posameznem viru (kar je načrtovano), obenem pa tudi na posameznem električnem razdelilcu. Zelo preprosto je namreč spregledati dejstvo, da mora biti tudi tako preprosta reč, kot je električni razdelilec, dimenzionirana na energetsko porabo celotne stojalne omare. V primeru, da je v stojalni omari manjše število naprav, ki pa so energetsko zelo zahtevne (npr. ohišja za strežniške rezine), se zato pogosto zgodi, da je večje število električnih odjemnih mest navidezno prostih, v resnici pa neuporabnih, saj bi z njihovo zasedbo preobremenili dovodni kabel.



Slika 3 – Dva primera priklopa na električno omrežje.

Na sliki 3 lahko vidimo primer napačnega (levo) in pravilnega (desno) električnega priklopa. V obeh primerih gre za priklop treh ohišij s po štirimi 650 W napajalniki. Napajalniki so podvojeni, se pravi, da je maksimalna poraba posameznega ohišja 1300 W, ki se v normalnih okoliščinah razporedi na vse štiri napajalnike. Težava je v tem, da ob vzdrževalnih delih ali težavah z enim od napajalnih virov (bodisi A ali B) celotno breme napajanja ohišja (1300W) nosita samo dva napajalnika, kar pomeni, da na napajalni letvici presežemo 16 A, kar povzroči izpad varovalke in s tem tudi storitve. Pomembno se je zavedati, da proste vtičnice še ne pomenijo tudi prostih napajalnih kapacitet! Na desni strani slike je prikazana pravilna izvedba, kjer ne preobremenimo napajalnih letvic tudi v primeru delovanja na enem viru.

4. Parametri okolja

Sicer splošno znano, vendar ne pretirano upoštevano, je dejstvo, da računalniške naprave potrebujejo ustrezno temperaturo in vlažnost zraka za normalno delovanje. Osebnim računalnikom sicer ustreza skoraj vse, kar ustreza tudi nam, medtem ko imajo podatkovni centri jasno definirane zahteve. Vsako večje odstopanje od teh zahtev lahko povzroči začasen (samo-) izklop naprave, odstopanje v daljšem obdobju pa povzroči bistveno skrajšanje življenjske dobe naprave oz. neposredno okvaro.

	Temperatura	Vlažnost
Optimalno	21 ^{o}C–23 ^{o}C	45%−50%
Sprejemljivo	10 ^{o}C–32 ^{o}C	25%−75%

Tabela 2 – Optimalni in sprejemljivi parametri okolja [1]

Strokovna literatura navaja, da dolgotrajno povišanje temperature nad optimalnim območjem v višini 10^{o} C pomeni približno 50% znižanje zanesljivosti oz. življenjske dobe strežnika. [1]

Ob tem velja omeniti, da tudi klimatske naprave za svoje delovanje potrebujejo velike količine električne energije. S tem postavimo naše (predvsem rezervne) napajalne sisteme pred še večje zahteve, saj jih ni zadosti dimenzionirati na porabo strežnikov, temveč tudi na porabo klimatskih naprav, ki te iste strežnike hladijo.

Ker je kontrola temperature v podatkovnih centrih eden večjih porabnikov električne energije, so pogosta razmišljanja, če ni bolje držati temperature pri vrhu dovoljenega območja kot pri dnu. Ta strategija sicer prinaša (velike) neposredne prihranke pri stroških, vendar močno zmanjšuje čas, ki je na voljo za odpravo morebitne napake na klimatskih sistemih. Kot primer naj navedemo, da se temperatura v podatkovnem centru po izklopu klimatskih naprav (kot npr. ob izpadu primarnega napajanja, če klimatske naprave niso vezane na generatorje) lahko dviga s hitrostjo tudi po 2 ^{o}C na minuto. [2]

Podobno kot pri elektronapajalnih sistemih je tudi klimatizacija prostorov veliko bolj kompleksno področje, kot je morebiti videti na prvi pogled. Razumevanje dinamike zračnih tokov v danem centru omogoča bolj učinkovito hlajenje, manjšo porabo energije ter več možnosti pri zagotavljanju zasilnega hlajenja v primeru odpovedi klimatskih naprav.

Omenimo še stabilnost naprav oz. tresljaje. Večina ljudi ob pojmu tresenje pomisli na potres v klasičnem pomenu, pri podatkovnih centrih pa ni povsem tako. Računalniška oprema je namreč bistveno bolj občutljiva na t. i. mikrotresljaje, ki jih človek sploh ne zaznava ali pa jih komajda. Povzročitelji so lahko nadvse raznovrstni, med najpogostejšimi pa so klimatske naprave, generatorji, bližina večjih cest, gradbena dela … Dolgotrajna izpostavljenost naprav takim tresljajem lahko povzroča slabe stike ali okvare komponent, kar v končni fazi pripelje do odpovedi.

5. Fizično ožičenje

Presenetljivo je, kako pomembno vlogo ima fizično ožičenje v zagotavljanju zanesljivosti delovanja. Na prvem mestu je kvaliteta samih kablov (bodisi napajalnih ali komunikacijskih), konektorjev in delilnikov ter pravilna in kvalitetna izvedba ožičenja, na drugem mestu pa je ustreznost oznak in dokumentacije.

V trenutku, ko opremo namestimo in damo v pogon, je zlahka spregledati pomen kvalitetnih oznak vsakega posameznega kabla (vključujoč napajalne). Pomen dokumentacije in oznak spoznamo šele, ko pride do težav. Žal imamo takrat obenem tudi najmanj časa, da bi se ukvarjali z iskanjem pravih kablov. [1]

Ker je tudi ožičenje (kot vse ostalo) podvojeno, smo pri napravah z večjim številom vmesnikov hitro soočeni s (pre)veliko gostoto kablov. V takih primerih je potrebno biti posebno pozoren na pravilno izvedbo ožičenja, da ne onemogočimo prostega dostopa do naprav in njihovih komponent (npr. ventilatorji, napajalniki, moduli …). Takšna napaka je praktično neopazna v začetni fazi projekta, lahko pa postane kritična v primeru odpovedi elementa, do katerega zato ni mogoče dostopati.

6. Vpetje v omrežje IP

V grobem bi lahko izzive vpetja v omrežje IP razdelili na zagotavljanje zanesljivosti (redundanca) in zagotavljanje kakovosti (mehanizmi prioritiziranja prometa).

Ker omrežje IP prevzame nase celoten prenos vsebin (tako signalizacijo kot tudi govor), je posledično ključnega pomena za zagotavljanje visoke razpoložljivosti sistema VoIP kot celote (oz. storitve).

Višjo zanesljivost zagotavljamo z večtočkovnim vpetjem, s podvojevanjem prenosnih poti, z naprednimi usmerjevalnimi protokoli in podobnimi mehanizmi. Težave, na katere lahko naletimo, vključujejo zanke v omrežju, napačno usmerjanje, mehanizme NAT, zasičenja, izgubo paketov, konfiguracijske napake …

V klasični telefoniji TDM se redundanca prenosnih poti do uporabnika sicer ni pojavljala, a je potrebno vedeti, da je bilo v proces vključenih bistveno manj aktivnih naprav, ki so bile že same po sebi bolj zanesljive (centrala TDM je manj bogata z raznimi možnostmi, vendar kot taka tudi bolj zanesljiva oz. manj podvržena napakam). Težava omrežja IP je v tem, da (ne)delovanje enega samega elementa lahko ključno vpliva na delovanje sistema kot celote. Kar je v danem trenutku prednost (agregacija prenosnih poti, optimalna izraba mrežnih elementov …), je lahko v naslednjem trenutku težava (izpad elementa, ki nima zveze s telefonijo, povzroči izpad telefonije).

Pri vpetju v omrežje IP je potrebno biti pozoren predvsem na to, da se zagotovi zadosti kvalitetno vpetje. Telefonija je realnočasovna aplikacija in kot taka izjemno občutljiva na kakovost prenosnega sistema (torej omrežja IP). Parametrov, kot so pasovna širina (bandwidth), zakasnitev (delay), tresenje (jitter) in podobno, telefonija TDM praktično ne pozna, v telefoniji IP pa so eden odločilnih faktorjev za zagotavljanje (kvalitetne) storitve.

Kot smo že omenili, tudi tukaj poskušamo težave preprečiti z redundanco, vendar rešitve postajajo čedalje bolj kompleksne. Redundance v omrežju IP se ne da doseči s preprostim podvajanjem elementov, saj bi to povzročilo težave z naslovi IP. To je plast, kjer se morajo naprave in aplikacije pričeti zavedati okolja okoli sebe (za razliko od do sedaj navedenih sistemov, kjer je bila redundanca izvedena na fizični plasti s kratkimi preklopnimi časi).

7. Zanesljivost podpornih sistemov

Za normalno delovanje storitve VoIP skrbi poleg osnovnega sistema še precejšnje število podpornih sistemov, ki tipično s telefonijo samo nimajo zveze. Sodijo nekako vmes med omrežno in aplikacijsko plast. Do neke mere jih jemljemo kot samoumevne, saj njihovo delovanje presega okvirje znanja posameznika, vendar se pogosto izkaže, da je vsaj osnovno poznavanje delovanja podpornih sistemov praktično nujno, saj brez tega ni mogoče niti osnovno diagnosticiranje težav, ki se pojavljajo.

Nekateri podporni sistemi vplivajo samo na udobnost delovanja (npr. portal za samostojno upravljanje s storitvami oz. »self-provisioning«). Odpoved takega sistema je neprijetna, vendar ne kritična.

Naslednja (nižja, hierarhično gledano) plast sistemov z nedelovanjem onemogoči vključitve novih naročnikov in spremembe pri obstoječih (provisioning), kar je že precej kritično in ima vpliv na produkcijo.

Hierarhično najnižja plast sistemov praktično že meji na omrežne sisteme IP (DNS, DHCP …). Nedelovanje oz. napačno delovanje teh sistemov je izjemno problematično, saj ne povzroči popolne odpovedi storitve, temveč nepredvidljivo delovanje, ki ga je težko diagnosticirati in reproducirati.

Doseganje visoke zanesljivosti podpornih sistemov je naloga upraviteljev le-teh. Naša naloga (kot upravitelja oz. arhitekta sistema VoIP) je predvsem takojšnja zaznava izpada posameznega podpornega sistema in čim bolj natančna diagnostika, s katero pripomoremo k hitri odpravi napake.

Ena najpogostejših težav, ki jih srečujemo pri podpornih sistemih, je ta, da – paradoksalno – pogosto preveč dobro delujejo in se z njimi nihče (aktivno) ne ukvarja. Posledično je precej preprosto pozabiti na njih. Ko pride do pravih težav, ekipe potrebujejo več časa, da se poglobijo v delovanje, kar neprijetno podaljša čas odprave napake. Rešitev je v zelo dosledni in kvalitetni dokumentaciji.

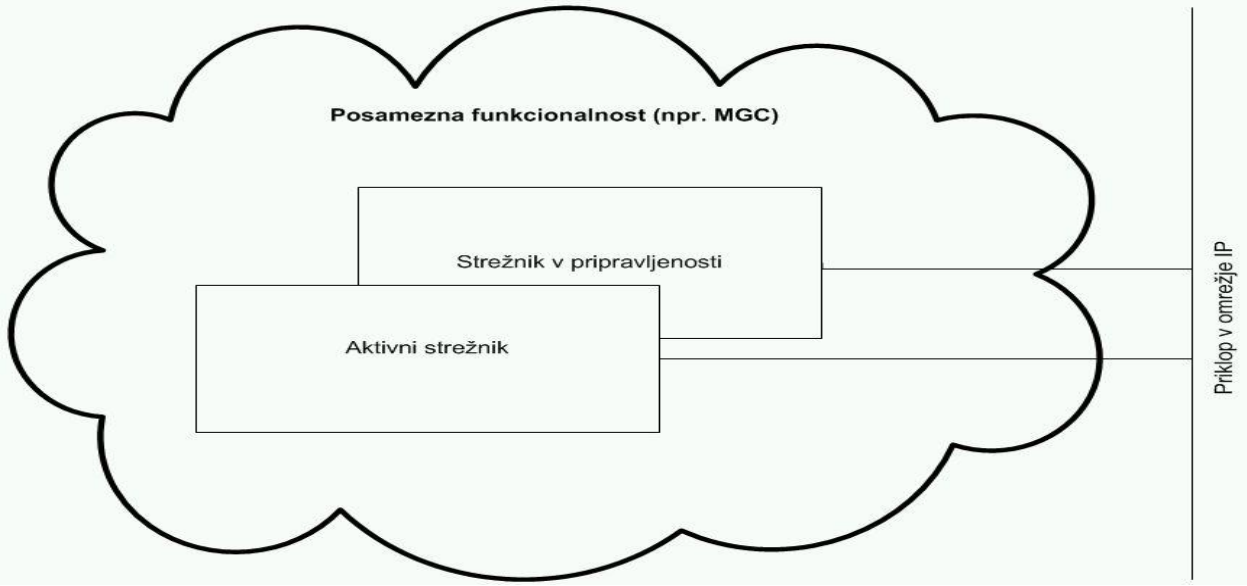
8. Redundanca strežnikov

Obstaja več vrst redundance strežnikov, od katerih ima vsaka svoje prednosti in pomanjkljivosti. Posebno pozornost je treba nameniti dejstvom, da je SIP protokol, ki s signalizacijskimi sporočili poseže na omrežno-komunikacijsko plast ter da se na osnovi izmenjanih sporočil vzpostavijo stanja, ki imajo vpliv na bodočo komunikacijo (npr. registracija). Zaradi tega so določene oblike redundance strežnikov bolj primerne za signalizacijo, druge pa za vsebino.

9. Visoka razpoložljivost

Pojem visoka razpoložljivost [8] (HA – High Availability) pomeni, da sta za posamezno funkcijo namenjena dva strežnika, ki sta medsebojno v odnosu »aktivni« − »v pripravljenosti«. Strojna oprema mora biti (v večini primerov) povsem enaka za oba strežnika, ravno tako verzija programske opreme, ki na teh strežnikih teče (v primeru različne verzije programske opreme navadno ne pride do sinhronizacije in se sproži alarm). Aktivni strežnik je tisti, ki opravi vse delo, medtem ko strežnik v pripravljenosti periodično preverja dosegljivost aktivnega. Načeloma je pravilno, da imata povsem sinhronizirane konfiguracijske datoteke. Večja težava kot s konfiguracijskimi datotekami se pojavi z aktivnimi sejami oz. vzpostavljenimi stanji (ter seveda s postopki, ki so v fazi izvajanja). Ker je sinhronizacija proces, ki se poganja periodično (med drugim tudi zaradi količine podatkov, ki jih je treba prenesti), je torej zelo težko oz. neučinkovito in nepopolno usklajevati stanja in dogodke, ki so lahko poljubno kratki (kot npr. telefonski pogovor).

Očitno ob izpadu aktivnega strežnika določene podatke in stanja izgubimo:
- procese v fazi izvajanja. Najpogosteje so to usmerjevalne odločitve, klici v fazi vzpostavitve, komunikacija s podpornimi sistemi …
- vse konfiguracijske spremembe, vnesene po zadnji sinhronizaciji.



Slika 4 – Posamezna funkcionalnost v obliki dveh strežnikov v postavitvi HA.

Visoko razpoložljivost je mogoče aplicirati praktično na vse strežnike, vendar je to obenem tudi zelo drago. Potrebno procesorsko moč (za izpolnitev dane naloge) podvojimo brez kakršnekoli vidne koristi (razen seveda ob izpadu aktivnega strežnika). Negativna stran take vrste razpoložljivosti je torej predvsem cena:

- nabava dvojnih strežniških kapacitet,
- plačilo ustreznih licenčnin (programska oprema, ki zna delovati v postavitvi HA, navadno stane nekaj več),
- dvojna poraba elektrike (kar pri današnjih priklopnih močeh strežnikov še zdaleč ni zanemarljivo),
- dvojna količina potrebnega prostora za namestitev,
- dvojna proizvodnja toplote, ki jo je potrebno odvajati oz. hladiti (torej ustrezno dimenzioniranje prezračevalnih sistemov) in
- dvojna poraba mrežnih vmesnikov na aktivni opremi, kamor vpenjamo sistem (stikala, usmerjevalniki).

Kot vidimo, je precej stvari, ki jih je potrebno podvojiti, da bi določen strežnik deloval v načinu visoke razpoložljivosti. To seveda ni problem, ko govorimo o strežniku, ki je kritičnega pomena za delovanje storitve, se je pa potrebno vprašati, ali je mogoče doseči želeno zanesljivost tudi na kak drug, učinkovitejši način. Pozitivna stran takega načina zagotavljanja visoke razpoložljivosti je to, da tudi ob izgubi celega strežnika (za določeno funkcijo) ohranimo celotno kapaciteto, saj je na voljo povsem enak strežnik v pripravljenosti. Poveča se zgolj izpostavljenost tveganju odpovedi storitve zaradi izpada naslednje naprave, česar pa uporabniki ne občutijo.

Vzdrževalna dela na strežnikih v pripravljenosti so povsem neproblematična, saj v ničemer ne prizadenejo produkcijskega prometa. Zavedati se je treba le tega, da v času vzdrževalnih del povečamo izpostavljenost, saj strežnik v pripravljenosti v tistem trenutku ni zmožen prevzeti delovanja sistema, če pride do izpada aktivnega strežnika. V primeru kratkotrajnih posegov je

tako tveganje minimalno, še dodatno pa zmanjšamo tveganje s tem, da tudi dela na strežnikih v pripravljenosti izvajamo ponoči.

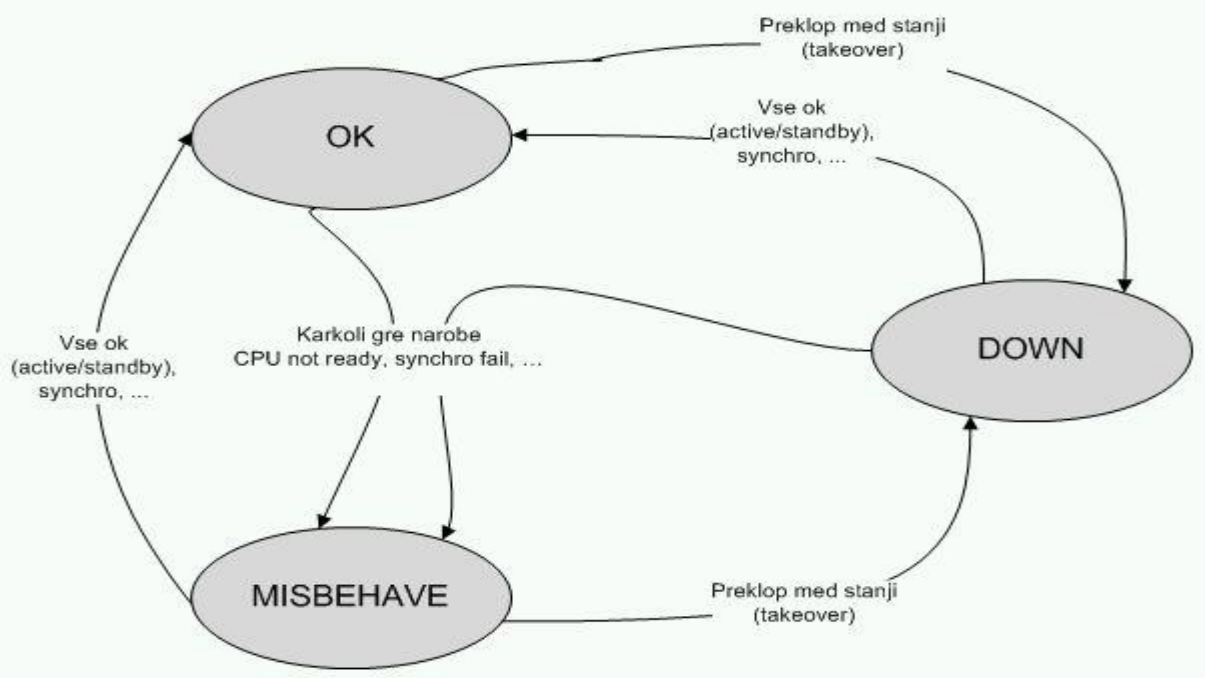
Tudi na aktivnih strežnikih so določena vzdrževalna dela izvedljiva brez prekinitev oz. preklopa na strežnik v pripravljenosti, saj je veliko komponent interno dodatno podvojenih (trdi disk, napajalne enote, ventilatorji …). Če je poseg večji, je potrebno izvesti preklop na strežnik v pripravljenosti. Da bi se izognili kakršnikoli izgubi podatkov (npr. provisioning) ali stanj (registracije klientov), se predvidene preklope navadno izvaja ponoči.

Vse zgoraj navedeno nam v praksi daje precej opcij za vzdrževanje in posege na sistemu, ne da s tem povzročimo izpad storitve in slabo voljo uporabnikov. V najslabšem primeru je potrebno počakati na obdobje nizke prometne obremenitve, kar je za predvidene posege večinoma povsem sprejemljivo.

CPU 1	active	active	active	standby	config	config	off	off
CPU 2	standby	config	off	active	active	off	config	active

Tabela 3 − Primeri stanj strežnikov − sistemov HA.

V tabeli 3 vidimo vse možne kombinacije stanj strežnikov znotraj HA gruče. Samo stanje active/standby velja kot »OK«, vsa ostala so »MISBEHAVE«. V primeru preklopa aktivnosti iz enega strežnika na drugega pride vmes do stanja »DOWN«, ki mu takoj sledi bodisi »OK« ali pa »MISBEHAVE«.



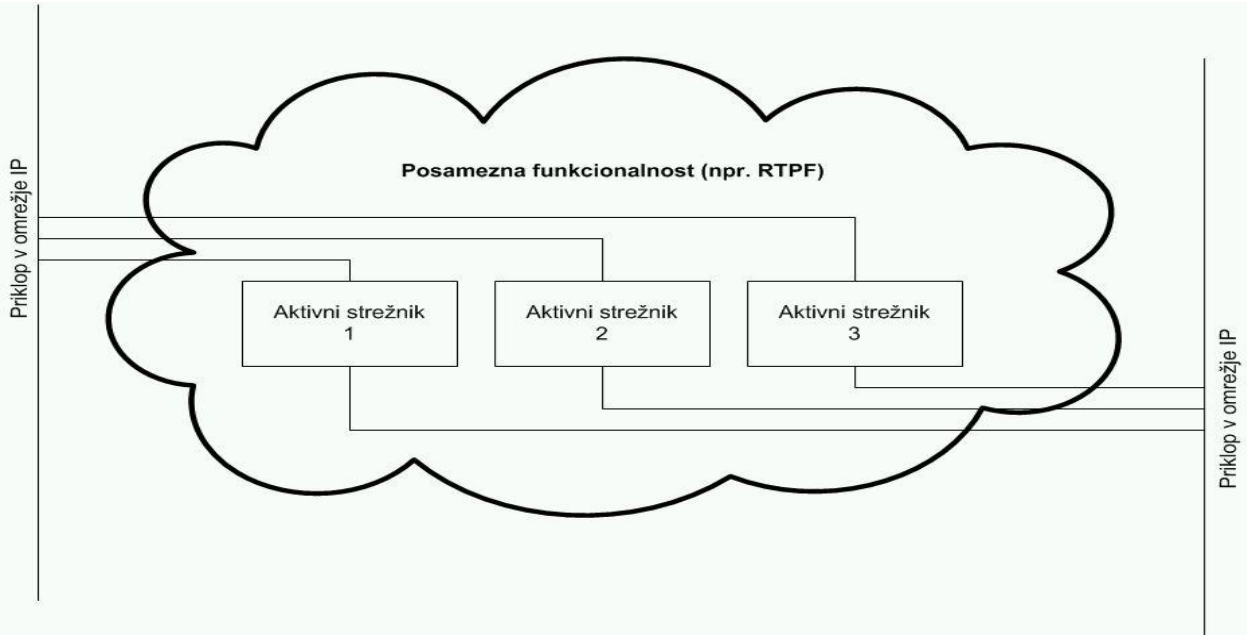
Slika 5 – Prehodi med posameznimi stanji strežnikov HA [3]

10. Delitev dela

Delitev dela (Load Sharing) je oblika redundance strežnikov, kjer so vsi strežniki v produkciji, torej obremenjeni. Odpoved enega strežnika sicer pomeni prekinitev aktivnih sej in izgubo določenih kapacitet, vendar je razmerje cena/zmogljivost veliko bolj ugodno kot pri redundanci z visoko razpoložljivostjo.

V čem je torej težava, da delitve dela ne uporabljamo kar za vse strežnike? Stvar je v tem, da določenih aktivnosti ni mogoče deliti na več strežnikov, saj so procesno gledano centralizirani. Kot primer lahko pogledamo telefonski številski prostor (skladno s telefonsko numeracijo E.164). Načeloma za en blok dodeljenega številskega prostora skrbi ena sama podatkovna baza (ki je seveda postavljena v načinu visoke zanesljivosti − HA). Delitev enega bloka telefonskega številskega prostora na več strežnikov bi povzročila velike težave z usklajevanjem ter zahtevala bolj kompleksno programsko opremo. Poleg tega bi to postavljalo nove zahteve pred sistem za vnos in vzdrževanje parametrov, ki bi moral upoštevati razpršenost baze.

Primer funkcije, ki je izjemno primerna za delitev dela je »media proxy«. Gre za funkcionalnost, ko se posameznemu telefonskemu klicu dodeli kombinacija naslov IP + port, kjer bo potekala govorna seja. Po zaključku seje kombinacija izgine oz. se sprosti za vnovično dodelitev. V primeru odpovedi strežnika sicer izgubimo aktivne seje (aktivni klici na tem strežniku se prekinejo), vendar sistem kot celota ob zmerni izgubi kapacitet (kolikor pač dotični strežnik predstavlja v celotnem naboru kapacitet – lahko tudi 50 % ob samo dveh strežnikih) nemoteno nadaljuje z delom. Prekinjene seje se lahko ponovno vzpostavijo ročno (uporabniki enostavno ponovno pokličejo), v določenih primerih pa celo avtomatsko (signalizacijski strežnik zazna prekinitev in pošlje RE-INVITE).



Slika 6 – Funkcionalnost »media proxy«, razpršena med tri strežnike.

Posebna oblika zagotavljanja visoke razpoložljivosti z delitvijo dela je signalizacijski proxy. Funkcijsko gledano je signalizacijski proxy naprava, ki vsebuje informacije o statusu klientov. Kot tak načeloma ni primeren za delitev dela, saj je izjemno pomembno (oz. edino delujoče), da uporabnikova signalizacija pride na tisti signalizacijski proxy, kjer je uporabnik registriran (zahteva protokola SIP). Kljub temu pa je delitev dela potrebna, saj z večjim številom uporabnikov enostavno presežemo kapaciteto posameznega proxy strežnika (in smo s tem praktično prisiljeni v neko obliko delitve dela). Težavo rešimo tako, da pred skupino proxy strežnikov (ki si delijo delo) postavimo izravnalnik prometa (Load Balancer). To je element, o katerem bomo natančneje govorili kasneje, pomembno pa je, da s tem zagotovimo, da signalizacija posameznih klientov vedno pride na isti proxy strežnik. S tem zadovoljimo funkcijske zahteve protokola SIP, obenem pa ustvarimo okolje, ki omogoča delitev dela (in s tem tudi obliko zagotavljanja visoke razpoložljivosti, saj bo ob odpovedi proxy strežnika signalizacija vseeno krenila na enega od ostalih).

11. Redundanca ohišja

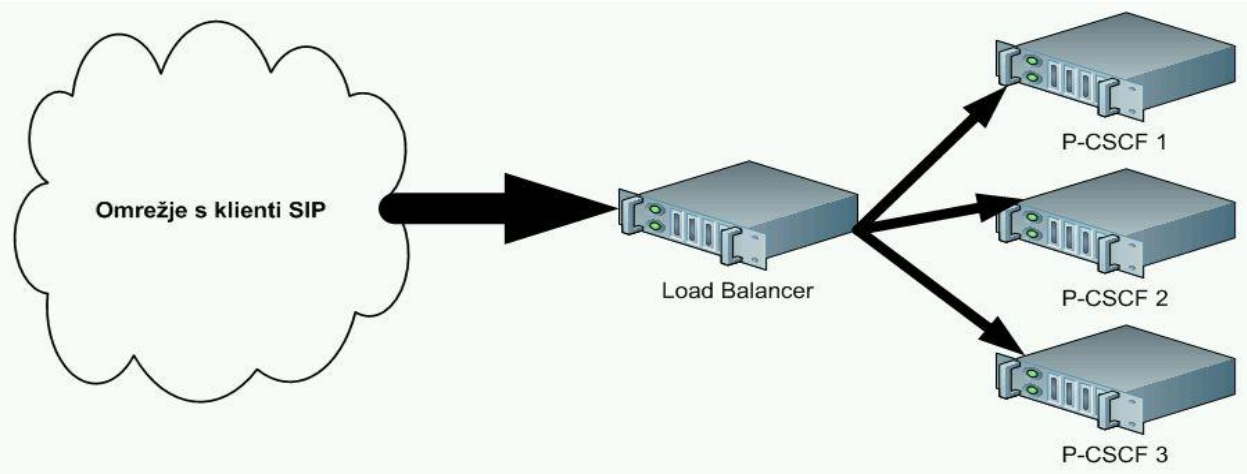
Kljub mehanizmom za visoko razpoložljivost in delitev dela še vedno ostajajo posamezne točke v sistemu, ki jih je v določenih okoliščinah praktično nemogoče podvojiti. Tipično je ta pojav prisoten pri manjših sistemih, kjer se poskuša kar najbolj izkoristiti strežniške kapacitete in se jih še ne razprši v več strežniških ohišij (ker še ne obstajajo potrebe za tako veliko kapaciteto).

Kot primer poglejmo ohišje za strežniške rezine (Blade Center), v katerem se nahaja sistem strežnikov v načinu visoke razpoložljivosti. Samo ohišje ima npr. štirikratno električno napajanje, vsaj dvojno vpetje v omrežje IP, strežnik je podvojen (aktiven/v pripravljenosti), trdi diski znotraj strežnika so podvojeni … Toda šibka točka sistema je prav ohišje, v katero so vse posamezne naprave vpete in preko katerega komunicirajo (npr. backplane).

Rešitev težave z redundanco ohišja je na nek način tudi odgovor na željo po geografski redundanci, saj je posamezna ohišja mogoče namestiti na različne lokacije, ne da bi to zaznale. Kot bomo videli malo kasneje, je to sicer izvedljivo, vendar s tem vnesemo v sistem povsem nov koncept, ki poleg finančnega vložka zahteva tudi precej znanja in truda na nivoju cele ekipe (še posebno omrežje IP).

12. Izravnalnik prometa

Izravnalnik prometa (LB - Load Balancer) je naprava z navidez zelo preprosto funkcijo, obenem pa z izjemno širokim spektrom uporabe. Primarni namen je razvrščanje dohodnega prometa oz. zahtev na dva ali več ciljnih strežnikov. To razvrščanje lahko temelji na določenih kriterijih, lahko pa je povsem statistično. Na sliki 7 vidimo grafično predstavitev razvrščanja zahtevkov SIP na tri signalne strežnike (kriterij razvrščanja je izvorni naslov IP, kar na sliki ni razvidno).



Slika 7 – Izravnalnik prometa razvršča zahteve klientov.

V našem primeru se pokaže, da statistično razvrščanje (na primer »Round Robin« ki je najpreprostejše) ni možno. Razlog za to so karakteristike oz. način delovanja protokola SIP ter proxy strežnikov SIP.

Poglejmo si primer:

Preprosto statistično razvrščanje prometa, ki ga ustvarjajo klienti SIP, bi lahko izvajali že s pomočjo strežnikov DNS, in sicer tako da bi za ciljni naslov registrskega strežnika in odhodnega proxy strežnika (npr. diploma.voip.si) navedli štiri naslove IP, ki pripadajo posameznim proxy strežnikom. V trenutku, ko bi klient A želel izvesti registracijo, bi od strežnika DNS dobil naslov proxy_1, preko katerega bi se tudi registriral. Ker klient A intenzivno uporablja modem ADSL, ki je obenem tudi klient SIP (oz. ga vsebuje), mu je v roku 10−15 minut zapis za »diploma.voip.si« potekel V resnici je tako, da sploh nismo odvisni od intenzivnosti uporabe modema in pretečenega zapisa DNS – firmware v CPE (Customer Premises Equipment – oprema, nameščena pri uporabniku) opremi se pogosto ne drži nikakršnih standardov razen lastnih, zato ne moremo računati na optimalno obnašanje. Ko torej klient A želi opraviti klic, mora modem za naslov ponovno vprašati strežnik DNS, ki mu tokrat odgovori z naslovom proxy_4 (na primer, lahko bi bil katerikoli od štirih). Klient pošlje SIP INVITE na naslov proxy-_4, vendar ga ta zavrne, saj nima podatka o veljavni registraciji (kljub temu da ima klient A veljavno registracijo na proxy strežniku 1). Odločitev proxy strežnika za zavrnitev klienta je lahko malce čudna na prvi pogled, vendar ne smemo pozabiti, da je ravno to ena od primarnih nalog proxy strežnika – filtriranje prometa neregistriranih klientov.

Rešitev te težave je očitno v tem, da med strežnik DNS in proxy strežnike vrinemo element, ki bo zmožen poskrbeti, da bodo klienti vedno pošiljali zahteve na isti strežnik. Temu elementu rečemo izravnalnik prometa. Osnovni kriterij za usmerjanje zahtev klienta je izvorni naslov IP. Za posamezna omrežja določimo, na katere proxy strežnike naj se usmerjajo. Tukaj obstaja potencialna težava, če bi strežnik DHCP pogosto dodeljeval klientom različne naslove IP, in sicer iz preveč različnih naslovnih prostorov. Zopet vidimo vlogo usklajenosti delovanja ključnih podpornih sistemov, kar strežnik DHCP zagotovo je.

Kljub vsemu pa še zdaleč nismo zaključili z zahtevami, ki jih imamo do izravnalnika prometa. Klient namreč v poslani zahtevi SIP kot ciljni naslov navede tisti naslov, ki ga pridobi od strežnika DNS ob razrešitvi naslova FQDN (Fully Qualified Domain Name – popoln domenski naslov), kar pa (mi vemo) ni prav. To je namreč naslov izravnalnika prometa, kar je za resnični strežnik SIP (bodisi proxy bodisi registrar bodisi pa kaj tretjega) nesprejemljivo. Izravnalnik prometa mora torej svoje delo opravljati povsem transparentno. Da bi to dosegel, mora poseči v samo strukturo usmerjanih zahtev SIP in jih ustrezno spremeniti. Kot ciljni naslov navede naslov proxy strežnika, ki mu je zahteva namenjena, in tako doseže, da se proxy strežnik ne zaveda obstoja vmesne aktivne naprave. Proxy strežnik bo odgovor poslal direktno klientu, čeprav se temu lahko tudi izognemo.

Tej metodi poseganja v vsebino paketov se reče DPI – Deep Packet Inspection. Proces je procesorsko zahteven, saj je treba paket (namesto zgolj preusmeriti) razpakirati, pregledati, najti želeno vrednost in jo zamenjati ter opremljeno z novim naslovom poslati dalje. Poleg same procesorske zahtevnosti je postopek tudi občutljiv na napake, saj se naprava načeloma transportne plasti vpleta v podatke aplikacijske plasti.

Najzahtevnejša naloga izravnalnika prometa pa je (vsaj s stališča celostnega delovanja sistema) zaznavanje nedelovanja posameznega ciljnega strežnika in izločitev le-tega iz procesa usmerjanja. Težava je namreč v tem, da je potrebno zelo natančno (ter predvsem celovito s stališča storitve) opisati, kaj točno razumemo kot nedelovanje ciljnega strežnika. Zelo preprosto je zaznavati omrežno dosegljivost, vendar nam to še nič ne pove o stanju aplikacije ali o pravilnosti njenega delovanja.

Na izravnalniku prometa je zato potrebno definirati nabor testov in kriterijev, ki jih bo periodično izvrševal in na osnovi rezultatov presodil, ali je ciljna naprava (v našem primeru proxy strežnik) še aktivna. Ti testi se gibajo od preprostih omrežnih (ping) pa do povsem aplikacijskih (pošljemo zahtevo SIP in pričakujemo točno določen odgovor). V primeru, da katerikoli od testov ne da pričakovanih rezultatov, bo izravnalnik predvideval, da je strežnik nedosegljiv in ne bo več usmerjal prometa na ta strežnik.

V tem primeru sicer zopet pridemo do situacije, ko so klienti SIP usmerjeni na drug proxy strežnik, kot jim je bil originalno dodeljen, kar pripelje do začasnega nedelovanja storitve za dotične kliente, vendar je to ob odpovedi proxy strežnika praktično neizogibno. Situacija se reši sama od sebe, in sicer takoj ko klienti pošljejo zahtevo za registracijo. Nova registracija se realizira skozi nadomestni proxy strežnik, ki nato normalno sprejema vso komunikacijo klienta s programskim stikalom SSW (softswitch).

Pri klientih SIP je privzeta vrednost za čas obnove registracije 3600 sekund, pri čemer velja, da se klienti navadno oglasijo že pred potekom veljavnosti registracije (npr. 1/10 časa ponovne registracije pred iztekom, torej 6 minut v našem primeru). V praksi to pomeni, da se bodo klienti ponovno registrirali v povprečju v 27 minutah. Če upoštevamo še dejstvo, da se je na pokvarjenem proxy strežniku nahajal samo del klientov (število vseh uporabnikov/število proxy strežnikov) in da statistično gledano povprečen uporabnik telefonira manj kot 10 minut na dan, je zelo velika verjetnost, da bo imel izpad minimalen vpliv na delovanje sistema oz. storitve.

Ko napako na proxy strežniku odpravimo, je potrebno uporabnike preusmeriti nazaj. Kljub relativno majhnemu ocenjenemu vplivu na storitev (ob preklopu strežnikov) je bolje, če to storimo v času, ko sistem ni obremenjen (ponoči). Od konfiguracije izravnalnika prometa je namreč odvisno, ali se bo ta preklop zgodil samodejno (ko izravnalnik zazna, da je proxy strežnik zopet aktiven) ali pa bo potreben ročni poseg.

13. Zanesljivost aplikacije

Programske napake so v vsakdanjem življenju tako prisotne, da se jih pogosto niti ne zavedamo več. Ko se aplikacija »obesi«, jo enostavno (ročno) ponovno poženemo. Žal to pri aplikacijah, kjer želimo doseči visoko razpoložljivost, ni mogoče. Zato je v sistemih te vrste implementiran nadzorni mehanizem, ki nenehno preverja delovanje kritičnih procesov na strežniku. Če v kateremkoli trenutku pride do nepredvidenega izpada procesa, bo nadzorni mehanizem (watchdog) proces ponovno pognal. Od vrste procesa in napake, ki je prekinitev povzročila, je odvisno, ali bodo ob ponovnem zagonu procesa obnovljeni tudi parametri in stanja starega procesa ali ne. V primeru, da watchdog procesa ne uspe pognati, pomeni, da gre za veliko resnejšo napako, ki najverjetneje pomeni (začasno) odpoved strežnika. Dogodki take vrste so administratorjem sistema najpogosteje relativno neznani, saj jih je skoraj nemogoče simulirati ali testirati.

Kot vidimo, gre pri watchdog mehanizmu za podobno stvar kot pri izravnalniku prometa, kjer se preverja dosegljivost ciljnih strežnikov. Razlika je v tem, da imamo pri izravnalniku prometa možnost vplivanja na delovanje tega mehanizma, medtem ko je watchdog popolnoma samostojen mehanizem, na katerega upravljalci sistema nimajo vpliva.

Izvedba »watchdog« mehanizna je lahko bodisi strojna bodisi programska, odvisno predvsem od narave (kritičnosti) strežnika ter seveda cene. V »telco« sistemih, ki naj bi dosegali 99,999% stopnjo zanesljivosti, so praktično vedno strojne izvedbe. [3]

14. Vpliv konfiguracije

Na zanesljivost delovanja sistema konfiguracija zagotovo vpliva, pa vendar – zakaj je to tako pomembno, da omenjamo v ločenem poglavju?

V tako zapletenih sistemih, kot je programsko stikalo VoIP, se konfiguracije ne delijo zgolj na pravilne in napačne. Obstajajo tudi npr. pravilne, pa vendar obenem omejujoče oz. problematične. Tu mislimo predvsem na količinsko opredeljene in ne logične (»da«/»ne«) parametre. Ta opredelitev se praktično vedno nanaša na količino dodeljenih kapacitet – kot npr. število prenosnih kanalov TDM, dovoljeno število hkratnih zvez, količina medpomnilnika, število procesorjev DSP, namenjenih obdelavi posameznega tipa signala …

Parametrov takega tipa je v sistemu ogromno, zato ni presenetljivo, da jih upravitelji sistemov najpogosteje ne poznajo prav vseh (nekateri so še posebej redko aktualni in posledično precej zanemarjeni). Težava je v tem, da so vsi ti parametri ob postavitvi sistema nastavljeni na neke izhodiščne vrednosti, ki so sicer odlične za začetek (pa tudi za nekaj predvidene rasti), se pa pogosto zelo slabo izkažejo, ko sistem preseže določeno kritično velikost. Da bo zadrega s parametri še večja, se njihova neustreznost navadno ne pokaže kot jasna odpoved sistema. Le zakaj bi se, saj parametri niso napačni, so le neustrezni za velikost, ki jo je sistem (postopoma!) dosegel.

Poglejmo si dva primera – »konfiguracijski« in »sistemski«

Konfiguracijska težava, ki negativno vpliva na delovanje in s tem stabilnost sistema, je premajhna vrednost pri nastavitvah za največje dovoljeno število hkratnih zvez na glavnem (lahko pa tudi na kakem od pomožnih) klicnem zbirniku (»peer«). Težava te vrste ni preprosto ponovljiva, saj se ob ponovnem klicu zlahka zgodi, da se je nekaj drugih klicev (in s tem tudi kapacitet na zbirniku) sprostilo, kar sicer omogoči klic, vendar onemogoči natančno diagnosticiranje težave. Pritožbe uporabnikov se zdijo naključne, neponovljive in celo neutemeljene, saj ob kontrolnem klicu le-ta uspe. Ker je dimenzioniranje zbirnikov (sploh glavnih) relativno redko opravilo, se zlahka zgodi, da traja precej dolgo, preden odkrijemo napako.

Primer sistemske težave je nastavitev baze (ponavadi SQL), namenjene uporabniškim profilom, in veljavnosti registracije klienta SIP. Baza v osnovi ni napačno nastavljena in odlično deluje, vendar se z naraščanjem števila uporabnikov (ali pa s spremembo obnašanja klientov – pogostejše registracije) pred njo postavljajo nove, precej večje zahteve. Ko do take situacije pride, je potrebno težavo ustrezno diagnosticirati, kar pa se pokaže za zelo zahtevno, saj težava zopet ni enakomerno ponovljiva. Preobremenjenost baze se kaže v pogosto nenavadnih, »sekundarnih« simptomih – poteče timer SIP in zveza se podre. Ne obstaja nikakršna indikacija, da je za dogodek kriva baza SQL, ki je zaradi preobremenjenosti (lahko tudi na diskovnem podsistemu) pričela izpuščati zahteve oz. je obdelava posamezne zahteve predolgo trajala.

Sistemskih težav upravitelji sistema navadno ne rešujejo sami, temveč jih zgolj prijavijo na ustrezen nivo podpore (drugi nivo − integrator oz. tretji nivo − proizvajalec sistema). Rešitev je sicer lahko programska (oz. konfiguracijska), še pogosteje pa je potrebna nadgradnja strojne opreme oz. ustrezno dimenzioniranje.

Pri težavah, povezanih s konfiguracijo, je izjemno koristno vzdrževati podroben dnevnik sprememb konfiguracije, kjer zabeležimo tudi morebitne opombe. Občasno se namreč zgodi, da določena sprememba povzroči težave, ki se opazijo šele s časom. V takem primeru je pomembno vedeti, kdaj točno je bila sprememba uveljavljena ter kaj točno je bilo spremenjeno, da se to lahko poveže s prijavljenimi napakami. Ne bo odveč omeniti, da so redne varnostne kopije konfiguracijskih datotek obvezne.

Sicer ne povsem neposredno povezana z zagotavljanjem visoke razpoložljivosti, pa vendar zelo pomembna, je testna platforma. Le-ta nam omogoča, da vse kritične in potencialno disruptivne nastavitve testiramo v nadzorovanem in varnem okolju. S tem se izognemo neprijetnim presenečenjem v produkciji in posledično povečamo zanesljivost delovanja. Omeniti je treba, da določenih scenarijev kljub vsemu ni mogoče testirati na testni platformi, saj ji manjka najbolj kritična komponenta – velika količina prometa.

15. Uporabniška terminalna oprema

Kljub temu da CPE (uporabniška terminalna oprema) nedvomno ni neposreden del vzdrževanega sistema (s stališča operaterja), je pomemben člen v verigi zagotavljanja storitve, kot jo dojema uporabnik. Žal se v praksi pokaže, da je za največ težav odgovorna ravno oprema CPE – tista, na katero ima operater najmanj vpliva.

15.1. Fizični vidik

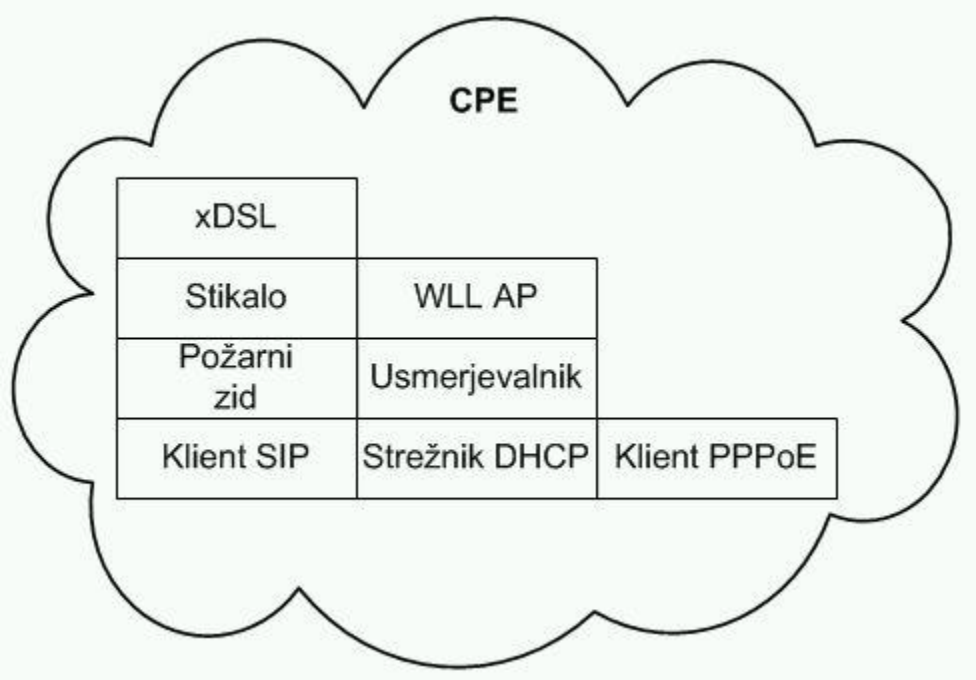
Prva, a še zdaleč ne edina težava je napajanje. Izjemno redki so rezidenčni uporabniki, ki svojo komunikacijsko opremo ščitijo s sistemom za neprekinjeno napajanje (UPS). Izpad električnega omrežja torej pomeni izpad telefonske storitve v celoti.

Težave domačega okolja se nadaljujejo z okoljem – kontrolo temperature. Naprave za domačo rabo so sicer zasnovane tako, da prenesejo širok temperaturni razpon, pa vendar potrebujejo ustrezno hlajenje. Nemalokrat se zgodi, da uporabniki iz estetskih razlogov namestijo opremo v neustrezen prostor ali pa jo celo pokrijejo. Tako ravnanje povzroča pregrevanje, ki se izkazuje na različne načine. Popolna odpoved opreme (najpogosteje napajalnika) je sicer neprijetna, vendar najlažja za diagnozo. Bolj nenavadni simptomi vključujejo občasno nedelovanje ali pa nepravilno delovanje.

V pravilnost izvedbe priklopa opreme pri uporabniku se ne bomo spuščali, kljub temu da tudi to vpliva na zagotavljanje storitve. Potrebno je le vedeti, da je pri reševanju težav z zagotavljanjem storitve vsekakor potrebno upoštevati tudi ta vidik.

15.2. Programska oprema

Programska oprema na opremi CPE (firmware) je po mojih izkušnjah statistično najpogostejši vzrok za težave oz. nedelovanje storitve. Del težave je vsekakor smiselno iskati tudi v izjemni zapletenosti firmwara, saj poleg klienta SIP opravlja naloge klienta xDSL, usmerjevalnika, klienta PPPoE, stikala, pristopne točke WLL, klienta DHCP/strežnika … Tolikšna kompleksnost terja svoj davek in ta je zanesljivost. Pri napravah za hišno uporabo je postalo sprejemljivo (in je nekakšen splošni recept za odpravo težav), da je v primeru težav najboljša rešitev ponovni zagon.

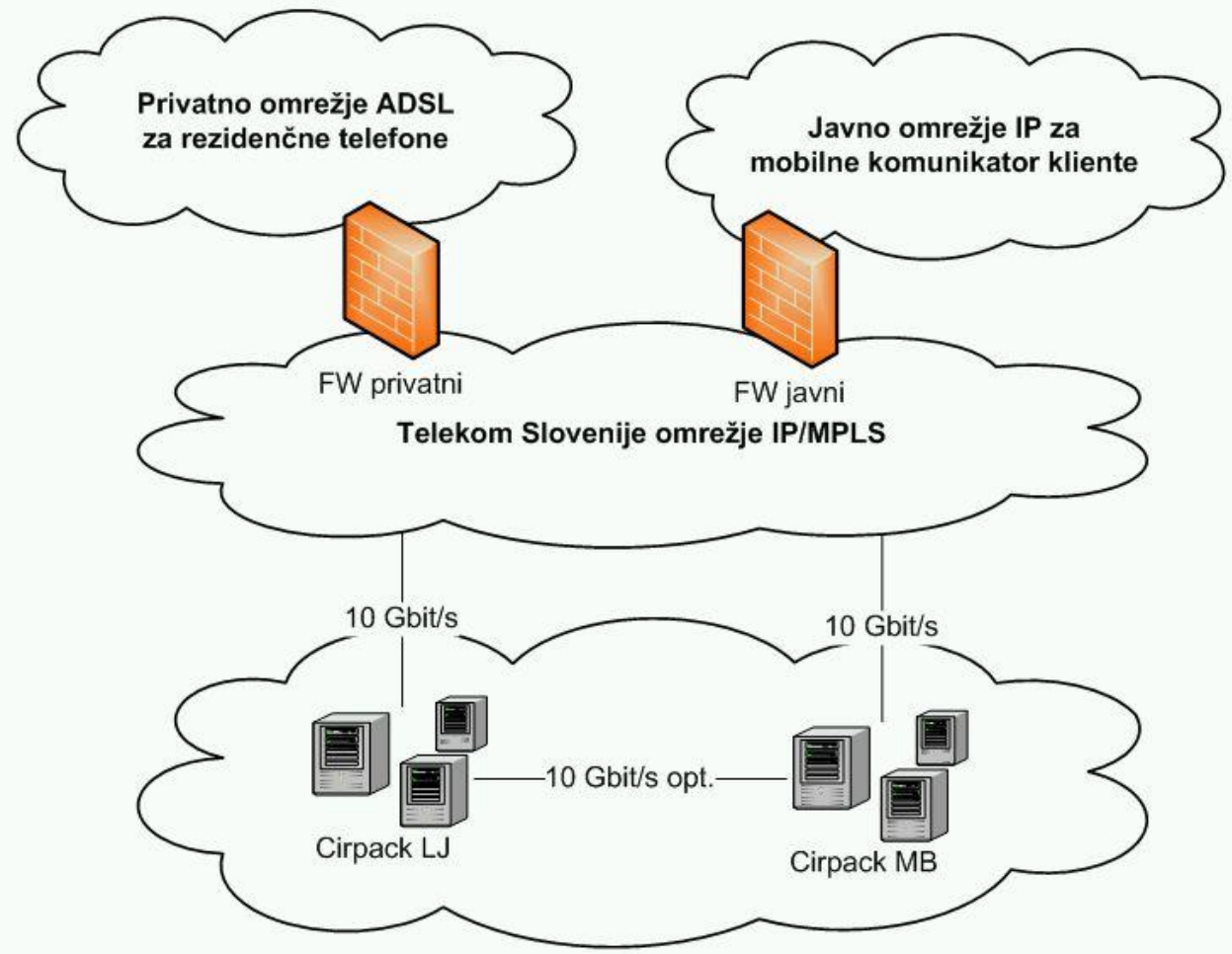


Slika 8 – CPE in nekatere od funkcij, ki jih izvaja firmware.

16. Varovanje pred lastnimi uporabniki

16.1. Požarni zid

Požarni zid je splošno uveljavljen in neizbežen način zaščite omrežja pred (pretežno, a ne izključno) zunanjimi vplivi. V našem primeru s pomočjo požarnega zidu omrežja ne ščitimo zgolj pred zunanjimi grožnjami (internet), temveč tudi pred lastnimi uporabniki. Kot notranje omrežje namreč štejemo izključno samo opremo, nad katero imamo neposreden nadzor, kar pomeni, da uporabniški klienti SIP obveljajo kot nezanesljivi. Nivo te nezanesljivosti pa le ni enak javnemu internetu, zato je potrebno narediti dve domeni – privatno in javno (ki pa sta obe ločeni od strežnikov VoIP). Na sliki 9 vidimo, da so tako interni (xDSL) kot tudi javni (internet) uporabniki od sistema ločeni s požarnim zidom.



Slika 9 – Vsi uporabniki so od sistema ločeni s požarnim zidom.

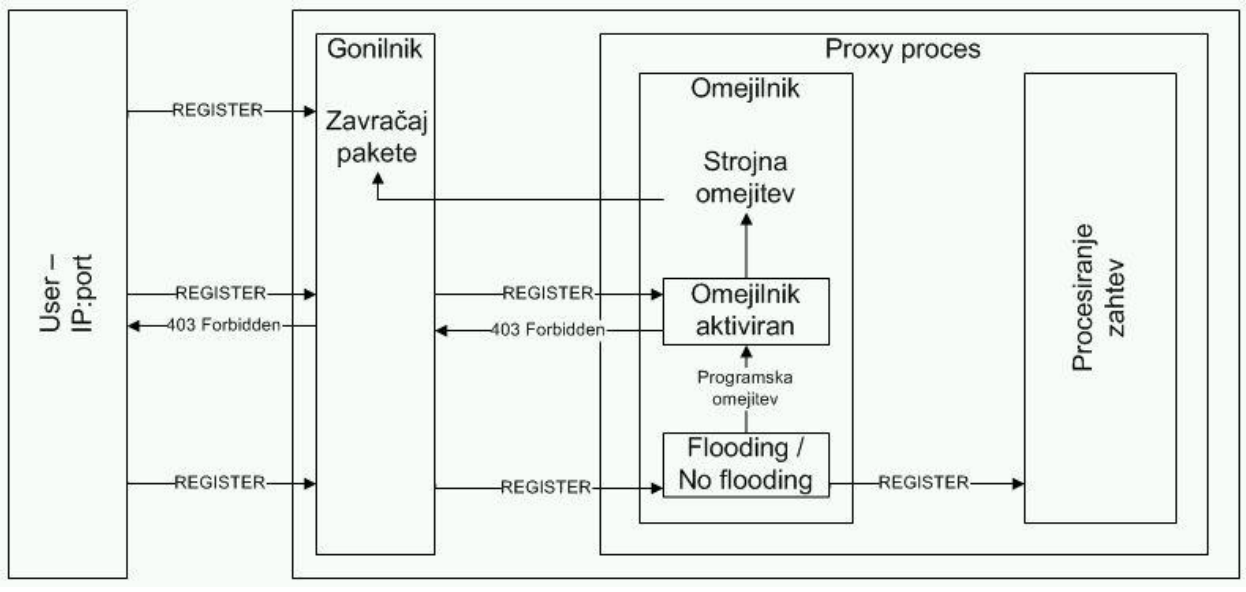
Pri zagotavljanju visoke zanesljivosti storitve VoIP imajo požarni zidovi vlogo preprečevanja očitno zlonamernega (ali vsaj neustreznega) prometa ter omejevanja dostopa na izključno predvidene storitve. Ker pa požarni zidovi delujejo zgolj znotraj plasti IP, je očitno potrebno poseči še eno plast višje. Naprava, ki se s tem ukvarja, je proxy strežnik.
Proxy je naprava s podobno vlogo kot požarni zid, vendar se za razliko od le-tega zaveda vsebine prometa. Lahko bi rekli, da gre za požarni zid, ki razume vsebino in se v njo po potrebi tudi vplete.

16.2. Strežnik P-CSCF

Terminologija je tukaj občasno malo pikolovska, zato povejmo, da se proxy lahko imenuje SBC (Session Border Controller oz. razmejitveni nadzornik sej) in je najpogosteje uporabljen v razmejevanju različnih omrežij VoIP med seboj (torej tranzitno oz. medoperatersko), medtem ko naprave, ki jih mi opisujemo, imenujemo SAP (SIP Access Proxy oz. dostopovni posrednik SIP) v terminologiji NGN (Next Generation Networks oz. omrežja naslednje generacije) ter P-CSCF (Proxy - Call Session Control Function oz. posredniška funkcija nadzora govorne seje) v okolju IMS (IP Multimedia Subsystem).

Delovanje strežnika P-CSCF vključuje:

- prejemanje celotne signalizacije SIP (torej promet, že filtriran s strani požarnih zidov),
- pošiljanje celotne signalizacije SIP (skrivanje topologije omrežja),
- analizo zahtev in selektivno ukrepanje (beleženje veljavnosti registracije, preverjanje registracije, posredovanje signalizacije …),
- beleženje pogostosti zahtev glede na tip zahteve ali na izvorni naslov zahteve in
- omejevanje posameznih tipov zahtev ali klientov.



Slika 10 – Omejilniki P-CSCF [4] in potek registracijskih zahtevkov.

Na sliki 10 vidimo primer, ko število registracijskih zahtevkov posameznega klienta preseže (nastavljive) dovoljene vrednosti. P-CSCF sprva klienta opozori, nato pa prične (za določen čas) odmetavati pakete IP s tega izvornega naslova.

Vse to so mehanizmi, ki s svojim delovanje bistveno pripomorejo k zanesljivosti delovanja storitve, saj omejujejo možnosti nepravilnega ali zlonamernega načina uporabe omrežja in s tem prevelike porabe sistemskih zmogljivosti, kar bi vodilo v zmanjševanje kakovosti oz. v izpad storitve.

17. Veliki skok – geografska redundanca

17.1. Visoka razpoložljivost

Mehanizem visoke razpoložljivosti (HA) smo že omenjali (gruča strežnikov), vendar vedno v istem ohišju za strežniške rezine (razen če govorimo o samostojnih strežnikih, kjer pa izgubimo prednosti arhitekture strežniških rezin). Tisti trenutek, ko programsko podpremo postavitev strežniških rezin HA v ločena ohišja, dobimo možnost izvedbe prave geografske redundance. Programski popravek, ki ga omenjamo, ni tako nedolžen, saj je »tipanje« sosednjega strežnika neprimerno lažje, dokler sta oba v istem ohišju. V trenutku, ko prestopimo na geografsko redundanco, se logika HA prične zanašati zgolj na omrežje, ki pa z geografsko redundanco izjemno pridobi na kompleksnosti.

17.2. Delitev dela med strežniki

Delitev dela oz. »Load Sharing« strežnikov na geografsko redundančni lokaciji je izjemno preprosta. Strežniki se namreč ne zavedajo svoje okolice oz. sosednih strežnikov istega tipa, zato jih lahko enostavno razdelimo 50 : 50 med lokaciji (oz. v drugačnih razmerjih, če je lokacij več). Vse, česar se je potrebno zavedati, je to, da ima posamezna lokacija zgolj 50 % kapacitete originalnega sistema. Če je ciljna kapaciteta posamezne geografske lokacije enaka kapaciteti originalnega sistema, je potrebno podvojiti število strežnikov (za razliko od mehanizma HA, kjer so kapacitete že podvojene).

17.3. Nove zahteve omrežja IP

Eno najbolj kritičnih vlog v procesu zagotavljanja geografske redundance ima omrežje IP. Potrebno se je namreč odločiti, ali bo ena od lokacij primarna ali pa bosta obe povsem enakovredni (s stališča omrežnega vpetja). Ne glede na odločitev morajo strežniki na obeh lokacijah videti omrežje povsem enotno (geografska ločitev je transparentna).

V primeru primarne lokacije je omrežje IP zgolj raztegnjeno na drugo lokacijo in ne zagotavlja geografske redundance omrežja IP (na enak način, kot je zagotovljena geografska redundanca sistema VoIP). Tak pristop je arhitekturno bistveno enostavnejši in tudi cenejši. To seveda ne pomeni, da ni določene redundance na nivoju omrežja IP – le-ta je zagotovljena znotraj primarne lokacije, ki pa kljub vsemu ostaja neizbežna točka transporta.

Dvojno vpetje sistema v omrežje IP zahteva zelo napreden koncept omrežja, s povsem podvojenimi praktično vsemi komponentami (stikali, usmerjevalniki, požarnimi zidovi, izravnalniki prometa …). Podvojijo se tudi prenosne poti, število zasedenih vmesnikov pa se lahko v določenih primerih celo početveri (križno vpetje).

Poleg nedvomno prisotnega finančnega momenta je tukaj morebiti še bolj prisoten faktor znanja. Opisana rešitev namreč že za vzdrževanje in dnevne konfiguracijske posege potrebuje izjemno šolano ekipo strokovnjakov.

18. Arhitekturne pasti

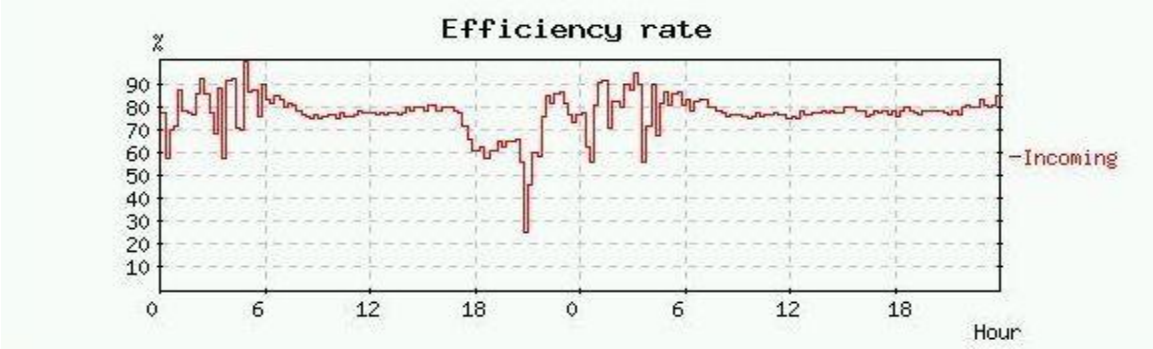
Obstajajo komponente sistema, na katere je potrebno biti (ob geografski redundanci) še posebej pozoren. Dober primer tega so medijski prehodi TDM, ki so sicer interno ščiteni z mehanizmi HA ter N+1, vendar so kot fizična enota nedeljivi. Ker je nesprejemljivo, da bi samo ena lokacija vsebovala medijski prehod TDM (s tem izničimo pomen geografske redundance), je potrebno zagotoviti podvojen prehod tudi za drugo lokacijo (ne glede na morebitno nezasedenost vmesnikov). S tem medijski prehodi efektivno postanejo »load sharing« naprave, ki pa so interno še HA varovane.

V primeru, da bi zaradi rasti števila naročnikov dodali še en MGC v georedundančno postavitev, bi tako potrebovali kar štiri medijske prehode!

19. Metode za nadzor in ugotavljanje napak

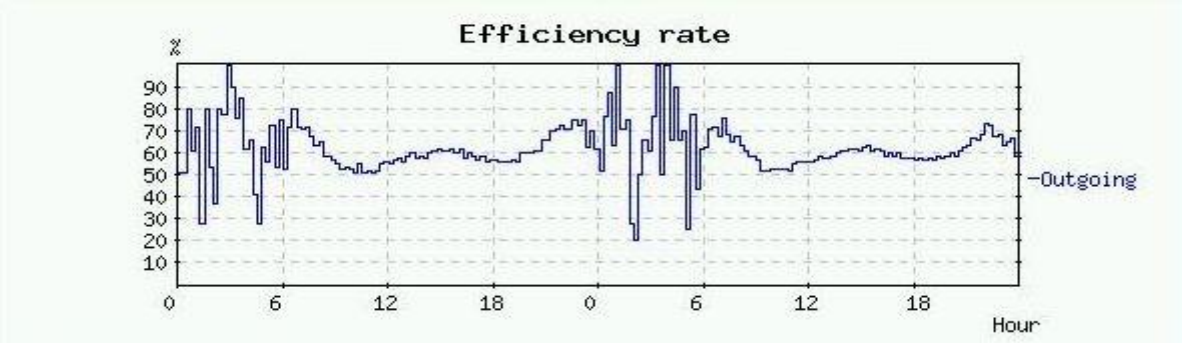
Brez izjeme so vsi zgoraj navedeni mehanizmi in ukrepi namenjeni preprečevanju izpada storitve, kar pa ne pomeni, da ne prihaja do napak. Če bi dopustili kopičenje (pojavljajočih se) napak, bi kmalu presegli redundančne zmožnosti sistema in s tem povzročili izpad storitve. Hitro in pravilno zaznavanje napak na sistemu je torej zelo pomembno. Uveljavljena metoda nadzora deluje s pomočjo protokola SNMP. Le-ta lahko deluje na dva načina – »SNMP traps« so pasti, ki se sprožijo ob vnaprej definiranem dogodku ali stanju, »SNMP poll« pa je mehanizem, ki pošlje sistemu periodične poizvedbe o vnaprej definiranih parametrih. Težava je v tem, da s pomočjo opisanih mehanizmov najpogosteje nadzorujemo fizično stanje naprav (ventilatorji, napajalniki, trdi diski …), kar pa nam ne pove praktično ničesar o pravilnosti delovanja procesov (tako tistih znotraj sistema kot tudi zunanjih, na katere nimamo vpliva, so pa pomembni za delovanje storitve). Prvi del nadzora in ugotavljanja napak je torej namenjen predvsem zaznavanju napak na fizični opremi, ki zaradi strojne podvojenosti (oz. kakega drugega mehanizma) ne vplivajo na uporabniško izkušnjo. V primeru izpada posamezne komponente storitev ni prizadeta, pride zgolj do povečane izpostavljenosti tveganju v primeru nadaljnjih odpovedi strojne opreme (ni več redundance).

Programske napake so bistveno težje za zaznavanje, obenem pa imajo tudi večje posledice. Odpovedi procesov (oz. napake v delovanju procesov, ki pa še ne sprožijo npr. »watchdog« mehanizma), nepravilne konfiguracije, preobremenitev posameznega strežnika, odpoved zunanjih podpornih sistemov in podobno so težave, ki se jih navadno ne da zaznati z jasnimi, vnaprej definiranimi kriteriji.
Zato smo izdelali lastno aplikacijo za nadzor delovanja storitve, merjeno skozi parametre uporabniške aktivnosti na sistemu (kot celoti). Ideja temelji na dejstvu, da je pri zadostnem številu uporabnikov obremenjenost sistema (oz. spremljanih parametrov) statistično zelo pravilna in ponovljiva. Tako npr. lahko na osnovi števila hkratnih klicev (»concurrent calls«), povprečnega trajanja klicev (»Average Call Duration«) in razmerja med uspešnimi ter neuspešnimi klici (»Answer/Seizure Ratio«) sklepamo na pravilnost delovanja storitve oz. sistema kot celote (ob upoštevanju primerljivih časovnih intervalov). Vsako večje odstopanje od zabeleženih vrednosti v preteklih (primerljivih) časovnih obdobjih sproži opozorilo, na osnovi katerega upravitelj sistema lahko hitreje reagira in prepreči morebitni daljši izpad storitve (do motnje storitve je očitno že prišlo). Na sliki 11 vidimo primer grafa ob težavah oz. nedelovanju enega od medijskih prehodov (lepo je viden strm padec v učinkovitosti malo pred 18h).



Slika 11 – Graf parametra ASR v primeru težav.

Pa vendar, tudi ta sistem za zgodnje zaznavanje težav ima pomanjkljivost – nočni interval. Ponoči je namreč tako malo prometa, da vhodni podatki niso statistično zanesljivi. Primer na sliki 12 nam kaže gibanje parametra ASR v nočnem času (npr. med 00 h in 06 h), ko je zaradi premajhnega števila klicev povsem nezanesljiv in statistično ni relevanten. Taki dogodki ne smejo sprožiti alarma.



Slika 12 – Gibanje parametra ASR v nočnem času.

20. Vzdrževalna pogodba kot del zagotavljanja razpoložljivosti sistema

V trenutku, ko težave presežejo znanje upraviteljev sistema, je pomembno imeti vzdrževalno pogodbo, ki nam omogoča, da se obrnemo na integratorja/dobavitelja (tipično drugi nivo podpore) ter po potrebi tudi na proizvajalca sistema (tretji nivo podpore). Podpora, ki nam jo zagotavljajo, je v večini primerov bolj informativne narave in ni urgentna, občasno pa se kljub vsem zgoraj naštetim ukrepom zgodi, da pride do večje odpovedi sistema. V takih trenutkih je ključnega pomena, da nam vzdrževalna pogodba zagotavlja jasne odzivne čase (»Time to Respond«), čase odprave napake (»Time to Repair«) ter nivo storitev, ki jih potrebujemo. Da bi lahko ponudnik vzdrževalne pogodbe zagotovil vse našteto, mora imeti na voljo ustrezen kader, zadostno zalogo rezervnih delov ter demo sistem, na katerem je mogoče določene postopke simulirati, preden se jih izvede v produkciji. Žal se v praksi pogosto pokaže, da dobavitelji/integratorji pri visoko specializiranih sistemih (kamor nedvomno spadajo tudi sistemi VoIP) zelo težko zadostijo navedenim zahtevam (predvsem je težava v kadru), zato je še toliko bolj pomembno, da pogodba vključuje tudi podporo samega proizvajalca opreme.

Na tem mestu velja omeniti še težavo, na katero lahko naletimo v heterogenih sistemih (sestavljenih iz opreme dveh ali več proizvajalcev). Če gre za dvoumno oz. težje dokazljivo napako, neskladje v standardih, ki je lahko posledica različne interpretacije, in podobno, se nam lahko zgodi, da dobavitelj opreme A vali krivdo na opremo proizvajalca B (in obratno). V takih primerih se pogosto zgodi, da je breme dokazovanja napake na nas, kar negativno vpliva na čas odprave napake.

21. Zadnji izhod – varnostna kopija naročniške baze in nastavitev

Za konec nam ostane še najbolj črn scenarij – uničenje vseh podatkov na strežnikih. Razlog je lahko bodisi programske (virus, huda napaka upraviteljev sistema, malomarnost …) ali pa fizične narave (požar, poplava, okvara več trdih diskov hkrati …). Ne glede na vzrok je težava oz. posledica enaka: strojno opremo je možno (kljub daljšemu izpadu storitve) nadomestiti, konfiguracijskih podatkov in naročniške baze (vključno z vsemi osebnimi nastavitvami) pa ne, zato je nujno vzdrževati varnostno kopijo podatkov, ki nam omogoča, da tudi v primeru povsem nove strojne opreme obnovimo sistem v stanje pred nezgodo. Tako kopijo sistema je najbolje hraniti v t. i. varni sobi, ki je zaščitena pred še tako neugodnimi zunanjimi vplivi (in človeškimi posegi).
Navedeni ukrep je povsem zadnji izhod, ki nam omogoča, da tudi v primeru najbolj črnega scenarija (kljub verjetno obsežni časovni prekinitvi storitve) obnovimo sistem brez izgube najpomembnejšega – podatkov. [1]

Zaključek

Te dni mineva pet let, odkar smo v SiOL-u (pod okriljem Telekoma Slovenije) postavili Cirpack programsko stikalo v produkcijsko okolje. Gledano nazaj skozi čas je jasno, kako veliko se je bilo treba naučiti spotoma, tudi na napakah. Proces učenja in izboljšav na sistemu pa še zdaleč ni zaključen. Prej bi rekel, da je neke vrste zanka; zanesljiv sistem (kvalitetna storitev) prinese več naročnikov, več naročnikov prinese nove, drugačne, večje izzive. Tako se zopet vrnemo v fazo učenja in nadgrajevanja sistema.

Žal (ali pa na srečo) merodajne statistike izpadov sistema ni možno navesti, saj so enostavno preveč redki. Z gotovostjo lahko trdimo, da je čas izpada sistema kot celote manj kot ena ura na leto, kar zadostuje za nazivno 99,99 % zanesljivost delovanja. Kje torej leži razlog za občasno nezadovoljstvo uporabnikov s storitvijo?

Praksa je pokazala, da težave relativno redko tičijo (zgolj) v strojni opremi. Sklop zgoraj navedenih (predvsem arhitekturnih) ukrepov poskrbi za zadostno robustnost sistema, ki je v stanju premostiti izpad praktično katerekoli posamezne (pogosto pa tudi več kot ene) komponente. Uporabniki takega izpada najpogosteje niti ne zaznajo, v najslabšem primeru pa sistem ostane brez določenega dela kapacitet, kar se lahko demonstrira v ozkem grlu na storitvi. V takih primerih je zelo pomemben pravočasen in predvsem ustrezen odziv upraviteljev sistema, saj lahko neustrezen odziv spremeni obvladljivo težavo v neobvladljivo, izpad strežnika pa v izpad storitve.

Bistveno pogosteje kot na strojni opremi, se težave pojavljajo s programsko opremo in nastavitvami. V grobem bi lahko težave razdelili na napake v nastavitvah, ki se jim načeloma lahko izognemo in napake v programski opremi, ki jih je potrebno hitro zaznati in točno diagnosticirati. Oba tipa napak se lahko pojavita v obliki, ki ne povzroča neposrednega izpada, temveč zgolj (občasno) nepravilno delovanje storitve. Takim napakam bi lahko rekli tudi »neusklajenost delovanja«.
Ker v takem primeru izpada na sistemu ni, uporabniku pa storitev ne deluje (oz. deluje pomanjkljivo), je očitno ravno tukaj bistvo razhajanja med uporabnikom in upraviteljem sistema, glede dojemanja zanesljivosti delovanja sistema / storitve.

Odgovornosti za »neusklajenost delovanja« ne kaže zgolj pavšalno pripisati upraviteljem sistema. Precej pogosto se zgodi, da posamezna programska komponenta ne sledi dosledno standardom za svoje področje. Odprava teh vrst napak je naporna, dolgotrajna in zahteva intenzivno sodelovanje dobavitelja opreme.

Kljub zgoraj naštetemu menim, da je prevladujoč vzrok za izpade na storitvi ravno človeški faktor. Naknadna analiza težav pogosto pokaže, da bi se dalo določeno situacijo predvideti, preprečiti, ali pa bolj učinkovito rešiti.

Verjamem, da so strojne in programske rešitve za zagotavljanje visoke razpoložljivosti sistemov (VoIP, pa tudi drugih) potreben, ne pa tudi zadosten pogoj. Ključnega pomena so človeški viri, ki morajo s strokovnim znanjem slediti razvoju tehnoloških rešitev, obenem pa morajo ob čedalje večji specializaciji na svojem področju biti v stanju aktivno (in strokovno) sodelovati z upravitelji drugih (podpornih) sistemov. Ker vse to zahteva velike finančne investicije, bomo v bodoče priča poenotenju storitev in združevanju manjših sorodnih sistemov v večje (z namenom boljše izrabe obstoječih virov).
Kljub vsemu pa se zdi, da obstaja neka razumna meja, h kateri je smiselno stremeti glede zanesljivosti oz. razpoložljivosti sistema. Vsi nadaljnji ukrepi postanejo izjemno dragi, učinek pa je v praksi težko merljiv (če že ne izničen s človeškimi napakami).

Seznam slik in tabel

Literatura

[1] K. Jayaswal, "*Administering Data Centers: Servers, Storage and Voice over IP"*, Indianapolis, Wiley Publishing, Inc., 2006

[2] R. Miller, "*How Much Time, Once the Cooling Fails?"* 2008, dostopno na: http://www.datacenterknowledge.com/archives/2008/02/08/how-much-time-once-the-cooling-fails/

[3] (2009) Cirpack Public Telephony Switches, High Availability. Dostopno na: http://www.thomsonbroadbandpartner.com/softswitch-ims-solutions/softswitch-ims-solutions/getfile.php?id=657

[4] (2009) Cirpack Public Telephony Switches, User Limiter. Dostopno na: http://www.thomsonbroadbandpartner.com/softswitch-ims-solutions/softswitch-ims-solutions/getfile.php?id=657

[5] (2010) High-availability cluster. Dostopno na: http://en.wikipedia.org/wiki/High-availability_cluster

[6] (2010) Redundancy - Engieering. Dostopno na: http://en.wikipedia.org/wiki/Redundancy_%28engineering%29

[7] (2010) OSI model. Dostopno na: http://en.wikipedia.org/wiki/OSI_model

[8] T. Vidmar, "*Informacijsko-komunikacijski sistemi*", Ljubljana, Založba Pasadena, 2002