UNIVERZA NA PRIMORSKEM

FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

PROJEKTNI SEMINAR II – POROČILO

Postavitev sistema za nadzor https://dev.mysql.com/downloads/

Pripravil: Duško Topić

JUNIJ 2017

Kazalo vsebine

1. UVOD

V tem dokumentu bo prikazano delovanje sistema ter procesa, kako se lotiti reševanja problema z zgodnjim odkrivanjem anomalij na komunikacijskih mrežnih napravah, pa tudi kako se s pomočjo ustrezno postavljenega nadzornega sistema lahko skrajša čas odprave napake ter posledično izpada delovanja informacijskih sistemov.

Komunikacijske mrežne naprave so vse naprave, ki služijo komunikaciji informacijskega sistema:

- Usmerjevalnik (ang. *router*)
- Požarna pregrada (ang. *Firewall*)
- Stikalo (ang. *switch*)
- Dostopna točka (ang. *access point*)

V sklopu projekta bodo prikazane tehnične zahteve za postavitev nadzornega sistema, opisane bodo tudi spremembe v izvorni kodi zaradi prilagoditve določenih modulov. Na koncu bo predstavljenih še nekaj primerov uporabe na realnih primerih v praksi.

1.1. Razumevanje problema

Problematika pri spremljanju stanja komunikacijskih mrežnih naprav je v tem, da je ob pojavitvi anomalij potrebno ukrepati v čim krajšem možnem času, da bi preprečili morebiten izpad delovanja informacijskih sistemov. Ker je takih ključnih naprav več, je nemogoče ročno spremljati stanje, zato je potrebno postaviti sistem, ki bo samodejno pregledoval vse potrebne lastnosti teh naprav.

Cilj projekta je postaviti tak sistem, ki bo znal opozoriti ob pojavitvi ključnih anomalij, da bi lahko pravočasno ukrepali ter preprečili morebiten izpad delovanja.

2. PRIPRAVA OKOLJA

Orodje, katero bo izvajalo nadzor mrežnih naprav, se imenuje Cacti[1]. Gre za odprtokodno rešitev za spremljanje stanja različnih senzorjev na mrežnih napravah, npr. zasedenost CPU, RAM, spremljanje prepustnosti (ang. *bandwidth*) na fizičnem vmesniku itd.

Na voljo je veliko podobnih orodij, a specifika Cacti-ja je ravno v odprtokodni rešitvi, konstantno se posodablja ter razvija prek svetovno znane platforme GitHub[2], poleg tega je možno lastnoročno prilagoditi module po lastnih željah oz. potrebah – kar bomo tudi naredili v nadaljevanju.

2.1. Tehnične zahteve

Konkretne strojne tehnične specifikacije strežnika za nemoteno delovanje sistema Cacti niso eksplicitno definirane, saj je odvisno od tega, koliko naprav ter v kolikšnem obsegu se bo sistem uporabljal. V splošnem zadostuje dvojedrni procesor z 2GB pomnilnika ter trdi disk velikosti 20GB. S tako postavitvijo je možno nadzorovati vsaj 600 naprav hkrati.

Cacti je sicer podprt tako na Windows kot Linux platformah, a je prilagojen uporabi na Linux različici, saj pri Windows operacijskem sistemu zahteva uporabo Cygwin[3] in podobnih orodij za simuliranje Linux okolja. Iz tega razloga smo se odločili za uporabo Linux distribucije CentOS.

Glede programskih zahtev, je potrebno imeti nameščeno naslednje:

- RRDTool: odprtokodni sistem za prikazovanje podatkov v obliki časovnih vrst
- MySql 5+: Odprtokodna podatkovna baza.
- PHP 5.1+: skriptni jezik, na katerem je postavljena spletna aplikacija Cacti
- Spletni strežnik s podporo PHP: Apache ali IIS.
- SNMP klient: klient za pridobivanje vrednosti stanja mrežnih naprav prek SNMP protokola (ang. *Simple Network Management Protocol*).
- Cron: Časovni razporejevalnik opravil

2.2. Namestitev sistema

Ko je strežnik pripravljen z zgoraj navedenimi strojnimi zahtevami ter nameščenim CentOS operacijskim sistemom, sledi namestitev zahtevanih programov, potrebnih za delovanje.

Na strežniku mora biti nameščena podatkovna baza MySql, različica vsaj 5, zadostujejo privzete nastavitve. Ob namestitvi se na podatkovni bazi ustvari uporabniško ime in geslo za dostop, katerega bo uporabljala aplikacija Cacti.

Nameščen mora biti tudi skriptni jezik PHP, različica vsaj 5.1, za naslednjimi razširitvami:

- Mysql: za poizvedbe v MySql bazo
- SNMP: za uporabo omenjenega protokola
- XML: za branje XML datotek
- Session: razširitev za vzdrževanje sej
- Sockets: za vzpostavitve sej
- LDAP: v primeru uporabe LDAP avtentikacije v aplikacijo
- GD: za obdelavo slik

Pogoj za objavo spletne aplikacije je spletni strežnik, predlagan je Apache, lahko se uporabi privzete nastavitve.

Namestitev Cacti aplikacije se izvede z razširitvijo datoteke »cacti-različica.tar.gz«, ki je dosegljiva na platformi GitHub. Pred prvo uporabo se v MySql podatkovno bazo uvozi privzeto Cacti bazo:

```
shell> mysql cacti < cacti.sql
```

V konfiguracijski datoteki, ki se nahaja v direktoriju »include/config.php«, je potrebno definirati podatke za povezavo na podatkovno bazo:

```
$database_type = "mysql";
$database_default = "cacti";
$database_hostname = "localhost";
$database_username = "cactiuser";
$database_password = "cactipwd";
```

Zadnji korak je vpis procesa za periodično poganjanje skripte, ki na definiran čas (npr. vsakih 5min) požene skripto za pridobitev novih vrednosti želenih parametrov na mrežnih napravah. Za ta del skrbi proces »crontab«. Primer vpisa procesa:

```
*/5 * * * * cactiuser php /var/www/html/cacti/poller.php > /dev/null 2>&1
```

3. FUNKCIJE

V tem poglavju bodo predstavljene bistvene funkcionalnosti sistema, potrebne za vsakdanje delovanje ter vzdrževanje sistema, od prijave do dodajanja naprav ter nastavljanja mejnih vrednosti za opozarjanje. Poleg tega bo opisana še prilagoditev izvorne kode, ki dodaja nove uporabne funkcionalnosti.

3.1. Programska koda

Kot že omenjeno, je Cacti odprtokodna rešitev, ki se neprestano razvija in je dosegljiva na portalu GitHub. Rešitev je modularna, kar pomeni, da obstajajo razširitve, ki ponujajo določene funkcionalnosti, ki jih uporabnik potrebuje. Med takimi razširitvami je potrebno izpostaviti razširitev »Thold«, ki spremlja dve zadevi:

- razpoložljivost naprav, kjer preverja, ali je naprava dosegljiva na podlagi ICMP protokola,
- nastavljene mejne vrednosti na dodanih grafih, npr. obremenjenost CPU.

Orodje je izredno uporabno ravno zaradi posredovanja opozoril prek e-pošte v primeru preseganja nastavljenih mejnih vrednosti, oziroma če je katera od naprav nedosegljiva. A pomanjkljivost rešitve je v tem, da sistem posreduje le opozorilo, ko je naprava nedosegljiva in ko je le-ta ponovno dosegljiva (DOWN/UP dogodki). Funkcionalnost, ki bi sistemskemu administratorju podala več informacij, je zaznava dogodka, ko pride do ponovnega zagona naprave (REBOOT dogodek).

Ker omenjena funkcionalnost ni implementirana v omenjeni razširitvi, bo potrebno prilagoditi izvorno kodo ter nekoliko razširiti podatkovno bazo z dodatnimi parametri. Najprej si oglejmo Sliko 1, ki prikazuje atribute v podatkovni bazi za tabelo »Host« - torej napravo ter za tabelo »thold_data«, ki beleži vse parametre, potrebne za zaznavo mejnih vrednosti. V tabeli »Host« smo dodali dva atributa:

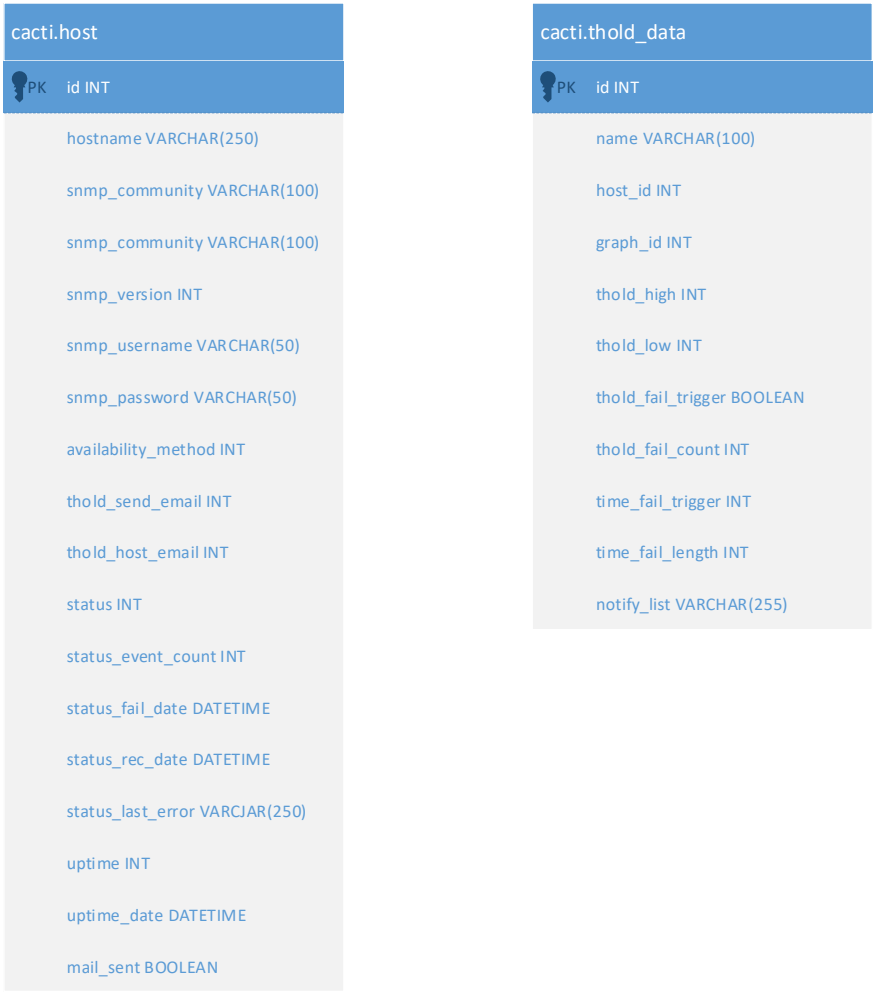
- uptime (INT): zabeležimo zadnjo znano vrednost, koliko časa je naprava dosegljiva, v sekundah
- uptime_date (DATETIME): zabeležimo datum, odkar je naprava dosegljiva.
- mail_sent (BOOLEAN): zabeležimo, da je sistem poslal obvestilo po e-pošti za REBOOT dogodek.

Prva dva parametra sta ključnega pomena za zaznavo REBOOT dogodka, saj prvi zabeleži zadnjo znano vrednost, ki jo pridobi od same naprave prek SNMP protokola, medtem ko drugi parameter zabeležimo ročno, torej v podatkovno bazo zapišemo datum, kdaj se je naprava nazadnje zagnala. Sistem nato primerja razliko med datumom zadnjega ponovnega zagona naprave s trenutnim datumom (vrednosti so pretvorjene v sekunde po UNIX timestamp formatu) – v kolikor je ta razlika večja od razlike med zadnjo vrednostjo razpoložljivosti

(uptime_new_int) ter trenutno vrednostjo razpoložljivosti (uptime_int), pomeni da se je naprava ponovno zagnala, torej je prišlo do REBOOT dogodka. Bistveni del izvorne kode se nahaja spodaj, kjer je navedena vejitvena zanka ter morebitna izvedba, torej pošiljanje e-pošte definirani skupini prejemnikov:

```
if($date_now - $uptime_date > $uptime_new_int - $uptime_int) {
      thold_mail($alert_email, '', $subject, $msg, '');
      db_execute('UPDATE host SET mail_sent=1 WHERE id='.$host['id']);
}
```

Na koncu še posodobimo vrednost atributa »mail_sent«, da preprečimo pošiljanje e-pošte za UP dogodek, ki bi ga zaznal v nadaljevanju iste funkcije.



Slika 1: ER diagram podatkovne baze Cacti.

Na desni tabeli v Sliki 1 je opisana še tabela »thold_data«, kjer se beležijo nastavljene mejne vrednosti za posamezen graf na posamezni napravi, zato imamo poleg atributa »host_id« zapisan še atribut »graph_id«, ki je v bistvu kazalec na sam graf. V kolikor se katera izmed vrednosti atributov »thold_high« ali »thold_low« preseže, se spremeni vrednost atributa »thold_fail_trigger« na TRUE, hkrati pa se pošlje e-pošta seznamu prejemnikov, zapisanih v atributu »notify_list«.

Oglejmo si še delovanje dveh bistvenih razredov celotnega sistema, razredni diagram se nahaja na Sliki 2.

Slika 2: Razredni diagram dveh najpomembnejših funkcij sistema.

Razred »poller« je srce sistema, saj periodično (običajno v intervalih 1min ali 5min), zažene funkcijo »exec_poll()«, kjer pridobi nove vrednosti vseh dodanih grafov ter posodobi izris le-tega. Ob enakih časovnih intervalih se periodično izvajata tudi funkciji »update_host_status« ter »check_all_thresholds« iz razreda »threshold«. Prva funkcija posodobi stanje vseh naprav, torej UP/DOWN/REBOOT. Zatem se izpelje druga funkcija, ki nad vsemi dosegljivimi napravami (UP in REBOOT status) pregleda vse nastavljene mejne vrednosti, ali jih trenutne vrednosti presegajo. V kolikor jih presegajo, sproži alarm ter pošlje e-pošto ustreznemu seznamu pošiljateljev.

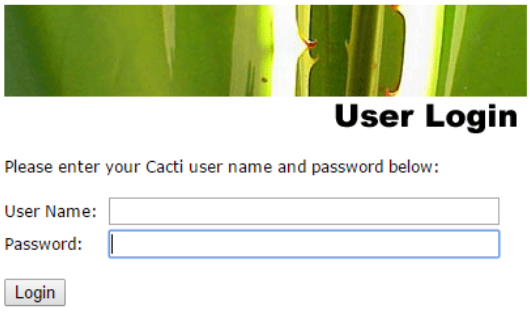
3.2. Spletni vmesnik

Sistem se upravlja na dva načina, administratorske zadeve na strežniku (npr. brisanje logov, ponovni zagon procesov itd.) se upravljajo s prijavo prek SSH protokola. Vse ostale zadeve, vezane na aplikativni del, se upravljajo prek spletnega vmesnika, ki bo predstavljen v nadaljevanju. Privzeta nastavitev je, da spletni vmesnik deluje prek nešifriranega HTTP protokola. S pomočjo dodatne razširitve je možno povečati stopnjo varnosti z uporabo varne šifrirane povezave.

3.2.1. Prijava v sistem

Prijava v sistem se lahko izvede na dva načina:

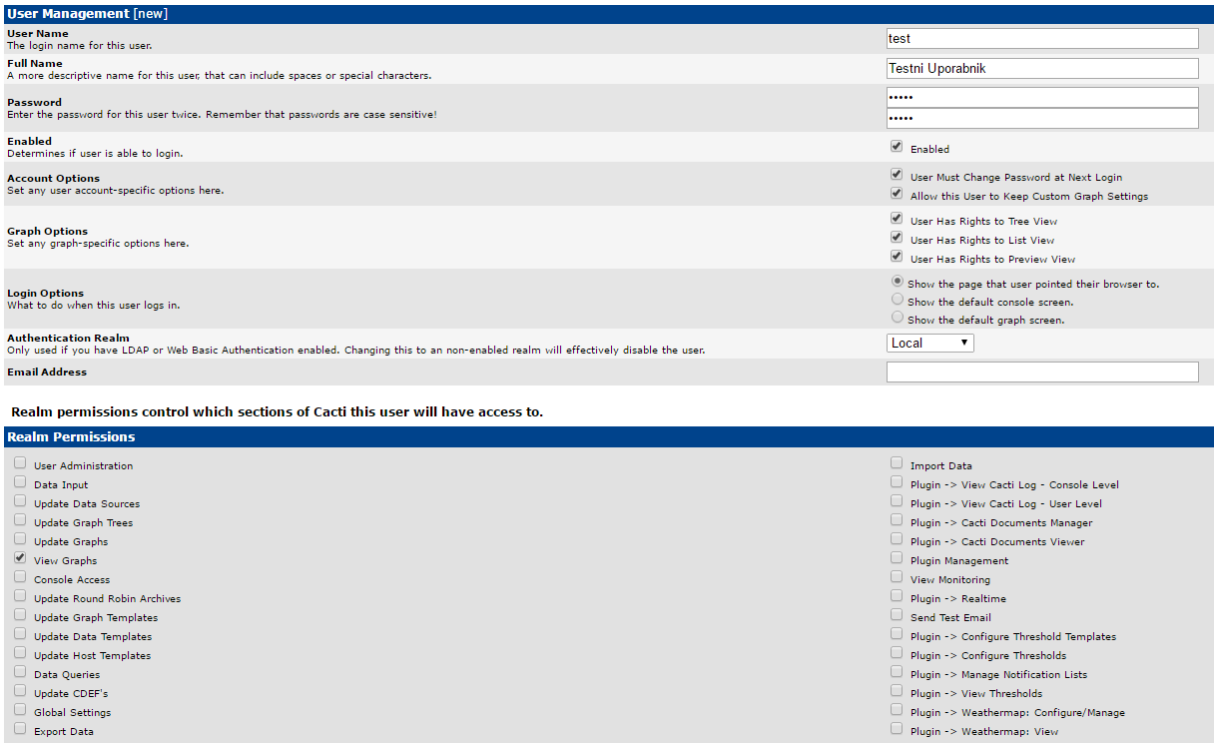
- lokalna avtentikacija z naborom lokalnih uporabnikov,
- LDAP avtentikacija, kjer se lahko uporabi poljuben nabor uporabnikov ali uporabniških skupin, definiranih na LDAP imeniku.



Slika 3: Prijavno okno.

3.2.2. Dodajanje uporabnika

Možnost dodajanja novih uporabnikov ter urejanja pravic imajo le administratorji sistema. Vse funkcionalnosti ter možne pravice uporabnika so razvidne v Sliki 4, kjer se nahaja obrazec za ustvarjanje novega uporabnika oz. urejanje njegovih pravic, če je uporabnik že kreiran.



Slika 4: Urejanje pravic uporabnika.

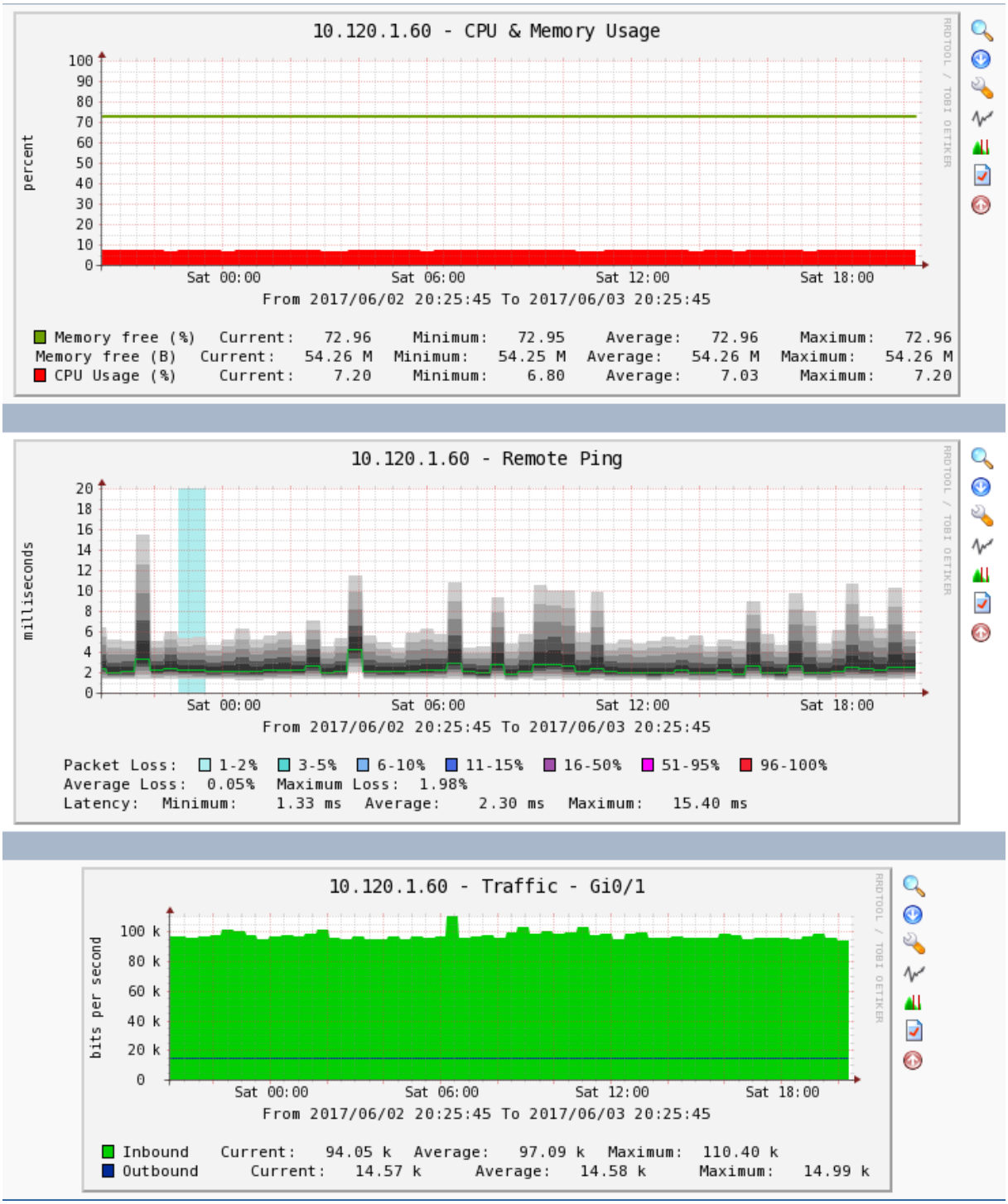
Pomembna možnost z vidika varnosti je ta, da se uporabniku ob prvi prijavi prikaže obrazec za spremembo gesla. Poleg tega je za vsakega uporabnika možno definirati, do katerih razširitev bo imel dostop ter ali bo možen samo vpogled, ali tudi urejanje nastavitev za posamezno razširitev.

3.2.3. Pregled grafov

Slika 5 prikazuje nekaj možnih izrisov vrednosti na grafu. Prvi graf hkrati spremlja obremenjenost CPU ter RAM na mrežni napravi. Na spodnjem delu grafa so izpisane 4 vrednosti za posamezen tip spremljanja: trenutna vrednost, najnižja, povprečna ter najvišja izmerjena vrednost. Na ta način se lahko ob pogledu na graf prepričamo, ali so trenutne vrednosti v mejah normale, ali pa gre za kakšno izstopanje. Ker pa seveda teh vrednosti ni možno ročno spremljati cele dneve, za to obstaja avtomatizem z nastavljanjem pragov – ta del bo opisan nekoliko kasneje.

Drugi graf na Sliki 7 beleži odzivnost sistema na ICMP pakete (oz. ping), v smislu odzivnosti ter deleža izgubljenih paketov. Zelena premica predstavlja povprečno vrednost skozi čas, črna vertikalna premica pa razpon med najvišjo ter najnižjo izmerjeno vrednostjo. Poleg tega graf beleži še delež izgubljenih paketov. Na ta način se na učinkovit način lahko pridobi občutek, ali je morebitno počasno delovanje informacijskega sistema morda posledica zakasnitev oz. izgub paketov.

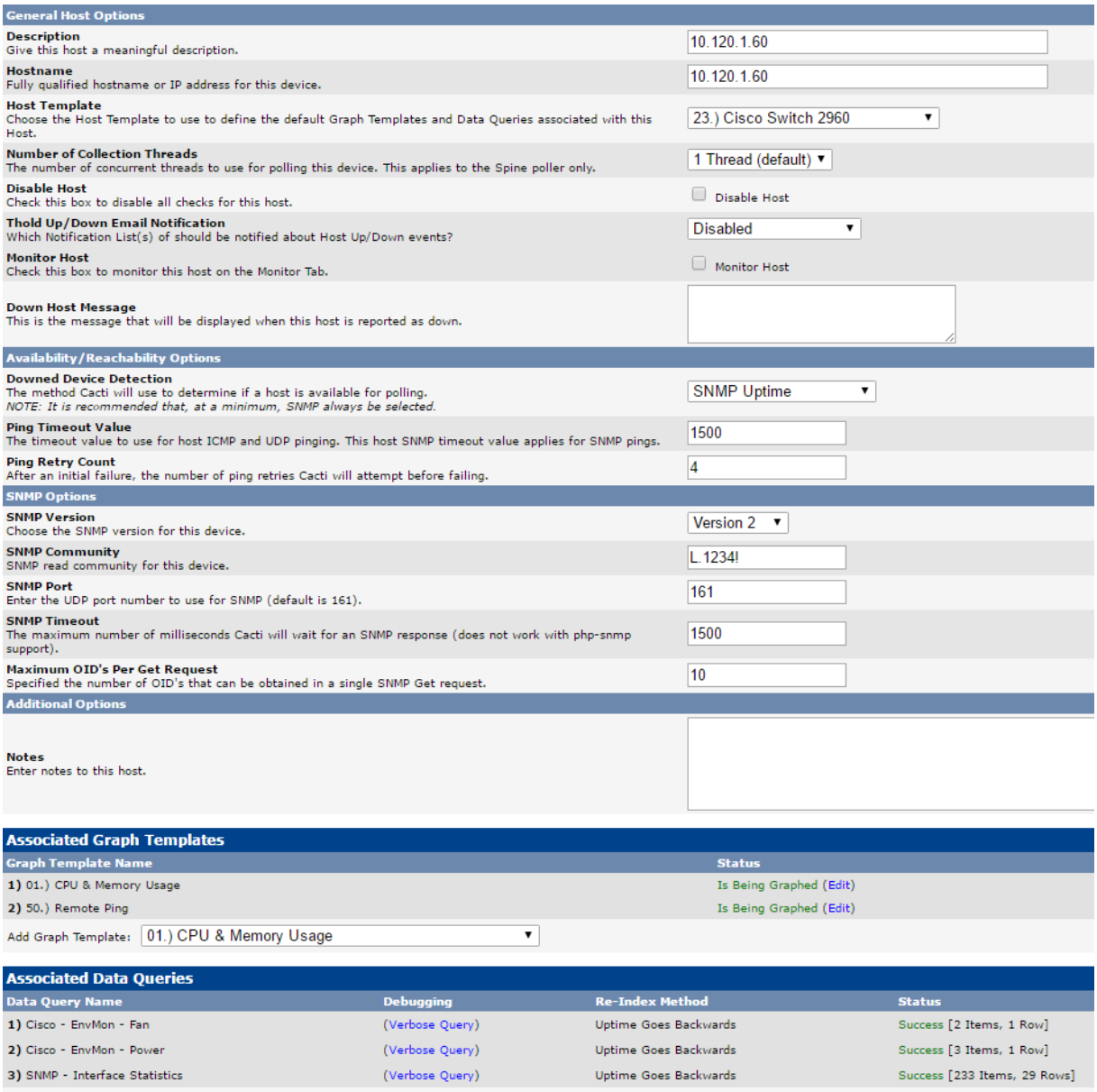
Tretji graf je prav tako izrednega pomena, saj prikazuje izmerjeno vrednost pretočnosti prometa (ang *bandwidth*) skozi fizičen vmesnik na mrežni napravi. Iz opisa naprave na tretjem grafu na Sliki 7 (napis »Gi«) je razvidno, da vmesnik podpira 1Gbit/s prepustnost, trenutno dosežena prepustnost pa je okrog 100kbit/s.



Slika 5: Primer prikazovanja vrednosti na grafih.

3.2.4. Dodajanje naprav ter grafov

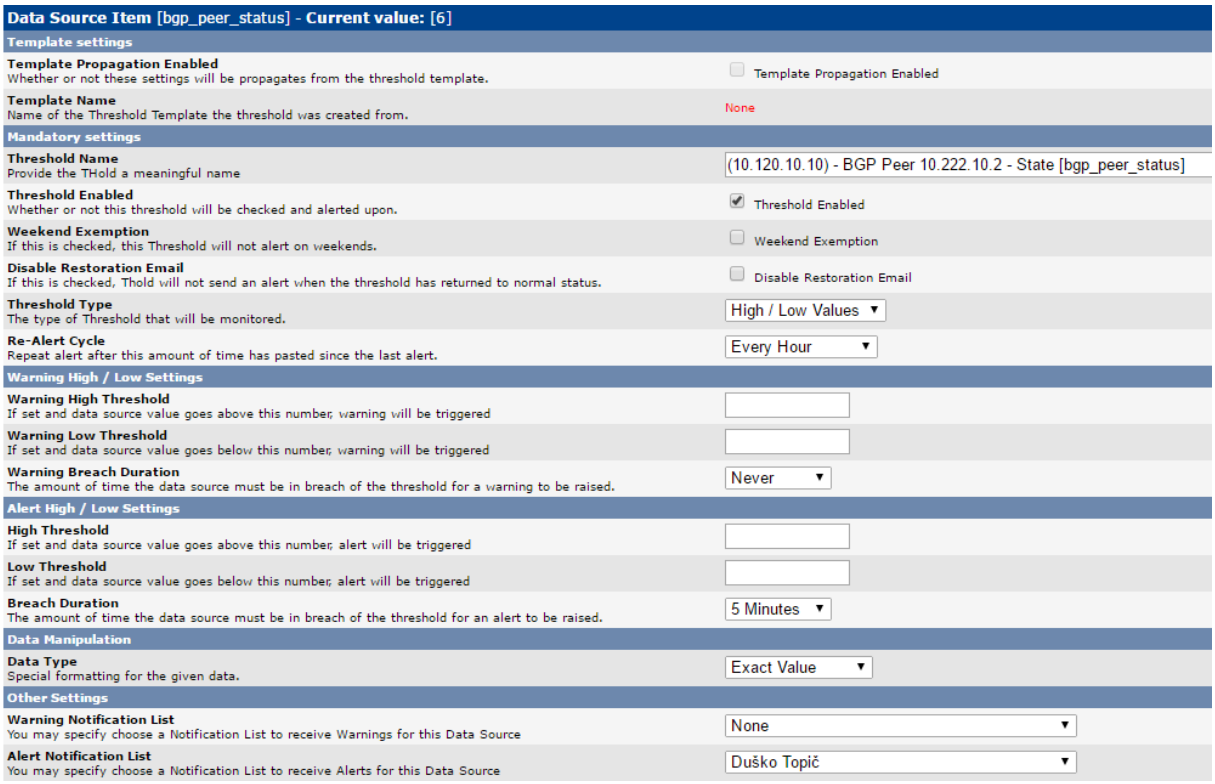
Možnost dodajanja novih naprav v sistem imajo le administratorji sistema. Primer izpolnjenega obrazca za dodajanje nove naprave se nahaja na Sliki 6. V prvem delu se definira ime naprave, IP naslov ter tip naprave iz nabora – na podlagi izbranega tipa se prednaložijo ustrezni grafi, ki se nahajajo v spodnjem delu na Sliki 6. V tem primeru je šlo za stikalo Cisco serije 2960. V istem obrazcu se definira tudi seznam uporabnikov, ki bodo prejemali e-pošto v primeru nedosegljivosti naprave (UP/DOWN/REBOOT dogodki).



Slika 6: Primer dodajanja nove naprave z ustreznimi grafi.

3.2.5. Nastavljanje pragov

Prag (ang. *threshold*) se imenuje razširitveni modul, ki samodejno pregleduje želene vrednosti na grafih, ter opozori v primeru, ko so nastavljene mejne vrednosti – imenujemo jih pragovi - presežene. V primeru preseženih vrednosti se samodejno pošlje e-pošta z vsebino, katera mejna vrednost je presežena. Na Sliki 7 se nahaja primer dodajanja praga z mejnimi vrednostmi za poljuben graf. Bistvene nastavitve so »High Threshold«, »Low Threshold« ter »Breach Duration«. S temi tremi nastavitvami nastavimo zgornjo oz. spodnjo mejo, ter po kolikšnem času naj se pošlje e-pošta, odvisno od stopnje kritičnosti preseženih vrednostih – lahko je od nekaj minut do nekaj ur.



Slika 7: Primer dodajanja novega praga z mejnimi vrednostmi.

Zgoraj je naveden primer ročnega dodajanja novega praga z ročnim vnosom mejnih vrednosti. V primeru, ko imamo več naprav in moramo hkrati za vsako napravo nastaviti enake mejne vrednosti na enakih grafih, bi tak postopek bil izjemno zamuden. Zato je poleg ročnega vnosa možno ustvariti predlogo (ang. *template*). V tem primeru ob enkrat definiramo vse želene vrednosti, ter apliciramo predlogo na vsakem posameznem grafu.

3.2.6. Pregled pragov

Seznam pragov ponuja pregled vseh nastavljenih vrednosti ter hiter pregled seznama tistih, ki so v trenutku ogleda presežene. Na Sliki 8 se nahaja primer seznama za nekaj grafov, kot so spremljanje obremenitve CPU, RAM ter zasedenosti diska. Z rdečo barvo so označeni tisti primeri, katerih vrednosti so trenutno presežene, z zeleno barvo pa tisti, katerih vrednosti so znotraj predpisanih.

Name	Type	High	Low	Trigger	Duration	Repeat	Current	Triggered**	Enabled
(10.120.8.19) - BGP Peer 10.227.10.1 - State [bgp_peer_status]	High/Low	10	-	*Never*		Every 8 Hours	3	yes	Enabled
(10.1.10.2) - 5 Minute CPU [5min_cpu]	High/Low	-	-1	*Never*		Every 12 Hours	-	no	Enabled
(10.120.2.133) - cisco free memory (proc) [cisco_mem_free]	High/Low	-	-1	*Never*		Every 8 Hours	19604320	no	Enabled
(10.120.1.205) - Used Space - /var/log [hdd_used]	High/Low	-	-1	*Never*		Every 4 Hours	37521399808	no	Enabled

Slika 8: Primer seznama nastavljenih pragov.

Potrebno je še omeniti, da je ta pogled seznama koristen predvsem za stranko oz. uporabnika informacijskega sistema, ko se želi prepričati, da mrežni del sistema nima posebnih odstopanj od običajnih vrednosti.

4. PROCESI

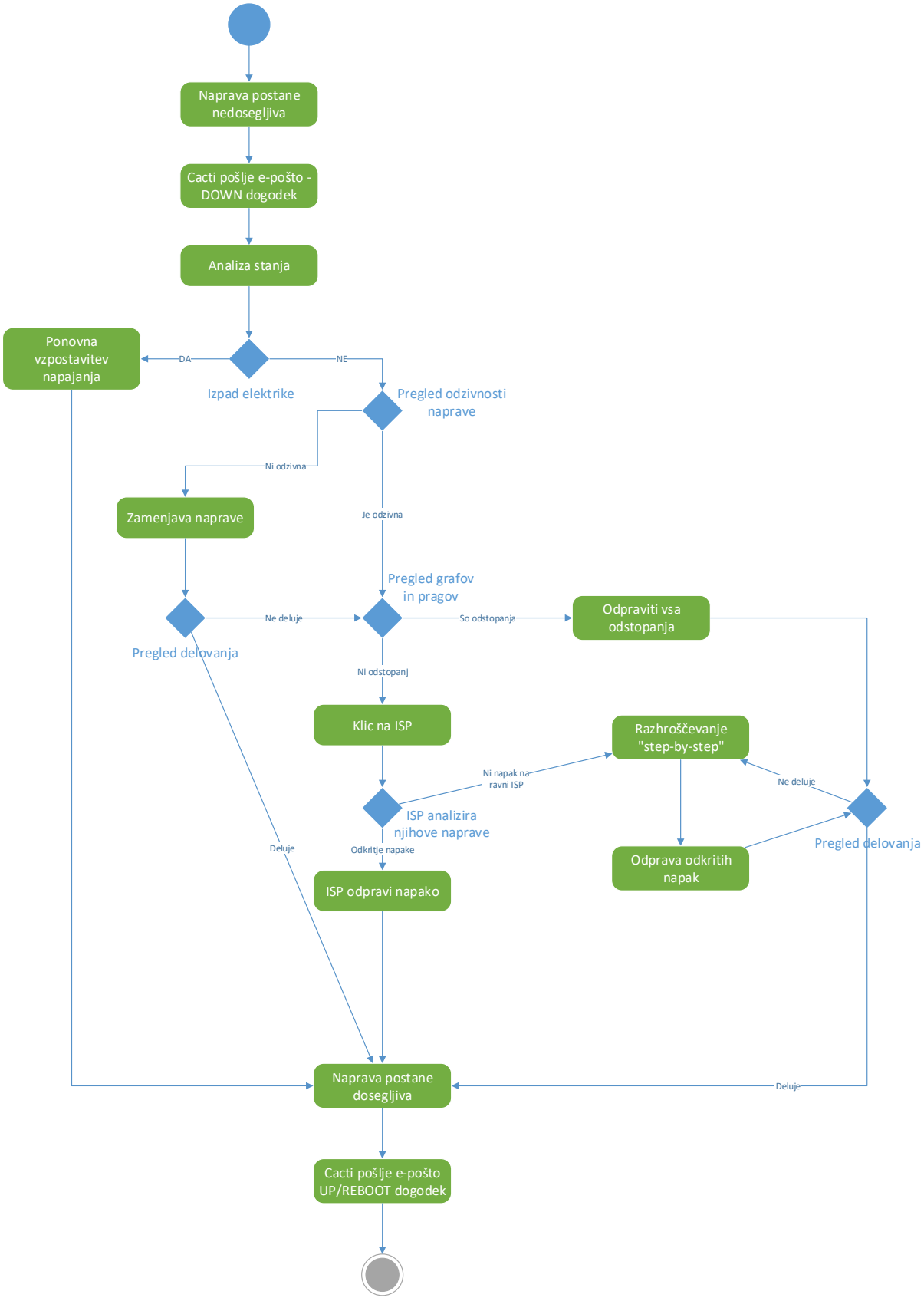
Prva faza projekta je implementacija ter ustrezna priprava sistema s primernimi pragovi itd. Na ta način si zagotovimo nek avtomatizem, da je sistemski administrator oz. vzdrževalec opreme v čim krajšem roku ustrezno obveščen o pojavitvi anomalij oz. izpadov v mrežni infrastrukturi, ki lahko pomeni izpad informacijskega sistema v podjetju. Ampak samodejno obveščanje še ne odpravi težave. Naslednji koraki so prav tako ključnega pomena, saj je le na podlagi hitrega odzivnega časa ter organiziranega pristopa k reševanju odprave napake možno učinkovito preprečiti oziroma vsaj znižati čas izpada delovanja.

Zato projektu sledi še druga faza, in sicer definiranje procesnega modela. To pomeni, da je potrebno na nedvoumen način definirati, kaj je potrebno storiti v specifičnih primerih, ko pride do izpada ali preseženih vrednosti.

Prvi primer procesnega modela je definiran na Sliki 8. V uporabo pride v primerih, ko pride do nenapovedanega izpada dosegljivosti usmerjevalnika, ki je povezan neposredno v zunanje omrežje (internet). Prva dva koraka sta avtomatizirana, torej Cacti prek e-pošte obvesti sistemskega administratorja o izpadu dosegljivosti naprave. Administrator nato izvede analizo stanja, kjer preveri dosegljivost naprave prek javnega IP naslova. V kolikor je naprava dosegljiva, je lahko šlo za kratkotrajen izpad. V nasprotnem primeru se najprej preveri, ali je do mrežne naprave prisotno delujoče napajanje. Če je prišlo do izpada napajanja in v primeru, da ni zagotovljenega redundančnega oz. nadomestnega napajanja (npr. UPS, agregat), je potrebno počakati na povrnitev napajanja in naprava bi se morala samodejno povezati v omrežje.

V primeru, da ni prišlo do izpada elektrike, je potrebno pregledati odzivnost usmerjevalnika (statusne LED lučke itd.). V kolikor ni nobenega odziva, torej statusne lučke ne kažejo nobenih znakov delovanja, je zagotovo prišlo do fizične okvare usmerjevalnika. V tem primeru se na lokaciji zamenja napravo z novo, katero je seveda potrebno predhodno konfigurirati na enak način. Če se za tem korakom usmerjevalnik poveže v zunanje omrežje, je težava odpravljena, sicer sledi naslednji korak – pregled grafov in nastavljenih pragov na usmerjevalniku. Ta korak izpeljemo tudi v primeru, da statusne lučke delujejo in ne kažejo nobenih anomalij (torej zamenjava usmerjevalnika ni potrebna).

Ob pregledu grafov je praviloma hitro razvidno, ali je težava na nivoju internetnega ponudnika storitev (ISP) – simptom je praviloma povečan delež izgube paketov nekaj minut pred izpadom. V tem primeru se obvesti ustreznega ISP, naj analizira ter odpravi napako. V primeru, da se je na grafih odkrilo drugačna odstopanja (npr. pomanjkanje RAM, povečan CPU), jih je potrebno poskusiti odpraviti s ponovnim zagonom določenih procesov ali celotne naprave. V primeru, da tudi zatem naprava ni dosegljiva, je potrebno lokalno na usmerjevalniku izpeljati ti. postopek postopnega razhroščevanja (ang. *step-by-step debugging*), kjer se analizira celoten tok prometa in delovanja sistema. Ta korak se izvaja, dokler se ne odkrije napaka v delovanju, lahko poteka nekaj minut, v skrajnih primerih tudi do nekaj ur, če je potrebno vključiti podporo specialista s strani proizvajalca opreme. Ko se napaka odkrije, se jo odpravi in naprava bo ponovno postala dosegljiva, Cacti pa bo poslal e-pošto z UP ali REBOOT dogodkom, odvisno kateri primer se je zgodil.



Slika 8: Definiran proces za primer nenadnega izpada naprave.

Izpad delovanja usmerjevalnika zahteva specifičen tip procesa, saj je več možnih vzrokov in včasih ni najbolj enostavno locirati napako. Sedaj pa si oglejmo še definicijo procesnega

modela za primer, ko sistem Cacti pošlje e-pošto z dogodkom o preseženih mejnih vrednosti, torej ko mrežna oprema (in s tem informacijski sistem) še deluje, a lahko v kratkem pride do izpada, če ne izpeljemo ustreznih ukrepov. Proces je definiran na Sliki 9. Recimo, da smo nastavili prag, naj pošlje opozorilo, ko ena izmed dveh povezav med stikaloma postane neaktivna. To pomeni, da je aktivna samo še ena povezava. Običajen uporabnik tega izpada ne bo opazil, saj je celoten sistem še vedno delujoč prek preostale delujoče povezave. Če odpove tudi preostala delujoča povezava, pa pride do polnega izpada.

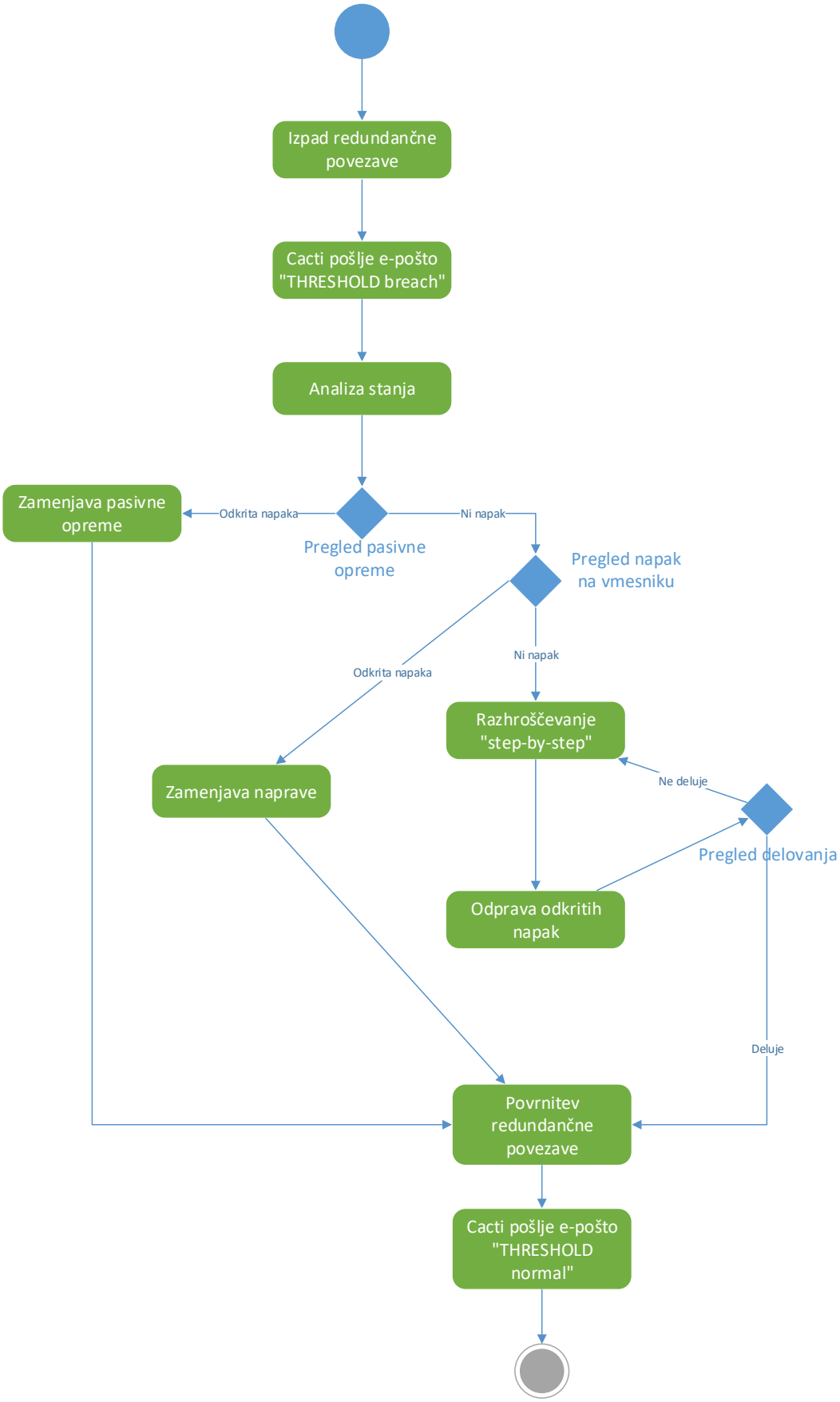
Ko administrator prejme e-pošto s takim obvestilom, najprej vzpostavi povezavo do naprave ter analizira stanje ali je zares prišlo do izpada povezave. Če je zares prišlo, je najprej potrebno preveriti morebitne težave s pasivno opremo (kabli, konektorji itd.). Če se odkrijejo kakšne fizične napake na pasivni opremi, se le-ta zamenja ter ponovno preveri delovanje.

V primeru, da napak na pasivni opremi ni, se je potrebno povezati na napravo ter preveriti stanje vmesnika, ali se morda pojavljajo kakšne vhodne napake, CRC itd. Če se odkrije napaka na samem vmesniku, je potrebno zamenjati celotno napravo, oziroma če to ni izvedljivo zaradi izpada delovanja drugih storitev, ki so vezane na to stikalo, potem se začasno vzpostavi povezavo prek drugega delujočega vmesnika, stikalo pa se zamenja npr. izven delovnega časa.

Če niti na vmesniku ni zaznanih napak oz. težav z delovanjem, je potrebno sprožiti postopek razhroščevanja, kjer se odkrije, v kateri fazi pride do napake. V nekaj primerih lahko pride tudi do primera, ko je izpad povezan z napako v programski opremi, zato je potrebna posodobitev le-te na novejšo različico. Postopek razhroščevanja se izvaja, dokler se napaka ne odkrije ter odpravi, takrat se sekundarna oz. redundančna povezava ponovno vzpostavi, Cacti pa pošlje obvestilo, da so mejne vrednosti praga ponovno v mejah normale.

Dva opisana procesa sta osnova za nadaljnje delovanje. Prvi proces je namenjen korakom v primeru, ko je naprava že nedosegljiva. V tem primeru je potrebno najprej preveriti delovanje napajanja ter vrednosti grafov v trenutkih pred izpadom delovanja. Na ta način se najbolj učinkovito odkrije vzrok, posledično se skrajša tudi čas odprave napake. V praksi se izkaže, da je v veliki večini primerov vzrok za nedelovanje izpad napajanja ali težave z ISP. Preostali koraki so opisani, a v praksi se izvedejo v manj primerih, kot je morda za pričakovati.

Drugi proces pa je namenjen izvajanju korakov, ko je naprava še dosegljiva in ko prejmemo opozorilo s preseženimi mejnimi vrednostmi katerega od pragov. Tu je praviloma nastavljenih veliko različnih pragov, a logika pristopa k reševanju težav je vedno taka, kot je opisano na Sliki 9. Torej ob prejetju opozorila se je potrebno najprej povezati na napravo ter pregledati dnevnik zapisov oz. loge, ali izpisujejo kakšno napako. V praksi se izkaže, da so današnje mrežne naprave bolj napredne, torej že v dnevniku zapisov beležijo morebitne napake v delovanju (npr. okvarjen ventilator, zato pride do povišane temperature, posledično je slabša odzivnost naprave). V primeru, da ni možno razbrati nič oprijemljivega, je potrebno preveriti delovanje pasivne opreme, ki lahko tudi povzroči težave z delovanjem (npr. zaradi slabšega vzdrževanja).

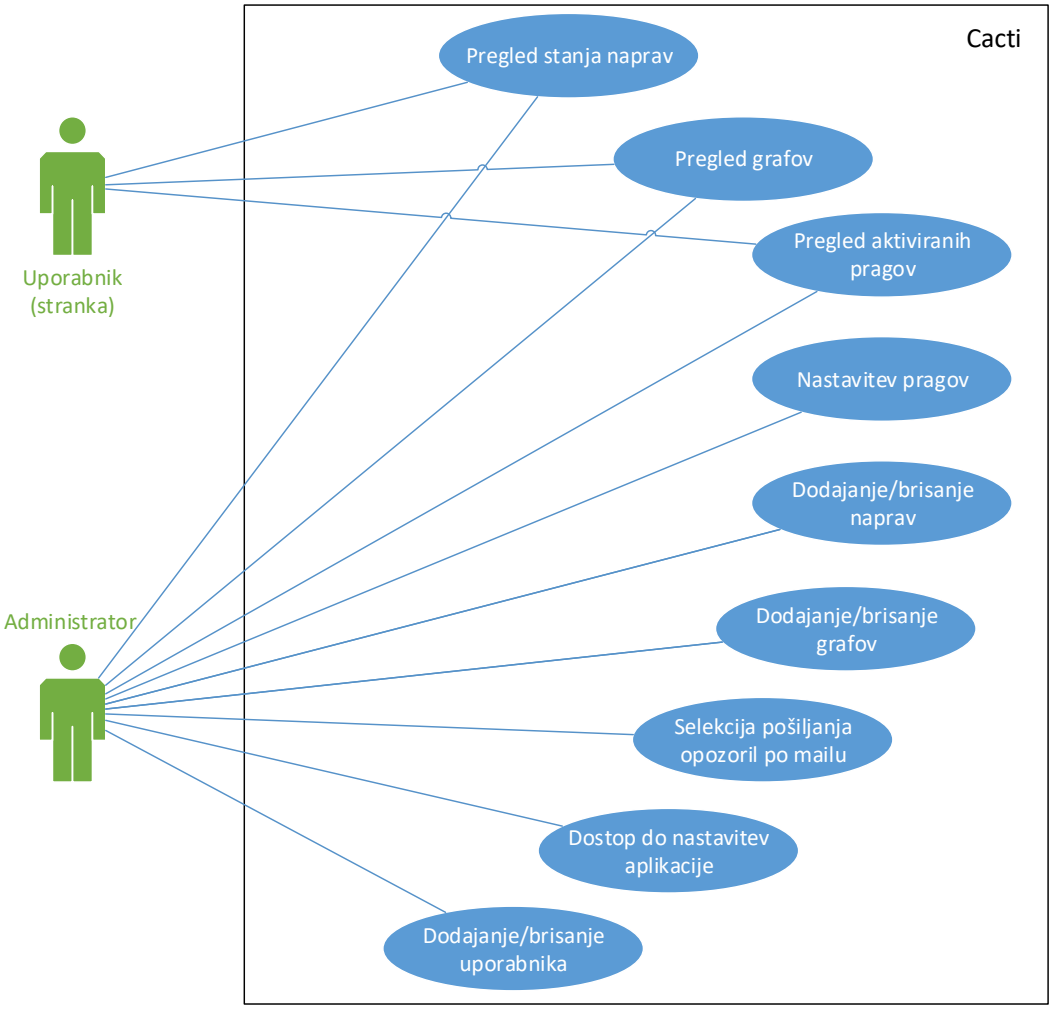


Slika 9: Definiran proces za primer zaznave izpada sekundarne povezave.

5. PRIMERI UPORABE

V tem poglavju bo opisanih nekaj konkretnih primerov uporabe aplikacije ter postopki odkrivanja ter odprave napak. Upoštevalo se bo logiko procesov, predstavljenih v prejšnjem poglavju. Za boljšo predstavo, kakšne so pravice uporabnika ter administratorja v sistemu Cacti, si najprej oglejmo diagram na Sliki 10, ki predstavlja diagram uporabe sistema Cacti. Pravice uporabe se delijo na pravice vpogleda ter pravice spreminjanja nastavitev. Običajen uporabnik (praviloma stranka oziroma uporabnik informacijskega sistema) ima vpogled v naslednje funkcionalnosti:

- Pregled stanja naprav, ali so vse naprave dosegljive oz. ali je katera naprava nedosegljiva,
- Pregled grafov, kjer lahko preveri, ali je odzivnost sistema sprejemljiva ter konstantna, torej da ni pretiranega nihanja v delovanju,
- Pregled pragov, kjer lahko preveri seznam nastavljenih pragov in ali je morda kateri aktiviran.



Slika 10: Diagram primera uporabe sistema Cacti.

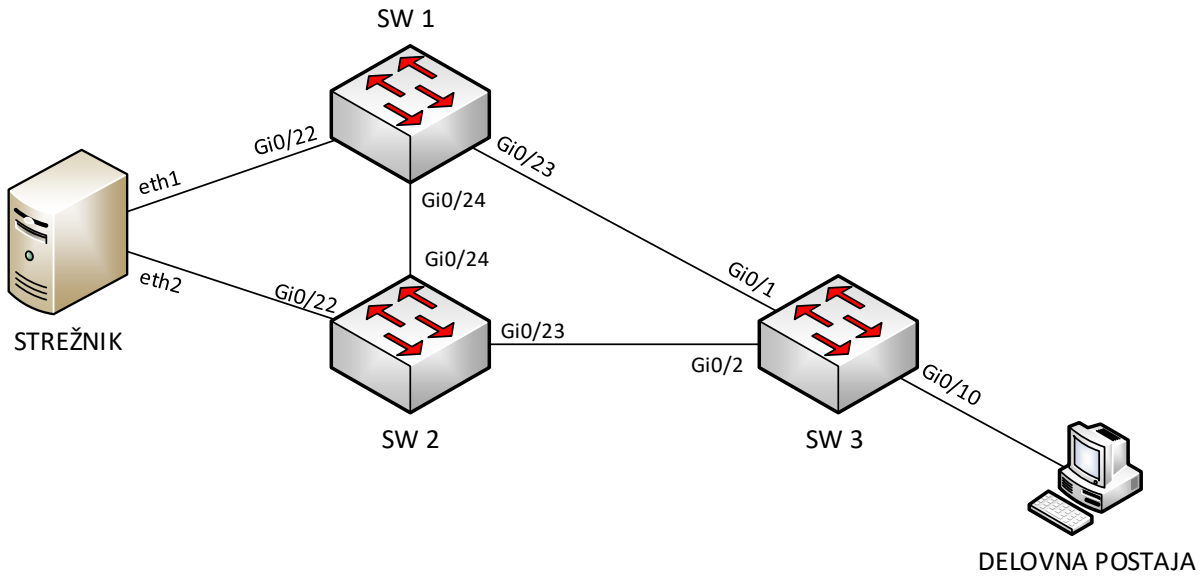
Če povzamemo, so pravice omejene, a običajen uporabnik dodatnih funkcionalnosti niti ne potrebuje, saj si želi imeti orodje, s katerim se lahko na kratek in jedrnat način z nekaj kliki prepriča, ali je delovanje sistema normalno.

Pravice administratorja pa so poleg pravic običajnega uporabnika, naslednje:

- Nastavitev pragov, lahko ročno ali po ustvarjenih predlogah,
- Urejanje naprav, torej dodajanje novih ali brisanje obstoječih naprav,
- Urejanje grafov, torej dodajanje oziroma brisanje grafov,
- Selekcija pošiljanja opozoril po e-pošti, to pomeni določanje seznama uporabnikov oz. administratorjev, ki bodo prejemali določena obvestila,
- Dostop do nastavitev aplikacije, kjer se definira način prijave v sistem, načini vizualizacije itd.
- Urejanje uporabnika, torej ustvarjanje novih ali brisanje obstoječih, dodelitev pravic.

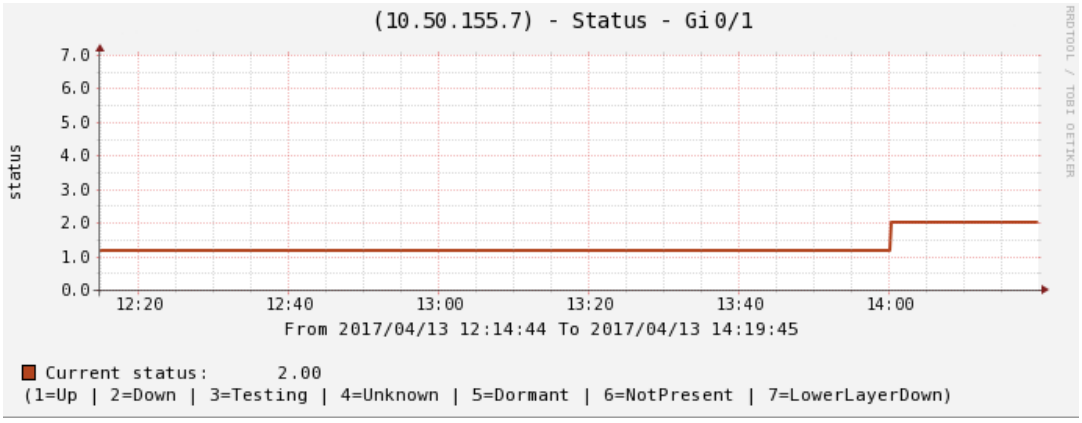
5.1. Primer 1

Oglejmo si primer delovanja sistema v praksi. Slika 11 prikazuje shemo omrežja, kjer so delovne postaje priključene na stikalo z oznako »SW 3«, to stikalo pa ima dve povezavi do stikal »SW 1« ter »SW 2« za zagotovitev dvojne oz. redundančne povezave, saj v primeru izpada ene povezave (npr. okvara stikala, okvara napeljave) uporabnik ne bo čutil izpada delovanja informacijskega sistema, saj bo do strežnikov lahko dostopal prek druge še delujoče povezave.



Slika 11: Shema omrežja za primer 1.

Sredi delovnega dne se zgodi, da pride do okvare UTP kabla, ki povezuje stikali »SW 1« ter »SW 3«, posledično povezava med omenjenima stikaloma preneha delovati. Uporabnik tega izpada ni zaznal. Cacti ob naslednjem ciklu osveževanja grafov spremeni vrednost stanja vmesnika iz 1 (UP) na 2 (DOWN), kot je razvidno na Sliki 12. Hkrati pošlje e-pošto skupini sistemskih administratorjev, ki je na ta način nemudoma obveščen o izpadu in prične z analizo stanja tako, da se najprej poveže na stikalo in preveri, ali je povezava zares nedosegljiva.

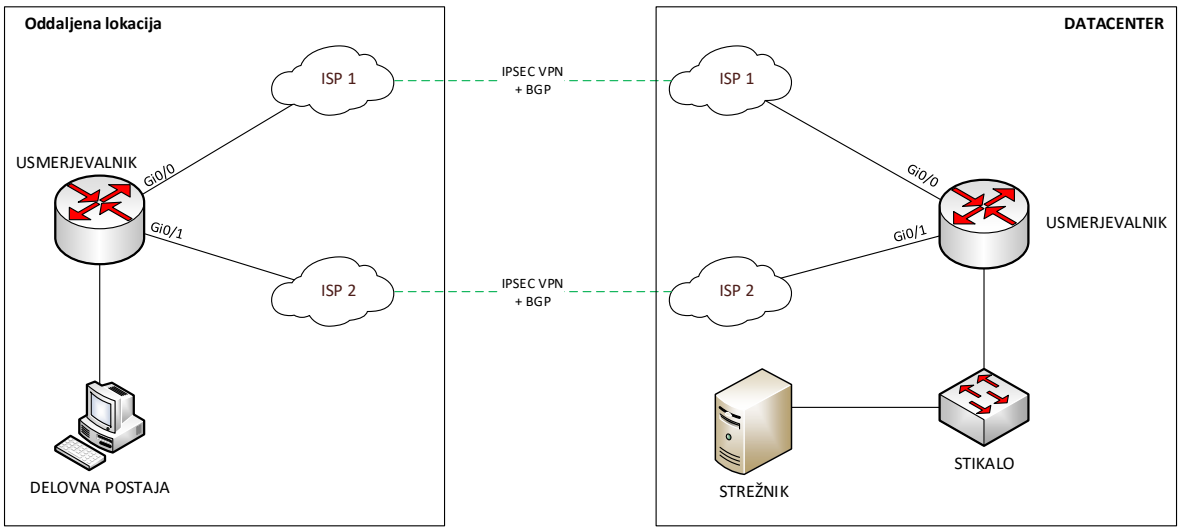


Slika 12: Graf, kjer spremlja vrednost stanja vmesnika na stikalu.

Ko se prepriča o resničnosti napake, odide na lokacijo in z ustreznim orodjem preveri ustreznost delovanja pasivne opreme, v tem primeru UTP kablov. Orodje prikaže okvare v fizični napeljavi, zato zamenja okvarjen kabel ter preveri delovanje. Povezava se s tem ponovno vzpostavi, ob naslednji osvežitvi grafa se vrednost ponovno vrne na 1 (UP) ter pošlje e-pošta z ustreznim obvestilom o povrnitvi praga v normalno stanje.

5.2. Primer 2

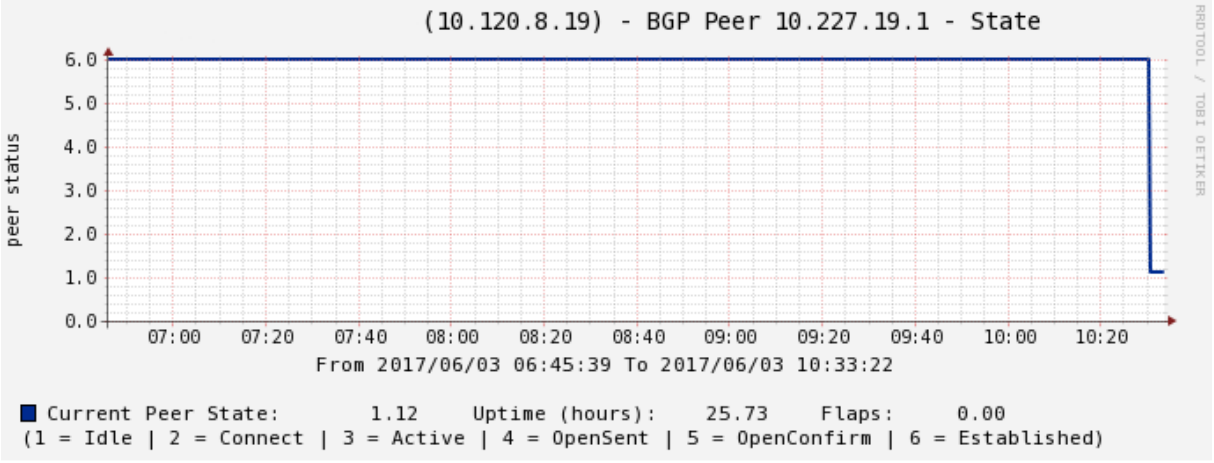
Pri naslednjem primeru imamo scenarij, ko imamo oddaljeno lokacijo, ki se povezuje do informacijskega sistema v Datacenter, ki se fizično nahaja na drugi lokaciji. Shema omrežja je prikazana na Sliki 13. Obe lokaciji sta med seboj logično povezani prek IPSEC VPN protokola ter BGP protokolom za dinamično usmerjanje. Obe lokaciji imata hkrati 2 ponudnika internetnih storitev za zagotavljanje nemotenega delovanja v primeru izpada enega izmed njih.



Slika 13: Shema omrežja za primer 2.

V tem primeru se zgodi, da nenadoma odpove povezava s primarnim ponudnikom internetnih storitev na oddaljeni lokaciji, na sliki je označen kot »ISP 1«. Cacti bo ob naslednjem osveževanju grafov med drugim spremenil vrednost grafa, ki je prikazan na Sliki 14 – graf spremlja stanje BGP protokola. Stanje z vrednostjo 6 pomeni, da je protokol aktiven, s tem

tudi dinamično usmerjanje, medtem ko stanje z vrednostjo 1 pomeni, da protokol ni aktiven, ker naprava ne najde svojega soseda (usmerjevalnik v datacentru) prek povezave »ISP 1«.



Slika 14: Graf, ki spremlja vrednost stanja BGP protokola.

V tem trenutku je informacijski sistem še vedno dostopen iz oddaljene lokacije prek sekundarnega ponudnika internetnih storitev, označenega z »ISP 2«. Cacti medtem zazna preseženo vrednost nastavljenega praga ter posreduje e-pošto z opozorilom. Sistemski administrator se poveže na usmerjevalnik na oddaljeni lokaciji ter analizira dnevniške zapise oz. loge. V zapisih zazna spodnji zapis:

```
Jun  3 10:33:00.913 UTC+2: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
Jun  3 10:33:01.730 UTC+2: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
Jun  3 10:33:15.775 UTC+2: %BGP-5-ADJCHANGE: neighbor 10.227.19.2 Down BGP Notification sent
Jun  3 10:33:15.775 UTC+2: %BGP-3-NOTIFICATION: sent to neighbor 10.227.19.2 4/0 (hold time expired) 0 bytes
```

Prvi dve vrstici pomenita, da je vmesnik z oznako »Gi0/0« postal neaktiven, kar pomeni, da je padla povezava s primarnim ISP. Posledično se z nekajsekundnim zamikom zapišeta še zadnji dve vrstici, ki pomenita, da BGP protokol ni več aktiven, ker prek ISP 1 ne vidi soseda na lokaciji v Datacentru.

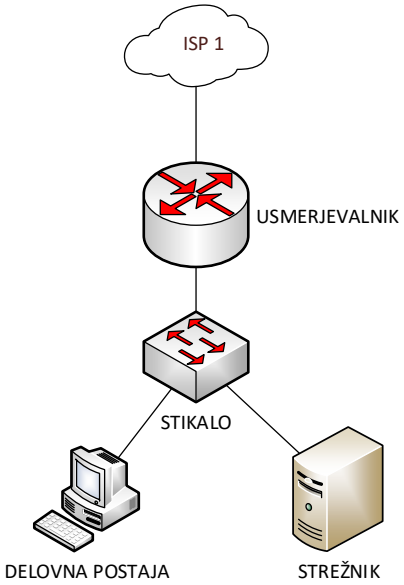
Administrator iz tega pride do sklepa, da je težava na strani primarnega ISP, zato ga tudi kontaktira ter opiše napako. ISP nato analizira stanje na njihovi strani ter potrdi in hkrati tudi odpravi napako na njihovi strani. Nekaj sekund kasneje se v dnevniškem zapisu izpiše spodnje:

```
Jun  3 11:10:39.100 UTC+2: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
Jun  3 11:10:40.106 UTC+2: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Jun  3 11:10:50.136 UTC+2: %BGP-5-ADJCHANGE: neighbor 10.227.19.2 Up
```

Iz teh zapisov je razbrati, da se je povezava ponovno vzpostavila.

5.3. Primer 3

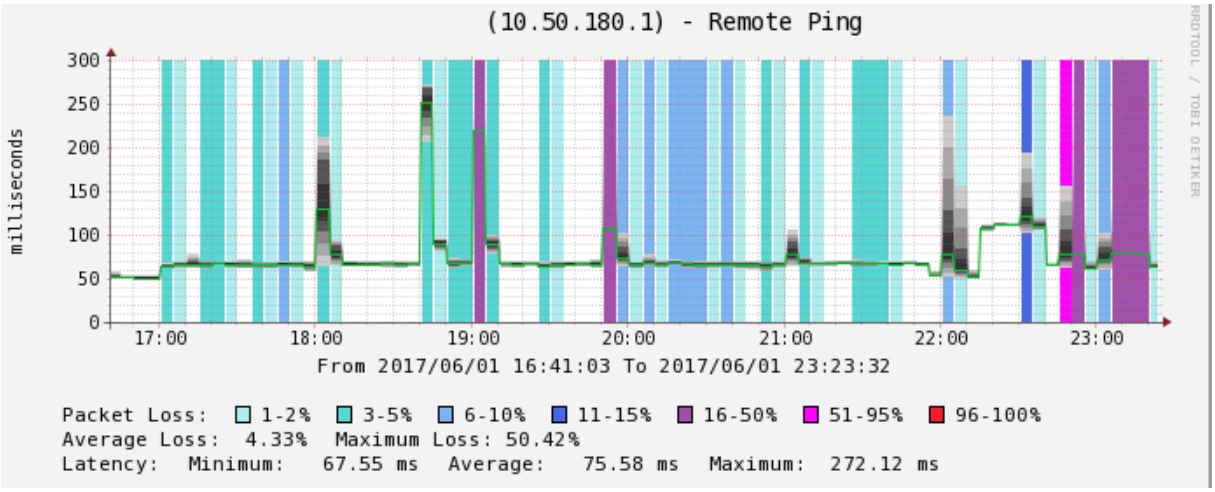
V tretjem primeru imamo klasično postavitev omrežja, kjer se uporabniki in strežnik z informacijskim sistemom nahajata v isti lokaciji, ISP ponudnik je tokrat le eden. Shema omrežja se nahaja na Sliki 15.



Slika 15: Shema omrežja za primer 3.

Pri tem scenariju pride do izpada ISP ponudnika ob 23:20 uri zaradi izjemno povečanega prometa proti internetu. Ker tokrat ni sekundarnega ponudnika, celotna lokacija postane nedosegljiva proti internetu, kar pomeni, da uporabnikom ne deluje dostop v internet, medtem ko sistemski administrator nima omogočenega oddaljenega dostopa do naprave, kar pomeni, da vpogled v dnevniški zapis na daljavo ni možen.

Cacti izpad zazna ob naslednjem osveževanju grafov ter pošlje opozorilo sistemskemu administratorju. Ta nemudoma pokliče relevantno osebo, ki se nahaja na lokaciji ter povpraša ali je morda prišlo do izpada napajanja. Ker izpada napajanja ni bilo, je potrebno preveriti, ali so kontrolne lučke na usmerjevalniku aktivne ali morda prikazujejo kakšno napako. Ker v tem scenariju napak ni bilo, pomeni da je naprava aktivna in delujoča, zato se loti pregledovanja grafov za napravo, da analizira stanje pred izpadom ter odkrije morebitne anomalije.



Slika 16: Graf, ki spremlja odzivnost naprave na ICMP protokol (ping).

Pri grafu, prikazanem na Sliki 16, ki prikazuje odzivnost naprave, je pred izpadom videti, da je predvsem v zadnjih nekaj minutah prišlo do večjih zakasnitev ter povečano stopnjo izgube

paketov. Ob pregledu grafa prepustnosti vmesnika proti internetu je zaznati, da je nekaj minut pred izpadom bila izjemno povečana količina prenesenih podatkov.

Stranko se obvesti, da uporabljajo preveliko prepustnost proti internetu, zato naj ugasnejo tisto storitev, ki porabi prevelik delež prepustnosti proti internetu. Po normaliziranju pretočnosti se povezljivost proti internetu povrne, Cacti pa pošlje obvestilo z »UP dogodkom«.

6. ZAKLJUČEK

V tem projektu smo postavili sistem Cacti z namenom skrajšanja odzivnega časa od pojavitve težav do pristopa k reševanju napake, predvsem po zaslugi samodejnega preverjanja preseženih mejnih vrednosti. Hkrati je definiran procesni model, ki jasno definira korake, ki jih je potrebno izpeljati za učinkovito reševanje problema.

Potrebno se je zavedati, da je tak sistem potrebno neprestano dopolnjevati ter posodabljati, saj le na tak način lahko dosežemo učinkovito delovanje in zadostimo sprotnim pojavljanjem potreb po novih vrstah razširitev.

Poleg razširitvenega modula »threshold« Cacti ponuja še cel nabor drugih modulov, ki so prav tako uporabni. Morda je vredno izpostaviti naslednje:

- GPS Map: ob dodajanju nove naprave se zapišejo še GPS koordinate, kjer se naprava nahaja. Tako lahko v primeru izrednih razmer, ko pride do izpada delovanja internetnih storitev v celotni regiji, hitro zaznamo, ali je vzrok za nedelovanje povezan s splošnimi težavami ISP,
- Weathermap: izris topologije omrežja, kjer so grafično razvidne prepustnosti med napravami.
- Clog: Cacti log, kjer imamo možnost vpogleda v dnevniške zapise Cacti sistema – razširitev pride v poštev predvsem v primerih, ko je sistem Cacti v težavah zaradi katerekoli napake.

7. LITERATURA

[1] Cacti – The Complete RRDTool-based Graphing Solution. http://cacti.net

[2] GitHub – The world's leading software development platform.
https://github.com/Cacti/cacti

[3] Cygwin. http. Mail: https://cygwin.com/index.html