UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

POLONA ANTONČIČ

MONITORIRANJE RAČUNALNIŠKIH OMREŽIJ

DIPLOMSKO DELO

UNIVERZITETNI ŠTUDIJSKI PROGRAM PRVE STOPNJE
RAČUNALNIŠTVO IN INFORMATIKA

LJUBLJANA, 2012

UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

POLONA ANTONČIČ

MONITORIRANJE RAČUNALNIŠKIH OMREŽIJ

DIPLOMSKO DELO

UNIVERZITETNI ŠTUDIJSKI PROGRAM PRVE STOPNJE
RAČUNALNIŠTVO IN INFORMATIKA

Mentor: izr. prof. dr. Miha Mraz

LJUBLJANA, 2012

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00007/2011
Datum: 05.09.2011

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

Kandidat: **POLONA ANTONČIČ**

Naslov: **MONITORIRANJE RAČUNALNIŠKIH OMREŽIJ**
COMPUTER NETWORKS MONITORING

Vrsta naloge: Diplomsko delo univerzitetnega študija prve stopnje

Tematika naloge:

Kandidatka naj v svojem diplomskem delu predstavi osnovne gradnike računalniških omrežij, problematiko njihovega monitoriranja in razpoložljiva programska orodja za izvajanje te dejavnosti. V nadaljevanju svojega dela naj izvede monitoriranje vzorčnega omrežja in predstavi dosežene rezultate.

Mentor:

prof. dr. Miha Mraz

Dekan:

prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

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

diplomskega dela

Spodaj podpisani/-a Polona Antončič,

z vpisno številko 63040004,

sem avtor/-ica diplomskega dela z naslovom:

Monitoriranje računalniških omrežij

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom (naziv, ime in priimek)

  izr. prof. dr. Mihe Mraza

  in somentorstvom (naziv, ime in priimek)

  _____

- 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«.

V Ljubljani, dne 14.3.2012 Podpis avtorja/-ice: _____

Zahvala

Zahvaljujem se izr. prof. dr. Mihi Mrazu za mentorstvo in pomoč pri izdelavi diplomske naloge.

Iskrena hvala tudi Jelki, Bojanu in Alešu, ker ste verjeli vame, mi stali ob strani ter mi nesebično pomagali.

Kazalo

Kratice in simboli

ARP: Address Resolution Protocol

GIS: Geographic Information System

GPL: General Public License

IP: Internet Protocol

ISP: Internet Service Provider

LAN: Local Area Network

MAC: Media Access Control

MIB: Management Information Base

NMS: Network Management System

OID: Object Identifier

OSI: Open Systems Interconnection

QoS: Quality of Service

RRD: Round Robin Database

SMI: Structure of Management Information

SNMP: Simple Network Management Protocol

SSH: Secure Shell

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

WAN: Wide Area Network

Povzetek

V diplomski nalogi z naslovom Monitoriranje računalniških omrežij so predstavljene osnove računalniških omrežij, namen in pridobivanje podatkov z naprav v omrežju, programska oprema za spremljanje ter primer monitoriranja realnega omrežja z nekaj desetimi mrežnimi napravami, kjer smo uporabili metrike za oceno kvalitete delovanja računalniškega omrežja.

Omrežja predstavljajo pomemben del v sodobni informacijski tehnologiji, služijo izmenjavi podatkov in virov, zato je njihovo brezhibno delovanje ključnega pomena.

Ob pravilni in učinkoviti konfiguraciji sistema lahko z monitoriranjem omrežja preprečimo izpade delovanja in hitro ukrepamo ob morebitnih težavah v omrežju. Prav tako pa si lahko pomagamo pri analizi, potrebni za morebitne nadgradnje ter vzdrževanju omrežja.

Abstract

The present thesis entitled Computer Networks Monitoring introduces the basics of computer networks, the aim and the computer data reclamation from networking devices, software for the system follow-up together with the case of monitoring a real network with tens of network devices.

The networks represent an important part in the modern information technology and serve for the exchange of data and sources which makes their impeccability of crucial importance.

Correct and efficient system configuration, together with the network monitoring can prevent failures and bring a quick response in case of potential network problems. In addition to the above mentioned it may help us with the analysis, necessary for the potential upgrading and network maintenance.

1. Uvod

Računalniška omrežja so ključna za povezovanje informacijske infrastrukture, tako lokalno kot globalno. So nepogrešljiv del sodobnih organizacij v zasebnem in javnem sektorju. Stalna razpoložljivost informacijskih storitev je velikega pomena za uspešno poslovanje. Z zanesljivostjo ter zmogljivostjo sta povezani tudi storilnost in donosnost, kar dosežemo le s premišljenim načrtovanjem ter vzdrževanjem omrežij.

Računalniška omrežja imajo velik vpliv na življenja ljudi v razvitem svetu. So pravzaprav tkivo, ki povezuje ostale gradnike infrastrukture, da lahko končni uporabnik dostopa do informacij in storitev. Z razvojem računalniških omrežij se je pojavilo veliko novih možnosti in storitev (računalništvo v oblaku, nakupovanje iz naslonjača, videokonferenčni sistemi, itd.). Ogromno pa je tudi takšnih, ki so obstajale že prej in so z razvojem računalniških omrežij bliskovito napredovale (televizija, telefonija, dostopnost izobraževalnih vsebin, itd.).

Monitoriranje oz. nadzor nad delovanjem informacijske infrastrukture lahko zmanjša težave na najmanjšo možno mero ali jih celo prepreči. Omogoča stalen vpogled v delovanje vseh vitalnih informacijsko-komunikacijskih gradnikov in storitev. Rezultati omogočajo pravočasno zaznavo napak ter pomoč pri optimizaciji in načrtovanju omrežij oz. informacijske infrastrukture.

Podrobno spremljanje omrežja omogoča identifikacijo odstopanj od pričakovanih ali priporočenih vrednosti monitoriranih parametrov ter pravočasno ukrepanje ob zaznanih napakah. Rezultate je potrebno pravilno ovrednotiti glede na tip, uporabo ter vlogo naprave v omrežju. S spremljanjem vitalnih parametrov mrežnih naprav lahko ocenimo prihodnje dogodke in tako preprečimo marsikatero težavo ali celo izpad v omrežju.

Pričujoče diplomsko delo obsega splošen opis računalniških omrežij, ki se nahaja v drugem poglavju in vključuje definicijo računalniškega omrežja, pregled topologij ter komponente. Tretje poglavje opisuje namen, pridobivanje podatkov in parametre spremljanja omrežij. Četrto poglavje ponuja pregled čez obstoječa programska orodja za monitoriranje ter podrobnejši opis orodja Cacti, ki smo ga uporabili za spremljanje realnega omrežja. Monitorirano omrežje ter rezultate enomesečnega spremljanja vzorčnih naprav smo grafično predstavili ter komentirali v petem poglavju. Pravilna razlaga ter korelacija dobljenih podatkov je ključna za pravilno razumevanje rezultatov ter njihovo uporabo v prihodnje.

2. Sestava računalniških omrežij

Računalniško omrežje je množica neodvisnih računalnikov povezanih z enotno tehnologijo. Dva računalnika lahko smatramo kot povezana, če med seboj lahko izmenjujeta informacije [1]. Računalniško omrežje sestavljajo mrežne naprave, prenosni mediji ter programska oprema. Namen povezovanja računalnikov v omrežja je prenos podatkov in izmenjevanje virov (strojnih, programskih, podatkovnih).

Najpreprostejša oblika omrežja sta dve napravi, med seboj povezani z eno povezavo. Pojem računalniško omrežje pogosteje označuje kompleksnejša omrežja z več različnimi mrežnimi napravami, ki med seboj povezujejo večje število osebnih računalnikov, strežnikov, sistemov za hrambo podatkov, itd. Vzdrževanje in nadzor omrežja sta zelo pomembna za učinkovito in zanesljivo delovanje porazdeljenih računalniških sistemov.

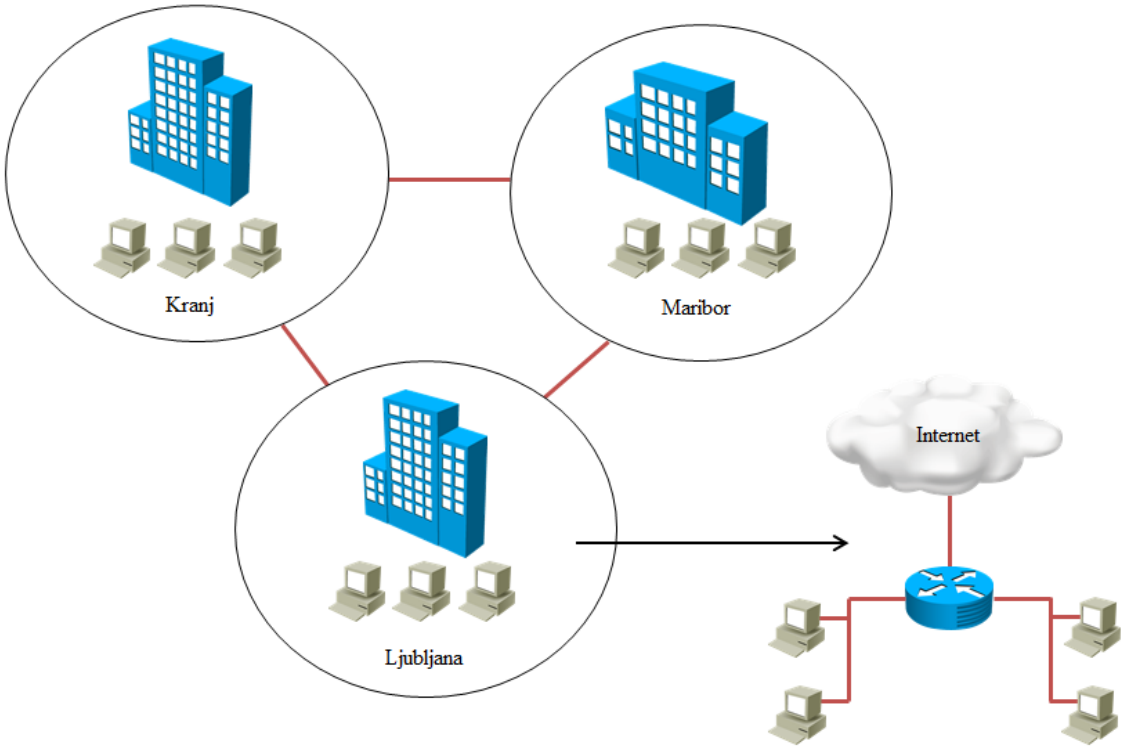
2.1. Delitev računalniških omrežij

Računalniška omrežja delimo glede na:

- lastništvo,
- oddaljenost in
- topologijo.

Glede na lastništvo omrežja delimo na javna in privatna, ki niso dostopna iz zunanjega sveta. Primer javnega omrežja je Internet, privatno omrežje pa je npr. omrežje podjetja ali organizacije.

Glede na oddaljenost delimo omrežja na lokalna (angl. *LAN – Local Area Network*) ter globalna ali prostrana omrežja (angl. *WAN – Wide Area Network*). Lokalna omrežja so omejena na radij nekaj sto metrov, globalna pa povezujejo naprave, ki so lahko oddaljene več kilometrov. Slika 1 ponazarja primer treh lokalnih omrežjih povezanih preko globalnega omrežja.



Slika 1: Prostrano in lokalno omrežje.

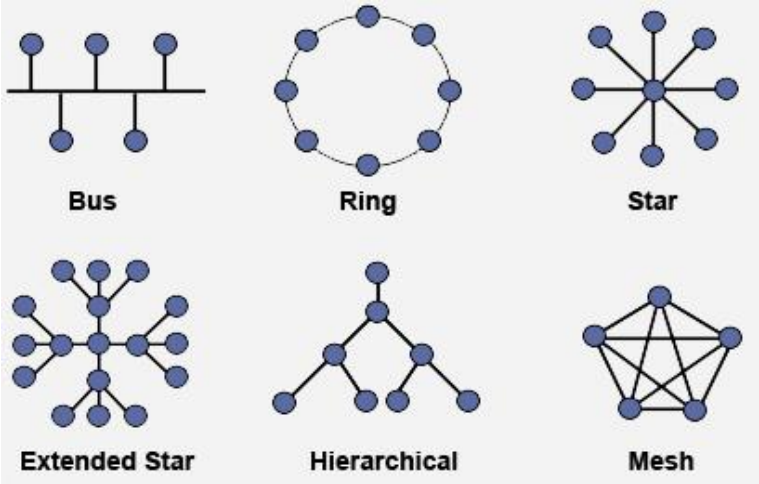
Naprave so v omrežje lahko povezane na več načinov s fizičnimi in logičnimi topologijami. Vsaka naprava lokalnega omrežja ima eno ali več povezav do ene ali več drugih naprav. Z mapiranjem povezav in naprav grafično predstavimo fizično topologijo omrežja. Logična topologija pa predstavlja tok podatkov. Fizična in logična topologija sta lahko v istem omrežju različni.

Seznam možnih topologij je sledeč [2]:

- vodilo (angl. *bus*) - vodilo povezuje med seboj vsa vozlišča, tako da vsa sprejemajo po mediju prenešena sporočila,
- obroč (angl. *ring*) - vozlišča so povezana samo z dvema sosednjima in skupaj tvorijo zaključeno povezavo v obliki obroča,
- zvezda (angl. *star*) - obrobna vozlišča so vezana na centralno vozlišče,
- razširjena zvezda (angl. *extended star*),

- drevesna (angl. *hierarchical*) - vozlišča so povezana samo z enim nadrejenim ter enim ali več podrejenimi vozlišči,
- zankasta (angl. *mesh*) - samodejno nastajajoča omrežja, ki poleg lastnega usmerjajo tudi promet drugih vozlišč.

Slika 2 prikazuje grafično ponazoritev zgoraj omenjenih topologij.



Slika 2: Grafična ponazoritev topologij v računalniških omrežjih [3].

2.2. Komponente računalniških omrežij

Računalniška omrežja so sestavljena iz pasivnih in aktivnih komponent.

2.2.1. Pasivne komponente

Pasivne komponente so tisti deli računalniškega omrežja, ki za delovanje ne potrebujejo električnega napajanja [4]. To so prenosni mediji oz. koaksialni, parični in optični kabli, ki s priklopom na aktivne komponente prenašajo električne ali optične signale.

Koaksialni kabli

Jedro koaksialnih kablov je sestavljeno iz bakrene žice (obdane z izolacijo), prepletenega kovinskega oklopa in zaščitnega plašča [5]. Oklop vsrkava motnje električnih signalov (šum), da ne pridejo do vodnika in ne motijo prenosa podatkov. Jedro prenaša električne signale, obdaja pa

ga električno neprevodni sloj, ki loči jedro od mrežne žice. Prepletena mrežna žica služi kot zaščita jedra pred električnimi motnjami in pred nezaželjenim signalom iz sosednje žice oz. presluhom.

Koaksialne kable se uporablja predvsem pri prenosu zvoka in videa ter prenosu podatkov na daljše razdalje.

Parični kabli

Sukana parica je sestavljena iz dveh izoliranih bakrenih žic, ki sta med seboj prepleteni. Po dva vodnika sta sukana v par, da se prepreči presluh. Več kot je zavojev na meter žice, manjša je možnost presluha. Več prepletenih parnih žic je pogosto sklenjenih skupaj in tvorijo parični kabel. UTP je najbolj uporabljen tip paričnih kablov v lokalnih omrežjih. Najdaljša razdalja, ki jo podpirajo kabli UTP, je približno 100 metrov.

Parične kable delimo v 6 kategorij, odvisno od hitrosti povezave [6]:

- Kategorija 1: vsebuje parične telefonske kable (lahko prenašajo glas, ne pa tudi podatkov),
- Kategorija 2 (razred A): za prenos podatkov več kot 4 megabitov na sekundo (Mb/s), sestavljena je iz štirih prepletenih parov bakrenih jeder,
- Kategorija 3 (razred B): za prenos podatkov več kot 16 megabitov na sekundo (Mb/s), kabli so sestavljeni iz štirih prepletenih parov bakrenih žic (trije zavoji na meter),
- Kategorija 4 (razred C): za prenos podatkov več kot 20 Mb/s,
- Kategorija 5 (razred D): za prenos podatkov več kot 100 Mb/s, kabli so sestavljeni iz štirih prepletenih parov bakrenih žic,
- Kategorija 6 (razred D): za prenos podatkov več kot 250 Mb/s, kabli so sestavljeni iz štirih prepletenih parov bakrenih žic,
- Kategorija 7 (razred E): za prenos podatkov več kot 600 Mb/s, kabli so sestavljeni iz štirih prepletenih parov bakrenih žic.

Optični kabli

Optični kabli prenašajo digitalne podatkovne signale v obliki pulzov oz. svetlobe. Optična vlakna za vodenje svetlobe izkoriščajo pojav popolnega notranjega odboja.

Optično vlakno je sestavljeno iz [7]:

- jedra - tanko stekleno središče vlakna, po katerem potuje svetloba,
- zunanjega optičnega materiala (obdaja jedro), ki odbija svetlobo,
- zunanje plastne zaščite, ki ščiti optično vlakno pred poškodbami in vlago.

Steklena vlakna prenašajo signal samo v eno smer, zato je optični kabel sestavljen vsaj iz dveh vlaken. Eno vlakno se uporablja za sprejem, drugo pa za oddajo podatkovnih signalov.

Vlakna, ki imajo premer jedra 50 ali 62,5 μm, imenujemo večrodovna (angl. *multi–mode*) [7]. Po njih se lahko razširi večje število žarkov. Ker prenašajo več svetlobnih signalov, je disperzija večja in se lahko signale prenaša na krajše razdalje (nekaj kilometrov).

Enorodovna vlakna (angl. *single–mode*) [7] lahko uporabljamo pri zelo veliki pasovni širini. Ker imajo majhno slabljenje, so namenjena prenosu velike količine podatkov na daljše razdalje (nekaj sto kilometrov).

Brezžična omrežja

Brezžične tehnologije predstavljajo pomemben del sodobnih omrežij. Brezžične povezave v omrežjih potekajo tipično preko radijskih valov. Brezžični signali so elektromagnetni valovi, ki potujejo po zraku in ne potrebujejo fizičnega prenosnega medija [8].

Računalnike lahko med sabo povežemo na dva načina in sicer s topologijo zvezde ali pa v omrežje »vsak z vsakim«. V brezžičnem omrežju s topologijo zvezde za prenos podatkov med računalniki v omrežju skrbi dostopna točka (angl. *access point*). Računalniki oz. odjemalci z brezžičnimi omrežnimi vmesniki se povežejo na dostopno točko, le-ta pa skrbi za prenos podatkov med povezanimi odjemalci. Navadno omogoča tudi priklop na ožičeno omrežje in predstavlja tudi povezavo med ožičenim in brezžičnim delom omrežja.

Pri načinu "vsak z vsakim" se omrežni vmesniki računalnikov med sabo povežejo v omrežje, vsaka naprava v omrežju pa ima dostop neposredno do vseh naprav v dosegu brezžičnega omrežnega vmesnika. Takih brezžičnih omrežij ne moremo povezati z ožičenim omrežjem.

2.2.2. Aktivne komponente

Aktivne naprave so tiste, ki za svoje delovanje potrebujejo napajalno napetost [9]. Nabor aktivnih komponent se z razvojem tehnologij stalno povečuje. Stikalo ter usmerjevalnik sta najpomembnejša gradnika večine sodobnih omrežij.

Stikalo

Stikalo je naprava, ki deluje na povezovalni plasti referenčnega modela OSI in je namenjena filtriranju in posredovanju paketov med različnimi segmenti lokalnega omrežja. Deluje na osnovi naslovov MAC (*angl. Media Access Control*) in prepozna ciljni naslov poslanih paketov, zato le-te pošlje samo na tista vrata, kamor so namenjena. Stikala lahko hkrati pošiljajo in sprejemajo informacije. Poleg tega poznamo tudi t.i. »layer 3« stikala, ki delujejo na tretji plasti referenčnega modela OSI (angl. *Open Systems Interconnection*).

Usmerjevalnik

Usmerjevalnik je naprava, ki usmerja promet med omrežji ter povezuje dve ali več različnih omrežij. Usmerjevalnik pakete usmerja na podlagi IP naslovov, ki so definirani na tretji (mrežni) plasti ISO/OSI modela. Omogoča delitev omrežij na podomrežja, filtriranje prometa in prenos paketov po vzporednih poteh. Usmerjevalnik ustvari usmerjevalno tabelo, ki shrani najhitrejše poti do določenega omrežnega cilja.

3. Monitoriranje računalniških omrežij

Monitoriranje omrežij pomeni nadzor nad vitalnimi parametri delovanja mrežnih naprav ter prometa med njimi.

3.1. Namen monitoriranja

Omogoča odkrivanje težav delovanja mrežnih naprav in omrežij. Zaznamo lahko preobremenjenost naprav (centralna procesna enota, bralno-pisalni pomnilnik), neprimerno okolje (previsoka temperatura), puščanje pomnilnika [10] (angl. *memory leak*) zaradi napak programske opreme, težave z internetno povezavo, težave s povezavo med mrežnimi napravami v lokalnem omrežju, itd.

Podatki, ki jih pridobimo s stalnim nadzorom omrežja, nam lahko pomagajo pri:

- analizi delovanja omrežja,
- vzdrževanju omrežja,
- oceni, kdaj potrebujemo nadgradnje, kdaj povečati zmogljivosti,
- preverjanju SLA (angl. *Service Level Agreement*) z internetnim ponudnikom, itd.

3.2. Pridobivanje podatkov

Prenos podatkov med nadzornim sistemom in napravo poteka preko protokola SNMP (angl. *Simple Network Management Protocol*), podpora omenjenega protokola pa je tudi pogoj, da napravo lahko monitoriramo.

3.2.1. SNMP

SNMP je podrobno določen z dokumentom RFC 1157 [11] in je eden izmed protokolov internetnega sklada protokolov (angl. *Internet protocol suite*) oz. TCP/IP modela, ki obsega štiri sloje. To so mrežni, internetni, transportni ter aplikacijski sloj. SNMP spada med protokole aplikacijskega sloja, ki združuje plast seje, predstavitveno plast ter aplikacijsko plast referenčnega modela OSI, kot prikazuje slika 3.

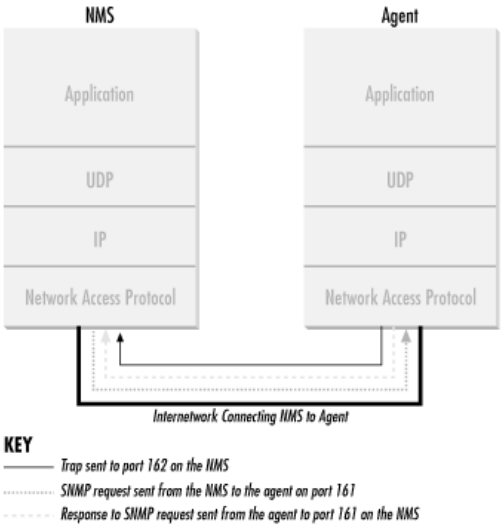
<table>
<tr><td>Protokol</td><td>TCP/IP</td><td>ISO/OSI</td></tr>
<tr><td rowspan="3">SSH, TELNET, SNMP, DHCP, DNS, FTP, SMTP, POP, http</td><td rowspan="3">Aplikacijski sloj</td><td>Aplikacijski sloj</td></tr>
<tr><td>Predstavitveni sloj</td></tr>
<tr><td>Plast seje</td></tr>
<tr><td>TCP, UDP</td><td>Transportni sloj</td><td>Transportni sloj</td></tr>
<tr><td>ICMP, IP (IPv4, IPv6), ARP</td><td>Internetni sloj</td><td>Omrežni sloj</td></tr>
<tr><td rowspan="2">OSPF, Ethernet,</td><td rowspan="2">Sloj dostopa do omrežja</td><td>Povezavni sloj</td></tr>
<tr><td>Fizični sloj</td></tr>
</table>

Slika 3: Umestitev protokola SNMP v TCP/IP ter referenčnega OSI modela.

SNMP uporablja UDP (angl. *User Datagram Protocol*) kot transportni protokol za izmenjevanje podatkov med sistemom za upravljanje omrežja in agentom, ki mora biti nameščen na nadzorovani napravi. Kot je prikazano na sliki 4, se v ta namen navadno uporablja vrata UDP [12]:

- 161 za pošiljanje in sprejemanje zahtev in
- 162 za sprejemanje sporočil »TRAP«.

Sistem pošlje zahtevo agentu in čaka na odgovor. Če odgovora ne dobi, predvideva da je paket izgubljen in ponovno odda zahtevo. Čakalna doba in število ponovitev sta nastavljiva.

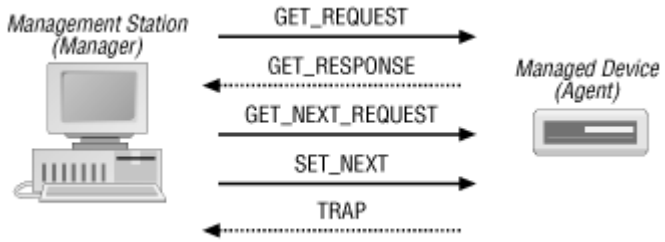


Slika 4: Izmenjava podatkov med nadzornim sistemom in agentom [12].

NMS (angl. N*etwork Management System*) in agent si lahko izmenjata pet tipov sporočil [12]. Ti so:

- GET_REQUEST,
- GET_NEXT_REQUEST,
- SET_REQUEST,
- GET_RESPONSE in
- TRAP.

Prva tri sporočila NMS lahko pošlje agentu z zahtevo za akcijo (informacijo glede vrednosti objekta ali nastavitev vrednosti objektu). Agent odgovori z GET_RESPONSE, sporočila TRAP pa pošlje agent, da v realnem času opozori na morebitno napako strojne opreme, nedosegljivost, itd. Zaradi nezanesljivosti izbranega transportnega protokola UDP se lahko zgodi, da je agent sporočilo TRAP poslal, vendar to ni prišlo do nadzornega sistema, ta pa tudi nima informacije, da mu je bilo sporočilo neuspešno poslano [13].



Slika 5: Izmenjava sporočil med NMS ter agentom na napravi [13].

Agenti imajo nastavljene tri nize »*community strings*« in sicer samo branje (angl. *read only*), branje in pisanje (angl. *read-write*) ter »trap«, ki omogočajo nadzor nad aktivnostmi branja, pisanja ter pošiljanja sporočil »TRAP«.

3.2.2. Baza upravljalskih informacij

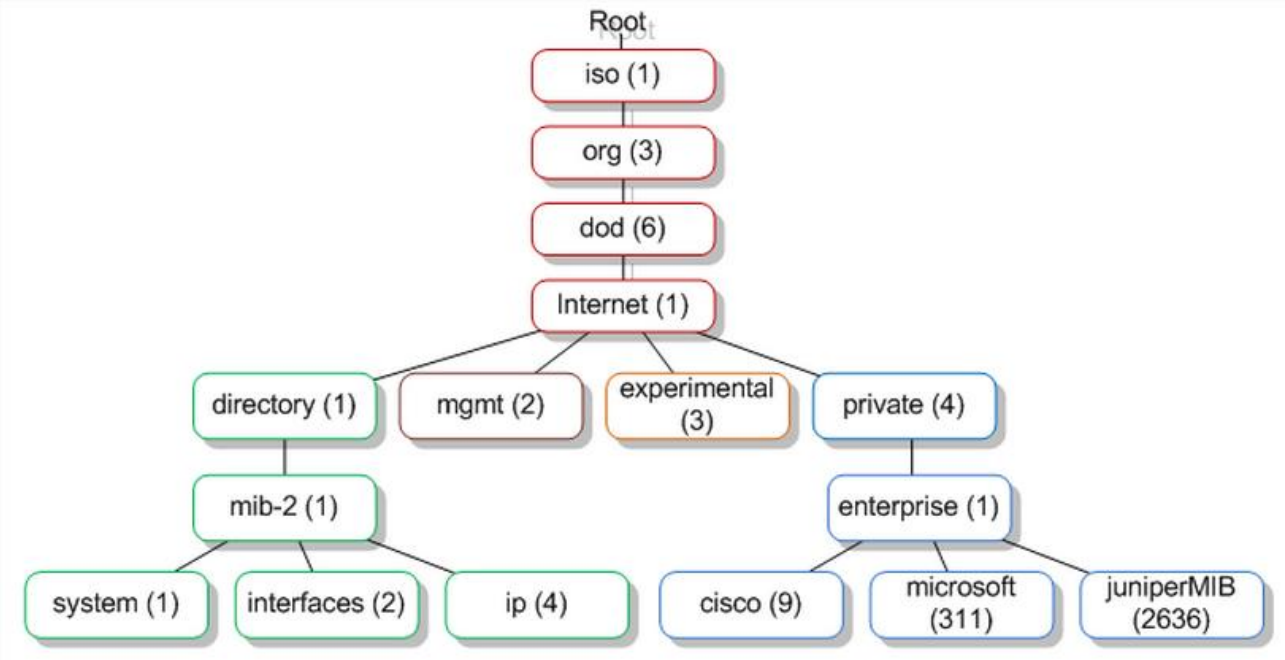
Baza upravljalskih informacij oz. MIB (angl. *Management Information Base*) je urejen nabor podatkov o napravah v omrežju, ki se uporablja za njihovo upravljanje. Je v obliki hierarhične

strukture, ki se začne z brezimenskim korenom in nadaljuje s posameznimi imeni različnih organizacij. MIB objekt je sestavljen iz več instanc, ki so definirane z OID (angl. *object identifier*). Z iskalniki, ki so na voljo na spletu, lahko OID-je iščemo po numeričnih vrednostih ali drevesni strukturi.

Struktura OID

OID-ji so določeni s strukturo hierarhičnega drevesa SMI (angl. *structure of management information*), kot prikazuje slika 5. Za lažjo predstavo si to drevo lahko predstavljamo kot mape datotečnega sistema, kjer je vsaka mapa označena s številko. Tako namesto iso\org\dod\internet, zapišemo 1.3.6.1 [14].

Vrh drevesa se imenuje koren (angl. *root*), posamezni deli z nasledniki so poddrevesa ali veje (angl. *subtrees*), končni objekti pa se imenujejo vozlišča (angl. *leaf nodes*). Poddrevo iso(1).org(3).dod(6).internet(1) je razdeljeno na štiri veje in sicer: *directory, mgmt, experimental* in *private*. *Directory* se trenutno ne uporablja, *mgmt* definira množico *Internet management objects*, veja *experimental* je namenjena testiranju in raziskavam, objekti v veji *private* pa so pod kontrolo posameznikov in organizacij.



Slika 6: SMI drevo [15].

3.2.3. Nadzor porabe centralno procesne enote na usmerjevalniku

V tem razdelku je opisan primer nadzora porabe centralno procesne enote na napravi tipa usmerjevalnik. Z uporabo SNMP Object Navigator-ja v drevesni strukturi poiščemo OID za pet minutno zasedenost centralno procesne enote v procentih za izbrano napravo, v našem primeru usmerjevalnik Cisco 871 [16].

Slika 7: Drevesna struktura SNMP Object Navigator-ja [16].

Kot prikazuje slika 8, nam podroben opis najdenega objekta poda informacije o:

- imenu objekta,
- OID-ju
- podatkovnemu tipu,
- bralno-pisalnih pravicah,
- statusu,
- enoti,
- obsegu,
- MIB-u,
- opisu.

Specific Object Information	
Object	cpmCPUTotal5minRev
OID	1.3.6.1.4.1.9.9.109.1.1.1.1.8
Type	Gauge32
Permission	read-only
Status	current
Units	percent
Range	0 - 100
MIB	CISCO-PROCESS-MIB ; - View Supporting Images
Description	"The overall CPU busy percentage in the last 5 minute period. This object deprecates the object cpmCPUTotal5min and increases the value range to (0..100)."
More Information	• How to Collect CPU Utilization on Cisco IOS Devices Using SNMP

Slika 8: Podroben opis objekta [17].

OID lahko preizkusimo na izbrani napravi preko SSH (angl. *secure shell*) povezave na napravo z ukazom »snmpwalk« in parametri *community string*, IP naprave ter OID, kot je prikazano v prvi vrstici spodnjega izpisa.

```
polona:~$ snmpwalk -v 2c -c commstr 10.1.56.1 1.3.6.1.4.1.9.9.109.1.1.1.1.8
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.8.1 = Gauge32: 1
```

Druga vrstica je odgovor naprave. Obremenjenost CPE zadnjih pet minut je en procent.

3.3. Parametri

V sodobnih omrežjih je v uporabi veliko različnih naprav. Od mrežnih naprav (stikalo, usmerjevalnik, točke dostopa, ...), do strežnikov, virtualnih in osebnih računalnikov, tiskalnikov, itd. Parametre za monitoriranje moramo tako izbrati pametno, glede na tip in vlogo naprave v omrežju. Izbira parametrov močno vpliva na učinkovitost delovanja sistema za monitoriranje.

Navadno nas najprej zanima dosegljivost naprave, da jo lahko sploh monitoriramo. V splošnem pa nas zanimajo osnovni parametri, ki kažejo na pravilnost ali nepravilnost delovanja naprave v omrežju. Ti so:

- obremenjenost centralno procesne enote,
- poraba pomnilnika,
- temperatura,
- delovanje ventilatorjev,
- promet na vmesnikih,
- itd.

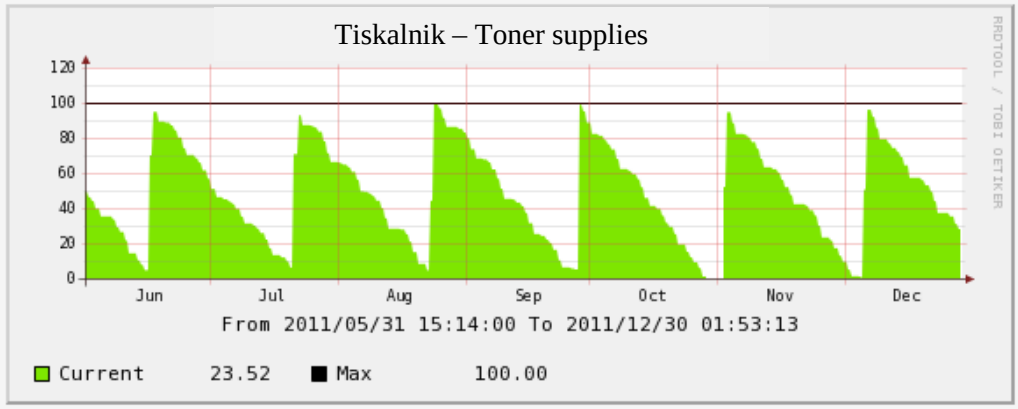
Posebnosti izbire parametrov glede na tip naprave

Določene naprave imajo glede na tip naprave ali vlogo v omrežju posebne parametre, s katerimi lahko spremljamo delovanje ali obremenjenost naprave ali omrežja.

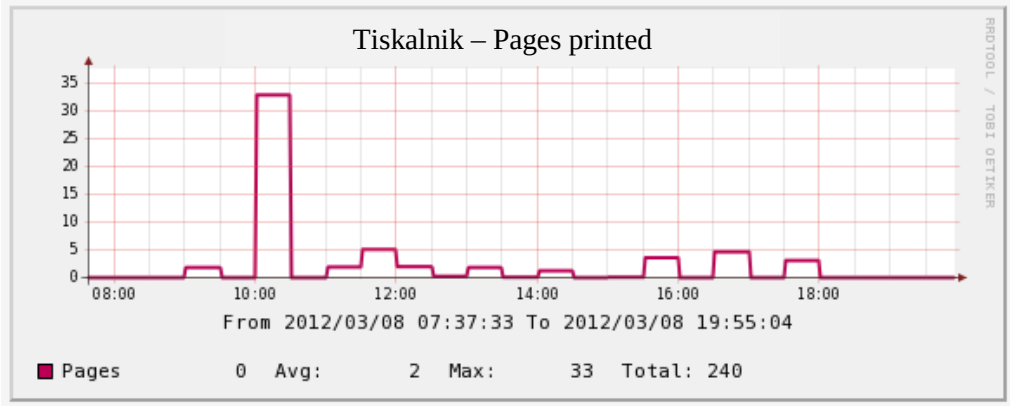
Opisali bomo posebne parametre pri:

- tiskalniku,
- pristopni točki,
- požarni pregradi in
- usmerjevalniku.

Posebna parametra pri tiskalniku sta poraba tonerja in število natisnjenih strani, kar prikazujeta sliki 9 in 10. Posebno pri prvem je pomembno, da si glede na preteklo porabo alarm nastavimo dovolj zgodaj, da bomo toner lahko pravočasno kupili in zamenjali.

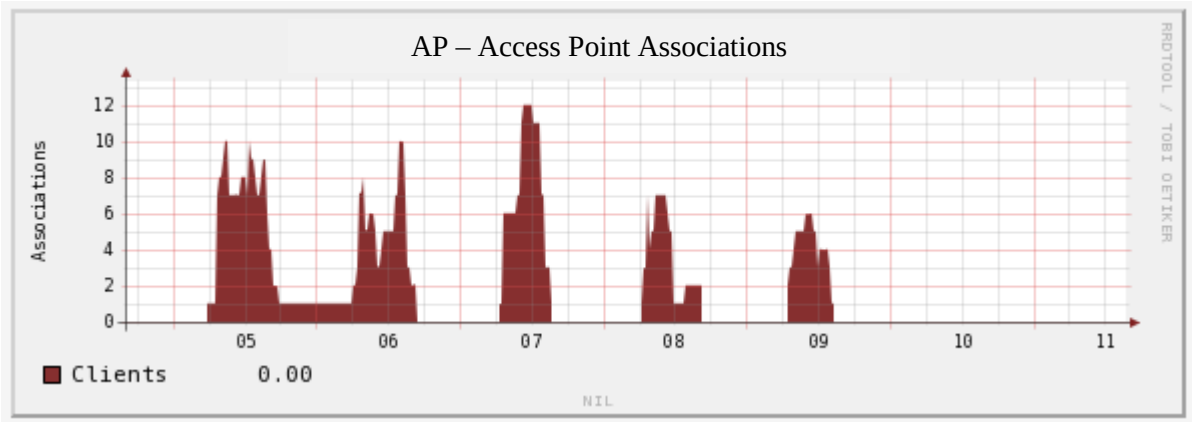


Slika 9: Poraba tonerja pri tiskalniku za sedemmesečno obdobje.



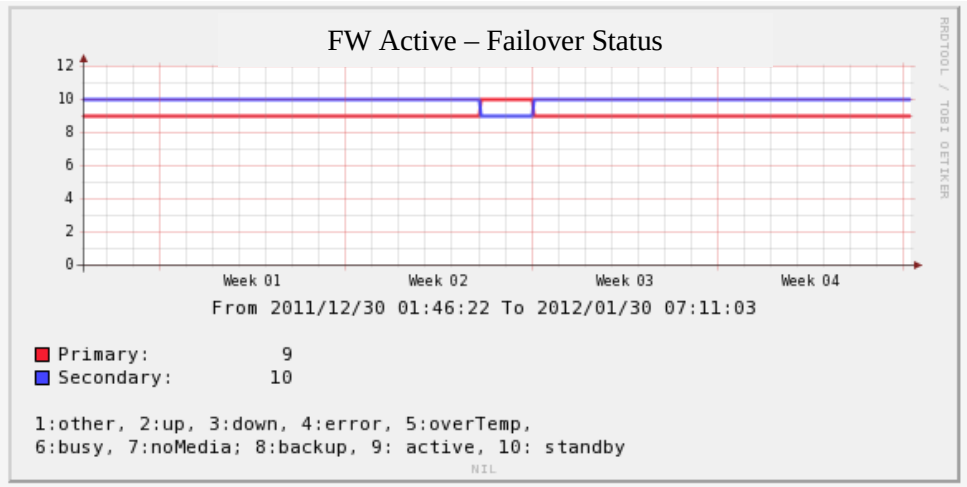
Slika 10: Število natisnjenih strani v delovnem dnevu.

Pri spremljanju pristopne točke je poseben parameter število uporabnikov, povezanih na dostopno točko, kar prikazuje slika 11.



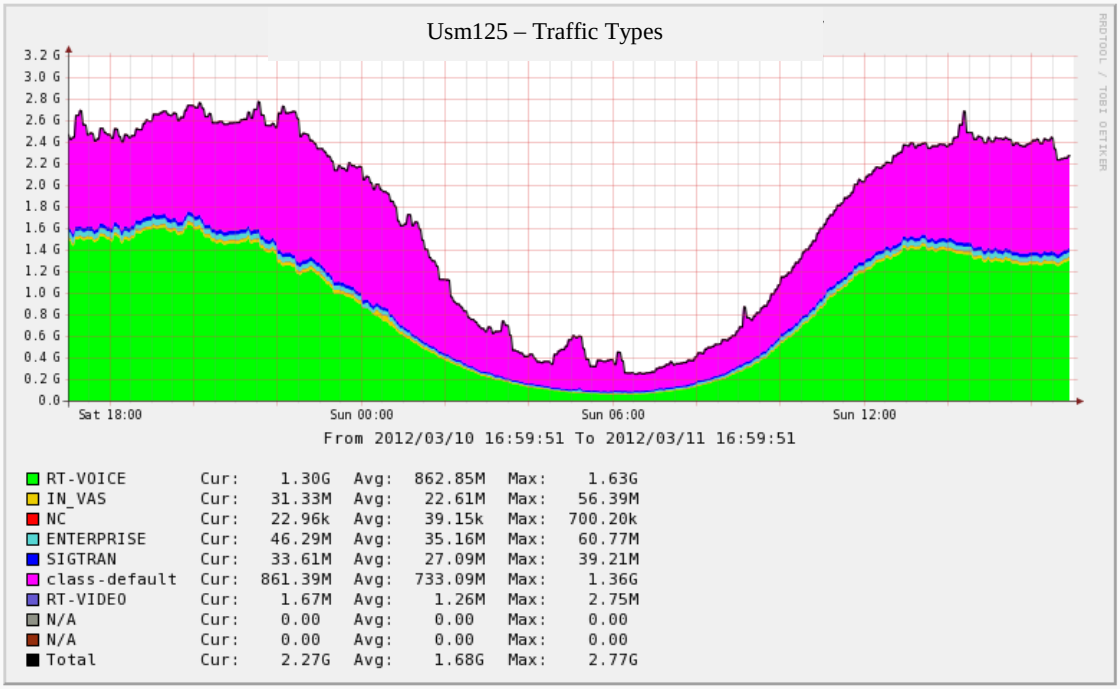
Slika 11: Tedenski graf povezav uporabnikov na dostopno točko.

Zelo pomemben parameter pri monitoriranju redundančnih požarnih pregrad je *failover status*, ki nam pove, v katerem stanju (primarnem ali sekundarnem) je požarna pregrada. Slika 12 prikazuje požarni pregradi, ki sta med delovanjem zamenjali stanji.



Slika 12: Graf spremljanja primarne in sekundarne požarne pregrade.

S spremljanjem tipov prenesenega prometa preko WAN povezav lahko enostavno identificiramo najbolj prisotne podatkovne seje ter nezaželene po potrebi tudi blokiramo. Tip prometa identificiramo z uporabo QoS (angl. *Quality of Service)* mehanizmov na usmerjevalnikih.



Slika 13: Tipi prometa.

4. Programska oprema za nadzor računalniških omrežij

Z rastjo omrežja raste tudi zapletenost nadzora in upravljanja. Sistem za upravljanje omrežja oz. NMS zbira, prikazuje in dinamično oz. periodično posodablja podatke o izbranih parametrih naprav v omrežju ter z alarmiranjem obvešča o preseženih vrednostih nastavljenih pragov. Sistem za upravljanje omrežja je sestavljen iz programskega orodja ter strojne opreme. Navadno nadzorujemo lokalna omrežja, ki pa so lahko od sistema za nadzor ločena s prostranim omrežjem. Da so meritve točne, jih moramo izvajati znotraj lokalnega omrežja, pridobljene podatke pa potem lahko po varni povezavi prenašamo do centralne lokacije, kjer jih prikazujemo in obdelujemo v izbranem orodju.

Množica informacij nam ne pomaga veliko, če jih ne znamo ovrednotiti. Zato je zelo pomembno, da je alarmiranje nastavljeno v skladu z namenom in uporabo naprave ter priporočili proizvajalca, saj se drugače lahko zgodi, da nas sistem prepogosto opozarja s pomembnimi in nepomembnimi opozorili, iz katerih pa je potem težko razbrati, kaj se v omrežju zares dogaja.

V primeru, da imamo prag alarmiranja za temperaturo nastavljeno na 25 stopinj in v enem izmed prostorov, kjer je mrežna oprema, poleti temperatura niha med 24 in 26 stopinjami Celzija, nas bo sistem stalno opozarjal na dvig temperature nad nastavljen prag. Glede na priporočila proizvajalca mrežna oprema pri takih temperaturah deluje brezhibno in so opozorila brezpredmetna. Če želimo vzpostaviti učinkovit sistem, je pravilna konfiguracija ključnega pomena.

4.1. Sistemi za upravljanje omrežij

Sistemi za upravljanje omrežja se med sabo razlikujejo glede na:

- licenciranje,
- vmesnik,
- metodo shranjevanja podatkov,
- funkcionalnosti.

Obstaja več vrst licenc, ki določajo dostopnost programskih paketov. V skupino orodij s komercialno licenco spadajo IBM Tivoli Network Manager, HP Network Node Manager,

Nimsoft Monitoring Solution, itd. Pod licenco GPL (angl. *General Public License*) med drugimi sodijo Cacti, Icinga, Nagios, Zabbix in Zenoss. Nekatera orodja, npr. Zenoss so dostopna brezplačno (Zenoss Core), lahko pa jih nadgradimo s plačljivo verzijo, ki vsebuje več funkcionalnosti (Zenoss Enterprise).

Najpogostejši uporabniški vmesnik je spletni vmesnik. Imajo ga vsi zgoraj omenjeni produkti, čeprav je pri nekaterih namenjen samo pregledovanju, ne pa tudi konfiguraciji (Icinga).

Shranjevanje podatkov lahko razdelimo na dve veji in sicer na shranjevanje v bazo ter z uporabo RRDtool-a. RRDtool je de facto standard za zbiranje in grafično prikazovanje podatkov, ki nastajajo v odvisnosti s časom in je podrobneje opisan v razdelku 4.2.

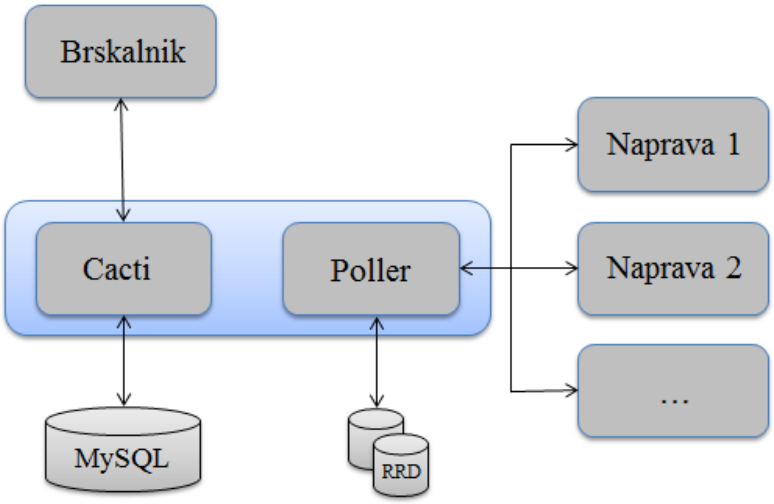
Sistemi za upravljanje omrežja se razlikujejo predvsem pri bolj zahtevnih ali specifičnih funkcionalnostih. To so npr. predikcija trendov, GIS (angl. *Geographic Information System*) ali Syslog podpora, itd.

4.2. Cacti

Cacti je eno izmed odprtokodnih orodij za monitoriranje omrežij. Osnovni gradniki orodja Cacti so [18]:

- strežnik s »pollerjem«,
- podatkovna baza MySQL,
- brskalnik,
- RRD datoteke.

Uporaba in administracija potekata preko spletnega vmesnika, podatki pa se shranjujejo v bazo MySQL. Poleg podatkovne baze je na istem strežniku tudi »poller«, ki se zažene iz razporejevalnika opravil operacijskega sistema in v določenih časovnih presledkih sprašuje naprave o vrednostih izbranih parametrov. Rezultati se shranijo v RRD datoteke, od koder se črpajo podatki za risanje grafov. Na grafih je možno prikazovanje več parametrov hkrati, kar je uporabno v primeru redundančnih ventilatorjev na omrežnih napravah. V takih primeri je pomembno, da pravilno uredimo tudi legendo, v katero lahko vključimo prikaz robnih vrednosti (minimum, maksimum) in povprečje. Grafe lahko poljubno povečujemo in zmanjšujemo na časovne intervale (nekaj ur, dni, mesecev, itd.).

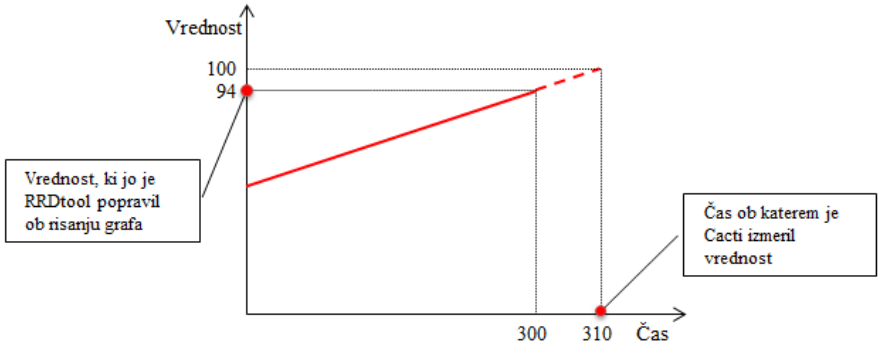


Slika 14: Gradniki orodja Cacti.

4.2.1. RRDtool

RRDtool se uporablja za shranjevanje podatkov spremljanih parametrov naprav v omrežju. Delovanje nakazuje že z imenom RRD (angl. R*ound Robin Database*). Zbirko podatkov si lahko predstavljamo kot vrtiljak, kjer se novi podatki zapisujejo na obod. Ko je krog sklenjen, začnejo novi podatki prepisovati stare. Velikost zbirke RRD je torej vedno enaka oz. konstantna. RRDtool lahko uporabimo tudi za izračun spremembe glede na prejšnjo vrednost in nato v zbirko podatkov shranimo izračunano vrednost glede na prej določene časovne intervale.

RRDtool avtomatično normalizira podatke [19] na izbran interval (običajno 5 minut oz. 300 sekund), kot je prikazano na sliki 15.



Slika 15: Delovanje RRDtool-a.

4.2.2. Alarmiranje

Alarmiranje je mogoče samo za tiste parametre, ki jih grafiramo in navadno poteka preko izbranega elektronskega naslova.

Primer poslanega alarma ob povišani temperaturi naprave na 48 stopinj in pragom 47 stopinj prikazuje spodnji izpis:

```
An alert has been issued that requires your attention.

Host: Device1 (195.245.203.38)
URL: http://cacti.monitor.si//graph.php?local_graph_id=2083&rra_id=1

Message: Device1 - CPU Temperature [cpu_temp] went above threshold of
47 with 48
```

Pragove za alarmiranje nastavimo glede na pričakovane oz. priporočene vrednosti spremljanih parametrov. Da se v čim večji meri izognemo lažnim alarmom, moramo pragove stalno prilagajati morebitnim posegom in spremembam v omrežju.

4.2.3. Vtičniki

Arhitektura omogoča dodajanje vtičnikov, ki so na voljo na spletu, ali pa jih razvijemo sami. Preko vtičnikov lahko orodju dodajamo nove funkcionalnosti. Za monitoriranje omrežij v realnem času sta najpomembnejša vtičnika »Tresholds« ter »Graphs«. Vtičnik »Tresholds« nam prikazuje vse naprave, pragove ter sprožene alarme. Za pregled grafov je nepogrešljiv vtičnik »Graphs«, ki z drevesno strukturo naprav omogoča potrebno preglednost nad množico grafov.

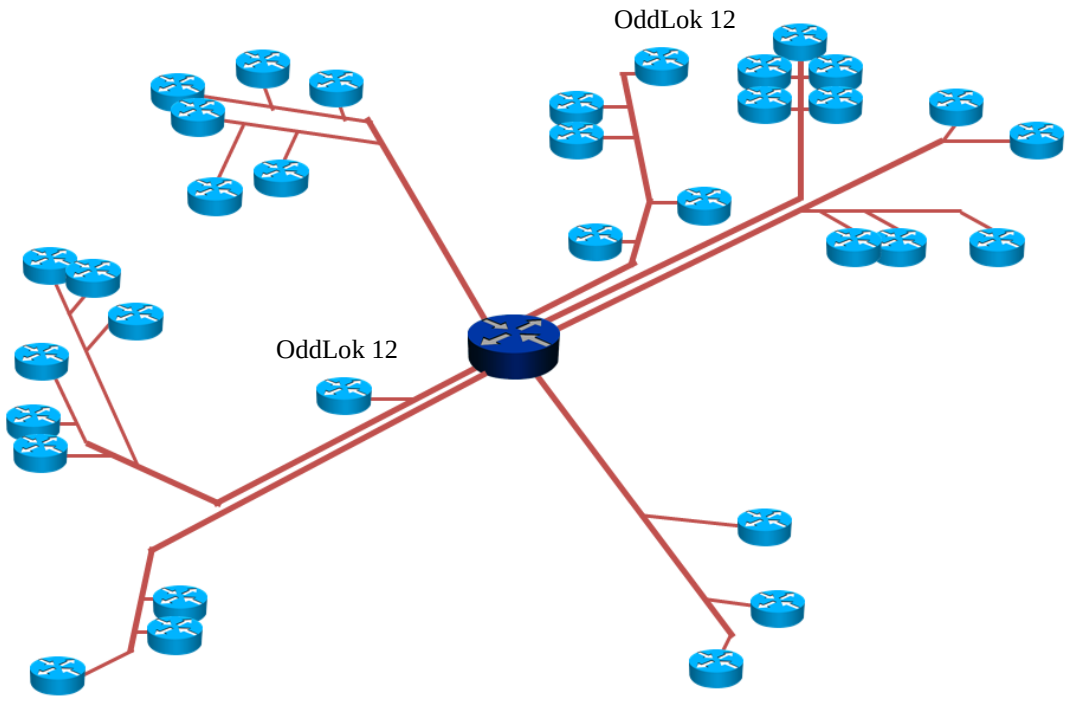
5. Primer monitoriranja omrežja

V pričujočem poglavju je predstavljeno realno monitorirano omrežje ter rezultati enomesečnega nadzora z orodjem Cacti, opisanim v razdelku 4.2.

5.1. Vzorčno omrežje

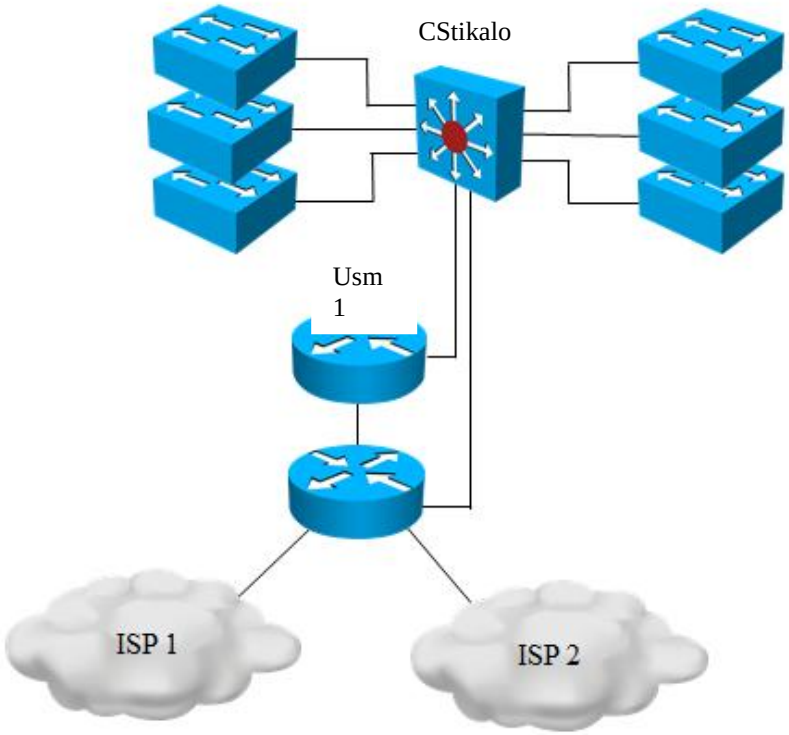
Nadzorovano omrežje predstavlja realno omrežje in zaradi zagotavljanja anonimnosti ni geografsko umeščeno na zemljevid. Prav tako so spremenjeni IP-ji in imena naprav, topologija in tip naprav pa sta realna. Omrežje je sestavljeno iz centralne lokacije ter oddaljenih lokacij (v radiju 150 kilometrov od centralne lokacije), kot je prikazano na sliki 16.

Štiriintrideset oddaljenih lokacij se zaključuje na glavnem usmerjevalniku na centralni lokaciji, ki je na sliki 16 označen s temnejšo barvo. Vse oddaljene lokacije za svojo povezljivost do centralnega usmerjevalnika uporabljajo tehnologijo IPsec/GRE, ki zagotavlja varen način prenosa podatkov skozi javno omrežje Internet.



Slika 16: Topologija realnega monitoriranega omrežja.

Lokalno omrežje centralne lokacije je zasnovano na zmogljivem stikalu Cisco Catalyst. Na centralno stikalo so priklopljena vozliščna stikala različnih družin stikal Cisco s topologijo, kot prikazuje slika 17. Dostop do Interneta je omogočen preko dveh neodvisnih internetnih ponudnikov ISP 1 ter ISP 2.



Slika 17: Lokalno omrežje centralne lokacije.

Seznam spremljanih naprav:

- 36 usmerjevalnikov Cisco,
- zmogljivejše stikalo Cisco Catalyst,
- 6 stikal Cisco,
- strežnik Cacti.

5.2. Rezultati

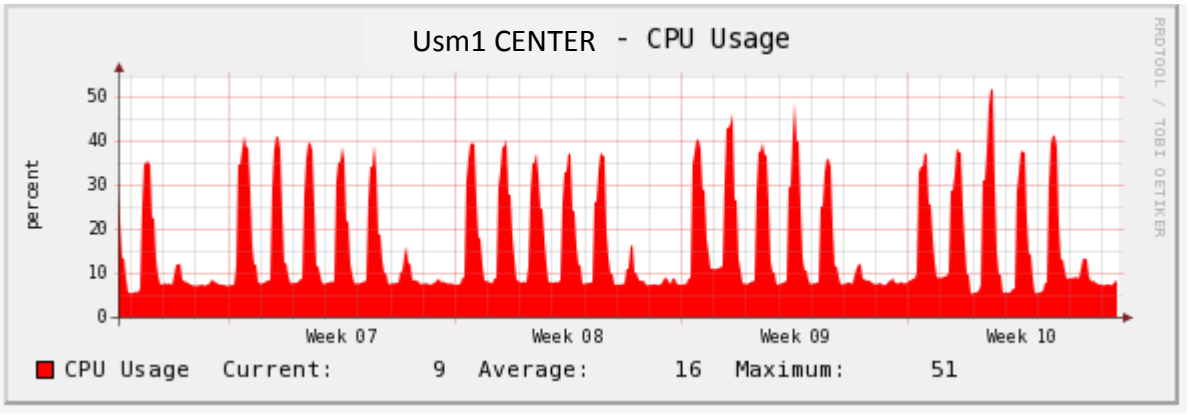
Rezultati so predstavljeni v obliki grafov, po sklopih, glede na tip naprav. Pri pomembnejših napravah navadno spremljamo več parametrov, kot pri napravah z manjšo vlogo v omrežju. Poleg spremljanja obremenitev mrežnih naprav, so pomembni tudi podatki o napajanju, temperaturah in hlajenju ter redundančnih mehanizmih (delovanje podvojenih napajalnikov, procesnih enot in modulov). Pogosto so v okoljih brez aktivnega monitoriranja prav tu razlogi za izpad storitev.

V monitoriranem računalniškem omrežju je veliko število usmerjevalnikov, zato smo upoštevajoč njihov tip in vlogo v omrežju za predstavitev rezultatov izbrali usmerjevalnik na centralni lokaciji ter dva naključna usmerjevalnika na oddaljenih lokacijah. Poleg tega so predstavljeni tudi rezultati meritev glavnega stikala v lokalnem omrežju centralne lokacije.

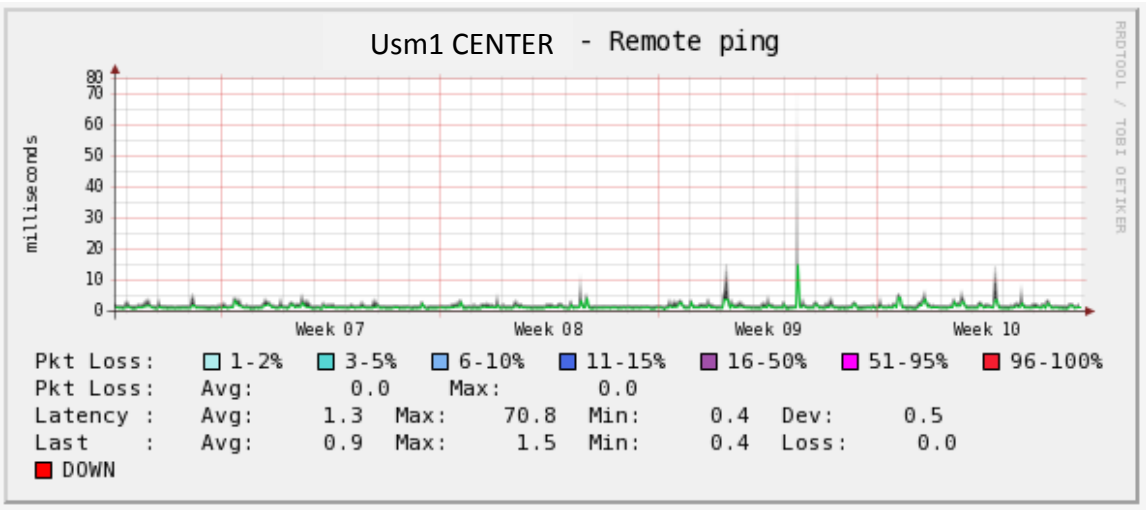
5.2.1. Rezultati monitoriranja usmerjevalnika Usm1

Usm1 je glavni usmerjevalnik na centralni lokaciji monitoriranega omrežja. Na njem se zaključujejo vsi tuneli štiriintridesetih oddaljenih lokacij.

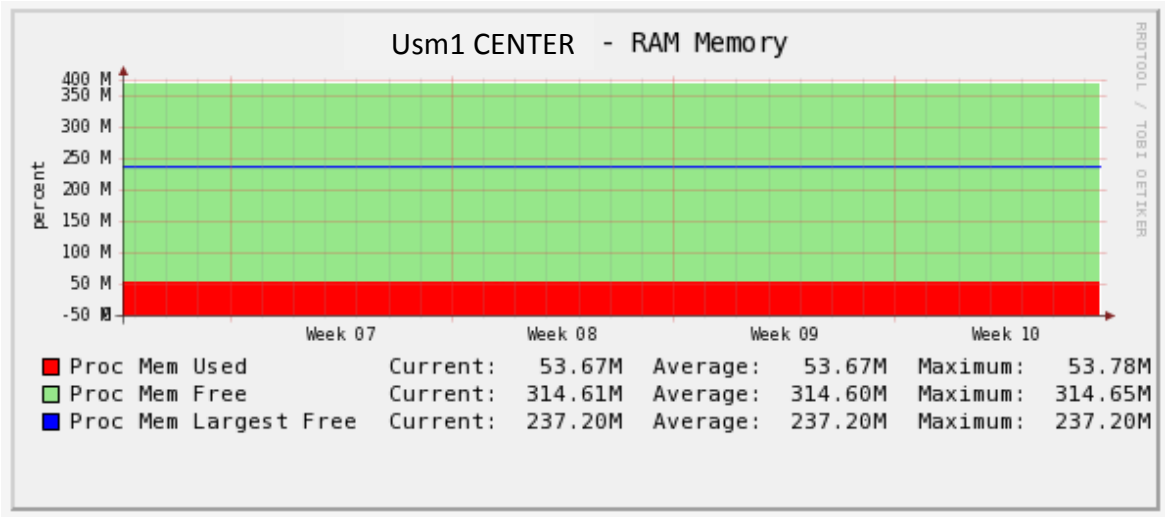
Slika 18 prikazuje obremenjenost centralno procesne enote, slika 19 dosegljivost naprave, slika 20 porabo pomnilnika, slika 21 tri meritve temperature (temperatura centralno procesne enote, naprave ter vhodna temperatura), slika 22 velikost ARP (angl. A*ddress Resolution Protocol*) tabele, slika 23 velikost tabele usmerjanja, slika 24 status ventilatorjev in primarne napajalne enote, slike 25, 26 in 27 pa promet od in do oddaljenih lokacij 12, 20 in 23.



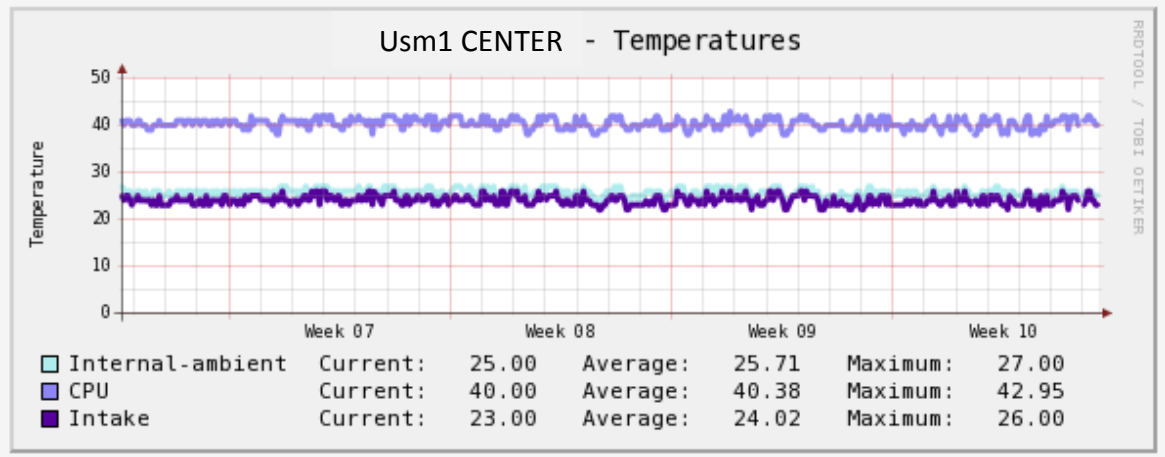
Slika 18: Obremenjenost centralno procesne enote.



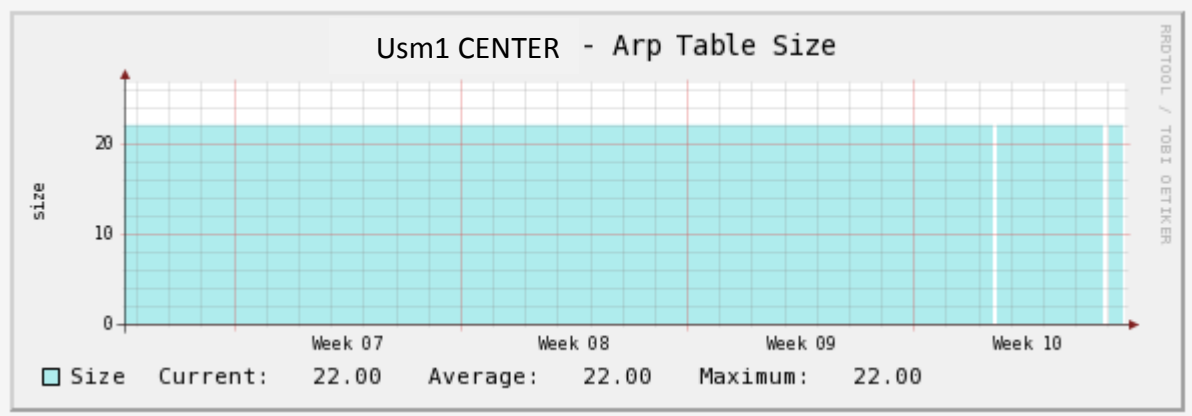
Slika 19: Dosegljivost.



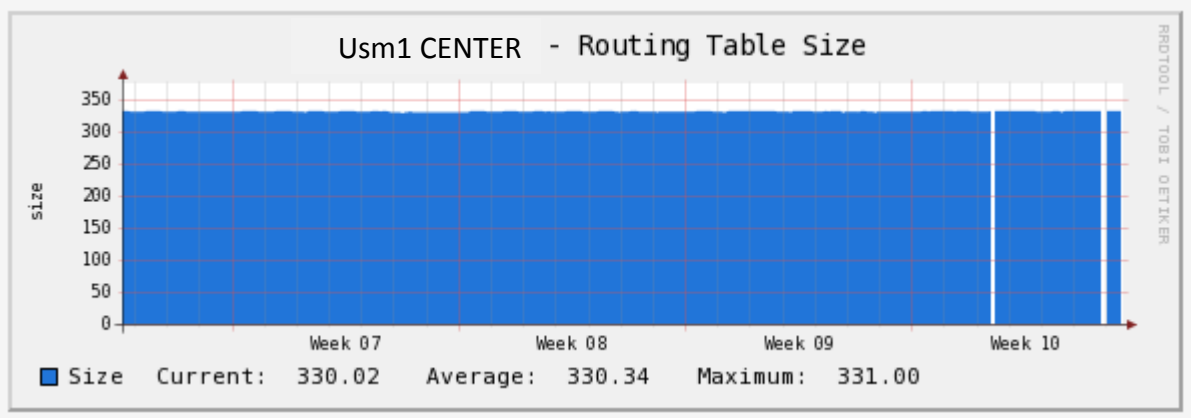
Slika 20: Poraba pomnilnika.



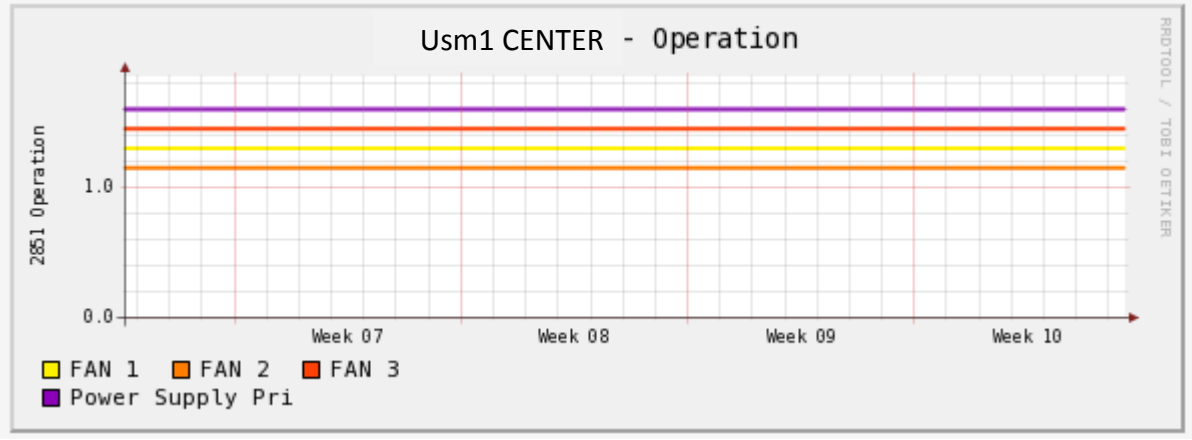
Slika 21: Temperature.



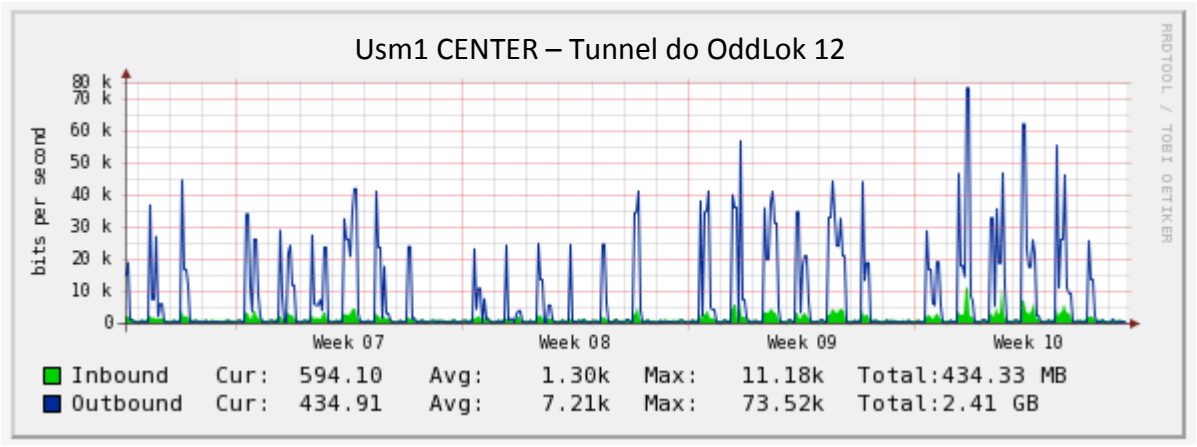
Slika 22: Velikost ARP tabele.



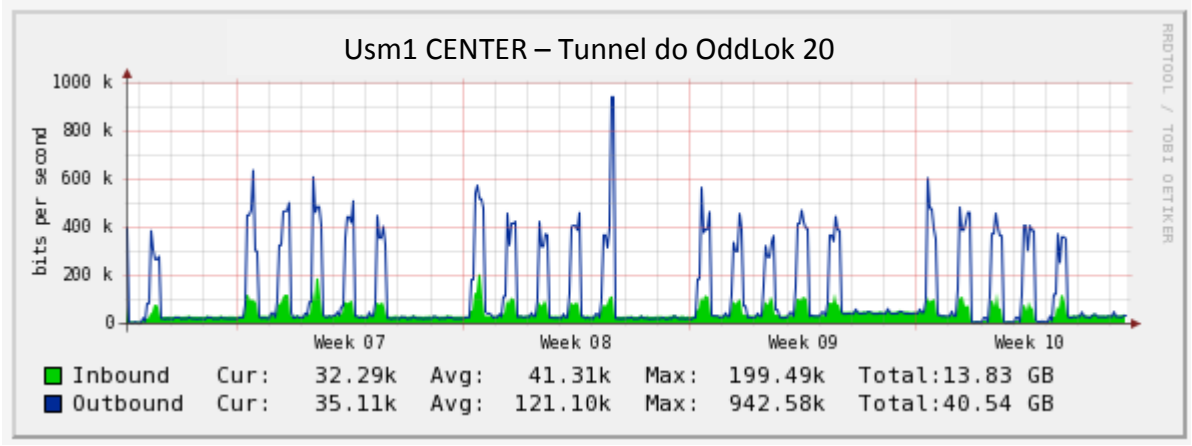
Slika 23: Velikost usmerjevalne tabele.



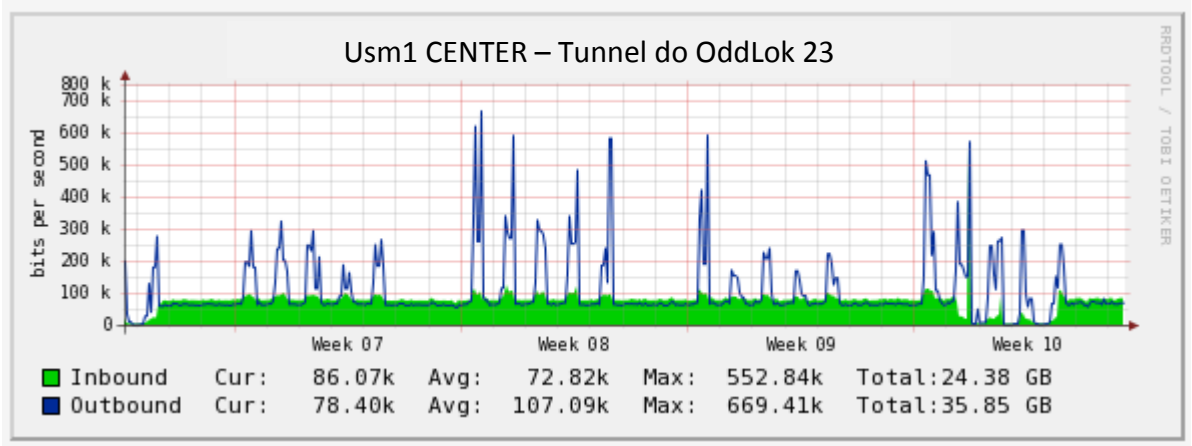
Slika 24: Stanje ventilatorjev.



Slika 25: Promet po tunelu do oddaljene lokacije 12.



Slika 26: Promet po tunelu do oddaljene lokacije 20.



Slika 27: Promet po tunelu do oddaljene lokacije 23.

Iz grafa obremenjenost centralno procesne enote lahko razberemo povečano delovanje pet dni v tednu ter rahlo povečano delovanje šesti dan v tednu. Visoke obremenitve nastopajo skladno z delovnim časom ter prometom preko usmerjevalnika.

Pri dosegljivost naprave, ne opažamo posebnosti.

Poraba pomnilnika je po pričakovanjih konstantna. Zelo pogosto se graf za porabno pomnilnika spreminja le ob zamenjavi strojne opreme ali puščanju pomnilnika.

Meritve temperature centralno procesne enote, naprave ter vhodne temperatura niso konstantne, vendar je razlika med najnižjo ter najvišjo v najslabšem primeru le tri stopinje, kar je v mejah normale. Temperatura centralno procesne enote je pričakovano višja od ostalih dveh, zaradi toplote, ki jo pri delovanju ustvarja procesor.

Velikost tabele ARP ter velikost tabele usmerjanja se spremenita le ob določenih posegih v konfiguracijo omrežja, do katere v času monitoriranja očitno ni prišlo.

Trije ventilatorji ter primarna napajalna enota delujejo normalno, stanje je nespremenjeno.

Vhodni in izhodni promet na tunelih do izbranih oddaljenih lokacij je, kot pri obremenjenosti centralno procesne, povečan promet ob delovnikih (ne pa tudi ob sobotah). Na sliki 27 lahko opazimo zmanjšan vhodni promet v zadnjem tednu monitoriranja, kar bi lahko nakazovalo na težave z internetno povezavo oddaljene lokacije 23.

5.2.2. Rezultati monitoriranja usmerjevalnikov na oddaljenih lokacijah

Zaradi visokega števila naprav enakega tipa na oddaljenih lokacijah bomo predstavili rezultate samo za dva naključno izbrana končna usmerjevalnika. To sta OddLok 12 ter OddLok 20.

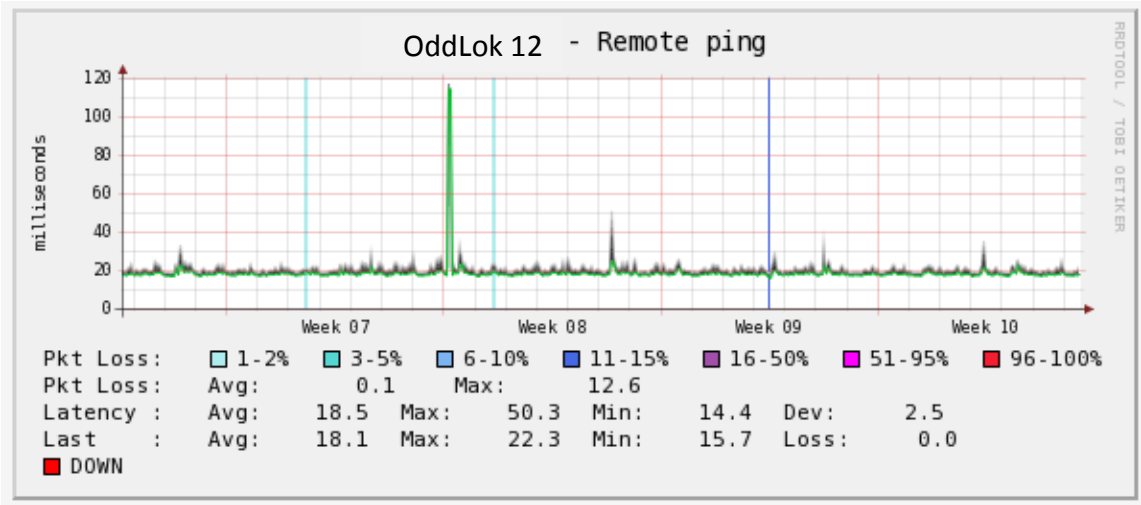
Na napravah z manjšo prioriteto v omrežju spremljamo tudi manjše število parametrov. Na usmerjevalnikih na oddaljenih lokacijah smo monitorirali naslednje parametre:

- dosegljivost,
- obremenjenost centralno procesne enote,
- stanje sekundarne internetne povezave linije in
- promet preko primarne internetne povezave proti centralnemu usmerjevalniku.

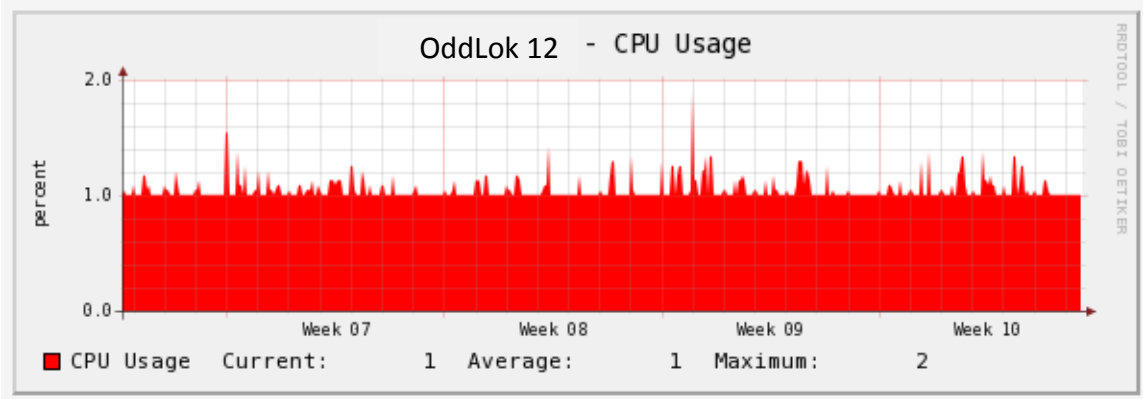
Rezultati monitoriranja usmerjevalnika OddLok 12

Usmerjevalnik OddLok 12 je končna naprava, na katero so priključeni računalniki končnih uporabnikov. Njegovo delovanje je nujno potrebno za opravljanje osnovne dejavnosti oddaljene lokacije.

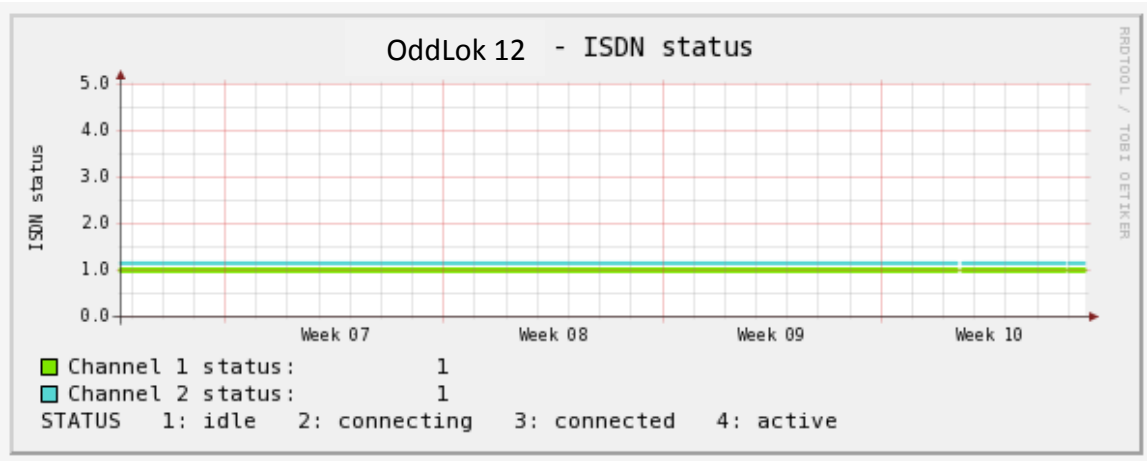
Slika 28 prikazuje dosegljivost naprave, slika 29 obremenjenost centralno procesne enote, slika 30 stanje rezervne ISDN linije, slika 31 pa promet na fizičnem vmesniku proti centralnemu usmerjevalniku.



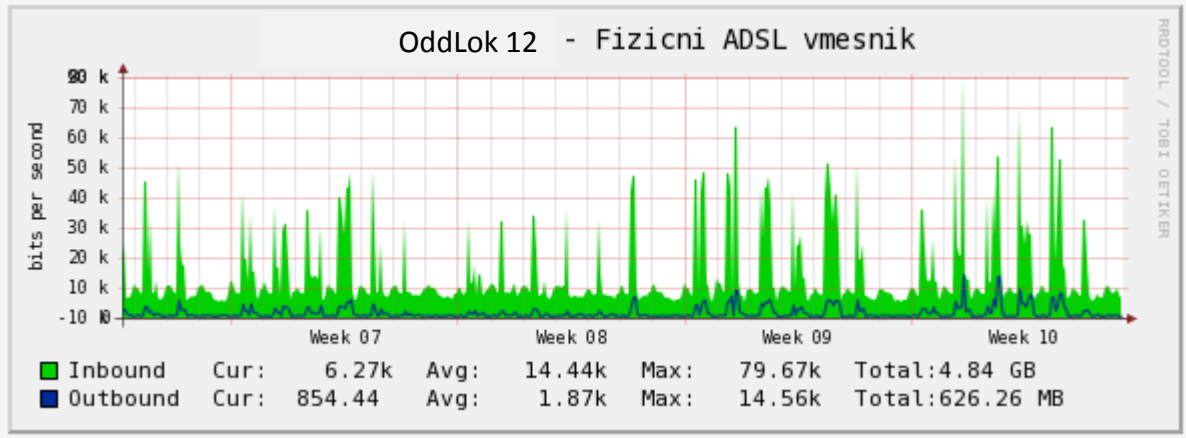
Slika 28: Dosegljivost.



Slik-a 29: Obremenjenost centralno procesne enote.



Slika 30: Stanje ISDN linije.



Slika 31: Promet proti centralni lokaciji.

V prvem, drugem, predvsem pa v tretjem tednu monitoriranja smo opazili kratkotrajne večje izgube paketov, ki pa glede na trajanje niso alarmantne.

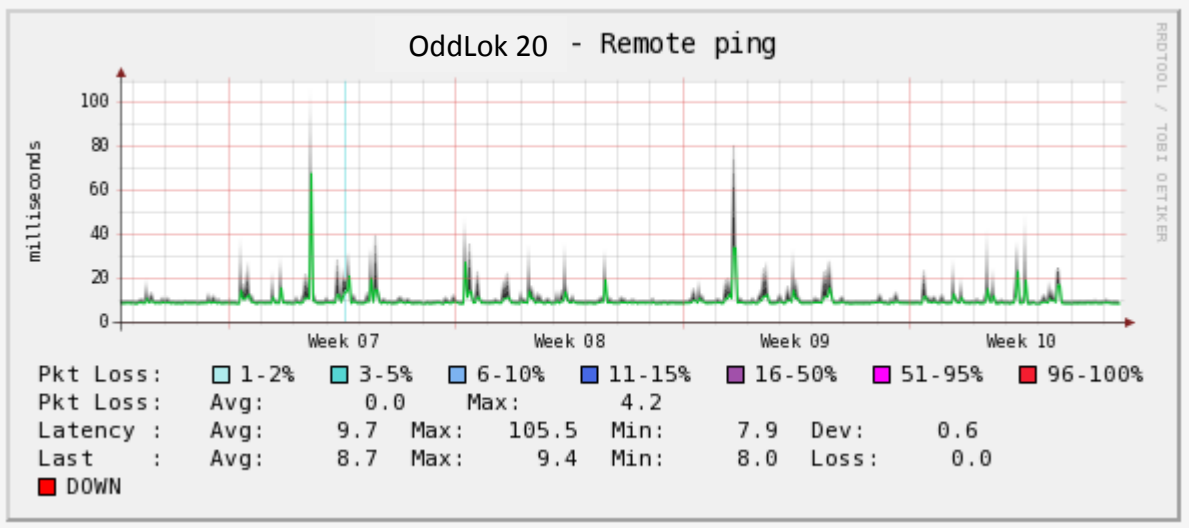
Obremenjenost centralno procesne enote je zelo nizka, maksimalna obremenitev je bila 2%, večinoma pa je procesor obremenjen med 1 in 2%.

Na oddaljeni lokaciji 12 sekundarno internetno linijo predstavlja ISDN linija, ki je v stanju mirovanja, kar je skladno tudi z grafom prometa primarne ADSL povezave. Vhodnega prometa je pričakovano več kot izhodnega, oba pa sta bila rahlo povečana v zadnjih dveh tednih monitoriranja. Graf na sliki 32 je skladen tudi z grafom na sliki 25, saj predstavljata promet na isti povezavi (med centralno in oddaljeno lokacijo).

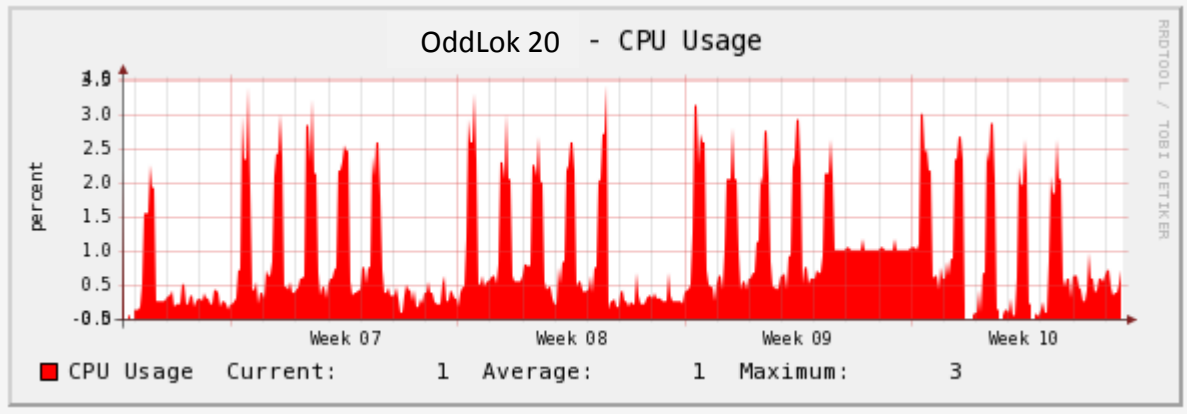
Rezultati monitoriranja usmerjevalnika OddLok 20

Usmerjevalnik OddLok 20 je še ena izmed končnih naprav v omrežju in je ključnega pomena za opravljanje osnovne dejavnosti oddaljene lokacije.

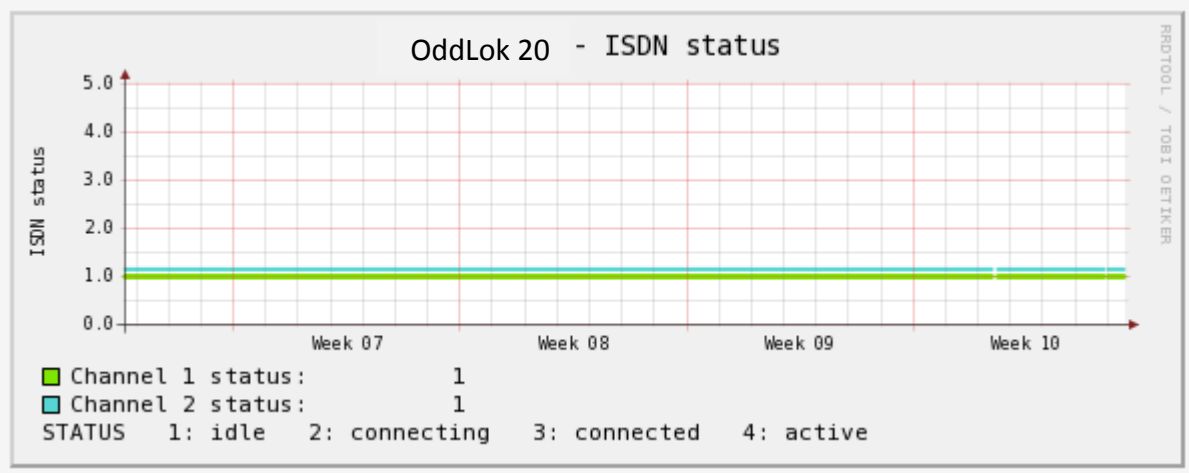
Slika 32 prikazuje dosegljivost naprave, slika 33 obremenjenost centralno procesne enote, slika 34 stanje rezervne ISDN linije, slika 35 pa promet na fizičnem vmesniku proti centralnemu usmerjevalniku.



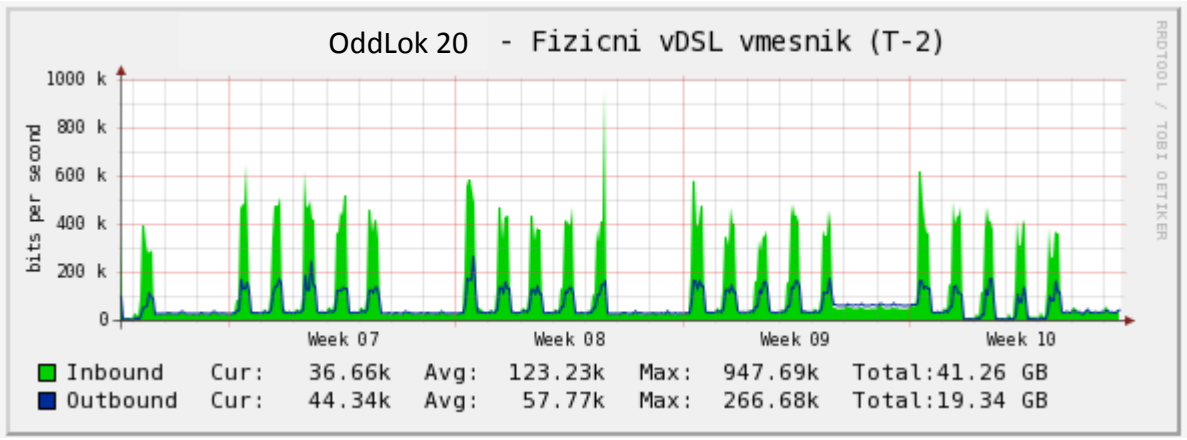
Slika 32: Dosegljivost.



Slika 33: Obremenjenost centralno procesne enote.



Slika 34: Stanje ISDN linije.



Slika 35: Promet na fizičnem vmesniku.

Graf dosegljivosti je brez večjih posebnosti.

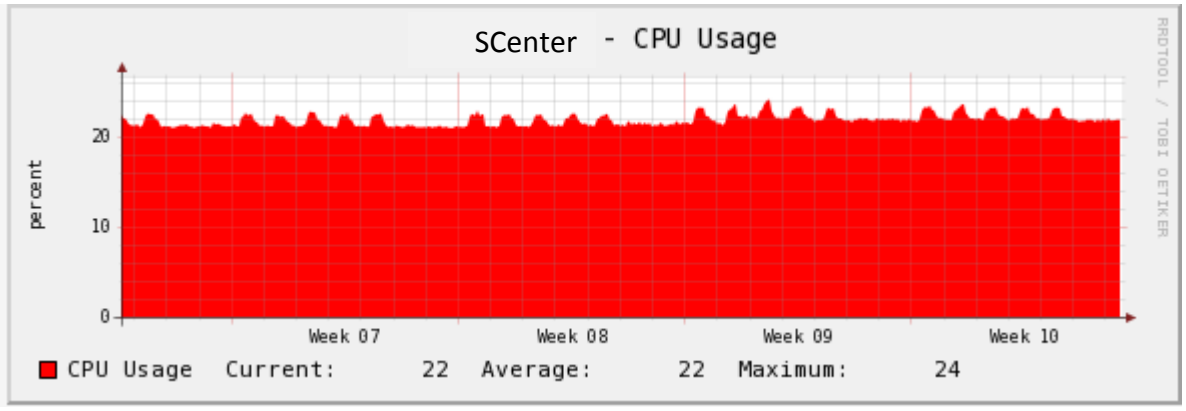
Obremenjenost centralno procesne enote je skladna z delovnim časom lokacije, opazili pa smo nenavadno visoko obremenjenost procesorja konec predzadnjega tedna, saj je več kot enkrat višja kot med ostalimi tremi vikendi v času monitoriranja. Vzroki so lahko različni, vsekakor pa so povezani s količino prometa na primerni internetni povezavi, saj je tudi ta ob istem času rahlo povišan.

Na grafu sekundarne internetne povezave ISDN ni posebnosti.

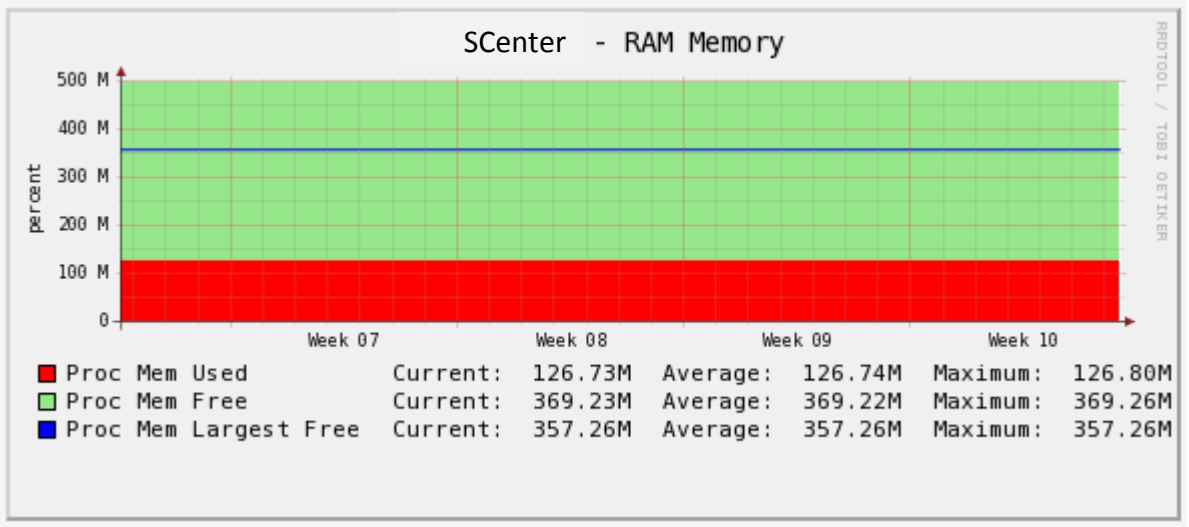
5.2.3. Rezultati monitoriranja stikala SCenter

Stikalo SCenter spada v družino zmogljivih stikal Cisco Catalyst in je glavno stikalo centralne lokacije, na katerega so priključena ostala nadstropna stikala. Njegovo delovanje omogoča povezavo ter delovanje vseh pomembnejših oddelkov organizacije.

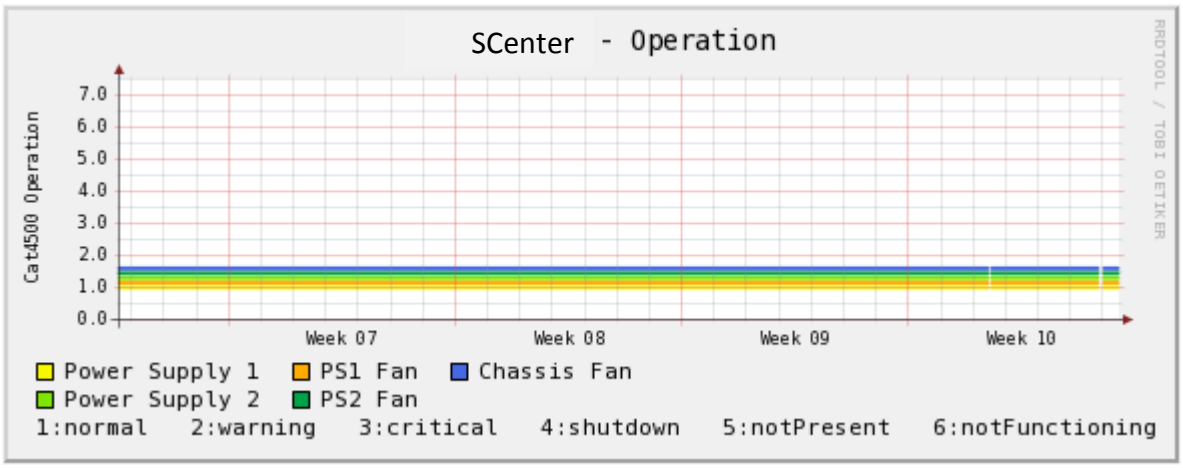
Slika 36 prikazuje obremenjenost centralno procesne enote, slika 37 porabo pomnilnika, slika 38 stanje ventilatorjev ter napajalnih enot, slika 39 temperaturo, slika 40 pa promet na vmesniku do strežnika za IP telefonijo.



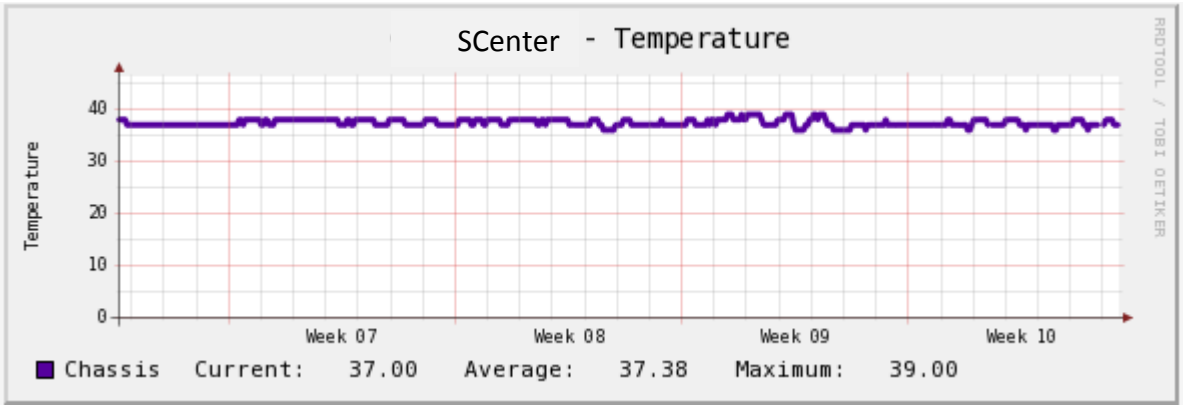
Slika 36: Obremenjenost centralno procesne enote.



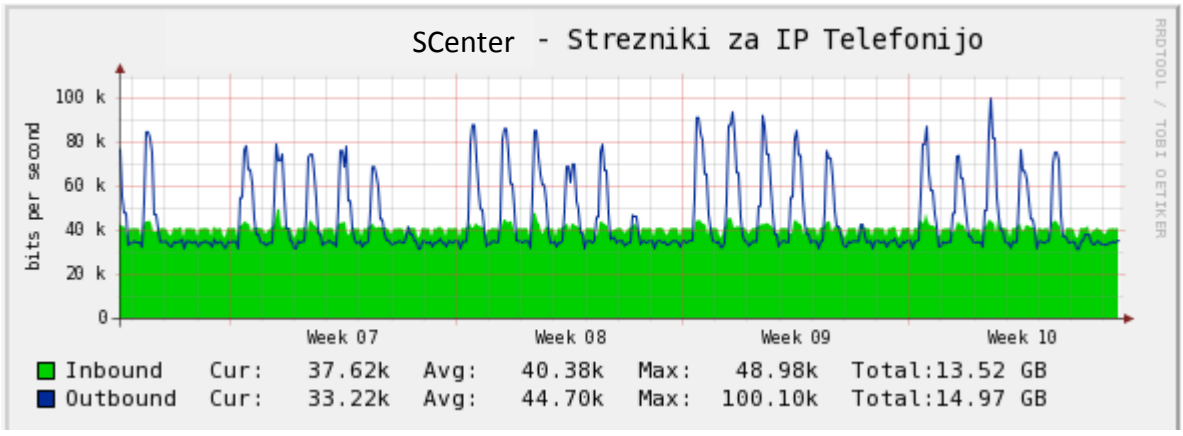
Slika 37: Poraba pomnilnika.



Slika 38: Stanje ventilatorjev ter napajalnih enot.



Slika 39: Temperatura.



Slika 40: Promet na vmesniku do strežnika za IP telefonijo.

Obremenjenost centralno procesne enote je nekoliko povečana ob delovnih dnevih, vendar ostaja v normalnih okvirjih.

Graf za porabo pomnilnika je brez posebnosti, poraba pomnilnika pa je konstantna.

Stanje treh ventilatorjev ter dveh napajalnih enot je normalno. Vse vrednosti so enake 1, vendar so zaradi večje preglednosti črte ena poleg druge in ne ena na drugi, zato se na prvi pogled morda zdi, da so vrednosti parametrov različne.

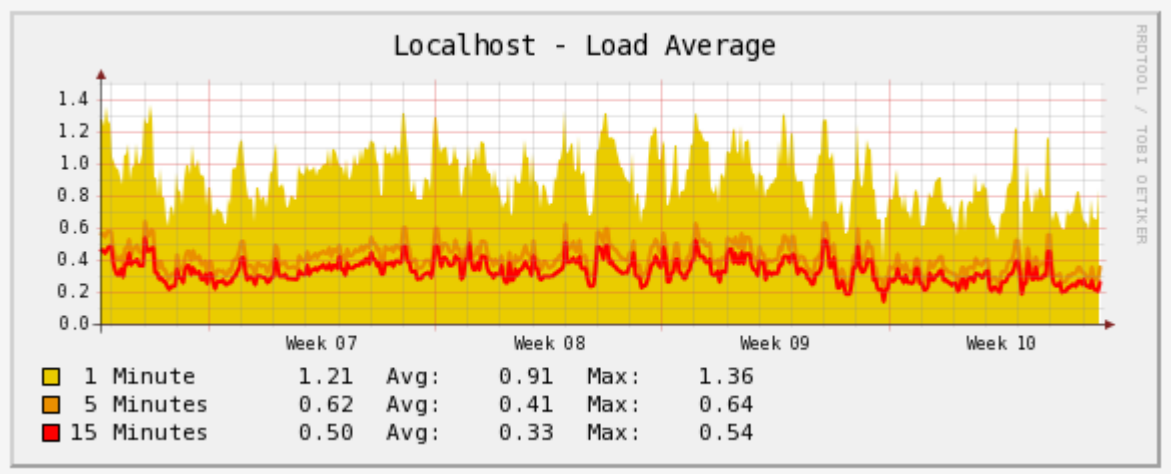
Temperatura niha med 37 in 39 stopinjami, kar je še vedno v skladu s priporočili proizvajalca.

Promet do strežnika za IP telefonijo je povečan ob delovnikih, na grafu ne opazimo nobenih posebnosti.

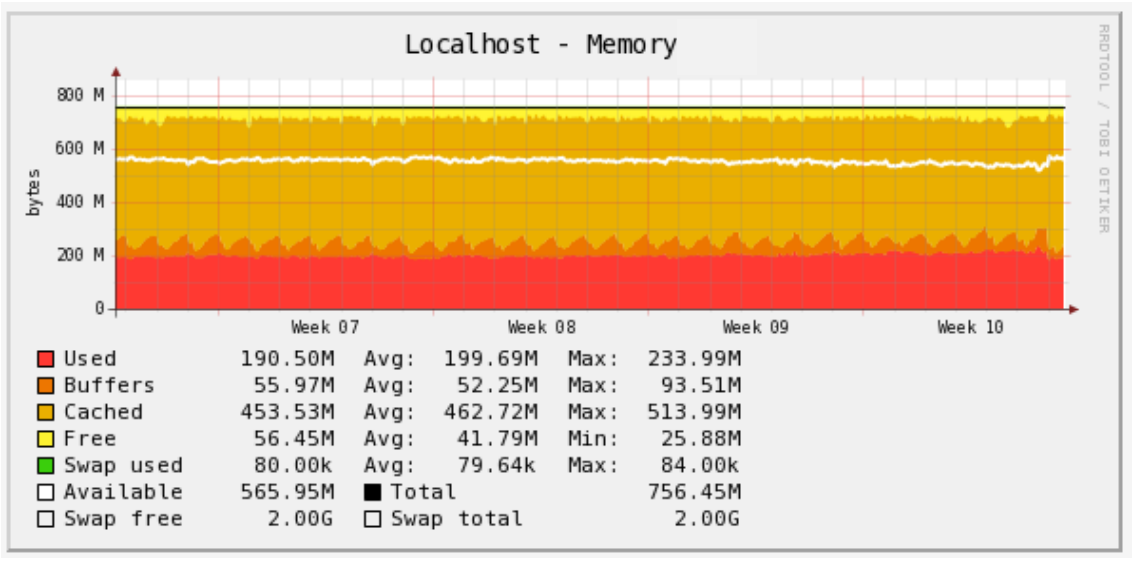
5.2.4. Rezultati monitoriranja Cacti strežnika

Cacti strežnik ima ključno vlogo pri spremljanju sistema s katerim monitoriramo omrežje. Nespametno bi bilo, da bi spremljali le informacijsko infrastrukturo, orodje pa zanemarili.

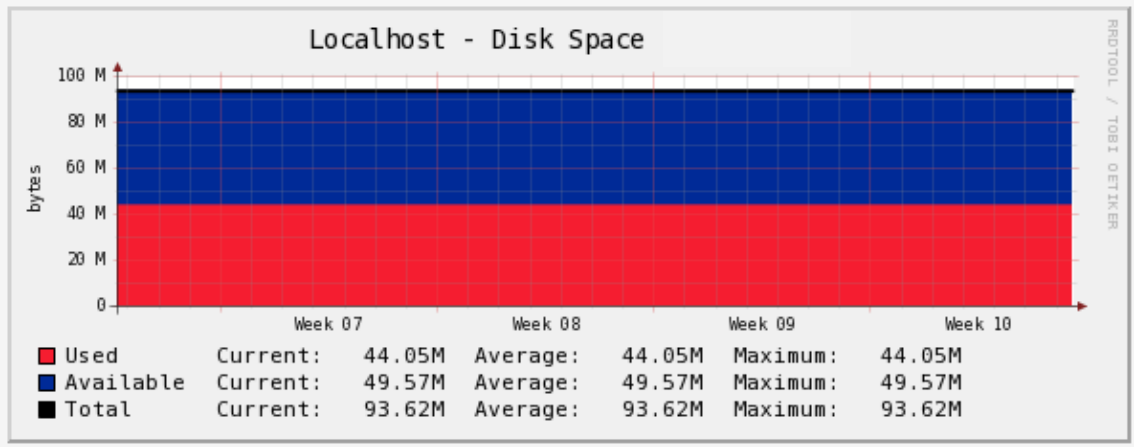
Spremljani parametri se razlikujejo od tistih pri mrežnih napravah, v splošnem pa tudi ti nakazujejo na delovanje ter obremenitev sistema. Slika 41 prikazuje povprečno obremenitev sistema, slika 42 porabo pomnilnika, slika 43 zasedenost diska, ter slika 44 število poizvedb v podatkovni bazi MySQL.



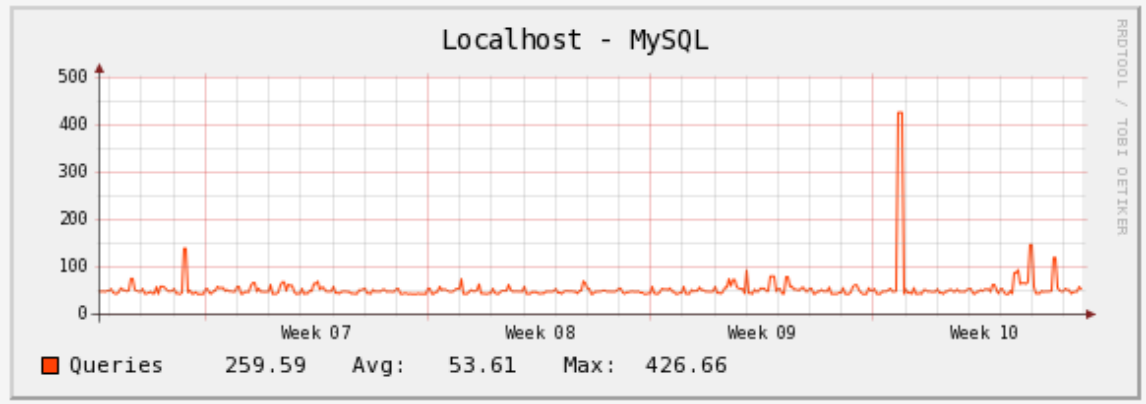
Slika 41: Povprečna obremenitev.



Slika 42: Poraba pomnilnika.



Slika 43: Zasedenost diska.



Slika 44: Število MySQL poizvedb.

Pomen oz. vrednost omenjenih grafov navadno pride do izraza šele ob netipičnem obnašanju sistema ter pri reševanju težav.

Povprečna obremenitev je močno odvisna predvsem od števila grafov oz. spremljanih parametrov. Več kot je grafov, večja bo obremenitev sistema. Rezultati prikazani na sliki 42 predstavljajo običajno sliko brez posebnosti.

Poraba pomnilnika prikazuje nekoliko več parametrov, kot pri mrežnih napravah, ker pomnilnik strežnika uporablja bolj napredno pomnilniško arhitekturo. Vrednosti na grafu so v mejah normale.

Glede na konstantno porabo lahko na podlagi grafa na sliki 44 ocenimo, da je velikost diska zadostna.

Število poizvedb v podatkovni bazi MySQL je v začetku zadnjega tedna monitoriranja močno naraslo. Vzroka nismo ugotovili, vsekakor pa nakazuje na neko anomalijo, ki ni v korelaciji z ostalimi spremljanimi parametri Cacti strežnika.

6. Zaključek

S pojavom in množično uporabno Interneta ter z razvojem vedno novih naprav ter storitev, ki podpirajo ali potrebujejo računalniška omrežja za delovanje, je dostop do Interneta postal ena izmed potreb sodobne družbe. Omrežja uporablja vedno več uporabnikov, zato je zelo pomembno, da delujejo dobro.

V diplomski nalogi smo predstavili ter komentirali rezultate enomesečnega monitoriranja srednje velikega omrežja. Uporabili smo odprtokodno programsko orodje Cacti, meritve pa so bile opravljene iz strežnika na centralni lokaciji. Rezultate smo predstavili v obliki grafov za obdobje enega meseca za vzorčne naprave, saj bi bilo nesmiselno predstavljati rezultate trideset in več usmerjevalnikov na oddaljenih lokacijah, ki imajo v omrežju enako vlogo in so enakega tipa. Rezultati so zelo podobni, nobena lokacija ne izstopa posebej, zato smo izbrani dve oddaljeni lokaciji izbrali naključno. Ugotovili smo, da so vrednosti na grafih močno povezane z delovnim časom monitoriranih lokacij ter korelacijo med grafi obremenjenosti centralno procesne enote ter prometa. Večjih težav ali izpadov nismo zaznali, kar nakazuje na to, da je bilo omrežje dobro načrtovano ter vzdrževano.

Sistem spremljanja bi lahko razširili z dodatnimi parametri ter z meritvami, ki bi jih izvajale sonde na več lokacijah. Tako bi lahko tudi preverjali dosegljivost raznih servisov oz. uporabniške izkušnje.

Monitoriranje je ključnega pomena, če želimo biti proaktivni pri odkrivanju težav, če želimo vedeti kaj se v našem omrežju dogaja, kaj lahko izboljšamo ter pri načrtovanju širitve omrežja. Vse to je zelo pomembno, če želimo zagotoviti, da bodo omrežja delovala dobro.

7. Viri

[1] Andrew S. Tanenbaum, Computer Networks, Prentice Hall, Upper Saddle River, 2002

[2] http://learn-networking.com/network-design/a-guide-to-network-topology

[3] http://www.learn-networking.com/wp-content/oldimages/network-topology.jpg

[4] http://www.islovar.org (pasivna naprava)

[5] http://www.ciscopress.com/articles/article.asp?p=31276&seqNum=2

[6] http://www.ciscopress.com/articles/article.asp?p=31276

[7] http://www.datacottage.com/nch/fibre.htm

[8] http://www.ciscopress.com/articles/article.asp?p=31276&seqNum=3

[9] http://www.islovar.org (aktivna naprava)

[10] http://www.islovar.org (puščanje pomnilnika)

[11] http://www.ietf.org/rfc/rfc1157.txt

[12] Douglas R. Mauro, Kevin J. Schmidt, Essential SNMP, O'Reilly, Sebastopol, 2001

[13] Joseph D. Sloan, Network Troubleshooting Tools, O'Reilly, Sebastopol, 2001

[14] http://www.networkmanagementsoftware.com/snmp-tutorial-part-2-rounding-out-the-basics

[15]http://www.networkmanagementsoftware.com/wp-content/uploads/SNMP_OID_MIB_Tree.png

[16] http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

[17]http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.4.1.9.9.109.1.1.1.1.8#oidContent

[18]http://docs.cacti.net/manual:087:2_basics.0_principles_of_operation#principles_of_operation

[19] http://docs.cacti.net/manual:087:8_rrdtool#rrdtool