DOI: 10.19279/TVZ.PD.2015-3-3-11

# NADZOR MREŽNIH UREĐAJA POMOĆU OPENNMS APLIKACIJE

# NETWORK DEVICE MONITORING BY OPENNMS APPLICATION

**Igor Jadan[1], Dubravko Žigman[2], Gordan Davidović[2]**

*[1]Student TVZ-a,*
*[2]Tehničko Veleučilište u Zagrebu, Elektrotehnički odjel*

## Sažetak

Nadzor mrežne komunikacijske infrastrukture osnova je rada mrežnih administratora koji se brinu da sustav radi sa što većom dostupnošću i na što bržem rješavanju problema. Kao osnova prikazan je FCAPS model i koje značajke su njime pokrivene. Definirani su načini komunikacije mrežnih uređaja sa NMS sustavom uz opis protokola koji se za to koriste. Kao jedno od dostupnih besplatnih rješenja odabran je i detaljno testiran OpenNMS sustav. Na realnom primjeru utvrđeni su tipični zahtjevi koji se pojavljuju u svakodnevnom poslu mrežnog administratora. Instalacijom OpenNMS sustava utvrđena je njegova upotrebljivost u navedenom slučaju.

***Ključne riječi:*** *Nadzor, mreža, NMS, FCAPS, OpenNMS*

## Abstract

Monitoring network communications infrastructure is the daily task for network administrators who are concerned that the system works with the maximum availability and take actions to quickly resolve problems. Presented FCAPS model and its features are the basis of network monitoring. Defined modes of communication describe interaction between network devices and NMS system with a description of the protocol that are used for communication. After market review and short overview of the best and most interesting tools for the monitoring of communications equipment, OpenNMS application is tested in detail. Usability of OpenNMS application for monitoring the status of network communications equipment of smaller and larger network environments is confirmed on defined network scenario.

***Keywords:*** *Network, management, NMS, FCAPS, OpenNMS*

## 1. Uvod

## 1. *Introduction*

Sve veća kompleksnost mrežne infrastrukture u kompanijama stavlja veći teret na mrežne administratore koji se brinu o njoj. Kako se u mrežama nalaze uređaji raznih proizvođača, tipova i generacija, održavanje sustava bez posebnih alata sve je teža. Veliki izazov mrežnima administratorima je pronaći adekvatne aplikacije koje će pružiti pravovremenu i ispravnu informaciju o stanju mrežne infrastrukture. Na tržištu postoji velik broj alata za nadzor mrežnih uređaja od skupih komercijalnih rješenja renomiranih kompanija, do besplatnih rješenja.

## 2. FCAPS model

## 2. *FCAPS model*

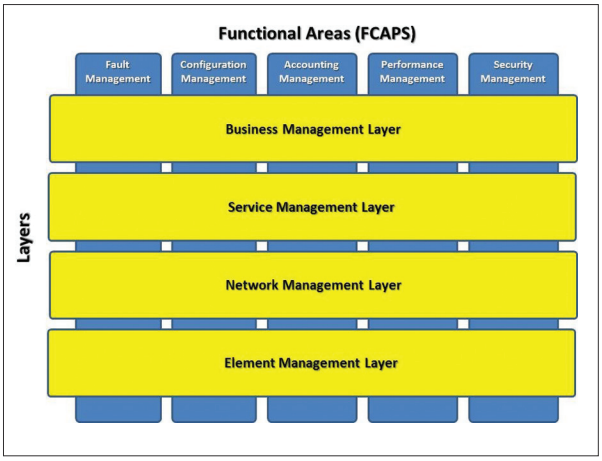
FCAPS model nastao je 1997. godine kao nadogradnja na TMN (*Telecommunications Management Framework*) standard kreiran za potrebe pružatelja telekomunikacijskih usluga. 1996. godine TMN je kreirao ITU-T (*International Telecommunications Union*), a opisuje servisne modele u 4 nivoa nazvanih: business management (upravljanje poslovanjem), service management (upravljanje servisima), fault and performance management (upravljanje pogreškama i performansama) i element and configuration management (upravljanje elementima i konfiguracijama). Cijeli koncept

opisan je kroz ITU-T preporuke M.3010 i M.3400. Već sljedeće godine nastaje njegova nadogradnja u vidu FCAPS-a koji se fokusira na pet funkcionalno različitih tipova zadataka koje vrše sustavi za upravljanje mrežom: fault management (upravljanje pogreškama), configuration management (upravljanje konfiguracijama), accounting management (obračun troškova), performance management (upravljanjem performansama) i security management (upravljanje sigurnošću) Tablica 1 prikazuje popis nivoa i kratak opis njihovog značenja.[1]

***Tablica 1*** *FCAPS nivoi*

***Tablica 1*** *FCAPS layers*

| | | |
|---|---|---|
| F | Fault | Prepoznavanje, ispravljanje i izolacija problema, alarmiranje, dijagnostika problema |
| C | Configuration | Skupljanje, arhiviranje, distribucija i praćenje promjena u konfiguracijama uređaja, automatska distribucija nadogradnji operativnog sustava na uređajima, praćenje i dokumentiranje informacija o opremi |
| A | Accounting | Praćenje korištenja resursa i raspodjela troškova po poslovnim jedinicama, upravljanje kvotama |
| P | Performance | Praćenje performansi na uređajima, prometa, brzine odgovora, iskorištenosti veza, pojave grešaka |
| S | Security | Provjera sigurnosnih događaja i alarmiranje na napade, kontrola dozvole pristupa uređajima, autorizacija |




***Slika 1*** *Isprepletenost TMN i FCAPS* [6]

***Figure 1*** *Interaction between TMN and FCAPS* [6]

## 3. Komunikacija s mrežnim uređajima

## 3. *Communication with network devices*

U svim imalo kompliciranijim mrežama koriste se uređaji raznih proizvođača i koji služe za razne namjene. Samim time prikupljanje podataka sa njih nije nimalo jednostavan posao i zahtijeva korištenje raznih protokola i direktnog pristupa opremi. Najrasprostranjeniji je pristup putem SNMP (*Simple network management protocol*) protokola koji podržavaju svi mrežni uređaji i putem njega, osim čitanja podataka, moguće je i konfiguracija uređaja. [2] SNMP protokolom definiran je MIB (*Management Information Base*) koji opisuje objekte koje može čitati i/ili mijenjati SNMP agent na uređaju. Kada nadzorna aplikacija i agent na uređaju komuniciraju, MIB objekte koje pozivaju nazivamo OID-ovima (*Object Identifier*). SNMP protokol omogućava mnogo, ali nije idealan i dostatan za upravljanje svim uređajima. U pomoć tada uskače pristup uređajima putem komandne linije gdje se mogu izvršavati i razne naredbe sa kojima je moguće izvući više informacija koje nekada nisu dostupne putem SNMP-a. Za pristup uređaju koristi se najviše SSH (*Secure shell*) protokol, a uređaji u pravilu podržavaju i TELNET protokol koji se nastoji izbjeći zbog lošeg sigurnosnog aspekta (promet se ne kriptira). Syslog poruke koje uređaji mogu slati koriste se najviše za detektiranje određenih događaja na opremi (npr. kada se izvadi modul iz kućišta velikog Cisco usmjernika, u syslog poruci se vidi vrijeme i opis tog događaja) koja aktiviraju alarme u nadzornoj aplikaciji, a mogu pružati i razne informacije koje korelacijom pružaju kvalitetniju analizu događaja. Svi ranije spomenuti načini prikupljanja informacija ili podešavanja uređaja su korišteni i prije uspona interneta i web tehnologija, tj. potječu iz 80-tih godina prošlog stoljeća (SSH je malo mlađi protokol i nastao je 1995.). Kako vrijeme brzo prolazi i dolaze nove tehnologije, a taj trend je posebno vidljiv u računalnom svijetu, pojavile su se i neki novi načini dohvata podataka i podešavanja komunikacijske opreme. Kako bi se doskočilo napretku tehnologije i poboljšalo upravljanje uređajima, IETF

(*Internet Engineering Task Force*) je 2006. predstavio novi prijedlog Netconf (*Network Configuration Protocol*) protokola za upravljanje komunikacijskim uređajima (RFC 4741 [7]). Tijekom 2011. godine predstavljena je nova unaprijeđena verzija standarda koja vrijedi i danas (RFC 6241 [8]). Glavna karakteristika je korištenje XML-a (*Extensible Markup Language*) za prenošenje informacija kodiranih UTF-8 kodnoj stranici. Korištenje XML-a omogućuje pregledniji i hijerarhijski način oblikovanja i prikaza podataka, a svakom proizvođaču opreme omogućuje i proizvoljno definiranje oznaka (tag). Komunikacija između klijenta i servera (aplikacije za nadzor) koncipirana je na jednostavnoj RPC (*remote procedure call*) razmjeni poruka između klijenta i servera, uz uspostavljanje logičke sesije. Transport poruka je kriptiran (u standardu je definirana obavezna podrška za SSH), a transportni protokol mora biti pouzdan i konekcijski kako bi se osigurala isporuka svih podataka. Gubitak dijela podataka prilikom konfiguriranja uređaja bi uzrokovao greške u konfiguraciji i naravno probleme sa takvim nepotpuno podešenim uređajima. [3] [4] [7] [8] [9]

## 4. Tržište

## 4. *Market*

Gartner je u najnovijem istraživanju tržišta NPMD (*Network Performance monitoring and diagnostics*) izvještaju analizirao alate za nadzor mrežne opreme i performanse aplikacija kako bi se mogao mjeriti i iskustvo krajnjeg korisnika. Ovdje se osim standardnog praćenja rada i performansi mrežnih komponenti, prate fizički i virtualni server, diskovni sustavi, mrežne veze, korisničko iskustvo korištenja usluge (dostupnost, brzina odziva sa mrežnog pogleda), analiza uobičajenog ponašanja mreže i sl. Prema zadanim kriterijima pojedinim alatima se


***Slika 2***
*Gartner Magic Quadrant 2014* [10]

***Slika 2***
*Gartner Magic Quadrant 2014* [10]

kvantificira sposobnost izvršavanja (*Ability to Execute*) i kompletnost vizije (*Completeness of Vision*). Kod sposobnosti izvršavanja ili pružanja kvalitetne usluge analizira se sam produkt, veličina i stabilnost kompanije, prisutnost na svjetskim tržištima i fleksibilnost modela licenciranja, kredibilitet kompanije kod korisnika i zadovoljstvo korisnika. Kod kompletnosti vizije promatra se marketinška i prodajna strategija kompanije, skalabilnost ponuđenog rješenja, inovativnost i dostupnost u svijetu. Smještajem u kvadrant dobiju se četiri polja koja prikazuju sljedeće kategorije: vođe (**Leaders**), izazivači (**challengers**), vizionari (**visionaries**) i nišni igrači (**Niche Players**). Kako se vidi na slici (Slika 2 Gartner Magic Quadrant 2014), proizvodi velikih kompanija (*CA Technologies, Hewlet-Packard*) ne znače da su najbolji i najkompletniji. U ovom slučaju Riverbed Cascade, Fluke Networks Visual TruView™ i JDSU-Network Instruments alati su jedini zaslužili titulu vođa [10].

Trend sve većih i kompliciranijih sustave zahtijeva detaljniju analizu i povezivanje podataka o praćenju komunikacijske opreme, poslužitelja, virtualnih okolina, diskovnih sustava, baza podataka kako bi se mogla pružiti najbolja usluga korisnicima i ubrzalo detektiranje problema u sustavu.

Osim rješenja velikih kompanija, na tržištu postoji mnoštvo aplikacija za nadzor mrežne opreme razvijenih od malih kompanija koji imaju puno nižu cijenu od velikih sustava, a mogu zadovoljiti velik dio korisnika. Svi korisnici ne trebaju cjelokupne pakete, već im je dovoljno pronaći što povoljnije rješenje za neki od svojih zahtijeva. Tako su dvije najbitnije stvari koje mrežni administrator mora imati pokrivene: upravljanje problemima (*Fault Management*) i praćenjem performansi sustava (*Performance Management*). Ukoliko ne postoji budžet ili je jako limitiran, korisnici mogu pribjeći nekoj od niže navedenih alternativa. Niža cijena u pravilu zahtijeva i veće znanju o načinu rada opreme, kao i pisanju skripti u raznim jezicima.

## 5. Postojeće stanje i zahtjevi na sustav

## 5. *Current situation and requirements*

Tvrtka manje veličine namjerava unaprijediti održavanje mrežne opreme kako bi smanjila broj ispada i dobila bolji uvid u opterećenost i iskorištenost mrežne opreme. Mrežna oprema je od proizvođača Cisco, a u nadležnosti mrežnih administratora je i uređaj za neprekidno napajanje (UPS) proizvođača APC. Uz sistem salu sa većim brojem uređaja, postoje i niz izdvojenih lokacija na kojima se u pravilu nalazi jedan Cisco usmjernik, jedan APC Smart UPS i minimalno jedan Cisco preklopnik. Uz zahtjeve iz tablice 2, postavljen je i dodatni zahtjev za korištenje besplatnog alata. Za testiranje ovog scenarija korišten je dio opreme iz produkcijske okoline jedne velike kompanije i napravljena je testna okolina, a odabran je OpenNMS sustav zbog svojih mogućnosti i cijene (besplatan). OpenNMS aplikacija može se instalirati na neki od sljedećih operativnih sustava: YUM/RPM, APT/Debian (uključujući i Ubuntu), Windows ili Mac OS X. U laboratorijskoj okolini kreiran je jedan virtualni server u VMware® Player 5 virtualizacijskoj

***Tablica 2*** *Traženi uvjeti*

***Tablica 2*** *Requirements*

| Broj | Uvjet |
|---|---|
| 1 | Automatsko prepoznavanje i modeliranje uređaja putem SNMP protokola |
| 2 | Alarmiranje na osnovi SNMP trap-ova |
| 3 | Alarmiranje na osnovi Syslog poruka |
| 4 | Pristup ovlaštenim korisnicima |
| 5 | Specifični alarmi |
| 5.1 | Alarm za svako podešavanje lokalnih korisnika na uređajima |
| 5.2 | Alarm za neispravnu bateriju u UPS-ovima |
| 5.3 | Alarm za gubitak napajanja UPS-a i skorom pražnjenju baterije |
| 5.4 | Alarm za neispravan ventilator na uređaju |
| 6 | Praćenje opterećenja odabranih portova uz grafički prikaz |
| 7 | Praćenje dostupnosti svih uređaja |
| 8 | Praćenje opterećenja procesora, slobodne memorije i temperature na uređajima uz alarmiranje ukoliko prelazi proizvoljno definirane pragove |
| 9 | Izvještaji |
| 9.1 | O nedostupnosti uređaja |
| 9.2 | O događajima i alarmima prethodnog dana |
| 9.3 | O temperaturi uređaja |
| 9.4 | O stanju baterije UPS-ova |
| 9.5 | O serijskim brojevima uređaja |

okolini i dodijeljeni su mu sljedeći resursi: 1024MB radne memorije, 1 jezgra i 20 GB diskovnog prostora. Virtualni server je radio na računalu sa 4GB radne memorije, Intel Core2 Duo E6850 procesoru i Windows 7 Ultimate, 64-bit 6.1.7601, Service Pack 1 operativnom sustavu. Dakle radi se o nekoliko godina starom računalu i virtualiziranoj okolini što se moglo osjetiti u nekim slučajevima kada je bilo potrebno nekoliko sekundi na odgovor i prikaz nove web stranice. Tijekom rada sa na ovom sustavu dolazilo je do sporosti odaziva web stranica. Preporuča se instalacija OpenNMS-a direktno na računalo ili server kada je rad sa njim bio mnogo ugodniji. Za drugu instalaciju iskorišteno je stolno računalo Acer Veriton 680G (Intel Pentium G6950, 2GB RAM, 500GB SATA HDD) na kojem je OpenNMS radio brzo i stabilno. Računalo je spojeno u produkcijsku okolinu i sa dijela mrežne opreme usmjereno je slanje syslog i SNMP poruka na njega. Ti uređaji su modelirani i uključeno je praćenje prometa sa četrdesetak portova uz standardno modelirane vrijednosti temperature, opterećenja procesora i sl.

## 6. OpenNMS

## 6. *OpenNMS*

Osim glavne aplikacije, za normalno funkcioniranje instalirana je Postgre 9.3 baza podataka, Java SDK 7 paket, syslog-ng syslog server i nekoliko OpenNMS dodataka: opennms – plugin – provisioning – snmp – asset koji omogućava skupljanje i kategoriziranje podataka o samim uređajima (npr. serijski broj), opennms – plugin – provisioning – map i opennms – plugin – provisioning – link koji omogućavaju prikaz uređaja na mapi i njihovo povezivanje. Podešavanje sustava moguće je putem web stranice ili editiranjem xml datoteka.
Neke naprednije funkcije i postavke moguće je mijenjati samo izmjenom odgovarajuće xml datoteke. Nakon nekog vremena i boljeg upoznavanja sa xml strukturom OpenNMS-a, editiranje xml datoteka može se pokazati kao najbrži način podešavanja sustava.
Skupljanje podataka i modeliranje uređaja vrši se putem SNMP protokola u bilo kojoj verziji (v1/v2c/v3) uz napomenu da se v3 postavke mogu podesiti kroz xml datoteku. SNMP komunikacija se koristi za skupljanje željenih podataka sa uređaja koji se mogu povijesno skupljati kako bi bili dostupni za grafički prikaz u željenom intervalu. Predefinirano je skupljanje podataka o stanju procesora, memorije, temperaturi i sličnim osnovnim podacima koje je potrebno pratiti na svakom uređaju. Podešavanjem praćenja određenog OID-a () uključuje se praćenje bilo koje zanimljive informacije. Kod praćenja pojedinih portova automatski se skupljaju informacije o količini prometa, unicast, multicast, broadcast, discard, error i dropped paketima. Praćenje prometa moguće je uključiti za sva ili samo odabrana sučelja na uređajima. Za APC UPS-ove prati se opterećenje (*Battery load*), napunjenost baterije, temperatura, vrijeme koliko još može UPS napajati opremu, VAC in/out i mrežni podaci sa porta. Ovo je dovoljno za kvalitetno praćenje stanja UPS-a i mogućnost kreiranja alarma za prelazak određenih pragova (npr. kada napunjenost baterije padne ispod 20%, preveliko opterećenje, previsoka temperatura).
Na osnovu zaprimljenih SNMP poruka kreirani su alarmi sa promijenjenom razinom kritičnosti ukoliko se na Cisco uređajima izvrši naredba koja mijenja lokalnu bazu korisnika. Prelaskom 80% opterećenja procesora aktivira se alarm koji se automatski prekida ukoliko isto opterećenje padne ispod razine od 50% u tri uzastopna očitanja vrijednosti.
Syslog podaci primaju se sa uređaja pomoću naknadno instaliranog syslog-ng servisa koji prosljeđuje odabrane poruke na OpenNMS syslogd servis. OpenNMS još jednom provjerava poruke i kreira događaje i alarme u sustavu ukoliko se pronađe odgovarajuće predefinirano pravilo koje poruka zadovoljava. Na taj način moguće je mijenjati i prilagođavati reakciju sustava na zaprimljenu poruku.
Ovaj način primanja podataka ima više koraka i kompliciraniji je za podesiti, ali je broj različitih Syslog poruka koje generiraju uređaji mnogo veći od SNMP poruka i u nekim slučajevima može biti bolji izvor podataka za neke ključne događaje. Osim liste alarma koje pojedini korisnik može preuzeti kako bi ih riješio, moguće je definirati posebne obavijesti za važne događaje. Ukoliko je potrebna brza reakcija na neku promjenu u mreži, generiranje obavijesti iz zaprimljenog događaja

omogućuje slanja poruke određenom korisniku ili grupi korisnika. Grupe korisnika slijedno primaju obavijest dok netko ne potvrdi primitak, a ukoliko događaj nitko ne potvrdi može se krenuti u drugi krug obavijesti prema višim razinama tvrtke. Na taj način važni događaji neće biti zaboravljeni ili zanemareni. OpenNMS je zadovoljio sve zadane uvjete (Tablica 2 Traženi uvjeti) i zadovoljava osnovne zahtjeve mrežnih administratora u malim i većim okruženjima. OpenNMS aplikacija za nadzor mrežne opreme je besplatna i pruža mnogo mogućnosti praćenja i prikupljanja podataka sa raznih tipova uređaja. Ukoliko ne postoje predefinirani opisi događaja sa nekog uređaja, moguće je definirati svoje događaje i prilagoditi ih da daju željenu reakciju. OpenNMS se može prilagoditi bilo kojem uređaju koji prihvaća SNMP upite, šalje SNMP trap-ove i syslog poruke što je karakteristika svih današnjih mrežnih uređaja. Upravljanje problemima (*Fault management*) i nadzor performansi (*Performanse management*) zadovoljit će većinu korisnika ukoliko koriste neki od poznatijih hardverskih platformi (Cisco, Juniper, HP, APC, Brocade,…) bez velike potrebe za intervencijom. Ukoliko se pojavi potreba za prepoznavanjem i dodavanjem novih senzora, to je lako napraviti kroz web sučelje ili editiranjem xml datoteka. Korisnici upoznati sa Linux/Unix serverima lako će se snaći i prilagoditi sve postavke kako bi dobili željen rezultat. Osim vizualnog prikaza mapa uređaja, Open NMS je radio izuzetno stabilno. Osnovni izvještaji pokrivaju glavne zahtjeve korisnika, a moguće je i kreirati nove izvještaje uz periodičko izvođenje i slanje korisnicima. Izrada izvještaja nije jednostavna i potrebno je naučiti koristiti dodatne alate, xml i strukturu baze podataka kako bi se dobio željeni izvještaj. OpenNMS alat može zadovoljiti potrebe većine korisnika, ali potrebno je uložiti puno truda kako bi se iz njega izvukao maksimum i potpuno prilagodio korisničkim željama. Dokumentacija i pomoć dostupna je na web stranicama proizvođača, ali nije uvijek točna i potpuna. Zahtjevniji korisnici mogu ugovoriti plaćenu podršku i time brže rješavati probleme i dobiti točniju informaciju za lakše podešavanje sustava. OpenNMS može zadovoljiti većinu potreba administratora mrežne opreme, ali zahtijeva i dobro poznavanje Linux/Unix sustava, SNMP (OID, mib datoteke) strukture podataka, strukture syslog poruka, regex izraza i izrade skripti kako bi se izvukao maksimum iz ovog alata. [5]

## 7. Podešavanje opreme

### 7. *Equipment adjustment*

Kako bi sve ove opisane funkcije radile, potrebno je podesiti komunikacijsku opremu za odgovaranje na upite OpenNMS sustava. Osnovno je podešavanje SNMP komunikacije, pa tako su u tablici prikazane konfiguracijske linije za podešavanje autentikacije, uključivanje i slanje SNMP trap-ova, slanje Syslog poruka i podešavanje slanja izvršenih CLI naredbi na Cisco opremi (Tablica 3 Podešavanje Cisco opreme). Radi sigurnosti preporuka je korištenje SNMPv3 protokola sa postavljenom enkripcijom i primjene pristupne liste kako bi se ograničio pristup uređaju tim putem. Ukoliko nema potrebe za konfiguriranjem putem SNMP-a, potrebno je koristiti pristupnu listu sa RO pravima (Read-Only – samo čitanje). APC Smart-UPS se konfigurira putem web sučelja i vrijede ista pravila kao i za Cisco opremu.

***Tablica 3*** *Podešavanje Cisco opreme*

***Tablica 3*** *Cisco equipment adjustment*

| Naredbe | Opis |
|---|---|
| `snmp-server view ONMS_view iso included`<br><br>`snmp-server group ONMS_read v3 auth read ONMS_view access 11`<br><br>`snmp-server user opennmstest ONMS_ read v3 auth md5 Pass!!opennms!!test priv des56 Priv##opennms##test access 11` | Podešavanje SNMPv3 korisnika i pristupa. Definiran je pogled naziva ONMS_view, grupa korisnika ONMS_read i korisnik opennmstest sa pripadajućim lozinkama. Za dodatnu sigurnost korištena je access-lista 11 koja definira koje IP adrese mogu komunicirati putem SNMP-a sa uređajem. Za grupu korisnika definirana je samo mogućnost čitanja podataka (read). |
| `snmp-server community SVR$##%VDSfsdf RO 11` | Za pristup putem SNMPv1/v2c protokola podešena je lozinka (community) SVR$##%VDSfsdf. Pristup je ograničen access-listom 11, a RO označava samo pravo čitanja SNMP podataka. |

| | |
|---|---|
| `snmp-server enable traps` | Uključuje slanje svih SNMP poruka na definirane servere. |
| `snmp-server host 192.168.1.4 public` | Slanje svih SNMP poruka na server 192.168.1.4 |
| `logging 192.168.1.4` | Ovime je određeno na koji server se šalju syslog poruke. |
| `logging history size 100`<br><br>`logging history debugging`<br><br>`logging facility local6`<br><br>`logging source-interface` | Dodatne postavke koje određuju koliko se poruka čuva u povijesti, koja razina poruka se bilježi (debugging – sve poruke), određuje se facility (local6) za kasnije lakše razvrstavanje poruka i interface sa kojeg dolazi poruka (npr. VLAN, loopback,…) čija će IP adresa biti prikazana u poruci. |
| `service timestamps log datetime msec localtime` | Određuje da vrijeme događaja koje se šalje syslog porukom bude prikazano u određenom formatu prema lokalnom vremenu na uređaju. |
| `archive`<br><br>`log config`<br><br>`logging enable`<br><br>`logging size 200`<br><br>`notify syslog contenttype plaintext`<br><br>`hidekeys` | Ove naredbe omogućuju kreiranje syslog poruke za svaku izvršenu naredbu putem CLI sučelja. Zahvaljujući hidekeys naredbi, lozinke i tajni podaci se maskiraju kako se ne bi slali u nesigurnom syslog formatu koji je lako pročitati. |

## 8. Rezultati istraživanja

## 8. *Research results*

Kompleksnost mrežne infrastrukture je u konstantnom porastu, osobito s aspekta mrežne sigurnosti potreban je veći broj uređaja kako bi se sustav obranio od neželjenih napada. Praćenje rada i održavanje mrežne opreme sve je zahtjevniji posao. Osnovni FCAPS model pokriva potrebe mrežnih administratora, te postoji mnogo pojedinačnih programa i paketa koji pokrivaju sve zahtjeve korisnika. Za kompletan nadzor mrežne infrastrukture potrebno je kombinirati dobivene informacije putem syslog poruka, SNMP upita, CLI naredbi i drugih dostupnih načina povezivanja sa opremom. Prikupljeni podaci moraju se korelirati i dedupliciratи alarme kako administratori ne bi bili zatrpani mnoštvom poruka koje bi odvratile pažnju od važnih događaja.

OpenNMS aplikacija za nadzor mrežne opreme je besplatna i pruža mnogo mogućnosti praćenja i prikupljanja podataka sa raznih tipova uređaja. Može zadovoljiti potrebe većine korisnika, ali potrebno je uložiti puno truda kako bi se iz njega izvukao maksimum i potpuno prilagodio korisničkim željama. Dokumentacija i pomoć dostupna je na web stranicama proizvođača, ali nije uvijek točna i potpuna. OpenNMS može zadovoljiti većinu potreba administratora mrežne opreme, ali zahtijeva i dobro poznavanje Linux/Unix sustava, SNMP (OID, mib datoteke) strukture podataka, strukture syslog poruka, regex izraza i izrade skripti kako bi se izvukao maksimum iz ovog alata.

Ubrzani razvoje tehnologije i sve veća kompleksnost računalnih mreža uzrokuje konstantno povećanje količine informacija sa infrastrukturnih uređaja koje administratori moraju provjeriti. U budućnosti će sve veći naglasak biti na praćenju korisnikovog iskustva korištenja usluge, a OpenNMS zahvaljujući svojim modulima i prilagodljivosti to već omogućuje. OpenNMS dimenzioniran je za obradu velike količine podataka, a zahvaljujući aktivnoj zajednici i mnoštvu nadogradnji pruža širu sliku događaja na mrežnoj i poslužiteljskoj infrastrukturi. Zbog svoje prilagodljivosti i jednostavnosti, OpenNMS će biti zanimljiv svim korisnicima koji traže besplatan alat sa širokim pogledom na mrežnu i sistemsku infrastrukturu.

## 9. Reference

## 9. *References*

[1] The Shorcut Guide To Network Management for the Mid-Market, Greg Shields, 2007. Realtime publishers, http://nexus.realtimepublishers.com/SGNMM.php

[2] Network Management: Principles and Practices, Mani Subramanian, Prentice Hall PTR, 2012

[3] Principles of Computer Systems and Network Management, Dinesh Chandra Verma, Springer Science +Business Media, LLC 2009

[4] Network Management know it all, Farrel Adrian, Morgan Kaufmann Publishers, 2009.

[5] The Practice of System and Network Administration Second edition, Thomas A. Limoncelli, Christina J. Hogan, Strata R. Chalup, Addison-Wesley, 2007

[6] http://www.metanoia-inc.com/blog/2012/05/14/operator-metrics-that-matter-from-network-metrics-to-business-metrics/, J.R. Smolka, 20.06.2014.

[7] http://tools.ietf.org/html/rfc4741, 22.04.2014

[8] http://tools.ietf.org/html/rfc6241, 24.04.2014

[9] http://en.wikipedia.org/wiki/NETCONF, 24.04.2014

[10] http://www.flukenetworks.com/content/gartner-npmd-magic-quadrant, 20.06.2014

## AUTOR · *AUTHOR*

**Dubravko Žigman**- nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 2, No. 1, 2014.

**Gordan Davidović**- nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 2, No. 1, 2014.