Usporedna analiza sustava za upravljanje i nadzor računalnih mreža

Vizner, Valentino

Undergraduate thesis / Završni rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:480521

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Valentino Vizner

Usporedna analiza sustava za upravljanje i nadzor računalnih mreža

ZAVRŠNI RAD

Zagreb, 2016.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

USPOREDNA ANALIZA SUSTAVA ZA UPRAVLJANJE I NADZOR RAČUNALNIH MREŽA

COMPARATIVE ANALYSIS OF MANAGEMENT AND MONITORING SYSTEMS OF COMPUTER NETWORKS

Mentor: doc. dr. sc. Ivan Grgurević

Student: Valentino Vizner, 0135228192

Zagreb, 2016.

USPOREDNA ANALIZA SUSTAVA ZA UPRAVLJANJE I NADZOR RAČUNALNIH MREŽA

SAŽETAK

Računalne mreže su promijenile i ubrzale način komunikacije u današnje vrijeme i temelj su za razvoj ostalih sustava, organizacija, poduzeća, jer omogućavaju kvalitetnu i brzu komunikaciju s ostalim korisnicima računalnih mreža. Kako bi se postigla kvalitetna i pouzdana mreža, potrebno je uspostaviti politiku upravljanja računalnih mreža, a kroz upravljanje odrediti parametre za nadzor računalnih mreža. Zbog ubrzanog rasta i ekspanzija računalnih mreža krajem prošloga stoljeća i početkom ovoga, većina mreža se nije kvalitetno prilagodila takvim brzim ekspanzijama. Zato postoje modeli koji nastoje ispraviti te probleme, kroz upravljanje i nadzor računalnih mreža. Za kvalitetniju provedbu upravljanja i nadzora računalnih mreža, potrebno je odabrati sustav (računalne programe) te provesti usporednu analizu sustava za upravljanje i nadzor računalnih mreža. Kroz usporednu analizu sustava za upravljanje i nadzor računalnih mreža, promatra se upravljanje i nadzor kao dvije odvojene cjeline, ali također prikazuje koliko su isprepletene i zajedno čine računalni sustav funkcionalnim.

KLJUČNE RIJEČI: računalne mreže; upravljanje i nadzor računalnih mreža; usporedna analiza; sustavi za upravljanje i nadzor računalnih mreža

SUMMARY

Computer networks have changed and accelerated mode of communication nowadays and are the basis for the development of other systems, organizations, companies, because they enable high-quality and instant communications with other users of computer networks. In order to achieve high-quality and reliable networks, it's necessary to establish a policy for the management of computer networks and through management to determine the parameters for monitoring computer networks. Due to rapid growth and expansion of computer networks at the end of the last century and the beginning of this, most of the networks are not well adapted to such rapid expansions. Therefore, there is a model that seeks to correct these problems, through the management and control of computer networks. For better implementation of the management and control of computer networks, it is necessary to select the system (computer programs) and to carry out a comparative analysis of the management and control of computer networks. Through a comparative analysis of the management and control of computer networks, management and control are treated as two separated

units, but also shows how they are intertwined and together make a well functioning computer system.

KEY WORDS: computer networks; management and monitoring of computer networks; comparative analysis; systems for management and monitoring of computer networks

Sadržaj:

1.Uvod 1
2. Značajke računalnih mreža 3
2.1. Mrežni hardver 3
2.1.1 Osobne računalne mreže (PAN) 4
2.1.2 Lokalne računalne mreže (LAN) 5
2.1.3 Mreža na području grada (MAN) 7
2.1.4 Široko područna mreža (WAN) 8
2.2 Mrežni softver 10
2.2.1 Protokolna hijerarhija 10
2.2.2 Dizajniranje slojeva 11
2.3 Referentni modeli 12
2.3.1 OSI referentni model 12
2.3.2 TCP/IP model 15
3. Upravljanje računalnim mrežama 16
3.1 Osnovni protokoli za upravljanje računalnim mrežama 16
3.1.1 Komunikacijski protokol za kontrolu poruka (ICMP) 16
3.1.2 Jednostavni mrežni protokol za nadzor i upravljanje (SNMP) 17
3.2 Politika upravljanja računalnim mrežama (FCAPS) 20
3.2.1 Upravljanje pogreškama (F) 20
3.2.2 Upravljanje konfiguracijama (C) 23
3.2.3 Upravljanje politikom naloga (A) 25
3.2.4 Upravljanje performansama (P) i Upravljanje sigurnošću (S) 26
4. Nadzor računalnih mreža 30
4.1 Model za nadzor računalnih mreža (FCAPS) 30
4.1.1 Nadzor pogrešaka (F) 31
4.1.2 Nadzor konfiguracija (C) 32
4.1.3 Nadzor politike naloga (A) 32
4.1.4 Nadzor performansi (P) i nadzor sigurnosti (S) 34
4.2 Nadzor pojedine mreže 37

4.3 Nadzor Interneta kao mreža svih mreža 38
4.4 Tehnike i protokoli za nadzor mreže 39
5. Sustavi za upravljanje i nadzor računalnih mreža 41
6. Usporedna analiza sustava za upravljanje i nadzor računalnih mreža 48
6.1 Usporedna analiza sustava za upravljanja i nadzor pogrešaka (F) 48
6.2 Usporedna analiza sustava za upravljanje i nadzor konfiguracijama (C) 53
6.3 Usporedna analiza sustava za upravljanje i nadzor politike naloga (A) 57
6.4 Usporedna analiza sustava za upravljanje i nadzor performansi (P) i sigurnosti (S) 60
7. Zaključak 67
Literatura 69
Popis kratica i akronima 71
Popis slika 75
Popis tablica 76

1.Uvod

Zadnja tri stoljeća su bila dominantna jednom od novih tehnologija, prvo su to bili mehanički sustavi, zatim doba parnih strojeva i na kraju dvadeseto stoljeće, informatičko doba. Računalne mreže su doživjele svoju ekspanziju u 20. stoljeću te i dalje rastu. Računalne mreže su izrasle u kompleksne sustave za skupljanje, prijenos, skladištenje i procesiranje informacija te granice između tih nekad odvojenih područja nestaju. Nakon pojave Interneta dolazi do velike ekspanzije računalnih mreža i potrebe za njima, tako da je potrebno veliku pažnju usmjeriti kako takve mreže upravljati, nadzirati i omogućiti im daljnji rast, skalabilnost. Tehnologija iz dana u dan napreduje i teško je predvidjeti što donosi sutra, ali računalne mreže zajedno s upravljanjem i nadzorom, čine se kao jedan neizostavni dio svih budućih računalnih tehnologija. Kroz jednostavnost upotrebe su računalne mreže postale dio te ljudske komunikacije i život bez ovog oblika komunikacije, gdje je jednostavno razmjenjivati informacije u sekundi se čini nemoguć.

Cilj završnog rada je provesti usporednu analizu sustava za upravljanje i nadzor računalnih mreža kroz alate za upravljanje i nadzor računalnih mreža te kakva je problematika i da li je moguće upravljanje bez nadzora i obratno.

Dok je svrha steći osnovna znanja vezana za računalne mreže te upoznavanje modela i načina kojim se obavlja upravljanje i nadzor računalne mreže. Svrha je također steći osnovna znanja o sustavima za upravljanje i nadzor te prepoznati razlike između upravljanja i nadzora kroz usporednu analizu.

Naziv završnog rada je **Usporedna analiza sustava za upravljanje i nadzor računalnih mreža** i podijeljen je na sedam povezanih poglavlja:

1. Uvod
2. Značajke mrežnih računala
3. Upravljanje računalnom mrežom
4. Nadziranje računalne mreže
5. Sustavi za upravljanje i nadzor računalne mreže
6. Usporedna analiza sustava za upravljanje i nadzor računalne mreže
7. Zaključak

Uvodno poglavlje opisuje informatičko doba i razvoj računalnih mreža te da je 20. stoljeće, stoljeće najveće ekspanzije računalnih mreža. U njemu se navodi cilj, svrha i struktura rada.

U drugom poglavlju su detaljno opisane značajke računalnih mreža, kako bi se stekao temelj za daljnje analize i usporedbe istih. Prvo se opisuje mrežni hardver te kakve vrste mreža postoji. Nakon toga će se objasniti protokolna hijerarhija kako bi se smanjila kompleksnost mreže i kako su se dizajnirali slojevi i povezani protokoli. Na kraju će se opisati dva referentna modela, koji se sastoje od tih slojeva i protokola kako bi se segmentirala kompleksnost mreže i lakše raspodijelilo upravljanje mrežom.

U trećem poglavlju se definira upravljanje računalnom mrežom, prvo glavni protokoli koji se koriste za upravljanje mrežom, a zatim i sama politika upravljanja računalnom mrežom. Model za upravljanje i nadzor, često zvan politika upravljanja (engl. *Fault, Configuration, Accounting, Performance, Security management*, FCAPS) je taj koji se koristi za upravljanje mrežom i svako područje toga modela će se detaljno objasniti.

Četvrto poglavlje se bazira na nadzoru računalne mreže, također će se opisivati kroz FCAPS model, međutim ne sa stajališta upravljanja mrežom, nego samo njen nadzor. Također će se svako područje detaljno opisati i referirati se na upravljanje mrežom.

Peto poglavlje objašnjava jedan cjeloviti sustav za upravljanje i nadzor računalne mreže, kroz računalni program SolarWinds. Ukratko će se opisati njegov izgled i od čega se sve sastoji te da li pokriva cijeli FCAPS model i čini jedan sustav za upravljanje i nadzor računalne mreže.

U šestom poglavlju provedena je detaljna usporedna analiza sustava za upravljanje i nadzor računalnih mreža. To je i glavna tema završnog rada, tako da će se selektirati posebno upravljanje i posebno nadzor te sve to kroz računalni program Solarwinds. Na kraju će se vidjeti koje su to razlike i da li je moguće upravljanje bez nadzora i obrnuto.

Na kraju se donosi zaključak u kojem se prolazi kroz cijeli rad i sustavno donose zaključci vezani za temu rada odnosno koliko je bitna usporedna analiza sustava za upravljanje i nadzor računalne mreže u današnjem svijetu.

2. Značajke računalnih mreža

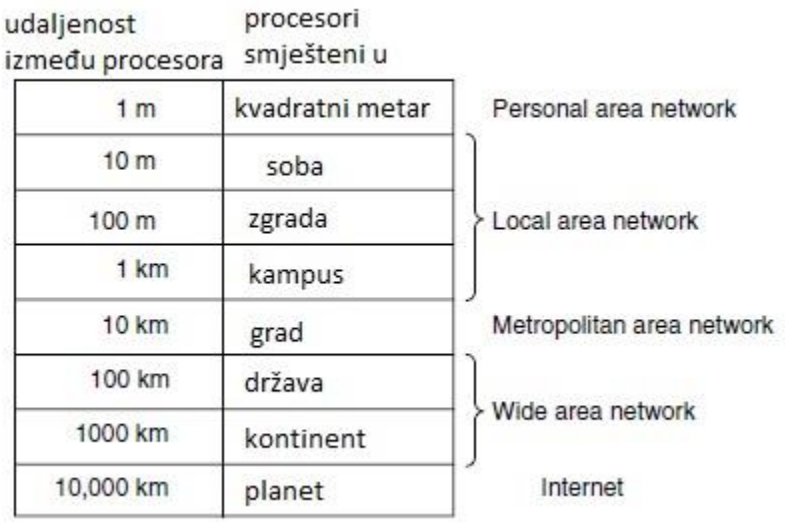
Na početku rada potrebno je definirati – pojam računalne mreže. Računalna mreža je skup autonomnih računala, povezanih određenom tehnologijom. Kada se kaže da su računala povezana, minimalno dva računala, to znači da su u mogućnosti izmjenjivati informacije. Povezanost ili umrežavanje se može postići putem bakrene žice, optičkog vlakna, mikrovalova, infracrvene tehnologije, satelitskim putem i tako dalje. Mreže mogu biti različitih oblika, veličina, a često su povezane međusobno kako bi činile jednu veliku mrežu. Najreprezentativniji primjerak takve mreže je Internet. Potreba za umrežavanjem posljedica je potrebe ljudi za razmjenom podataka u što kraćem roku. Kako bi se umrežio veći broj računala, potreban je i poseban hardver i softver te znati metode umrežavanja. Kroz sljedeće podnaslove će se detaljno pojasniti hardver i softver računalne mreže te također referentni modeli koji se koriste u računalnim mrežam [1].

2.1. Mrežni hardver

Kod računalnih mreža ne postoji opće prihvaćena taksonomija u koju sve pripadaju, ali zato se dvije dimenzije ističu kao značajke računalnih mreža, a to su: prijenosna tehnologija i opseg mreže. Široko govoreći, postoje dvije vrste prijenosne tehnologije koje se najviše koriste, a to su *broadcast linkovi* i *point-to-point* (p2p) veze. P2p veze povezuju individualan par računala, a *broadcast* omogućava odašiljanje paketa svima u mreži. Kako bi informacije stigle od izvora do odredišta u mreži s p2p vezama, kratke poruke, zvane paketi, često moraju proći kroz različite uređaje kako bi došli do odredišta. P2p transmisija sa točno jednim pošiljateljem i jednim primateljem se zove *unicasting*. Kontrast p2p-u je *broadcast* mreža, gdje komunikacijske kanale dijele sva računala unutar mreže. Kada se paket pošalje od jednog računala, svi ostali također dobiju taj paket. Svaki paket ima polje s adresom primatelja te kada računalo prima paket, provjerava tu adresu i ako je paket namijenjen za neku drugo računalo, samo ignorira paket. Klasičan primjer *broadcast* veze je bežična mreža, gdje se omogućava pristup mreži svim uređajima na nekom području. Takvu mrežu se može naći kod većih gradova, koji imaju tzv. *hotspot*[1], gdje se različiti uređaji mogu spojiti bežično, bez lozinke. *Broadcast* sustav također ima i posebnu adresu koja omogućava da sva računala na računalnoj mreži dobiju paket i mogu ga pročitati. Taj mod se zove *broadcasting*, a neki

[1] *hotspot* - je fizička lokacija gdje je moguće dobiti pristup Internetu, obično pomoću Wi-Fi tehnologije.

broadcast sustavi imaju mogućnost prijenosa samo odabranoj grupi uređaja i to se zove *multicasting*.



Slika 1. Prikazuje vrste mreže po opsegu

Izvor: [1]

Drugi kriterij za klasifikaciju mreže je po opsegu mreže, tj. po veličini područja koje pokriva. Također se različite tehnologije koriste za različiti opseg mreže te je potrebno navesti ih i objasniti, pojedinačno. Vrste mreža po opsegu se mogu vidjeti na slici 1. te koliko je njihovo područje pokrivenosti u metrima ili kilometrima [1].

2.1.1 Osobne računalne mreže (PAN)

Osobne računalne mreže (engl. *Personal Area Networks*, PAN) su mreže koje omogućavaju komunikaciju u neposrednoj čovjekovoj okolini, otprilike oko jednog metra. Tipičan primjer je bežična mreža koja povezuje računalo s uređajima poput bežične tipkovnice, miša i drugim uređajima, još zvani periferija računala[2]. Bez bežične mreže mora se provoditi strukturno kabliranje, što zahtijeva znatno više sredstava za osposobljavanje mreže za rad. Kako bi se pomoglo tim korisnicima, osmišljena je bežična mreža kratkoga dometa zvana *Bluetootha*[3], kako bi se komponente povezale bez žica s

[2] periferija računala - skup uređaja koji zajedno s računalom čine računalni sustav, a nisu ugrađeni u samo računalo već su mu izravno priključeni kabelom ili bežičnom vezom
[3] *Bluetooth* - tehnika bežičnoga povezivanja elektroničkih uređaja (mobitel, računalo, računalne periferije) radijskom vezom na malim udaljenostima (obično do 10 m)

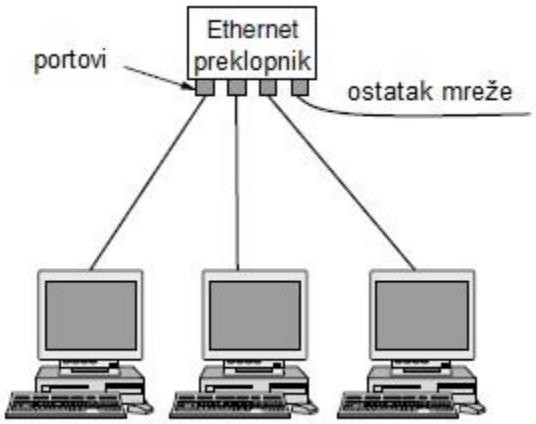
računalom. S obzirom da je danas veliki porast mobilnih uređaja, također dolazi i velika potreba za bežičnim slušalicama s mikrofonom radi lakšeg razgovaranja. Sasvim drugačija vrsta PAN mreže je s uređajima poput *pacemakera*[4], inzulinskim pumpicama, itd [1].

2.1.2 Lokalne računalne mreže (LAN)

Lokalna računalna mreža (engl. *Local Area Networks*, LAN), često zvana i privatna mreža koja pokriva područje jedne zgrade, kuće, ureda ili kampusa (do jednog kilometra). LAN je najrašireniji mreža u smislu korištenosti i broju LAN mreža. Koristi se za povezivanje osobnih računala, raznih elektronskih i terminalnih uređaja s ciljem razmjene informacija. Kada poduzeće koristi LAN, onda se LAN mreža zove *enterprise network*. Kada se govori o LAN-u, misli se na prijenos informacija putem žice, a dvije najkorištenije prijenosne tehnologije su bakrena žica i svjetlovodni vodič. Standard koji se koristi u LAN mrežama je IEEE 802.3, češće zvan *Ethernet*, daleko najkorišteniji za žičanu LAN mrežu i temelji se na okvirima (engl. *frame*[5]) načinu rada. *Frameovi* se pretvaraju u pakete i šalju unutar računalne mreže. LAN mreže imaju krajnju granicu kojeg opsega smiju biti, što znači da se zna vrijeme prijenosa u najgorem slučaju unaprijed (zbog postavljanja ograničenih veličina). Poznajući te granice, olakšava se dizajniranje mrežnih protokola. Brzine LAN mreža s bakrenom paricom se kreću od 100 Mbps (engl. *megabit per second*), koji se još zove i *Fast Ethernet*. Do 1 Gbps (engl. *gigabit per second*) se zove *Gigabit Ethernet*, a s novom tehnologijom se mogu postići i brzine do 10 Gbps kao najkorišteniji oblici *Etherneta*. LAN mreže su jako pouzdane, malo kašnjenje i malo pogrešaka. Topologija LAN-a koristi *point-to-point* linkove kao prijenosnu tehnologiju. Na slici 2. se vidi topologija *Ethernet* mreže s preklopnikom (*engl. switch*). Svako računalo koristi *Ethernet* protokol i spaja se na uređaj zvan preklopnik, tj. *switch* s p2p vezama. Preklopnik ima najčešće 48 mjesta za spajanje, a ta mjesta se zovu *portovi*[6]. Svaki je namijenjen za jedan terminalni uređaj. Uloga preklopnika je razmjena paketa između računala koja su spojena na preklopnik. Kako bi svaki paket došao do svoga predodređenog odredišta, ima adresu odredišnog računala. Za izradu većih LAN-ova, preklopnici se mogu spojiti jedan u drugoga, koristeći *portove*. Moguće je čak i povezati preklopnike u petlju, a protokoli su ti koji određuju kako će tada paketi doći do predodređenog računala. Također je jedan fizički LAN moguće podijeliti u dva manja, logička LAN-a, kako bi se sinkronizirala mrežna oprema sa organizacijskom strukturom. Primjer su dva različita odjela jednog poduzeća, financije i administracija, u istom dijelu

[4] *pacemaker* - elektrostimulatorom srca
[5] *frame* – okvir, koji nastajanjem razbijanja niza bitova na podatkovnom sloju
[6] *port* - konektor (priključak), na zadnjoj strani računala, mrežnih uređaja, u koji se može uključiti periferni uređaj, žičani kablovi (bakrena parica, koaksijalni kabel, optički kablovi).

zgrade. Nalaze se na istom fizičkom LAN-u, međutim lakše bi bilo upravljati kada bi svaki odjel imao svoju mrežu, zato se jedan fizički LAN, podijeli na dva logička i takav LAN postaje virtualna lokalna mreža (engl. *Virtual Local Area Network*, VLAN). U ovom dizajnu mreže, svaki *port* je označen s „bojom“ (konfigurira se svaki *port* i koji VLAN je dopušten na tome *portu*), na primjer administraciji je dodijeljena bijela boja, a financijama crna. Preklopnik tada usmjerava pakete tako da su bijeli *portovi* odvojeni od crnih *portova*, tj. selektiraju se računala na dvije cjeline. To je jako korisno u slučaju korištenja *broadcasta*, kada se želi poslati informacija za financije, računalima na crnim *portovima*, onda administracijski odjel, računala na bijelim *portovima*, neće primiti te pakete, jer to ionako nije njihovo područje djelovanja i zanimanja, samo nepotrebno trošenje vremena i resursa mreže [1].



Slika 2. Prikaz žičane LAN mreže s preklopnikom

Izvor: [1]

Osim žičanih lokalnih mreža, danas su jako popularne i na vrhuncu korištenosti bežične mreže (engl. *Wireless Local Area Network*, WLAN) mreže. Često su korištene u kućanstvu, starijim uredskim zgradama, uslužnim objektima, gdje je teže postaviti strukturirano kabliranje, a i jednostavnije je spajanje korisnika, tj. omogućava veliku mobilnost korisnika, bez ograničenja kretanja unutar pokrivenosti mreže signalom. Korištenje WLAN tehnologije je doseglo svoj vrhunac pojavom mobilnih terminalnih uređaja, tj. pametnim telefonima, zbog potrebe korištenja internet prometa za razne aplikacije i pretraživanje interneta. Da bi se moglo pristupiti WLAN mreži, uređaj mora imati malu radio antenu ili modem kako bi se mogao spojiti na pristupnu točku (engl. *Access Point*, AP), zatim na bežični usmjerivač (engl. *Router*) se može spojiti uređaj ili na baznu stanicu, koja se koristi u mobilnim komunikacijskim sustavima. Nakon što se uređaj spoji na jednu od ove tri opcije, dalje se spaja na Internet. Standard koji označava WLAN

je IEEE 802.11, popularno je zvan *Wi-Fi* i jako je raširen u svijetu. Brzine prijenosa podataka se kreću od 11 Mbps pa sve do nekoliko stotina Mbps [1].

Oboje, žičana i bežična *broadcast* mreža mogu biti podijeljene u statički ili dinamički način rada, ovisno o tome kako je kanal dodijeljen. Tipični statički način dodijele je takav da se vrijeme podijeli na diskretne intervale, korištenjem *round-robin*[7] algoritma, osim *round-robina*, postoji *First-Come, First-Served*[8]. Time se omogućava svakom uređaju da *broadcasta* u svoje određeno vrijeme. Statička dodjela ne omogućava korištenje punog potencijala kanala, jer kada uređaju dođe vrijeme njegovog emitiranja i nema ništa za *broadcastati*, to je nepotrebno trošenje resursa kanala. Zbog toga se osmislila nova metoda koja koristi dinamičku dodjelu vremena kanalu. Dinamička dodjela zajedničkih kanala može biti centralizirana ili decentralizirana. Kod centralizirane dodjele kanala, postoji entitet koji određuje tko je sljedeći na redu, kao što je bazna stanica u ćelijskim mrežama. Unutar toga entiteta postoji integriran algoritam koji prihvaća više paketa te određuje njihov prioritet i prosljeđuje redom.

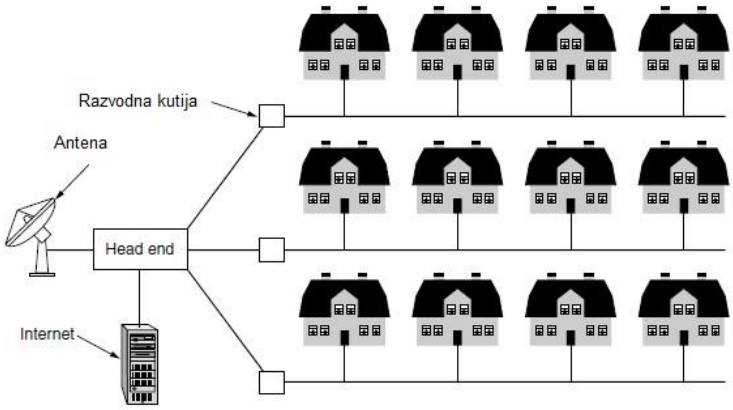
Kod decentralizacijske dodjele kanala ne postoji centralni entitet, svaki uređaj mora sam za sebe odlučit da li da šalje. Smatra se da će se LAN koristit sve više, pojavom pojma pametne kuće, gdje će praktički sve u kući biti umreženo i činiti jednu cjelinu, pametnu kuću [1].

2.1.3 Mreža na području grada (MAN)

Ovo je mreža koja pokriva područje grada. Najbolji primjer MAN mreže je kablovska televizija koju ima svaki grad. Ovi sustavi se pojavljuju u ranijim komunikacijskim antenskim sustavima, gdje je bio loš televizijski signal, postavljajući antenu na uzvišeno područje te bi se onda sproveo signal do pretplatnika. U početku su to bile privremene mreže, lokalno dizajnirane, a onda su poduzeća zatražila ugovore od lokalne vlade i povezale cijele gradove koaksijalnim kablovima. Time su se razvili i televizijski programi, specijalizirali. Kada je Internet počeo brojati veliki porast u zainteresiranosti korisnika, kablovski TV operateri su otkrili da uz male promjene sustava, mogu omogućiti Internet uslugu u dijelovima neiskorištenog spektra. Te su tako kablovski TV sustavi napravili transformaciju s jedne funkcije, distribucije televizije, na kompleksniju

[7] *round-robin* – napredniji algoritam koji smješta u red svaki aktivni tok podataka koji posjeduje pakete i naizmjenično prijenose pakete na dijeljenom kanalu u određenim periodima. Ako jednom toku ponestane paketa, sljedeći će tok preuzeti njegovo mjesto.
[8] *First-Come, First-Served* - najjednostavniji algoritam. Kada paket dođe u sustav stavlja se na kraj reda, a paketi se uzimaju s početka reda.

MAN mrežu. Slika 3. prikazuje primjer jedne MAN mreže, gdje se vidi prikaz distribucije televizije i Interneta kako se centralizira u *head end*[9] i dalje distribuira prema korisnicima.



Slika 3. Prikaz načina rada MAN mreže

Izvor: [1]

Postoji još jedan jako dobar primjer MAN mreže koji se danas proširio, a to je bežična tehnologija koja omogućava širokopojasni bežični pristup Internetu uz upotrebu radio frekvencijskog spektra (engl. *Worldwide Interoperability for Microwave* Access , WiMAX) tj. standard IEEE 802.16 [1].

2.1.4 Široko područna mreža (WAN)

WAN mreža obuhvaća velika geografska područja, često se odnosi na državu ili kontinent. Prvo će se objasniti žičana WAN, kroz primjer jednog poduzeća, koje ima urede diljem države, u različitim gradovima. Svaki od tih ureda se sastoji od računala kojima je svrha pokretanje korisničkih aplikacija. Ta računala se još nazivaju i *hostovi*[10], a ostatak mreže koji povezuje te *hostove* se zove *subnet* ili podmreža[11]. Njen zadatak je prijenos informacija od *hosta* do *hosta* i sastoji se od dvije komponente: prijenosnih vodova i preklopničkih elemenata. Prijenosni vod radi na razini bitova i prenosi ih između uređaja. Mogu bit napravljeni od bakrenih žica, optičkog vlakna, koaksijalnog kabla i radio veze. Većina poduzeća ne posjeduje prijenosne vodove, nego ih zakupljuju od telekomunikacijskih tvrtki. Preklopnički elementi su računala, specijalizirana koja povezuju dvije ili više prijenosnih vodova. Kada podatak dođe na dolazni vod do

[9] *head end* - postrojenje gdje se procesira i distribuira televizijski signal
[10] *host* - je uređaj povezan u računalnu mrežu koji može korištenjem standardnih protokola ostvariti komunikaciju s drugim sličnim uređajima na računalnoj mreži
[11] podmreža - predstavlja manju mrežu unutar neke veće mreže. Podmreža je potrebna kada postoji više od jedne LAN mreže

preklopnika, preklopnik određuje kuda taj podatak mora ići, tj. na koji odlazni vod treba poslati podatak. Ovi preklopnički elementi se zovu usmjerivači (engl. *Routers*) i najčešće se koriste kod WAN računalnih mreža. Dakle podmreža je skup usmjerivača i komunikacijskih vodova koji prenose pakete od izvornog do odredišnog *hosta*. WAN je dakle uvećana verzija LAN mreže, sa nekim razlikama. Uobičajeno je da u WAN mrežama, *host* i podmreža budu u vlasništvu različitih ljudi, gdje su zaposlenici odgovorni za svoja računala, a tvrtkin IT odjel za ostatak računalne mreže [1].

Druga razlika je ta da usmjerivači povezuju različite mrežne tehnologije. Primjer je da su računala unutar jedne prostorije povezane *Ethernet* tehnologijom, a na veće udaljenosti se koristi drugačija prijenosna tehnologija, drugačiji vodovi, to mogu biti sinkroni optički vodovi (engl. *Synchronous Optical Networking*, SONET). Dakle više WAN mreža je u stvari *internetworks*[12], kompozitne mreže koje se sastoje od više nego jedne mreže.

Postoje dvije različite verzije WAN mreža. Prva, umjesto da unajmljuje prijenosne vodove, tvrtka povezuje svoje urede na Internet te omogućava da povezanost između ureda bude pomoću virtualnih kanala koji koriste osnovni kapacitet Interneta. Ovakvo mrežno uređenje se zove virtualna privatna mreža (engl. *Virtual Private Network*, VPN). Za razliku od namjenskih uređenja, gdje se garantira stalna propusnost i skoro stalna latencija, VPN ima veću moć korištenja virtualizacijom. Omogućava fleksibilno ponovno korištenje resursa. Međutim VPN ima i manu kod korištenja resursa virtualizacijom, jer nema kontrolu nad osnovnim kapacitetom Interneta, dok je kod namjenskog voda to jasno. Dakle VPN mreža ovisi o Internet usluzi. Druga verzija WAN mreže je ta da podmreža može biti pokrenuta od druge tvrtke. Operater podmreže se često naziva *network service provider*, tj. davatelj mrežne usluge i uredi su njihovi korisnici. S obzirom na današnju potrebu za Internetom, ovakva mreža bi bila razočaravajuća ako bi korisnici mogli slati pakete samo između sebe. Tako da je potrebna podmreža s Internet uslugom, a takav operater koji osigurava i Internet se zove pružatelj Internet usluga (engl. *Internet Service Provider*, ISP), a podmreža se zove ISP mreža.

U većini WAN mreža, mreža posjeduje veći broj prijenosnih vodova, kojima se povezuje jedan par usmjerivača. Ako dva usmjerivača nemaju direktnu povezanost prijenosnim vodom, moraju komunicirati indirektno putem drugih usmjerivača. Tu se pojavljuje pitanje kako će mreža odlučiti kojim putem će paket putovati te su se osmislili algoritmi za usmjeravanje. Postoji još jedna skupina algoritama za prosljeđivanje, oni određuju kako će usmjerivač odrediti sljedeći korak, tj. put za paket.

[12] *Internetworks* - mreža formirana od nekoliko međusobno povezanih mreža kroz koju svaki korisnik može komunicirati s bilo kojim drugim korisnikom.

Još neki primjeri WAN mreža koji se baziraju na bežičnoj tehnologiji, kao satelitski sustavi su jedan od primjera takvih mreža sa zemaljskom antenom i sa satelitom u orbiti. Obično se ovakav sustav koristi za *broadcast* odašiljanje informacija. Drugi primjer su ćelijske mreže, gdje postoji već do pete generacije razina standarda. Od prve generacije koja je služila samo za prijenos glasa, do pete generacije gdje će brzine biti i do 10 Gbps. Svaka ćelija ima jednu baznu stanicu u sredini koja odašilje signal na području mnogo većem od WLAN-a [1].

2.2 Mrežni softver

Prva računalna mreža je bila dizajnirana tako da je cilj bio hardverski ih povezat, ali vrlo brzo je došla potreba softverskih rješenja. Današnje mreže su značajno softverski strukturirane. Kroz sljedeće odjeljke će se objasniti softverske tehnike strukturiranja [1].

2.2.1 Protokolna hijerarhija

Kako bi se smanjila kompleksnost mreže, organizirana je po slojevima, svaka kao nadogradnja na onu ispod sebe. Broj slojeva, imena slojeva, sadržaj slojeva i funkcija slojeva je različit od mreže do mreže. Svaki sloj je dizajniran poput virtualnog uređaja, koji nudi svoje usluge sloju iznad sebe, ne zamarajući gornji sloj implementacijom donjeg sloja. Osnovna ideja je ta da se određeni dio softvera ili hardvera pruža uslugu korisniku, ali zadržava unutarnje detalje i algoritme podalje od korisnika. Kako bi slojevi mogli komunicirati između sebe, koriste takozvani n protokol. Protokol je dogovor između dvije komunikacijske stranke, kako će se komunikacija vršiti.

Entiteti koji su na istoj razini odgovarajućih slojeve na različitim uređajima se nazivaju vršnjaci (engl. *peers)*. Vršnjaci mogu biti softverski procesi ili hardverski uređaji. Iako bi se dalo zaključiti da onda svaki sloj komunicira direktno sa svojim vršnjakom na drugoj strani, to u stvarnosti nije tako. Svaki sloj prosljeđuje podatke i kontrolne informacije sloju ispod do zadnjeg sloja. Ispod sloja jedan se nalazi fizički medij kroz koji se odvija komunikacija. Između susjednih slojeva se nalazi sučelje (engl. *Interface*). Sučelje određuje koje će operacije i usluge donji sloj omogućiti gornjem sloju. Kada se odlučivalo koliko će postojati mrežnih slojeva, jako je bitno bilo kreirati čisto sučelje između slojeva, tako da svaki sloj izvodi svoju funkciju i zajedno čine sustav. Čisto sučelje omogućava lakše izmjene protokola ili implementacije. Skup slojeva i protokola se zove

mrežna arhitektura, a lista protokola korištena za neki sustav, jedan protokol po sloju se zove *protocol stack* [1].

2.2.2 Dizajniranje slojeva

Pitanje dizajna slojeva u računalnoj mreži je bitno za kvalitetan rad računalne mreže. Prvo pitanje kod dizajniranja mreže je pouzdanost te kako napraviti kvalitetnu mrežu, koja se sastoji od raznih komponenti, a zbog toga postoji mogućnost gubitka paketa. Kako bi se to spriječilo, postoje mehanizmi koji to sprječavaju. Jedan od mehanizama je detekcija pogreške na odredištu. Kada su informacije zaprimljene netočne, obavlja se re-transmisija dok god nisu zaprimljene točno na odredištu. Kompleksniji mehanizam omogućava korekciju pogreške, gdje se neispravni bitovi koji su stigli na odredište pokušavaju zamijeniti sa onima iz ispravne poruke. Oba mehanizma rade dodavanjem redundantnih informacija, tj. bitova i koriste se u nižim slojevima kako bi se zaštitili paketi.

Drugo pitanje koje se pojavljuje vezano za pouzdanost je pronaći valjan put kroz mrežu za pakete. Pogotovo kada je mreža velikog opsega, kao što je Internet, moguće je da na putu do odredišta i nazad ima neispravnih usmjerivača. Zbog toga što ima velik broj računala, svakom sloju je potreban mehanizam za raspoznavanje pošiljatelja i primatelja koji će se nalaziti u poruci. Taj mehanizam se zove adresiranje. Vrlo bitna karakteristika koju mreža mora imati je skalabilnost, tj. da mreža nastavlja i dalje obavljati svoju funkciju i rad, onda i kada se povećava broj uređaja na mreži.

Treće pitanje dizajna mreže je raspodjela resursa. Kao što je prije rečeno, mreža pruža uslugu *hostovima* iz svojih osnovnih resursa, kao što je kapacitet prijenosnog voda. Kako bi se ravnopravno rasporedili resursi svakom *hostu* i da ne utječu jedan na dugoga, potrebni su mehanizmi za to. Većina mreža dinamički dodjeljuje propusnost, po kratkoročnoj potrebi *hostova*, a ne dodjeljivanjem svakom *hostu* fiksni dio pojasne širine, koji neće stalno koristiti, a zauzima resurse mreže. Takav dizajn se zove statističko multipleksiranje, dijeljenje resursa, bazirano na statističkim podacima potrebe. Kada mreža ima veći broj korisnika, može doći do zagušenja mreže, tj. zagušenje prometa informacijama, jer svaki korisnik ima potrebu razmjene podataka. Ponekad se od mreže zahtijeva pravovremenost dostave paketa. Primjer takve usluge je video uživo, gdje je potrebna dostava paketa u stvarnom vremenu i često te aplikacije zahtijevaju veliku propusnost. Mehanizam koji pokušava pomiriti konkurirajuće zahtjeve se zove kvaliteta usluge (engl. *Quality of Service*, QoS) [1].

Zadnje bitno pitanje kod dizajniranja mreže je sigurnost te kako je zaštititi od raznih vrsta napada. Prisluškivanje je jedan od tih napada te su potrebni mehanizmi koji bi to spriječili.

Postoje tri mehanizma koji zajedno mrežu čine znatno sigurnijom i kvalitetnijom. Ta tri mehanizma su:

- Povjerljivost (engl. *Confidentiality*)
- Cjelovitost (engl. *Integritiy*)
- Dostupnost (engl. *Availability*)

Povjerljivost osigurava da pohranjene i poslane podatke ne mogu čitati neautorizirani subjekti, kroz autentifikaciju korisnika. Integritet služi otkrivanju namjerne ili nenamjerne promjene pohranjenih/poslanih podataka, a raspoloživost mora osigurati pristup korisnicima kada je njima to potrebno [1].

2.3 Referentni modeli

Nakon objašnjenih slojeva kod računalnih mreža, objasnit će se realni primjeri, tj. modeli koji se koriste u mrežnoj arhitekturi. Objasnit će se dvije najvažnije mrežne arhitekture, a to su referentni modeli za otvoreno povezivanje sustava (engl. *Open Systems Interconnection*, OSI) i (engl. *Transmission Control Protocol/Internet Protocol*, TCP/IP). Iako se OSI model praktički više niti ne koristi, jedan je od prvih opće priznatih modela i ima generalno najbitnije slojeve, zato je vrlo bitan. TCP/IP model kao takav nije toliko koristan (odnosi se na definirane slojeve), ali zato što se njegovi protokoli danas masivno koriste, ovaj model je znatno korišteniji [1].

2.3.1 OSI referentni model

OSI model je baziran na prijedlogu koji je kreirala međunarodna organizacija za standarde (engl. *International Standards Organization*, ISO), kao prvi korak prema međunarodnoj standardizaciji protokola po slojevima. Model se službeno zove ISO OSI referentni model i povezuje otvorene sustave, tj. sustave koji su otvoreni za komunikaciju s ostalim sustavima.

OSI model se sastoji od sedam slojeva, a načela kojima se došlo do sedam slojeva su:

1. Sloj treba biti kreiran tako da su potrebne različite apstrakcije, esencijalne karakteristike,
2. Svaki sloj treba izvoditi definiranu funkciju,
3. Funkcija svakog sloja treba biti izabrana, tako da je u skladu s međunarodnim standardiziranim protokolima,
4. Granice slojeva se moraju odabrati tako da minimiziraju protok informacija kroz sučelje te
5. Broj slojeva mora biti dovoljno velik tako da različite funkcije mogu biti spojene zajedno radi potrebe i dovoljno mali slojeva tako da arhitektura računalne mreže ne bude nezgrapna.

Potrebno je napomenuti da OSI model nije sam po sebi mrežna arhitektura, jer ne specificira određene usluge i protokole, nego govori što svaki sloj odrađuje, koja mu je zadaća. Međutim, ISO je odredio i standarde za sve slojeve, iako oni nisu dio OSI referentnog modela. Ukratko će se svaki sloj objasniti, njihova glavna zadaća.

Fizičkom sloju je zadaća prijenos bitova preko komunikacijskog kanala. Nije dopustivo da se pošalje jedinica, a na odredištu dođe nula u binarnom sustavu[13]. Pitanjima kojima se bavi ovaj sloj su koji električni signali će se koristiti za binarni sustav, koliko nanosekundi će trajati jedan bit (najmanja količina informacije), da li će prijenos biti simultan (u oba smjera) ili jednosmjeran, kako će se uspostaviti konekcija itd. Ova dizajnerska pitanja se odnose na mehanička, električna i vremenska sučelja, kao i fizički prijenos preko medija.

Podatkovni sloj ima zadatak pretvorbu bitova u niz koji treba biti slobodan od neopaženih prijenosnih grešaka. Omogućava to maskiranjem stvarnih grešaka tako da ih mreža ne vidi, a to se postiže raspodjelom bitova u okvire određene duljine (od nekoliko stotina do nekoliko tisuća bajtova. Ako je usluga pouzdana, prijemna strana potvrđuje dospjele okvire i šalje potvrdni okvir (engl. *acknowledgement frame*). Jedno od pitanja koje se postavlja je kako zaustaviti bržeg odašiljača, da ne preplavi podacima sporijeg prijemnika. Mehanizmi za regulaciju prometa se time bave. *Broadcast* mreže imaju dodatno pitanje vezano za kontrolu pristupa (engl. *Media Acces Control*, MAC) u obliku podsloja, koji rješava taj problem [1].

Mrežni sloj kontrolira operacije vezano za podmrežu. Glavno pitanje kod dizajniranja mrežnog sloja je kako će se paketi usmjeravati od izvora do odredišta. Rute za pakete se mogu odrediti statičkim tablicama, koje su vezane za tu mrežu i rijetko se

[13] binarni sustav - predstavlja pozicijski brojevni sustav s bazom 2. To znači da u tom brojevnom sustavu za označavanje brojeva se koriste dvije znamenke, a to su nula i jedan

mijenjaju ili mogu biti automatski ažurirane. Mogu također biti određene na početku komunikacije, kao na primjer spajanje na udaljeno računalo. Također, tablice mogu biti dinamički ažurirane, a određuje se za svaki paket ovisno o realnom stanju na mreži. Potrebno je spriječiti pojavu uskog grla (engl. *bottleneck*)[14]. Takvo zagušenje, mreža također mora sanirati, a mrežni dio je odgovoran i za kvalitetu usluge. Mogući su razni problemi, poput različitih adresa, predugačkih paketa, različiti protokoli, a sve je to na mrežnom sloju da savlada te probleme i heterogenu mrežu poveže.

Transportni sloj, kao osnovnu zadaću ima zaprimiti podatke s gornjih slojeva i razdijeliti ih u manje jedinice, a ako je potrebno, proslijediti mrežnom sloju, da bi se potvrdio njihov ispravan dolazak na odredište. Transportni sloj također određuje koja će se vrsta usluge pružiti sesijskom sloju i samom korisniku na mreži. Najkorištenija vrsta transportne konekcije je *error-free* p2p kanal, koji dostavlja bajtove ili poruke redoslijedom kojim su poslani. Neke transportne usluge ne zahtijevaju garanciju da će dostaviti poruku redom kojim je poslana, koja će se vrsta usluge koristiti, određuje se na početku povezivanja. Transportni sloj je sloj koji povezuje krajnja dva uređaja i vrši komunikaciju te obavlja prijenos podataka od izvora do odredišta s kontrolom dospijeća i točnosti informacija. U nižim slojevima, tj. ovi koji su objašnjeni prije, vrši se prijenos podataka između uređaja i njegovih susjeda.

Sloj sesije omogućava da korisnici na različitim uređajima uspostave sesiju. Sesija nudi razne usluge, a najbitnije su kontrola dijaloga (tko je na redu za prijenos), upravljanje *tokenima*[15] (sprječava dvije strane da naprave istu kritičnu operaciju simultano) i sinkronizacija (za duži prijenos, potrebne su kontrolne točke, koje će omogućiti da se prijenos nastavi s tih točaka, ako se dogodi pogreška).

Prezentacijski sloj, za razliku od donjih slojeva se ne bavi kretanjem bitova, nego sintaksom i semantikom, prenesenih informacija. Omogućava da računala s različitim unutarnjim prezentacijskim podacima mogu komunicirati.

Aplikacijski sloj se sastoji od raznih protokola koji se često koriste od strane korisnika. Najpoznatiji aplikacijski protokol za prijenosa informacija na Webu (engl. *HyperText Transfer Protocol*, HTTP), koji je temelj za svjetsku mrežu (engl. *World Wide Web*, WWW). Kada se traži web stranica preko tražilice, šalje se ime stranice serveru[16] koji omogućava sadržaj, koristeći HTTP [1].

[14] usko grlo (*bottleneck*) – kada je za određeni tok podataka komunikacijski link u potpunosti iskorišten, kao i svi tokovi koji dijele ovaj link. Tako da se postiže maksimalna brzina prijenosa podataka diljem mreže i dolazi do zagušenja na mreži.
[15] *token* - posebni tri bajtni okvir koji putuje u krugu do svakog uređaja lokalne računalne mreže. Računalo domaćin koje posjeduje taj tro bajtni žeton ima pravo prijenosa podatke preko medija.
[16] server – ili poslužitelj je namjensko računalo ili softver koji šalje i prima podatke od mnogostrukih klijenata. Prema namjeni može biti web poslužitelj, datotečni poslužitelj, poslužitelj e-pošte, itd.

2.3.2 TCP/IP model

Iako je sličan OSI referentnom modelu, ima različitosti koje će se objasniti. Prva mreža većeg opsega koja je koristila TCP/IP je ARPANET i njegov nasljednik Internet. Kada su se na postojeću mrežu dodale radio i satelitske mreže, postojeći protokoli u vidu OSI-a, nisu bili zadovoljavajući. Tako je nastao TCP/IP protokol, koji je dobio ime po dva glavna protokola. TCP/IP model se sastoji od četiri sloja, sa istim imenima kao kod OSI sloja. S obzirom da ima sličnosti s OSI modelom, zapravo glavne razlike su protokoli koje koristi TCP/IP i zato će se objasniti protokoli po pojedinim slojevima koji obilježavaju ovaj referentni model. Prvi sloj je podatkovni i ima slične karakteristike kao i kod OSI referentnog modela, tako da se neće dodatno objašnjavati. Mrežni sloj sadržava jedan od dva najbitnija protokola koji obilježavaju ovaj referentni model, a to je IP protokol. Sve Internet komponente koje imaju mrežni sloj, moraju koristiti IP protokol. Neke od odlika su što ne ovisi o nižim protokolima, nespojna usluga, nepotvrđena usluga, nema mehanizama kontrole toka, nema garancije očuvanja redoslijeda paketa. Ovaj protokol se naziva *best effort* protokol, koji se trudi dostaviti točne informacije, ali ne garantira točnost. Protokol koji pomaže funkciji IP protokolu za kontrolu poruka je ICMP (engl. *Internet Control Message Protocol*), a o njemu će se kasnije govoriti.

Transportni sloj također kao i kod OSI modela, omogućava komunikaciju s kraja na kraj. Dva takva protokola s kraja na kraj su definirana, to su TCP i UDP (engl. *User Datagram Protocol*). TCP je pouzdan, dostavlja pakete redom, prije slanja paketa uspostavlja konekciju, ima kontrolu zagušenja, kontrolu toka. Koristi se kada je potreban siguran prijenos podataka, bez pogrešno poslanih informacija, kao npr. Elektronička pošta, prijenos podataka, udaljeno upravljanje uređajima, itd. Dok s druge strane, UDP nije pouzdan, ne uspostavlja se konekcija, paketi ne dolaze redom. Ovaj protokol se dosta koristi, iako ne garantira dostavu paketa, kod aplikacija gdje je bitnija brzina od točnosti, kao npr. Prijenosa uživo, tj. audio i video u realnom vremenu, Internet telefonije, video konferencije, upravljanje mrežom, itd. Kod UDP-a su paketi zvani *datagrami*[17] i kreću se po mreži od jednog do drugog *hosta*.

Aplikacijski sloj se sastoji od svih visoko razinskih protokola, a oni su: protokol za upravljanje uređaja na daljinu (engl. *TELephone NETwork*, Telnet), elektronička pošta (engl. *Simple Mail Transfer Protocol,* SMTP), protokol za davanje imena mrežnim adresama (engl. *Domain Name System*, DNS) kako bi ljudima bilo prihvatljivije, HTTP za dohvaćanje stranica na WWW-u i protokol za dostavu medija u stvarnom vremenu (engl. *Real-time Transport Protocol*, RTP) [1].

[17] *datagram* – osnovna prijenosna jedinica za prijenos podataka. *Datagramske* usluge su nepouzdane i za razliku od paketa, ovaj pojam se koristi na transportnom sloju, kod UDP-a

3. Upravljanje računalnim mrežama

Mreže i distribuirani sustavi za obradu su od kritične i rastuće važnosti u poslovanjima svih vrsta. S obzirom da je trend rasta računalnih mreža bio velik (a i danas je), sve kompleksnije je i upravljanje mrežama i njihovoj podršci. Velike mreže se ne mogu nadzirati samo ljudskim trudom, već su potrebni automatizirani mrežni alati za upravljanje mrežom. Potreba za takvim alatima je sve veća, a s time je i izazov napraviti kvalitetan alat, ne samo radi dobre funkcionalnosti i preglednosti, nego i zbog različitih proizvođača opreme. Povrh toga, trend decentralizacije mrežnih usluga kao što je prikazano sve većom važnošću radnih stanica i klijent/server, upravljanje mrežom je sve teže, jer je veći dio mreže daleko od osoblja za upravljanje mrežom. Bitno je naglasiti da je nadzor mreže dio upravljanja računalnom mrežom, tako da će se protokoli vezani za nadzor spominjati i u ovome poglavlju. U sljedećim poglavljima će se objasniti protokoli i načini upravljanja računalnim mrežama.

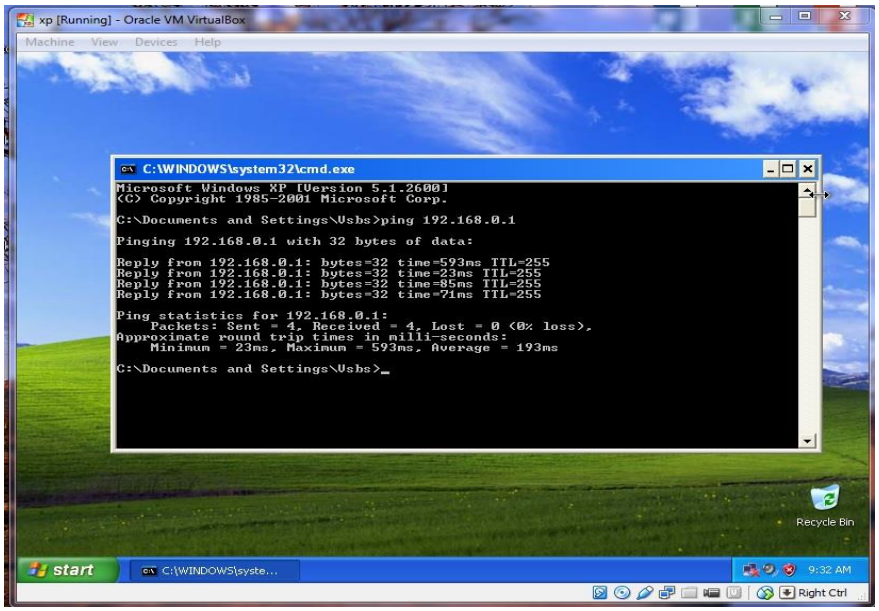
3.1 Osnovni protokoli za upravljanje računalnim mrežama

Postoje dva osnovna protokola za upravljanje mrežom, a to su komunikacijski protokol za kontrolu poruka (engl. *Internet Control Message Protocol*, ICMP) i jednostavni mrežni protokol za nadzor i upravljane (engl. *Simple Network Management Protocol*, SNMP). Ovi protokoli su u upotrebi od prvih računalnih mreža, a i dalje su korisni kao temeljni alati za rješavanje problema i upravljanje računalnim mrežama. Svaki protokol će se ukratko opisati i u koje svrhe se koristi.

3.1.1 Komunikacijski protokol za kontrolu poruka (ICMP)

ICMP je jedan od temeljnih Internet protokola za upravljanje računalnim mrežama i administraciju, koristi se za slanje pogrešnih poruka. ICMP je kontrolni protokol, što znači da ne nosi aplikacijske podatke, nego informacije o statusu same mreže. Postoji velik broj korištenih mrežnih alata, baziranih na ICMP porukama koji služe otkrivanju pogrešaka u osnovnim komunikacijama mrežnih aplikacija. Također provjerava dostupnost udaljenih *hostova*, mrežna zagušenja i kašnjenje.

Jedan od najpoznatijih mrežnih alata je *ping*[18] koji šalje ICMP paket i zahtijeva odjek i na taj način testira dostupnost uređaja ili *hosta* na mreži. *Ping* također mjeri vrijeme obilaska (engl. *round-trip time*, RTT) paketa od izvora do odredišta, kao što je prikazano na slici 4.



Slika 4. Rezultati *ping* testiranja

Izvor: izradio autor

Ping daje brze rezultate, fleksibilan i nema negativnih utjecaja na mrežu. *Ping* također može dostaviti i informacije o gubitku paketa [2].

3.1.2 Jednostavni mrežni protokol za nadzor i upravljanje (SNMP)

SNMP ide korak dalje od ICMP-a, tako što omogućava prikupljanje većeg broja podataka s uređaja (kasnije u radu će se prikazati koji su to podaci). S obzirom na veliku korištenost ovog protokola u prošlosti, praktično svaki mrežni uređaj, mnogi serveri i aplikacije su kreirani da raspoznaju i reagiraju na SNMP protokol, poslan od strane upravljačke mrežne centrale. Ovaj protokol se znatno koristi za nadzor mreže. Do danas postoje tri inačice SNMP protokola, SNMPv1, SNMPv2 i SNMPv3. Upravljačka stanica, često zvana SNMP *manager*, je računalni program koji nadgleda ili upravlja elementima

[18] *ping* - je administrativni alat koji služi za provjeru dostupnosti *hostova* na računalnim mrežama, temeljenim na IP protokolu

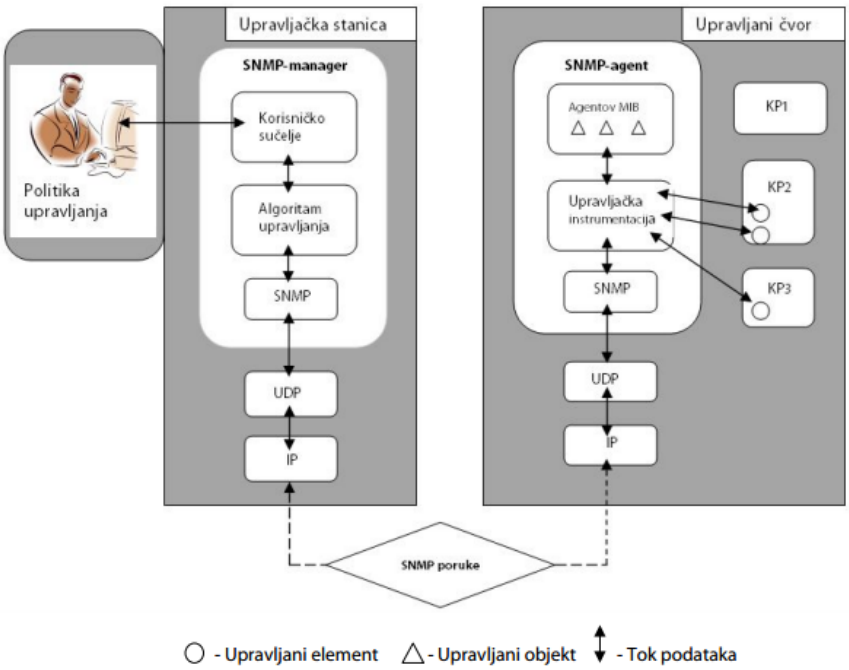
na upravljanim čvorovima mreže u skladu s politikom upravljanja, koja je određena od strane mrežnog administratora/upravitelja. Politika upravljanja ima podjelu na područja koja će se kasnije detaljnije navesti. Upravljani čvor je mrežni uređaj čijim se stanjima upravlja ili ih se nadgleda te se može izvesti akcija na uređaju ili zabraniti. Kod upravljanog čvora se koristi naziv SNMP *agent*. Upravljačke informacije, koje su fizički smještene u SNMP agentima, SNMP upravitelji vide ih kao skup upravljanih objekata, a taj skup objekata je objedinjen u jednu bazu upravljačkih informacija (engl. *Management Information Base*, MIB).

Svaki SNMP agent sadrži popis svih svojih upravljanih objekata i moraju sadržavat sljedeće zapise:

- Ime,
- OID (engl. *object identifier*),
- Tip podataka,
- Dozvole čitanja i pisanja te
- Kratki opis za svaki objekt SNMP agenta.

S obzirom na raznolikost opreme kreiran je formalni jezik apstraktnih zapisa koji opisuje pravila i strukture za zastupanje, kodiranje i prijenos podataka (engl. *Abstract Syntax Notation One*, ASN.1), kako bi se mogla omogućiti komunikacija između opreme različitih proizvođača. Ovim se standardom postiže definiranje tipova podataka korištenih za konstrukciju SNMP poruke, tako da SNMP agenti i upravljači mogu biti pisani u bilo kojem programskom jeziku. Jedan od tih tipova podataka je i OID, koji je i prije spominjan. ASN.1 sintaksa je vrlo moćna i kompleksna, ali zato pati od nedostatka učinkovitosti [3].

Standard za izgradnju MIB baze se zove SMI (engl. *Structure of Management Information*) i on je zapravo podskup od standarda ASN.1 uz neka proširenja. Ovime se standardom određuju vrste podataka koji se mogu koristiti u MIB-u. Time se postiže jednostavnost i proširivost MIB-a.



Slika 5. Sustav za upravljanje mrežom

Izvor: [3]

SNMPv1 se koristi od 1988. godine i prihvaćen je kao jedan od standarda TCP/IP modela. Sigurnost se kod SNMPv1 temelji na korištenju zajedničkih nizova (engl. *community string*), a to je zapravo niz ASCII znakova. Koristi se za autentifikaciju SNMP poruka između upravljačke jedinice i upravljanog uređaja. Problem je što nema nikakvu enkripciju, pa svatko može snimanjem IP paket pročitati sadržaj SNMP poruka, čak i zajedničke nizove, a naravno i samu konfiguraciju mrežnog uređaja. SNMPv2 je postao standard 1993. i nije donio dodatna poboljšanja što se tiče sigurnosti. Podržava tri načina pristupa upravljačkoj informaciji, dok SNMPv1 podržava prvi i treći, a to su sljedeći:

1. **Upravljač-agent**: SNMPv2 upravljač šalje zahtjev agentu, a agent odgovara slanjem traženih upravljačkih informacija korištenjem dohvaćanja i modificiranja upravljačkih informacija,
2. **Upravljač-upravljač**: jedan SNMPv2 upravljač šalje zahtjev drugom upravljaču, a drugi odgovara slanjem traženih upravljačkih informacija i
3. **Agent-upravljač**: SNMPv2 agent šalje poruku *trap*[19] upravljaču.

[19] *trap* - omogućava agentu da pošalje stanici za nadzor, notifikaciju, za provjeru opreme koja se nadzire, npr. temperatura iznad dozvoljene

SNMPv3 posjeduje bitno poboljšane sigurnosne mehanizme, kao što je mehanizam za autentifikaciju (na temelju korisničkog imena i lozinke) i zaštitno kodiranje SNMP poruka, tj. enkripcija [3].

3.2 Politika upravljanja računalnim mrežama (FCAPS)

OSI/ISO model za upravljanjem računalnim mrežama je FCAPS, a to je skraćenica nastala od pet područja koji standard definira. Svaki će se detaljno objasniti, a područja su:

- Upravljanje greškama (engl. *Fault management*),
- Upravljanje konfiguracijama (engl. *Configuration management*),
- Upravljanje politikom naloga (engl. *Accounting management*),
- Upravljanje performansama (engl. *Performance management*) i
- Upravljanje sigurnošću (engl. *Security management*).

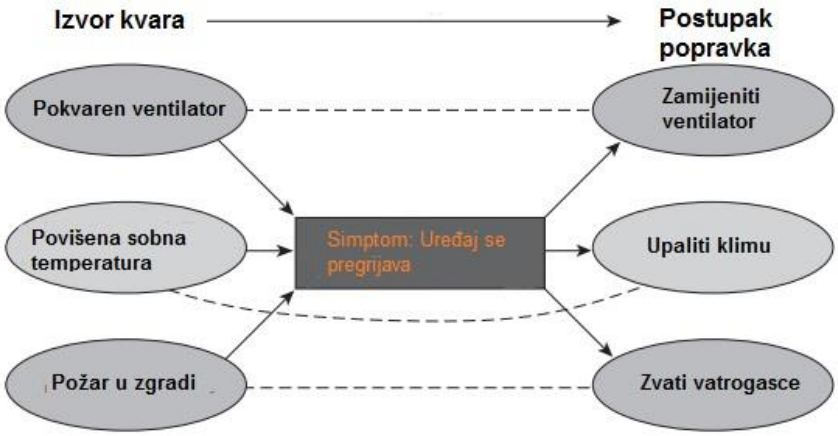
3.2.1 Upravljanje pogreškama (F)

To je proces lociranja, postavljanja dijagnoze i ispravljanja mrežnog problema. Pogreška ili kvar je događaj do kojeg je došlo nenamjerno ili nije definirano kao radni uvjeti mreže. Zatim je potrebno pronaći mjesto nastanka kvara i razlog, koje se prati alarmima te alarmi dolaze u obliku poruka do mrežnog upravitelja. Jedan životni ciklus upravljanja pogreškama se sastoji od nadzora, detekcije, analize i reakcije. Prvo je potrebna detekcija pogreške kroz zadane alarme i detekciju kvara u što kraćem roku. Idealno je napraviti redundantna svojstva, kako ne bi došlo do prekida usluge i funkcije mreže. Bitno je odrediti prioritete, jer nemaju svi kvarovi istu težinu, neke je potrebno što prije sanirati. Zatim izolacija kvara i pronalaženje izvora i razloga kvara, tehnikama alarma i događaja. Nakon toga dolazi rješavanje pogreške, popravkom, vraćanjem na prvobitno stanje i eventualna zamjena pokvarenih elemenata. Poslije toga slijedi testiranje, da li je vraćena funkciji i na kraju dokumentacija životnog ciklusa, radi bržeg rješavanja budućih pogrešaka. Osim reaktivnog upravljanja greškama, postoji i proaktivno. Gdje se pokušavaju riješiti problemi prije njihovog nastanka, to se postiže njihovim predviđanjem i preventivnim akcijama kroz nadzor i bilježenjem prošlih pogrešaka na mreži. Glavni cilj upravljanja greškama je da se poveća pouzdanost i efektivnost mreže, kao i produktivnost korisnika unutar mreže, jer ako do kvarova dolazi često, korisnik neće biti zadovoljan [5].

Dakle upravljanje greškama se sastoji od sljedećih funkcionalnosti:

- Nadzor mreže, s osnovnim alarmima za upravljanje te će se detaljnije objasnit pod nadzorom mreže,
- Dijagnoza pogreške, analiza razloga i izvora pogreške te rješavanje problema/ispravljanje grešaka (engl. *troubleshooting*),
- Zadržavanje prošlih zapisa alarma,
- Prijavljivanje problema u obliku tzv. *ticketa i*
- Proaktivno upravljanje greškama.

Nakon što se postave parametri za alarme i događaje koji se žele pratiti (koji će biti detaljnije objašnjeni pod nadzorom mreže) dolazi na red dijagnosticiranje pogreške i njeno ispravljanje. Mrežna dijagnoza se može usporediti s liječničkom dijagnozom gdje postoji set simptoma koji uzrokuju neku bolest, pojavu te je potrebno uzeti u obzir brojne parametre i razloge tih simptoma, što je prije moguće. Tako je i kada se dogodi pogreška u mreži, potrebno što prije donijeti dijagnozu, kako bi se smanjila šteta za korisnika i vratila funkcionalnost računalne mreže. Dijagnoza je temelj za odabir pravilne opcije za oporavak mreže i vraćanja u operativno stanje. Alarm samo javlja simptom, a ne uzrok. Na primjer pristigne alarm da se uređaj pregrijava kao što je prikazano na slici 6.



Slika 6. Primjer mogućih kvarova vezanih za pregrijavanje uređaja

Izvor: [7]

Kako odrediti koji od ovih uzroka je kriv za pregrijavanje uređaja (slika 6.), s obzirom da je vrlo vjerojatno da se mrežni administrator nalazi na udaljenoj lokaciji. Tek kada s dijagnosticira što se događa na udaljenoj lokaciji, može se odrediti koja će se

akcija za oporavak koristiti. Dijagnoza često koristi *troubleshooting*[20] funkcije, kao što su dodatni podaci dobiveni nadzorom uređaja, koji nisu dio alarma. Mogućnost ubacivanja testova u mrežu ili uređaj za potrebe ispravljanja grešaka donosi znatnu podršku za dijagnozu. Jedan od takvih testova je *loopback*, tj. vraćanje podataka prema izvoru, kako bi se testirala propusnost infrastrukture kod slanja i primanja podataka. Sve zajedno može se reći da su testovi zapravo definirani kroz parametre kvalitete usluge, kao što su kašnjenja, *jitter*[21], gubitak paketa itd. Za VoIP tehnologiju test je obavljen poziv. Ovi testovi zapravo služe kako bi se moglo proaktivno reagirati, prije nego to osjeti korisnik. Proaktivno upravljanje greškama može sadržavati analizu alarma koje prepoznaje uzorke alarma, nastali manjim greškama koji upućuju na veće probleme. Potrebno je odrediti na uređaju i namjestiti koji će se protokol koristiti za javljanje pogrešaka.

Što se tiče prijavljivanje poteškoća putem *ticketa*[22], to može biti iznimno kompleksno kod većih mreža koje poslužuju na tisuće korisnika, a i više. Kod tako velikih mreža često dolazi do malih problema, ali je bitno da ne dođe do katastrofalnih koji bi utjecali na cijelu ili dobar dio mreže. Pojedini korisnici mogu doživljavati probleme kao iznimno loše iskustvo korištenja te mreže, sporiji odaziv na zahtjeve, gubitak podataka, glasa itd.

Zbog tako velikog opsega računalnih mreža u današnje vrijeme, potrebni su i ljudski resursi. Ljudi koji će se baviti obradom prijavljenih problema, da li je to kroz alarme ili korisnici sami prijavljuju loše iskustvo korištenja mreže. Moderni davatelji usluga moraju imati korisničku podršku sa brzim odazivom na upućenu primjedbu. Tako da je ovaj sustav *ticketa* jako bitan s obzirom da se danas bazira oko korisnika i da imaju kvalitetnu uslugu. Ako poduzeće ima brz odaziv, znači da ima kvalitetan i stručan tim koji kvalitetno odgovora na korisničke zahtjeve, vrlo vjerojatno je da će poduzeće poslovati sa profitom [7].

[20] *troubleshooting* – je oblik rješavanja problema, koji se često primjenjuje za popravak neispravnih proizvoda ili procesa. To je logična i sustavna potraga za izvorom problema (pogreške), s ciljem rješavanja problema i vraćanja proizvoda ili procesa u operativno stanje.
[21] *jitter* - je mjera za razliku između kašnjenja dva susjedna paketa iste sesije na cijelom putu, odnosno od kraja do kraja mreže, još se zove i varijacija kašnjenja
[22] *ticket* - elektronička poruka ili obrazac koji se ispunjava online, preko koje klijent prijavljuje kvar kojeg posjeduje

3.2.2 Upravljanje konfiguracijama (C)

Upravljanje konfiguracijama služi definiranju uređaja na računalnoj mreži tako da uređaji nesmetano obavljaju svoju funkciju, bez poteškoća za korisnike i sveukupnu funkcionalnost računalnih mreža. S obzirom da u mreži može postojati velik broj uređaja, potrebno je svaki od uređaja dodatno konfigurirati da bude član mreže i da bi bio "živ". Upravljanje konfiguracijama je zapravo osnova. Postoje tri vrste konfiguracije, prva je fizička konfiguracija koja se odnosi na opis hardverskih i softverskih mrežnih komponenti. Kao što je hardverska konfiguracija usmjerivača, preklopnika (konfiguracija sučelja, *portova* itd.) i softverska konfiguracija servera (Web servera, operativnih sustava itd.). Drugo je konfiguriranje procesa za nadogradnju logičkih parametra sustava i treća logička konfiguracija se odnosi na rezultat konfiguriranih procesa (postavljanje upravljačkih parametra i njihovih vrijednosti). Kada se govori o fizičkoj konfiguraciji misli se na liste opreme, kako kablirati preklopnike itd., a kod logičke konfiguracije se misli na određivanje koji će se protokoli koristit, koje sučelje, dodjeljivanje adresa itd. Najizazovnije je kod konfiguracije to što postoji velik broj različitih uređaja i popratnih softvera za te uređaje, često se dogodi da ne postoji interoperabilnost između različitih uređaja. Nakon uspješno obavljene konfiguracije svi entiteti na mreži bi međusobno trebali komunicirati i vidjeti se. Baza koja upravlja konfiguracijama (engl. *Configuration Management Database*, CMDB) sadrži informacije o logičkim konfiguracijama svih uređaja na mreži. U toj bazi su podaci relativno statični i baza i mreža moraju biti sinkronizirani. Omogućava brz pristup konfiguracijskim informacijama. Upravljanje konfiguracijama sinkronizira opremu, omogućava udaljenu konfiguraciju i opremu konfigurira *up-to-date*[23]. Primjer jednog procesa konfiguracije je kod *enterprise* mreže, kada zaposlenik dobije telefonski uređaj, gdje mreža mora prepoznati korisnika, usmjeravati pozive prema njemu, kao i osigurati naplatu korištenja telefonskih usluga [5].

Upravljanje konfiguracija se može podijeliti u sljedeće podteme po funkcijama:

- Konfiguracija upravljanih resursa, neovisno da li su mrežna oprema ili pokrenuti servisi preko mreže,
- Revizija mreže i otkrivanje što je na njoj,
- Sinkronizacija upravljanja informacijama kroz aplikaciju unutar mreže,
- Kreiranje sigurnosne kopije mrežnih konfiguracija u slučaju kvara i
- Upravljanje verzijama softvera (engl. *software images*) na mrežnoj opremi

U jezgri upravljanja konfiguracijama su aktivnosti i operacije korištene za konfiguraciju onoga što se upravlja. To zapravo znači slanje redova komandi mrežnom

[23] *up-to-date* – u ovom kontekstu znači da je oprema ažurirana prema novim verzijama softvera i standardima

uređaju s ciljem da se promjene konfiguracijske postavke. Ponekada se to odnosi na izolirani uređaj, gdje se konfigurira sučelje za pojedini *port* preklopnika ili konfiguracija operacija koji će se izvršavati na uređaju, a ujedno im je zadatak da na mrežnoj razini imaju mogućnost promjene konfiguracije na brojnim uređajima diljem mreže. Primjer prije objašnjeno je statičko dodjeljivanja ruta za usmjeravanje, gdje je svaki *hop* predodređen. Upravljanje konfiguracijama na razini usluga se generalno odnosi na pružanje usluga (engl. *service provisioning*), a to znači mogućnost uključivanja usluge, kako bi se mogli modificirati određeni servisni parametri i uklanjanje određenih servisa, (koji zna biti zanemaren, ali je jednako bitan). Primjer je ako davatelj usluge ima korisnika koji ne podmiruje račune, potrebno je upozoriti korisnika i ako ne plati, isključiti ga.

Revizija služi za čitanje što je sve konfigurirano, tako da se šalje upit mreži. Korisno je kada se želi provjeriti da li je konfiguracija kakva se očekivala ili je nešto drugačija. Bez ove mogućnosti davatelji usluga bi teško mogli razumjeti što se događa na mreži. Osim revizije, funkcija otkrivanja objekata na mreži je također iznimno korisna. S obzirom da korisnici mogu utjecati na mrežu, mrežnim davateljima je ovo korisna funkcija za upravljanje mrežom. Neki od primjera utjecaja korisnika su netočna dokumentacija opreme (engl. *inventory*), osoblje radi promjene na mreži, ali ih ponekad ne bilježi kroz računalni programte. Zato postoji efikasniji i brži način, a to je otkrivanje mreže, automatska funkcija koja olakšava pregled mreže i promjene na njoj (u smislu novih uređaja).

Sinkronizacija je bitan dio mreže jer sprječava da postoje dva gledišta na istu informaciju koja su si kontradiktorna. To se postiže tako da se jedan set informacija postavi kao glavni, *maste*r[24]. Postoje dvije mogućnosti tko će imati glavnu riječ, jedna je da mreža bude *master*, te je ujedno i najčešća opcija koja se koristi. Druga opcija je da je upravljani sustav *master*. Ako dođe do greške a računalna mreža je *master*, smatra se da je mreža krivo postavljena i potrebno razmotriti razloge i uskladiti mrežu.

Kreiranje sigurnosne kopije konfiguracijskih podataka je od velike važnosti, jer su ti podaci su od kritične važnosti i trebaju se štititi, kao i što je baza korisnika od kritične važnosti. Neki katastrofalni događaj može srušiti cijeli jedan dio mreže i s njom i konfiguracije, koje će vjerojatno utjecati na tisuće korisnika. Vrijeme koje bi moralo biti utrošeno da se ponovno sve konfigurira i vrati na stare vrijednosti je praktički nedopustivo u današnje vrijeme, zato je potrebno napraviti sigurnosne kopije.

Zadnje je upravljanje verzijama softvera na uređajima, jer proizvođači opreme također objavljuju i nove verzije softvera. Potrebno je pratiti nove verzije, koje su promjene i kako ih instalirati [7].

[24] *master* – u ovom kontekstu označava set informacija koje su prioritet i imaju glavnu riječ, kada dođe do pogreške, *master* se smatra odgovornim

3.2.3 Upravljanje politikom naloga (A)

Politika naloga mjeri kolika je potrošnja mrežnih resursa od strane korisnika, tako što mjeri protok informacija od strane koga i kroz koje vrijeme. Nakon što se to odradi, onda se korisniku naplati ono što je koristio kroz određeni vremenski period. Naplata može biti određena jednom korisniku ili skupini, pritom se mora paziti da ne dolazi do iskorištavanje privilegija i terećenja mreže na štetu drugih korisnika. Za davatelje usluga ovo je jezgra njihove ekonomije i zato treba biti robusna sa velikom dostupnošću i pouzdanošću, da se ne bi dogodilo da netko plati uslugu i ne dobije je.

Također ako korisnik ne iskorištava mrežu koja mu je dodijeljena, mrežni upravitelj može to promijeniti kako bi se poboljšale performanse. Postoje dva modela naplate, *postpaid* i *prepaid*. *Postpaid* je usluga gdje se naplata vrši nakon korištenja (kod mobilnih terminalnih uređaja su to kartice s mjesečnom pretplatom), a *prepaid* gdje se usluga naplaćuje prije i za vrijeme korištenja usluge, tj. u realnom vremenu (kod mobilnih terminalnih uređaja to su kartice na bonove) [5].

Bitno je naglasiti razliku između naplate i politike naloga, ponekad se ta dva pojma miješaju, a naplata je zapravo samo jedan dio upravljanja politike naloga. Ako se kroz politiku naloga, podaci dobro ne saberu, davatelj usluge može davati besplatne usluge. Kako bi se mjerila potrošnja mrežnih servisa, moraju se postaviti mjere za skupljanje korištenih podataka. Kod poziva takva mjera se zove detaljni zapis poziva, koji se automatski generiraju te se pritom moraju svi prikupiti i duplikate eliminirati. Podaci koji se generiraju kod poziva su jačina zvuka, duljina i kvaliteta poziva, dok recimo kod prijenosa zvuka preko interneta (engl. *Voice over Internet Protocol*, VoIP) megabajti podatkovnog prometa, minute poziva, broj uslužnih transakcija i korištenje zagarantirane razine usluge protiv *best-efforta*. S obzirom da se usluge naplaćuju, svaki korisnik mora imati svoju privatni račun u obliku autentifikacije, koji ne smiju znati ostali korisnici mreže. Sve više je u trendu ponuda tzv. *flat* usluga, gdje se korisnicima omogućava neograničeno korištenje usluga sa naznakom *flat*. Glavni protokol koji se koristi kod politike naloga za mjerenje prometa je NetFlow i IP računovodstvo, kao i mjerenje potrošnje pojedinih korisnika te adekvatna naplata kroz ugovorene usluge (engl. *Service Level Agreement*, SLA). Ovaj dio se više odnosi na nadzor mreže te će se detaljnije objasniti kod nadzora mreže.

Jedna od najbitnijih funkcija koje se moraju postaviti kod upravljanja politike naloga je AAA (engl. *Authentication, Authorization and Accounting*). To je zapravo upravljanje korisničkim računima unutar poduzeća (organizacije), svaki zaposlenik/član mora imati svoj korisnički račun sa sučeljem za prijavu. Nakon što se korisnik prijavi onda se bilježi da je na mreži i može mu se kroz nadzor mjeriti promet koji generira. Osim prijave, bitno je upravljati pravima koji pojedini korisnik posjeduje, ne smiju svi korisnici imati pristup

mrežnom upravljanju ili pristupu obračunu plaća, poslovnim planovima ili krucijalnim podacima poslovanja. Zato je potrebno pametno upravljati korisničkim računima i njihovim pravima. Na kraju se vrši obrada prometa koji korisnik generira, iako sama mreža poduzeća ne naplaćuje pojedinom korisniku promet, nego dobije od pružatelja usluge ili drugih uslužnih poduzeća račun sa troškovima. Tako da podaci dobiveni nadzorom služe za praćenje i ponovno alociranje resursa unutar mreže, kao i sprječavanje korisnika koji iskorištavaju mrežu, da neopaženo to i dalje rade. Dakle podacima dobivenim iz nadzora će se ponovno odraditi upravljanje i poboljšati i optimizirati rad i kvaliteta mreže [7].

3.2.4 Upravljanje performansama (P) i Upravljanje sigurnošću (S)

Upravljanje performansama se svodi na osiguravanje da mrežni podaci ostanu dostupni i da ne dolazi do zagušenja u mreži. Sustavi su dizajnirani sa određenom razinom performansi mreže te se garantira određena kvaliteta usluge QoS, ovisno o potrebama. Jedan od načina da se rastereti mreža je klasifikacija (najčešće prema prometu ili prema korisniku) i određivanje prioriteta po klasama. Kako bi se garantirala razina usluge potrebna je kontrola i nadgledanje performansi mreže, a to će se detaljnije objasniti u poglavlju za nadzor mreže. Stoga ciljevi su da se postigne dosljednost i kvaliteta individualnih i sveukupnih mrežnih servisa. Zatim optimizacija mrežnih performansi i mogućnost razvoja mreže kako se razvija i poslovanje u smislu povećanja mrežnog prometa i planiranje potrebnih kapaciteta.

Mrežne performanse se mjere kroz:

- Propusnost se mjeri brojem jedinica koji se obavi komunikacijom po jedinici vremena, na podatkovnom sloju to su bajtovi po sekundi (B/s), na mrežnom sloju broj paketa po sekundi, a kod aplikacijskog sloja broj zatraženih web-ova ili broj obavljenih poziva,
- Kašnjenje na podatkovnom sloju je vrijeme potrebno da okteti dođu do odredišta, na mrežnom sloju je to vrijeme potrebno da IP paket stigne na odredište, a na aplikacijskom sloju vrijeme potrebno da zahtjev stigne do odredišta ili vrijeme potrebno da poziv pristigne,
- Pouzdanost (postotak gubitaka paketa i postotak izgubljenih poziva) i
- Iskorištavanje (kanala i usmjerivača).

Mrežnim administratorima su potrebni statistički podaci o performansama, kako bi lakše planirali, upravljali i održavali velike mreže. Statistički podaci mogu prepoznati potencijalna suženja, tj. *bottleneckse*, prije nego što se i dogode i stvore probleme za

krajnje korisnike. Mogu se promijeniti tablice usmjeravanja kako bi se promet pravilno rasporedio u doba dana kada je računalna mreža najviše opterećena te se na taj način rasterete maksimalno iskorištena čvorišta [5].

Kod upravljanja performansi potrebno je odrediti koji će se bitni dijelovi mreže nadzirati, međutim moguće je da je potrebno bilježenje performansi podataka iz cijele mreže, iako se ne nadzire konstantno. Ti podaci znaju biti iznimno bitni za provjeru kako se situacija razvijala do pojave kvara te se eventualno spriječe budući problemi i napravi analiza. Konstantno izvođenje podataka od uređaja može brzo dovesti upravljanje sustavom do nestabilne situacije, jer da na mreži postoji deset tisuća uređaja i na svakom se skupljaju podaci o deset parametra, to je iznimno puno procesa i praktički nemoguć napor za performanse mreže. Netflow je protokol koji rješava taj problem i biti će kasnije objašnjen. Još jedan način je konfiguriranje uređaja tako da mjeri performanse prvih petnaest minuta svakoga sata i zatim ih sprema na tvrdi disk ili na privremenu memoriju. Potrebno je tako upravljati mrežom da se može garantirat određena kvaliteta usluge i unatoč zagušenjima. Također i selektirati promet radi lakšeg upravljanja performansama. Dakle ispravno je reći da su glavni ciljevi upravljanja mrežnim performansama dosljednost i kvaliteta, optimizacija mrežnih performansi i planiranje kapaciteta mreže. Stoga potrebno je postaviti performanse koje će se mjeriti, nadzirati i dobivenim podacima od nadzora obaviti rekonstrukciju računalne mreže ako je potrebno, to je glavni cilj upravljanja [7].

Zadnje područje ovoga modela proučava zaštitu osjetljivih informacija na uređajima koji su spojeni na mrežu, kontrolirajući pristupne točke i zove se upravljanje sigurnošću računalne mreže. Kako bi se kvalitetno sprovela sigurnost prvo je potrebno identificirati osjetljive informacije, zatim pronaći pristupne točke i osigurati ih. Nakon toga je potrebno generirati, raspodijeliti i pohraniti enkripcijske ključeve za osjetljive informacije te dodijeliti lozinke i druge vrste autorizacija za pristup osjetljivim informacijama. Također je potrebno kontrolirat tko sve pristupa računalnoj mreži i svim njenim čvorištima. A to se postiže implementacijom mrežnih alata za detekciju napada na mrežu [5]. Zapravo postoje dva aspekta: sigurnost upravljanja i upravljanje sigurnošću. Sigurnost upravljanja osigurava da upravljane operacije budu osigurane, tako da samo ovlaštene osobe mogu upravljati mrežom. Primjer je da samo ovlaštene osobe mogu pristupiti sučelju na uređajima, kako bi se zaštitila mrežna konfiguracija od ne ovlaštenih osoba. Također se mora osigurati pristup aplikacijama za upravljanje, kako bi se objedinilo sa zaštitom sučelja i upravljanjem mreže. Ljudi koji će baratati tim aplikacijama moraju biti stručni i poznavati ih, jer se u tim aplikacijama mogu podesiti konfiguracije uređaja za usluge, smanjiti performanse mreže, dodijeliti pristup neovlaštenim osobama itd. Mreža se mora zaštititi ne samo od napada izvana, nego i od napada unutar mreže. Zato je potrebno dodijeliti pristup onima kojima je to doista i potrebno, kvalitetne lozinke kako se ne bi probile jednostavno, kao i njihova povremena izmjena i kreiranje sigurnosnih kopija u

slučaju katastrofalnih događaja. Drugi aspekt je upravljanje sigurnošću gdje se osigurava zaštita same mreže, a dok se kod sigurnosti upravljanja odnosilo na zaštitu upravljačkih elemenata, aplikacija. Danas je internet zapravo najveća prijetnja poslovnim mrežama, jer zaposlenici mogu ne namjerno otvoriti i preuzeti neke skrivene linije koda koje je *hacker* ubacio u originalni podatak i tako može naštetiti korisniku ili poduzeću. Neki od primjera takvih napada na mrežu su:

- DOS (engl. *Denial of service*) su napadi koji pokušavaju preopteretiti dijelove mreže kreiranjem nelegitimnog prometa i zaustavljanjem legitimnog prometa. Druga verzija napada je DDOS (engl. *Distributed Denial of service*), što su zapravo koordinirani napadi s više izvora,
- Virusi i crvi koji pokušavaju poremetiti rad sustava ili ga uništiti, zajedno sa podacima i
- *Spamom* se smatraju poruke koje su obično automatizirane i mogu se nagomilati do te mjere da opterećuju mrežu i njene servere, obično kroz elektroničku poštu [7].

Kako bi bi se osigurala računalna mreža, potrebna je potpuna zaštita mreže, a to se postiže sljedećim komponentama:

- Postavljanjem načela i procedure upravljanja prometom,
- Fizička zaštita opreme,
- Vatrozid (engl. *firewall*) i
- Antivirus.

Postavljanje načela i procedure upravljanja prometom se odnose na politiku upravljanja koju poduzeće provodi. Dakle što je prihvatljivo da se koristi u poduzeću, odnosi se na zabrane nekih internet stranica koje zaposlenicima ne trebaju i ne bi smjeli na poslu koristiti, zatim brojna kategorizacija načela vezane za email, pristup udaljenim uređajima, osobni uređaji i mobilni uređaji, aplikacije, mrežna načela, bežična mreža, itd. A što se tiče procedura, mora postojati procedura kako bi se izmijenile sigurnosne postavke. Kako se ne bi izostavila koja bitna sigurnosna stavka.

Fizička zaštita opreme se odnosi na zaštitu opreme koju ne koriste direktno krajnji korisnici, nego su to usmjerivači, preklopnici, vatrozidi. Oni se često nalaze u posebnoj sobi, zvane server sale gdje se nalaze i tvrdi diskovi sa važnim informacijama. Te sobe ne smiju biti dostupne svima, nego samo ovlaštenim osobama koji brinu o toj opremi i mora imati sigurnosne mjere.

Vatrozidi su uređaji koji se često nalaze u poslužiteljskim prostorijama (server salama) i služe kao vrata prema Internetu. Oni posjeduju svoj vlastiti softver koji je potrebno podesiti tako da odgovara politici upravljanja. Vatrozid se sastoji sustava za prevenciju napada, tj. IPS (engl. *Intrusion Prevention System*) i sustava za prevenciju curenja podataka i zaštitu od gubitka podataka, tj. DLP (engl. *Data leakage/Loss protection/Prevention*). Vatrozid je neizostavni dio svakog poduzeća, a i kod svih računala krajnjih korisnika na operativnom sustavu Windows[25], koji imaju softverski vatrozid kao opciju zaštite. Vatrozidi isto koriste svoj antivirus.

Međutim često taj softverski vatrozid kod krajnjih korisnika nije dovoljan za zaštitu od napada *hackera*. Tako da se osim njega još instalira antivirus kao softver koji služi za obranu. On je praktički neizostavan dio svakoga računala i često se nadograđuje kako bi bio u mogućnosti obraniti korisnike od novih malicioznih programa i linija koda kreiranih od zlonamjernih osoba [13].

[25] operativni sustav Windows – je vrsta grafičkoga korisničkog sučelja, koji služi za „oživljavanje“ sklopovlja. To je skup računalnih programa i alata koji čine jednu cjelinu i tako tvore operativni sustav. Najčešća uporaba ovoga operativnog sustava je za osobna računala, a još postoji u obliku za terminalne mobilne uređaje, servere, itd.

4. Nadzor računalnih mreža

Nadzor mreže je jedan od najbitnijih zadataka koje se sprovodi kroz upravljanje mrežom. Nadzor je samo jedan dio upravljanja mrežom, ali zbog toga što omogućava informacije vezane za status mreže, nadzor mreže je postao iznimno važan. Podaci dobiveni nadzorom mreže se koriste kako bi se otkrile i spriječile nenormalne i nepoželjne situacije, kao i kako bi se odredili realno potrebni mrežni parametri. Kako bi se prikupili ti podaci, većina alata i aplikacija koristi već prije objašnjeni SNMP protokol. Kroz SNMP komande, mrežni administratori mogu zatražiti vrijednosti iz baze upravljačkih informacija (MIB) za upravljani uređaj. SNMP također omogućava menadžerima da postave vrijednosti u MIB-u, tako da se definira ponašanje uređaja. S obzirom da je trend širenja mreža u porastu, mreže postaju sve kompleksnije i potrebne su kvalitetne aplikacije za nadzor računalnih mreža i njene adaptacije, kako bi mreža bila ekonomična i kvalitetna za krajnje korisnike. A za nadzor mreže se koristi model koji će se detaljno objasniti u nastavku [6].

4.1 Model za nadzor računalnih mreža (FCAPS)

Za nadzor mreže postoje pet osnovnih ciljeva, tj. isti model kao i kod upravljanja:

- Nadzor pogrešaka (engl. *Fault monitoring*),
- Nadzor konfiguracija (engl. *Configuration monitoring*),
- Nadzor politike naloga (engl. *Accounting monitoring*),
- Nadzor performansi (engl. *Performance monitoring*) i
- Nadzor sigurnosti (engl. *Security monitoring*).

Također FCAPS model koji se sastoji od pet funkcijskih cjelina koji je predložio ISO/OSI kao standard za upravljanje računalnim mrežama, a nadzor je dio svih tih područja. Dakle ovo je dokaz da je nadzor samo jedan dio upravljanja mrežom, ali znatan i veoma bitan.

4.1.1 Nadzor pogrešaka (F)

Nadzor pogrešaka se bavi mjerenjem problema unutar mreže. Postoje dva bitna pitanja kod nadzora pogrešaka. Kao prvo zbog velikog broja slojeva mreže kojim se bavi nadzor pogrešaka, pojavljuje se problem detekcije na kojem je sloju pogreška. Drugo, nadziranje pogrešaka zahtijeva uspostavljanje normalnih karakteristika mreža u nekom određenom vremenu. Uvijek postoji pogrešaka u mreži, ali to ne znači da mreža ima dosljedan problem. Mreža tek ima značajan problem kada se dogodi niz pogrešaka, iznad određenih granica, tako da je bitno odrediti te granice kroz testiranja [6].

Najbitniji aspekt nadzora mreže je upravljanje alarmima. Alarmi su nepoželjne poruke koje dolaze od mreže i upućuju na to da se dogodio neočekivani događaj te je ponekad i potrebna intervencija operatera. Ti neočekivani alarmi mogu doslovno biti o bilo čemu, primjer je da na preklopniku jedan *port* prestane obavljati svoju funkciju, vatrogasni alarm, smanjenje kvalitete signala, povišena temperatura u sobi pa do neovlaštenog upada na mrežu. Neki od osnovnih funkcija upravljanja alarma su prikupljanje alarma, održavanje točnih i trenutnih lista alarma i vizualizacija alarma i mrežnih stanja. Najbitnija funkcija je prikupljanje alarma i osiguravanje da se ništa bitno ne propusti, njihovo zaprimanje i spremanje u memorije ili baze, kako bi se mogli kasnije procesirati od strane aplikacije ili ovlaštenom osobom. Kod malo složenijih slučajeva, kolekcija alarma može sadržavati i provjeru da se niti jedan alarm nije izgubio i da zatraži eventualno izgubljeni alarm. Nakon što se alarmi prikupe, potrebno je kreirati listu alarma koji će se održavati i onda odgovarati na pitanja. Bitno je razumjeti kako su alarmi i mrežna stanja vizualno prezentirana korisniku. U najosnovnijem i važnijem formatu su vizualizirane u obliku tekstualnih lista s informacijama o alarmu. Te liste mogu biti pretraživane, sortirane i filtrirane prema različitim kriterijima, kao što su ozbiljnost alarma, vrsta alarma, broj oštećenih mrežnih elemenata, vrijeme alarma itd.

Vizualizacija se često pojavljuje kroz metodu topologijske mape, gdje ikone na mapi predstavljaju uređaje i mogu biti animirane za prikazivanje trenutnog stanja alarma. Zatim se mogu prikazati veze između uređaja i animirati da prikazuju različita stanja isto pomoću topologijske mape. A kako to izgleda će se prikazati kroz aplikaciju, gdje je zaista praktično za nadgledati takav sustav, jednostavno i efikasno. Neki od naprednih alarma su javljanje alarma direktno osobi koja je nadležna i onda ta osoba obavijesti korisnika da je dobiven alarm i da je problem u procesu rješavanja. Još jedna bitna stvar kod alarma je to što je potrebno alarme **filtrirati**, kako bi nadležna osoba ili napredna aplikacija mogla procesirati te sve alarme. Nisu svi alarmi jednake važnosti te ih je tako i potrebno kategorizirati po važnosti.

A drugi način da se spriječi nagomilavanje informacija je **korelacija**, gdje se informacije pred procesiraju i agregiraju od događaja i alarma u sažete i značajnije informacije. To se postiže pred procesiranjem gdje se informacije presreću na putu do upravljača mreže i onda se analiziraju i uspoređuju kako bi se ustvrdilo koji su alarmi vrlo vjerojatno povezani, jer ukazuju na iste simptome ili isti uzrok [7].

4.1.2 Nadzor konfiguracija (C)

Što se tiče nadzora konfiguracija ne postoji velik broj parametara koji se mogu nadzirati. Kod nadzora konfiguracija moguće je u realnom vremenu nadzirati promjene u konfiguracijama sa detaljima koji su se promijenili. Vidljivo je na kojim uređajima je obavljena nova konfiguracija uređaja, promjene sučelja, tj. *portova*, zatim koje verzije softvera su pokrenute na kojim uređajima (koje su vidljive nadzorom uređaja kroz alate za nadzor, tj. udaljenim pristupom na uređaj). Zapravo će se prikazati kroz računalni program koji će se kasnije koristiti u radu, jer nadzora konfiguracija zaista nije kompleksan. Najbitnije je nadzirati da li su svi uređaji konfigurirani onako kako je predviđeno planom upravljanja računalnim mrežama i koristiti nadzor kako bi se pratile promjene nastale promjenama konfiguracija na samim uređajima, radi evidencije. Informacije dobivene mogu poslužiti ako dođe do prestanka rada novo konfiguriranog uređaja te se može vidjeti tko je promijenio konfiguraciju i koje promjene su napravljene. Utvrđuje se tko je odgovoran za promjene i nastoji se vratiti predhodna konfiguracija, a s time i funkcionalnost uređaja. Za usklađeni rad uređaja na mreži je potrebno imati interoperabilnu opremu i pridržavati se propisanih standarda od pojedinih proizvođača opreme [13].

4.1.3 Nadzor politike naloga (A)

Nadzor politike naloga se bavi praćenjem korisnika i koju količinu informacija (prometa) generiraju, odnosno iskorištavaju resurse računalne mreže. Računalna mreža kroz nadzor vodi evidenciju koji korisnik preko kojeg uređaja koristi određenu količinu resursa mreže (mjerna jedinica za trenutnu potrošnju resursa je b/s, a za sveukupnu potrošnju (B, KiB, MiB, GiB)[26]), koliko često, koji sadržaj i kroz koje vrijeme. Ova vrsta informacije omogućava da se sprovede kvalitetna i točna naplata korisniku koji je

[26] B, KiB, MiB, GiB – bajt (B) je mjerna jedinica za količinu podataka u računalstvu i sastoji se od osam bitova. Jedinice veće od bajta su: kibibajt (engl. *kibibyte*, KiB) = 2^{10} bajtova, mebibajt (engl. *mebibyte*, MiB) = 2^{20} bajtova, gibibajt (engl. *gibibyte*, GiB) = 2^{30} bajtova, itd.

iskorištavao resurse mreže, a i korisno je za predviđanje budućeg iskorištavanje mrežnih resursa [6].

Kao što je rečeno prije protokol koji se najčešće koristi za nadzor politike naloga se zove NetFlow, iako je kreiran od strane jednog od najvećih proizvođača opreme (Cisco Systems, Inc.[27]) kao njihov softver, zapravo ga koriste razne druge aplikacije za nadzor. Služi za nadzor korištenosti aplikacija i mrežnih resursa te pripada u pasivni nadzor mreže i nadgleda promet koji prolazi kroz uređaje i mjeri količinu generiranog promet. NetFlow služi za mjerenje generiranog prometa po serveru, po usluzi, po aplikaciji te generiranog prometa na ili izvan mreže. Nadzorom ovih elemenata može se obaviti mrežno planiranje i prometno inženjerstvo na kompleksnoj mreži te tako pridonijeti upravljanju mreže. Podaci koji se dobiju nadzorom, proslijede se sektoru za upravljanje mreže te se može optimizirati rad mreže i znatno poboljšati njen rad, kroz pametno upravljanje resursima mreže. Nadzor mreže i prikupljanje podataka mora biti obavljen kao i kod korisnika, tako i kod samo jezgre. NetFlow uzima uzorke diljem računalne mreže i bilježi nadzirane podatke, oni se mogu kontinuirano uzimati, ali je potrebno oprezno odrediti učestalost uzimanja uzoraka. Tamo gdje je moguće, potrebno je koristiti nasumično uzimanje uzoraka, jer rasterećuje mrežu, a sabire potrebne podatke. U nekim slučajevima je potrebno konstantno nadzirati i uzimati uzorke te je zbog toga potrebno odrediti prioritete unutar računalne mreže (primjer takve mreže je bankarski računalni sustav, koji mora biti točan i dostupan). Još neke od vrijednosti NetFlow-a su te da ističe korisnike koji najviše iskorištavaju mrežu, koliko ih je aktivno u bilo koje vrijeme, odakle dolazi promet (iz mreže ili izvan mreže), kojem korisniku dolazi promet i gdje odlazi od korisnika, kada se dogodio prijenos podataka te se čak dotiče i sigurnosnog aspekta, analizom da li je mreža napadnuta. Služi i za dogovor vršnjaka, a najbitnije je to što kroz nadzor mjeri potrošnju i naplaćuje, a to je najbitnije za nadzor politike naloga. Jedna od mjera za nadziranje politike naloga bazirano na IP-u je usmjernički protokol koji služi za komunikaciju između autonomnih sustava (engl. *Border Gareway Protocol*, BGP). Gdje se mjeri i nadzire IP promet koji se šalje ili zaprima od različitih vršnjaka, a lista zajednice, broj i put autonomnog sustava su dodijeljeni kako bi se identificirao promet. Tako da se može zabilježiti put IP prometa i sukladno tome obaviti adekvatna naplata.

Nadzorom aplikacija se može mjeriti kvaliteta usluge (QoS), kao i da li davatelj usluge poštuje ugovorene stavke, tj. SLA. RMON (engl*. Remote monitoring*), standard koji služi za mjerenje prometa kroz svih sedam slojeva (isključujući fizički sloj). RMON2 je taj koji je operativan na aplikacijskom sloju i mjeri promet. Dakle da bi se obavio kvalitetan nadzor aplikacije potrebno je prikupiti specifične podatke, odrediti kako identificirati aplikacije, duboka analiza podataka, server koji posjeduje računovodstvene

[27] Cisco Systems, Inc. – internacionalno poduzeće osnovano 1984. godine, koje dizajnira, proizvodi i prodaje mrežnu opremu, smatra se najvećim poduzećem na svijetu u tome području.

funkcije i ako se koristi NetFlow koristiti uzimanje uzoraka. SLA je jako bitan i za nadzor performansi te će se još tamo detaljno objasniti.

Nadzirati korisnike je bitno kako bi se svakome pojedinom korisniku mogle naplatiti usluge koje koriste, a da korisnike ne oštećuje poduzeće, iskorištavajući za vlastite potrebe. Osim NetFlow-a, koristi se metoda AAA, koji svakoga korisnika registrira i zatim mu dodjeljuje određeni račun samo za tog korisnika. Na taj način se može kvalitetno nadzirati usluga i pratiti naplata od strane davatelja usluge.

Još jedna tehnologijska mjera s kojom se može nadzirati kvaliteta usluge je IP SLA. Ima zaista razne funkcionalnosti i radi zajedno sa SNMP-om i NetFlow-om. Nadzorom omogućava proaktivne notifikacije, analizira svaki hop i bilježi podatke s kraja na kraj. Jedna od proaktivnih notifikacija je da posjeduje definirani prag SLA-a i bilježi kada je usluga iznad ili ispod tog praga te pomoću SNMP *trapa* javlja da se ne poštuje ugovorena usluga [8].

4.1.4 Nadzor performansi (P) i nadzor sigurnosti (S)

Nadziranje performansi se bavi mjerenjem performansi mreže, kroz tri bitna pitanja za nadzor. Prvo, informacije dobivene nadzorom performansi su često korištene za planiranje budućih mrežnih ekspanzija i da se istaknu eksploatacijski problemi na trenutnoj mreži. Kao drugo, da bi se dobio model ponašanja mreže, a to se dobiva nadzorom performansi mreže kroz duži vremenski period. Treće se odnosi na određivanje mjera koje su bitne za mjerenje. S obzirom da postoji zaista veliki izbor stavki za mjeriti, razumno bi bilo kreirati listu stavki koje će se mjeriti, time će se postići i veća ekonomičnost. Lista stavki koja se mjeri se još naziva i mrežnim indikatorima. Neki od mrežnih indikatora su, dostupnost linka, dostupnost čvorova, broj korisnika koji ne mogu pristupiti mreži zbog opterećenosti (faktor blokiranja) i vrijeme odaziva na zahtjev [6]. Alati za nadzor mreže pružaju brojne informacije mrežnom administratoru kroz korištenje raznih mrežnih performansi, neke su već i prije spominjane, ali u drugim svrhama. Najčešće mjere koje se koriste za mjerenje i nadzor su dostupnost, propusnost, iskorištenje širokopojasnosti[28] i kašnjenje. Tablica 1. prikazuje koje su to mjere, njihov opis te klasifikacija u smislu što je poželjnije, veća ili manja vrijednost mjere. Kod dostupnosti je očito da je potrebna skoro stalna dostupnost računalne mreže (99.99%), što veća propusnost računalne mreže, bolja i za korisnike i za administratore računalnih mreža. Iskorištavanje treba biti optimalno, kako ne bi zbog velikog iskorištavanja došlo

[28] širokopojasnost – ili (engl. *bandwidth*) se definira kao raspoloživi prijenosni kapacitet, širina pojasa od izvora do odredišta. Bitno je napomenuti da ta mjera definira teoretski najveću brzinu prijenosa (b/s)

do kašnjenja, zbog zagušenosti ili malog iskorištavanja da se ne iskoristi potencijal mreže. Dok je za pogreške i kašnjenje vrlo očito, što ih je manje to bolje.

Tablica 1. Pokazuje koje su najbitnije mjere vezane za nadzor performansi s klasifikacijom i njihovim opisom

Mjere	Klasifikacija	Opis
Dostupnost	Što veća	Mjera koja govori koliku su često mrežni resursi dostupni korisnicima u postotku vremena
Propusnost	Što veća	Mjera koja pokazuje količinu prenesenih podataka u mreži kroz neki period, zapravo se još smatra kao dostupna širokopojasnost
Iskorištavanje širokopojasnosti	Optimalna	Mjera koja pokazuje iskorištenost linka, *porta* ili mrežnih resursa.
Kašnjenje	Što manje	Vrijeme potrebno da paket prijeđe, svejedno da li u jednom smjeru ili vrijeme obilaska kroz cijelu mrežu, jedan njen segment ili do mrežnog uređaja
Stopa pogreške	Što manja	Mjeri postotak paketa koji sadrže pogrešan bit na mrežnom link, segmentu ili uređaju

Izvor: [9]

Već prije spominjan QoS, koji garantira kvalitetu usluge dogovorenu kroz SLA, potrebno je konstantno nadzirati performanse mreže i kreirati alarme ako se dogodi kršenje i pad dogovorenih performansi. S obzirom da je mreža *best effort*, a zagarantirana usluga je jedna od usluga koja je iznimno bitnim određenim računalnim mrežama, QoS garantira određene mjere, a mjere su one iz tablice 1. QoS je zapravo samo dio upravljanja SLA, a napredno upravljanje SLA-om se sastoji od kvalitete usluge (QoS), mrežnim performansama i kvalitetom iskustva (engl. *Quality of Experience*, QoE). Sve se to još da nadzirati kako bi se dobili statistički podaci i poboljšali svi dijelovi SLA.

Što se tiče sigurnosti, nadzor se često veže uz pojam vatrozida. Danas svako poduzeće posjeduje neku vrstu vatrozida, a najčešća imena koja se pojavljuju su Cisco i Fortigate, kao najkorišteniji proizvođač vatrozida. Osnovne zadaće koje vrši vatrozid vezane za nadzor sigurnosti su duboka analiza prometa koja odlazi i dolazi na računalnu

mrežu organizacije. Gdje se zapravo vrši analiza prometa, paket po paket te DoS načelo koristi analizu prometa tako što prati kvantitetu paketa kao i izvornu i odredišnu adresu. Alat koji služi za kontrolu aplikacija analizira promet, kako bi se ustanovilo koja je aplikacija generirala promet. Već prije spomenuti IPS prepoznaje abnormalni i sumnjivi promet i upozorava mrežnog upravitelja. Još neke od osnovnih funkcija vatrozida su prije spomenuti DLP, zatim filtriranje emailova, filtriranje internet stranica, kontrola aplikacija i krajnjih korisnika. Sve ovo spomenuto je potrebno prvo prilagoditi potrebama organizacije i uskladiti sa standardima, dakle prvo je potrebno primijeniti politiku upravljanja i postaviti parametre za nadzor. To se postiže definiranjem razine prijetnje po vrijednostima određenih aplikacija, zaštite od neovlaštenih napada, detekcije *malwera*[29], inspekcija paketa i *web* aktivnosti. Nakon toga stupa na snagu nadzor i bilježenje prometa koji prolazi kroz vatrozid i upozorava na maliciozne podatke (pakete) te napade na mrežu. Jedan takav primjer je gdje se može dogoditi da računalo na mreži generira iznimno veliki promet prema van ili zaprima veliku količinu prometa. To potiče na sumnju da je računalo zaraženo te ga se preko softvera vatrozida odmah može blokirati i zatim se prijavljuje putem *ticketa* ljudima zaduženima za održavanje računala da pronađu problem i saniraju ga. Dakle sve se može nadzirati, emailovi, pretraživanje interneta, kontrola aplikacija i iznimno bitno za ovaj rad, nadzor prometa i njegova duboka analiza, paket po paket [16].

U nastavku će se objasniti nadzor mreže u smislu da postoji nadzor jedne mreže i nadzor interneta. Nadzoru pojedine mreže se daje puno veća pažnja, zato što poduzeće ovisi o kvaliteti te mreže bude zadovoljavajuća, gdje se mogu nadzirati svi mrežni uređaji i konfigurirati točno onako kako to odgovara poduzeću. Tako da će poduzeće kreirati svoju politiku upravljanja mrežom i koje parametre će nadzirati, tj. koji parametri su joj od esencijalne važnosti. Dok kod nadzora interneta postoji ogroman broj uređaja koji nije u nadležnosti onoga koji nadzire. Internet je mreža svih mreža, tako da ju je praktički nemoguće cijelu nadzirat, a zbog toga će se puno veća pažnja dodijeliti nadzoru pojedine mreže i njenih standarda [6].

[29] *malware* – ili štetni računalni program je pojam koji označava računalni program koji radi štetu korisniku. Radi se o računalnim programima koji se pokreću na računalnom sustavu bez stvarnog korisnikovog pristanka i imaju nepoželjni učinak, kao što je oštećenje programa i podataka koji se nalaze na sustavu, širenje na druge terminalne uređaje, krađa podataka (osobito povjerljivih podataka kao što su lozinke i brojevi kreditnih kartica), omogućavanje neovlaštenog udaljenog pristupa na računalo, masovno slanje neželjene elektroničke pošte (*spama*), itd.

4.2 Nadzor pojedine mreže

Kod nadzora mreže uglavnom se misli na udaljeni nadzor mreže, pomoću standarda i aplikacija za nadzor. Kod nadzora pojedine mreže spominju se tri standarda: RMON, RMON2 i SMON (engl. *Switched network monitoring*). Svaki od ovih standarda koriste SNMP protokol, koji informacije gleda kao set upravljanih objekata koji su definirani od strane MIB-a, a opisani i imenovani od strane SMI standarda. RMON je standard koji definira kako nadzirati mrežni promet i navodno se implementira RMON sonda (engl. *probe*) od strane prodavača mrežnih uređaja, tako da se sinkroniziraju uređaji i softver i budu na RMON standardu. Ta sonda prikuplja komunikacijsku statistiku te olakšava nadzor upravljačke stanice, tako što upravljačka stanica ne mora cijelo vrijeme prozivati mrežni uređaj. RMON pripada u kategoriju pasivnih protokola za nadzor gdje se mjeri pravi promet i dobar je za rješavanje problema. Svi statistički podaci se spremaju u RMON MIB, a SNMP upravitelj može pristupiti tim podacima. Još jedna prednost ovoga standarda je u slučaju pada veze, tj. *linka*, upravljanog uređaja i upravljačke stanice (SNMP upravitelj), gdje sonda obavijesti stanicu da je došlo do prekida veze, ali zato može javiti važne događaje u okolini upravljanog uređaja. Ciljevi i objašnjenja RMON-a se nalaze u tablici 2. [6].

Tablica 2. Definira RMON ciljeve i njihova objašnjenja

RMON ciljevi	Objašnjenja
Izvanmrežne operacije	RMON kompatibilni uređaji trebaju biti neovisni, tako da mogu funkcionirati i prikupljati statističke podatke i u izvanmrežnom stanju upravljanja mreže.
Proaktivan nadzor	RMON kompatibilni uređaji moraju konstantno vršiti dijagnostiku i bilježiti mrežnu statistiku onda kada i mreža ne doživljava probleme. Time se utvrđuje normalno ponašanje mreže i kada mreža padne, mrežni upravitelj može imati temelje za usporedbu sa trenutnim problematičnim stanjem mreže.
Detekcija pogrešaka i izvješća	RMON kompatibilni uređaji bi trebali detektirati probleme sami unutar sebe. Kada komponenta uređaja ne radi kako treba, uređaj mora obavijestiti mrežnog upravitelja.
Podaci s dodanom vrijednosti	RMON kompatibilni uređaji moraju bilježiti korisnu statistiku o mreži, iako se ta statistika ne koristi za pronalaženje mrežnih problema. Na primjer nadzor prometa na *hostovima*, da se ustvrdi koji *hostovi* su najkorišteniji, a to je vrlo bitan podatak za buduće mrežne ekspanzije.
Višestruki upravitelji	RMON kompatibilni uređaji mogu biti kontrolirani i podnositi izvješća više od jednom mrežnom upravitelju, radi redundancije i distribucija prikupljenih podataka na različitim lokacijama.

Izvor: [6]

RMON2 je nadogradnja na RMON i fokusira se na više slojeve prometa iznad MAC sloja. RMON2 ističe IP promet i promet aplikacijskog sloja. RMON2 omogućava aplikacijama za upravljanje mrežom, nadzor paketa na svim mrežnim slojevima. To je razlika od RMON-a, koji dopušta nadzor paketa jedino na MAC sloju ili niže. Kod RMON2, svaki upravljani objekt mora imati ime, sintaksu, pristupnu razinu i status implementacije. Postoji još niz dodataka koji poboljšavaju RMON2 u odnosu na RMON, međutim neće se ići toliko u detaljnije u ovome radu.

SMON je nadogradnja za nadzor preklopničkih mreža. RMON2 se koristi za nadzor mreža baziranih na okvire, kao dio paketa u *Ethernet*-u, a SMON je namijenjen za ATM mreže i preklopničke LAN mreže. Postoji nekoliko razlika u odnosu na mreže s okvirima. Prvo, podaci u preklopničkim mrežama su spojno orijentirani i samo jedan nadzor ne može uhvatiti podatke slušajući *broadcast* kao kod *Etherneta*. Drugo, nadzor s kraja na kraj kod preklopničke mreže zahtijeva više resursa. Treće, mora se razmatrati opcija VLAN-ova kako bi se selektirao promet, recimo može se virtualno podijelit preklopnik na dva dijela.

Četvrto je prioritizacija paketa kod preklopničke mreže. Peto, SMON se fokusira na nadzor paketa na višim slojevima mreže. SMON vidi tri tipa izvornih podataka: RMON, VLAN i fizički, gdje su svi podaci koji nisu od RMON-a ili VLAN-a se smatraju fizički [6].

4.3 Nadzor Interneta kao mreža svih mreža

Internet je mreža svih mreža, što znači da se sastoji od pojedinih mreža, rukovođena od raznih organizacija. Kao što je prije objašnjeno, nadzor interneta je sasvim drugačiji od nadzora pojedine mreže, jer kod pojedine mreže sve su komponente pod kontrolom jednog upravljanja mrežom. Dok kod interneta postoji puno različitih mreža sa različitim upravljačkim politikama.

Internet iz dana u dan raste, priključivanjem svakoga korisnika, internet se proširi, tako da je nadziranje interneta iznimno kompliciranо i teško. Ne postoji standardizirani alat za nadzor interneta, zato što različiti ljude koriste različite alate. Zato postoje svima dostupni alati za nadzor sa osnovnim funkcijama. Neki od najpoznatijih takvih alata su *ping*, protokol za prijenos podataka (engl. *File transfer protocol*, FTP) i *traceroute*. *Ping* je već prije objašnjen, a FTP služi za prijenos podataka od izvora do odredišta, a to omogućava mjerenje brzine prijenosa podataka.

Traceroute prikazuje broj *hopova* (to je broj uređaja, usmjerivača kroz koje prođe paket) do odredišta i performanse usmjeravanja. Postoji još cijeli niz alata, kao što su *arpwatch*, *nslookup* itd. [6].

4.4 Tehnike i protokoli za nadzor mreže

Postoje razne tehnike, tj. alati koji se mogu koristiti za nadzor. Neki su već prije objašnjeni, a to su ICMP i SNMP. Kod SNMP-a, a tiče se nadzora je jako bitan tzv. SNMP *trap*, koji se aktivira kod agenta da obavijesti stanicu za upravljanje mreže o događaju na mreži, bez da se traži upit od upravitelja. Kada je upravitelj mreže zadužen za nadzor velikog broja uređaja i svaki uređaj se sastoji od brojnih objekata, nepraktično je tražiti povremeno od svakoga uređaja informacije o njihovom statusu i zdravlju. Tako da se svakom agentu na upravljanim uređajima postavlja SNMP *trap* koji obavještava upravitelja o događaju i može se odrediti akcija zasnovana na događaju [10].

Jedan od glavnih i osnovnih protokola za pristup udaljenom računalu je *telnet* kod TCP/IP mreža te je jedan od protokola koji je istaknuo taj model. Telnet veza se najčešće koristi za interaktivni rad na udaljenom računala te se može upravljati tim uređajima, tako da telnet nije samo za nadzor nego i za upravljanje uređajima i njihovo konfiguriranje. Bazira se na LAN-u ili WAN-u. Za nadzor, telnet se koristi u svrhu provjeravanja dostupnosti uređaja na mreži, tamo gdje je *ping* blokiran, također se može provjeriti temperatura, da li su sve komponente uređaja u operativnom stanju, promet itd.

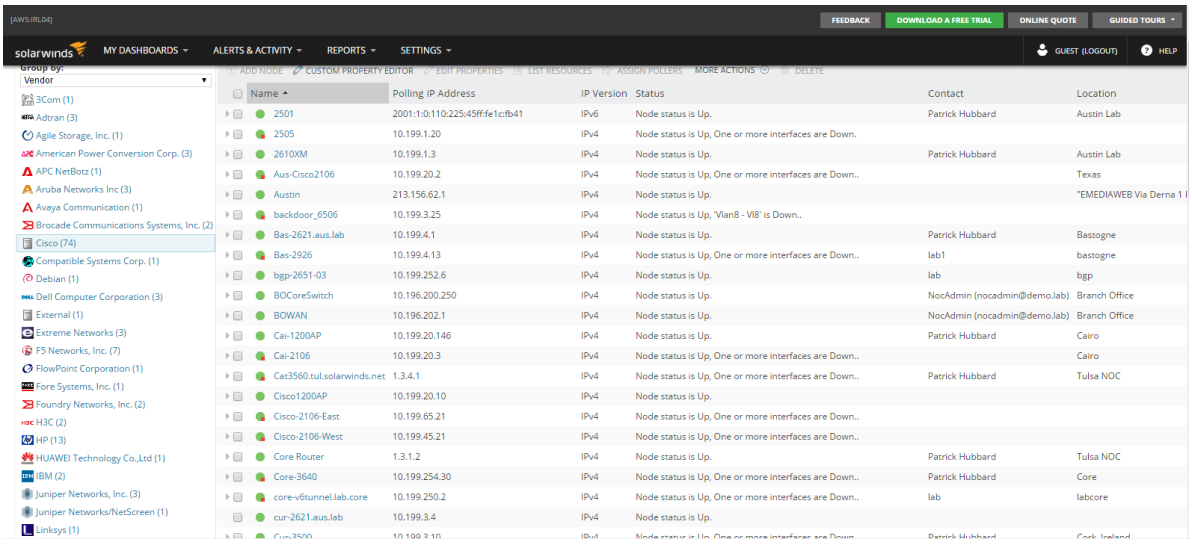
Drugi protokol za pristup udaljenom računalu je SSH (engl. *Secure Shell*), koji za razliku od telneta posjeduje sigurnosne mehanizme za zaštitu korisnika od neovlaštenih pristupa. Telnet je dizajniran za privatne mreže, a ne preko javne mreže gdje postoje prijetnje, dok SSH-a ima kriptirane podatke i potrebna je posebna lozinka (javni ključ) kako bi se pristupilo upravljanju i nadzoru uređaja. Za SSH-a je potrebna veća širokopojasnost nego za telnet, zbog kriptiranih podataka. Što se tiče funkcija koje posjeduje, iste su kao kod telneta i za upravljanje i za nadzor. Dakle može se nadzirati rad procesora i koliko je opterećen, zatim temperatura uređaja. Kada je veća korištenost kapaciteta procesora te je potrebno izbjegavati povremeni nagli rast temperature uređaja. Nadzor brzine i statusa ventilatora (temperatura i performanse ventilatora idu ruku pod ruku) osigurava rad ventilatora za balansirano hlađenje i optimalnu temperaturu uređaja. Zadnji element koji se nadzire je stanje napajanja

Sljedeća skupina mehanizama nadzora su vezani za vrste zapisa. Mehanizam koji se tradicionalno koristi je nadzor *log* podataka, gdje se aplikacija ili proces zapisuju u običan tekst na uređaj. Zatim se postavi nadzor na taj uređaj koji će očitavat te zapise i tražiti riječi koje su okidač da nešto ne radi kako bi trebalo. Potrebno je odrediti koje će to

riječi biti, kako ne bi uređaj slao lažne alarme ili da ne pošalje bitne. *Syslog* je jedan od tih mehanizama, koji koristi poruke slične SNMP *trapu*. *Syslog* preuzme događaj koji se dogodi na uređaju i šalje ga na udaljeni sustav (*syslog* odredišni server). Drugačiji je od SNMP *trapa* jer nije ovisan od MIB-OID strukturi. Može se koristiti kao zamjena za tradicionalni nadzor *log* podataka, tako što *syslog* šalje poruke putem *syslog* protokola do vanjskog uređaja, koji prikuplja *syslogove* sa različitih uređaja i djeluje na određene riječi, okidače (engl. *triggers*) koji se definiraju od krucijalne važnosti. *Syslog* se često koristi kod uređaja namijenjenih za poboljšavanje sigurnosti kao što je vatrozid ili sustav za prevenciju neovlaštenih upada [10].

5. Sustavi za upravljanje i nadzor računalnih mreža

Sustavi koji služe za upravljanje i nadzor računalnih mreža su često u današnje vrijeme zapravo skup računalnih programa odnosno programskih alata koji zajedno omogućavaju upravljanje i nadzor svih elemenata mreže. Kako bi sustav bio cjelokupno obuhvaćen potrebno je uzeti u obzir svako područje FCAPS modela. Neki od programa koji se koriste za upravljanje i nadzor računalnih mreža su: PRTG, Cisco Prime Infrastructure, Nagios, Pandora FMS, SolarWinds i razni drugi. Rijetko koji računalni program pokriva svako područje iznimno kvalitetno, jedan od takvih programa koji kvalitetno obuhvaća praktički sve dijelove FCAPS modela je SolarWinds i objasnit će se tako da pokrije sva područja FCAPS modela. Zapravo se SolarWinds platforma sastoji od raznih programa i alata implementiranih tako da djeluju i surađuju zajedno i čine jednu cjelinu. Sastoji se od nadzora mrežnih performansi, nadzora servera i aplikacija, upravljanje događajima i *logovima*, upravljanje mrežnim konfiguracijama, podrška za udaljena spajanja na uređaje, Netflow analizator prometa, upravljanje nadogradnjama sustava, *syslog* za servere, baza podataka analiza mrežnih performansi, upravljanje virtualnim uređajima, upravljanje kvalitete usluge i nadzor ugovorenih performansi, upravljanje sigurnošću kroz vatrozid itd. Za nadzor i upravljanje računalnim mrežama zaista postoji velik broj programa od samih proizvođača opreme pa do programa koji nastoje obuhvatiti velik broj proizvođača opreme u jedan sustav te pružiti različitim organizacijama jednostavno rješenje za upravljanje i nadzor računalne mreže. Kao što se može vidjeti na slici 7. gdje računalni program SolarWinds daje podršku raznim proizvođačima mrežne opreme i selektira uređaje na mreži po proizvođačima (Cisco Systems, Windows, HP, IBM, Juniper, 3Com itd.). Osim po proizvođačima uređaji na mreži se mogu grupirati po raznim kriterijima kao što su potrošnja energije, verziji SNMP-a, ulozi uređaja unutar računalne mreže (mreža, server, ostali), status uređaja, lokacija, nadležna osoba i tako dalje.



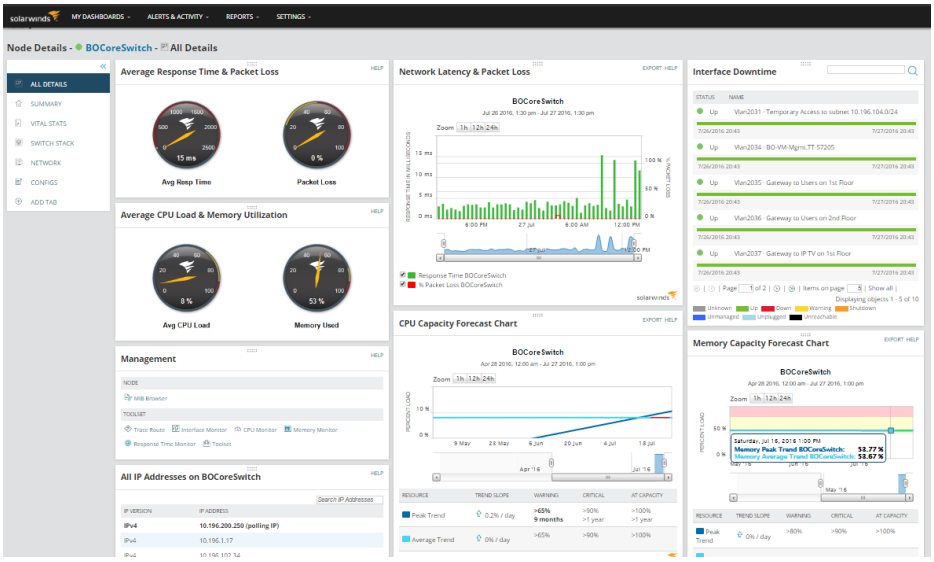
Slika 7. Prikaz proizvođača i njihove opreme u mreži

Izvor: [12]

Slika 7. prikazuje upravljanje čvorovima, uređajima na mreži, dakle odabere se kategorija grupiranja uređaje i mogu se vidjeti osnovni podaci uređaja (da li je uređaj u funkciji, IP adresa, proizvođač i model uređaja, vrijeme odaziva, gubitak paketa, opterećenje procesora, iskorištenost memorije) samo prijelazom pokazivača preko naziva uređaja. Odabirom uređaja se mogu vidjeti svi detalji o uređaju. Sučelje je iznimno jednostavno za korištenje i moguće je kreirati pokazatelje o uređaju u obliku slika, grafova, tablica, kao što je prikazano na slici 8. Moguće je vidjeti sve detalje o uređaju ili odabrati po kategorijama i tako olakšati pregled onoga što je u fokusu interesa u tom trenutku. SolarWinds je napravljen tako da bude vizualno zanimljiv, ali ujedno i informativan, sa raznim vrstama grafova, zatim mrežnim mapama, različitim bojama (radi bržeg uočavanja problema), vizualno pojednostavljeni prikaz podataka kroz interaktivne mjerače važnih podataka o uređaju i njegovih performansi. Neke od bitnih podataka koji se prikupljaju vezanih za FCAPS model, a nisu prije spomenuti su verzija softvera na uređaju, da li je fizički ili virtualan, broj procesora, poveznica kojom se spaja na uređaj putem telneta ili putem pretraživača. Zatim je moguće vidjeti iskorištavanje pojedinih sučelja na uređaju, koliko je promet na pojedinom portu uređaja i to se mjeri u bps, kbps, Mbps te također piše i postotak iskorištavanja sučelja na uređaju. Također je moguće mjeriti kvalitetu usluge kroz mjerenje prometa i nadzor aplikacija. S upravljačkog stajališta moguće je vidjeti mod *porta*, zatim vrstu sučelja kao što je *Ethernet*, tip sučelja za VLAN itd. Također prikazuje tablice usmjeravanja prometa, susjede za usmjeravanje, kašnjenje unutar mreže u obliku grafa, statistiku dostupnosti koja je prikazana u postocima. Ako postoji stog preklopnika također će biti prikazani sa oznakama koji je

master, a koji *slave*[30], to je iznimno korisno za upravljanje i nadzor resursa mreže te kolika je redundantnost mreže u slučaju kvarova.

Još jedna iznimno bitna funkcionalnost koju posjeduje SolarWinds je ta da pokazuje liste konfiguracija koje se mogu uređivati, brisati, umetati. Osim toga mogu se uspoređivati konfiguracije u smislu da se vidi trenutna konfiguracija koja se pokreće i ona koja se prije pokretala te program označava linije koda koju su promijenjene, koje su dodane i koje nedostaju u odnosu na prijašnju konfiguraciju. Za one kojima je zadatak nadzor i upravljanje konfiguracijama i koji poznaju konfiguracije i linije koda do sitnih detalja, ovo je iznimno koristan alata za usporedbu konfiguracija. Također za upravljanje konfiguracijama je iznimno dobro vidjeti „top 5“ posljednjih promjena konfiguracija, zatim je moguće preuzeti konfiguraciju s uređaja ili učitati konfiguraciju na uređaj putem SolarWindsa, te ponovno pokrenuti uređaj nakon što se konfiguracija učita. Zadnje, a vezano za nadzor i upravljanje pojedinog uređaja je sigurnost i javljanje pogreške, događaja. Iako se sigurnost češće upravlja i nadzire putem softvera od vatrozidnog uređaja, SolarWinds mjeri recimo ranjivost softvera ugrađenog na uređaju, koliko su ozbiljni napadi *hackera* te vodi bilješke o napadima. A što se tiče nadzora i upravljanja događajima, postoji informacija koji protokol se koristi za javljanje upravljaču mreže (koja verzija SNMP ili nekog drugog protokola), koji interval itd.



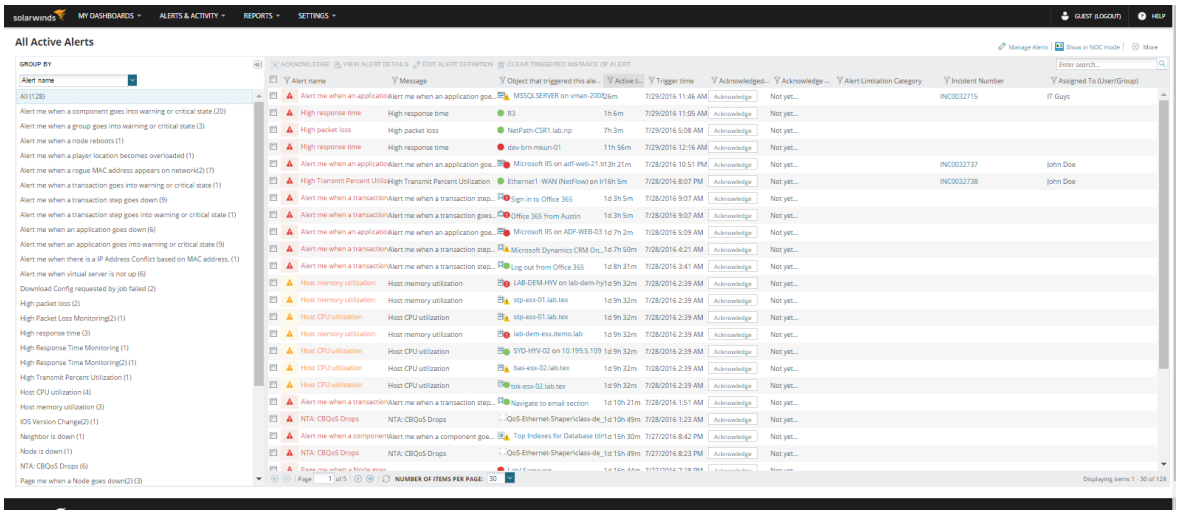
Slika 8. Prikaz podataka i dobivenih mjera nadzorom uređaja

Izvor: izradio autor

[30] *Master-slave* – pojam koji se često koristi u računalstvu i govori kakav je odnos između uređaja na računalnoj mreži, u ovom slučaju govori koji je uređaj aktivan i kroz kojeg prolazi promet (*master*), a *slave* služi kao redundantni uređaj i kada se *master* isključi zbog tehničkih razloga ili radi nadogradnje softvera, *slave* postaje *master* i ostaje, do nove promjene.

Kroz slike i kratke opise prezentirati će se ostale funkcionalnosti bitne za ovaj završni rad, a SolarWinds ih posjeduje. Što se tiče upravljanja i nadzor pogrešaka, SolarWinds ima pregledno grafičko sučelje gdje se vide svi alarmi i mogu biti grupirani po imenu alarma, objektima koji su pokrenuli alarm, ozbiljnost alarma, od koga je potvrđeno te kome je dodijeljen alarm za upravljanje, kao što je prikazano na slici 9.

Ovo je iznimno korisno, jer se postave samo oni alarmi koji odgovaraju politici upravljanja te što će se nadzirati i bilježiti. Na primjer, pritiskom na jedan od ovih alarma na pojedinom uređaju otvara dodatne detalje o alarmu na tom uređaju. Također prikazuje povijest alarma na uređaju te kada je alarm aktiviran, detaljniji opis alarma i opcije za upravljanje alarmima. Također kako će se alarm objaviti upravitelju mreže, može se preurediti definicija alarma ili ga ukloniti.



Slika 9. Prikazuje sve alarme pridošle od strane objekata

Izvor: [12]

Što se tiče upravljanja i nadzora događaja za pogreške, ima koristan pregled svih događaja na mreži, sažete za pokazivanje bitnih događaj. Većina ih je informacijska u smislu obavijesti da se vrši nadogradnja sučelja, tablica usmjeravanja, status promjena na čvorovima. Pokrenuti servisi na čvorovima, prestanak njihovog rada, izbrisani podaci od strane korisnika ili mrežnog upravitelja, uglavnom bilježe se sve promjene na mreži. Slika 10. prikazuje sažete događaje i pritiskom na prozor otvaraju se svi događaji i moguće je vidjeti detaljnije podatke o događaju, kao i grupirati ih po brojnim kriterijima i označiti ih kao viđene i riješene te ih izbrisati.

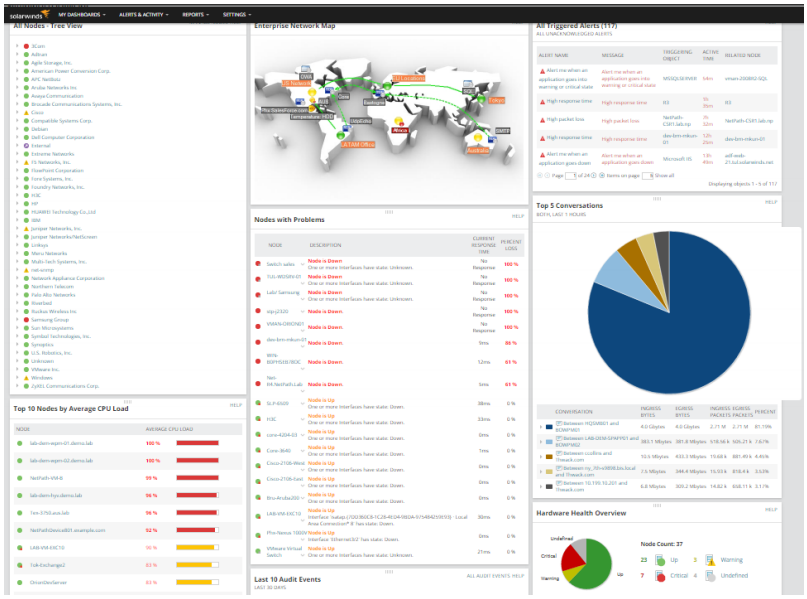


Slika 10. Prikazani sažetak događaja

Izvor: [12]

Osim događaja i alarma, postoji još prikaz *syslogova* i SNMP *trapova* kao alati koji javljaju podatke o uređaju, potrebno je postaviti na samome uređaju kroz konfiguraciju parametre za praćenje i što će uređaj javljati kroz SNMP *trapove* ili RMON poruke. Centar s porukama je središnjica kroz koju se može upravljati s alarmima, događajima, *syslogovima* i SNMP *trapovima*. Kako bi upravljaču mreže bilo moguće pratiti sve bitne događaje, poruke, *syslogove* i *trapove*, potrebno je napraviti selekciju i filtriranje samo onih koji su bitni za politiku upravljanja, kako bi imali prioritet saniranja, a ostale „zanemariti“, međutim potrebno ih je zabilježiti. Takva baza podataka je iznimno bitna kada dođe do pogreške, jer je može vidjeti da li je zbog nedavnih promjena samog uređaja i softvera došlo do te pogreške.

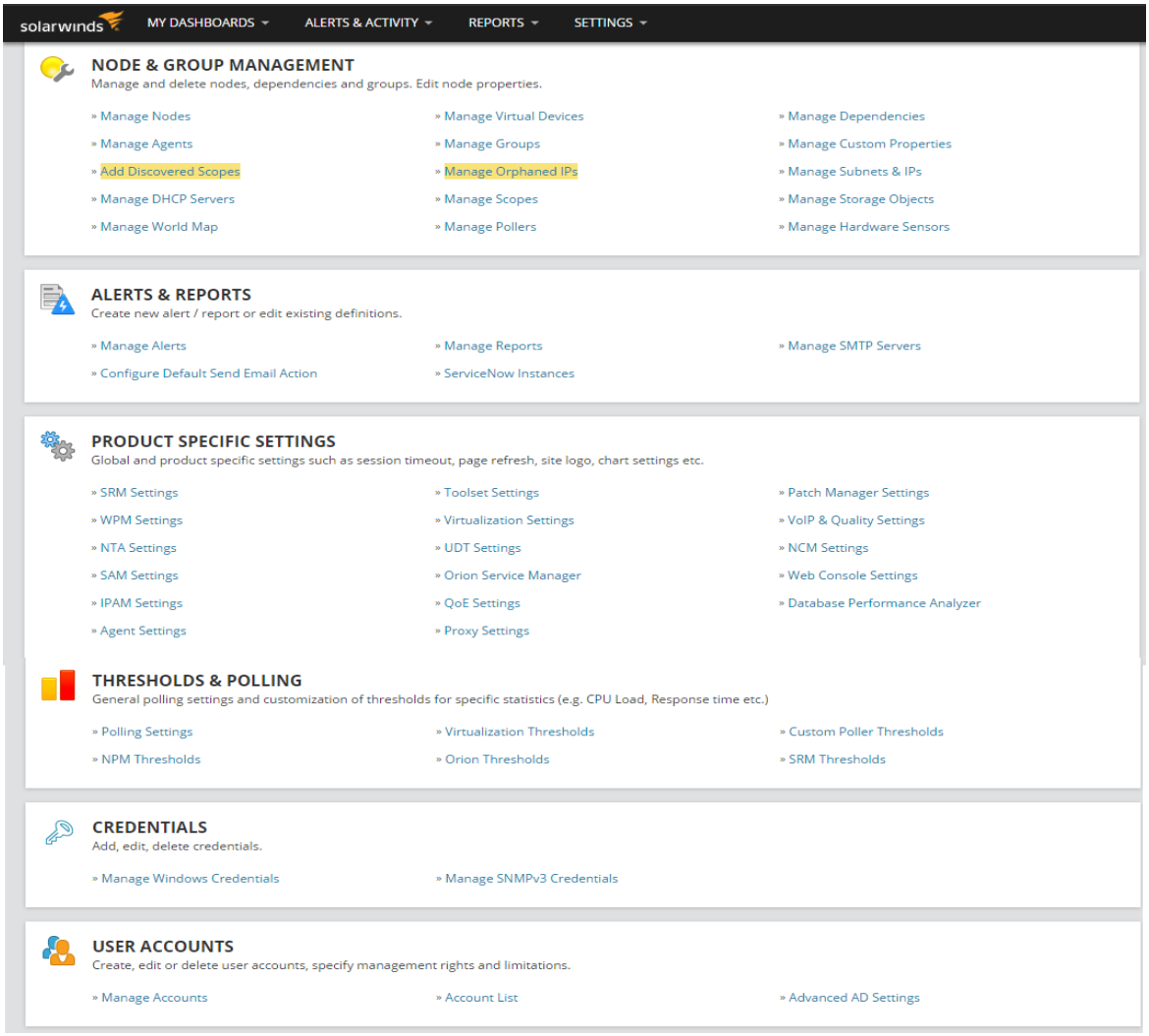
Kao sažetak cijelog sustava za nadzor i upravljanje, postoji opcija koja sažima sve najbitnije dijelove koji se žele nadzirati, a zatim od dobivenih podataka nadzorom i upravljati. Slika 11. prikazuje primjer sažetih bitnih podataka, naravno svaki mrežni upravitelj ima svoje prioritete za nadzor, tj. koje elemente želi pratiti u sažetku. Zato je dobro što je SolarWinds moguće uređivati tako da odgovara svakome i svačijim potrebama. Kao što je prikazano na slici 11. vidljivo je da se sastoji i od mape jednog poduzeća i prikazuje gdje se što nalazi diljem svijeta te koliko ima objekata na svakom od tih područja te da li radi ispravno ili ima problema. Zatim se vide alarmi, opterećenja čvorova, prikaz svih čvorova, zdravlje opreme, čvorovi koji generiraju najviše prometa i još mnogo drugih opcija, sve ovisno o mrežnom upravitelju i njegovim prioritetima.



Slika 11. Sažeti prikaz nadzora mreže po različitim područjima FCAPS modela

Izvor: izradio autor

Rezultati dobiveni nadzorom mreže su prikazani kroz slike u ovome poglavlju, a detaljnije će se objašnjavati u 6. poglavlju, međutim SolarWinds nije samo namijenjen za nadzor mreže, već ga je moguće urediti tako da odgovara potrebama korisnika, tj. mrežnih upravitelja. Slika 12. prikazuje postavke gdje se može upravljati apsolutno svime potrebno za upravljanje računalne mreže. Sva područja FCAPS modela su obuhvaćena, što se tiče upravljanja računalnom mrežom. Moguće je prilagoditi upravljanje alarmima po potrebi, upravljanje čvorova u mreži, pratiti čvorove, upravljanje performansama, sigurnošću, udaljeni pristup računalu kako bi se mogao konfigurirati, upravljanje politikom naloga i praćenje krajnjih korisnika, njihovih aplikacija itd. Osim opcija prikazanih na slici 12., postoji još centar za otkrivanje mreže i dodavanje uređaja te modifikacija izgleda programa i detalji vezani za bazu podataka, licenca itd.



Slika 12. Prikaz svih glavnih postavki unutar računalnog programa SolarWinds

Izvor: [12]

Nakon kratkog uvoda za upoznavanje računalnog programa SolarWinds i izgleda jednog takvog sustav za upravljanje i nadzor računalnih mreža, detaljnije će se opisivati njegove funkcije i mogućnosti. Kroz sljedeće poglavlje, koje je i najbitnije u ovome završnom radu, detaljno će se proći kroz svako područje FCAPS modela pomoću ovoga računalnog programa i usporedit će se upravljanje i nadzor računalnih mreža te da li upravljanje i nadzor ovise jedno o drugome [12].

6. Usporedna analiza sustava za upravljanje i nadzor računalnih mreža

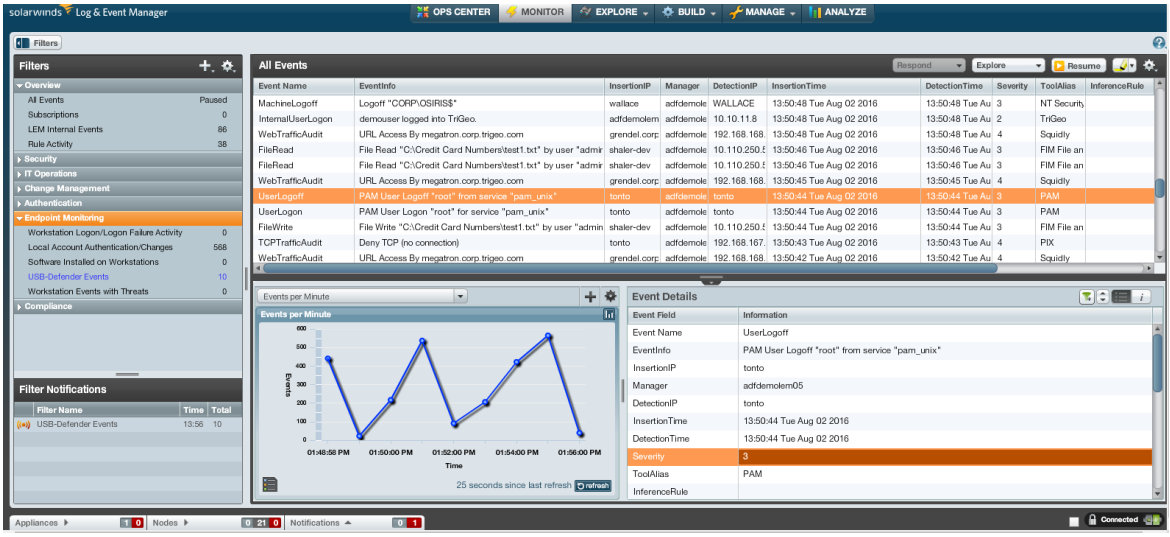
Ovim poglavljem definira se završni rad te se detaljno analiziraju sustavi za upravljanje i nadzor. Segmentacijom na dva različita sustava analizira se da li je moguće da jedan sustav funkcionira bez drugoga (ili su efikasniji kada rade zajedno kao cjelina). Analiza će se napraviti tako da će se svako područje FCAPS modela usporediti sa stajališta upravljanja i sa stajališta nadzora. Dobit će se jedan sustav koji objedinjuje funkcije za upravljanje i jedan sustav koji objedinjuje nadzor te u kakvom su odnosu. Provest će se kroz WAN mrežu i interaktivni program za probu, koji omogućava početna upravljanja i postavljanje elemenata za nadzor te dobivanje konkretnih rezultata nadzorom. Postoje podaci koji su dobiveni nadzorom, ali moguće je i dobiti podatke nadzorom na WAN mreži u interaktivnom programu za probu SolarWindsa. Nažalost, zbog toga što je SolarWinds potrebno kupiti, kako bi se otključale sve njegove mogućnosti, nije moguće pokazati sve njegove mogućnosti, međutim dovoljno za upravljanje i nadzor računalne mreže. Upravljačke elemente je moguće postaviti te će se postaviti i prikazati kroz slike dobiveni rezultati upravljanja, a i podaci dobiveni nadzorom WAN mreže.

6.1 Usporedna analiza sustava za upravljanja i nadzor pogrešaka (F)

Glavni ciljevi upravljanja i nadzora pogrešaka su prepoznavanje pogrešaka alatima i protokolima za nadzor i detekciju pogreške (često su to alarmi, *logovi*, događaji, *syslogovi* i ostali sofisticirani algoritmi za detekciju pogreške). Prvi cilj se odnosi na sami nadzor mreže, a SolarWinds omogućava praćenje alarma kao što je prikazano na slici 9. i praćenje događaja kao što je prikazano na slici 10. Osim praćenja i nadzora događaja, alarma na ovome sučelju, SolarWinds nudi još jedno sučelje za nadzor svih događaja i bilježenje *logova* kao što je prikazano na slici 13. SolarWinds omogućava nadzor svih događaja na mreži vezane za nadzor pogrešaka, kao i nadzor sigurnosti (to će se dodatno objasniti kod sigurnosti). Na slici je prikaz svih događaja i odabrani događaj (slika 13.), gdje se korisnik odjavio sa svoga korisničkom računa kao primjer koji pokazuje bilježenje toga događaja. Sučelje je slično programu Wireshark-a[31] gdje se prikazuju događaji dok

[31] Wireshark – je besplatni alat za analizu paketa te se koristi za *troubleshooting* i analizu prometa

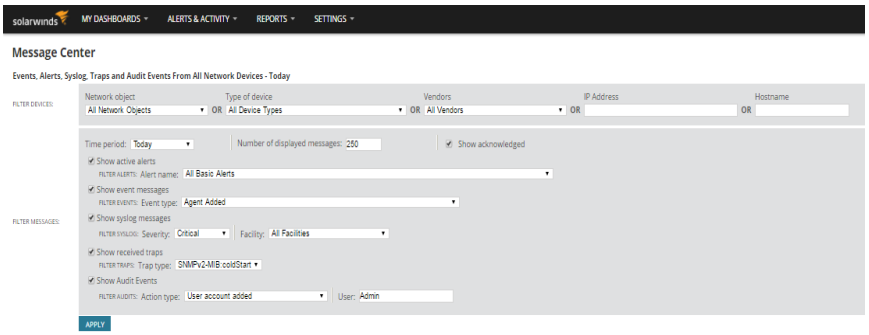
se ne pauzira alat. Ovdje se mogu detektirati nepoželjni događaji i zatim pokrenuti postupak ispravljanja pogreške u proaktivnom smislu.



Slika 13. Prikazuje sučelje za praćenje svih događaja na mreži i nadzor krajnjih korisnika

Izvor: izradio autor

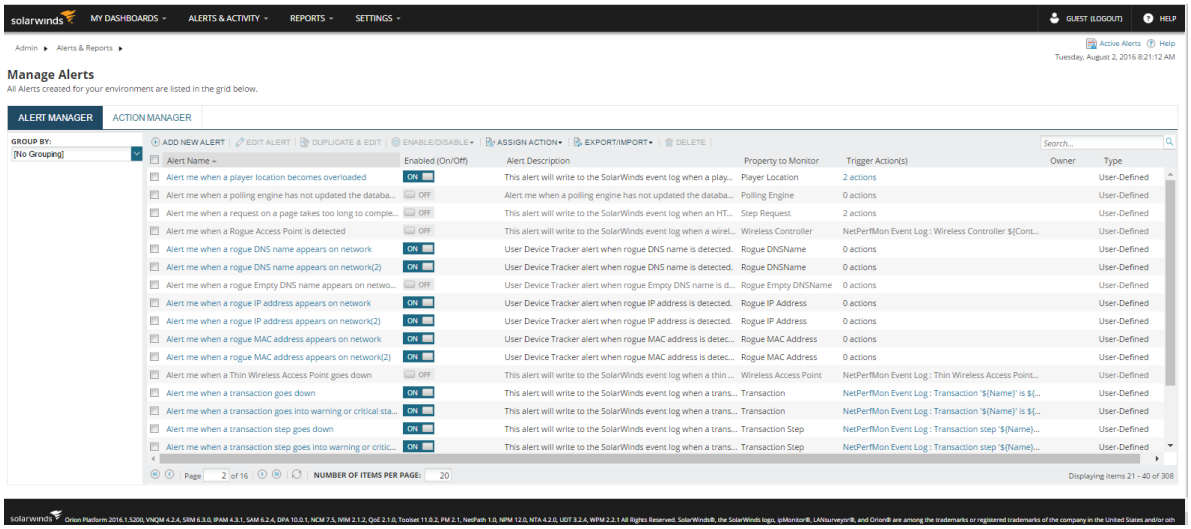
Međutim za nadzor pogrešaka su najbitniji alarmi koji detektiraju pogreške, a to sučelje je prikazano na slici 9. Ti alarmi su ključ nadzora pogrešaka i zaslužni su za detekciju pogrešaka i javljanja mrežnom upravitelju, kako bi mogao reagirati i ispraviti pogreške. Rezultat nadzora kroz ove alate je detekcija pogrešaka i obavještavanje mrežnog upravitelja o njima. Bitno je naglasiti da mrežni upravitelj mora postaviti te alarme i znati točno koje alarme postaviti na različite uređaje i napraviti kvalitetno filtriranje tih alarma, tj. poruka (*syslogova*, *logova*, događaja i SNMP *trapova*). SolarWinds pruža jedan takav centar za poruke koji omogućava jednostavno filtriranje za nadzor svih poruka po zadanim parametrima koje mrežni upravitelj želi filtrirati, kao što je prikazano na slici 14.



Slika 14. Centar za poruke s opcijama za filtriranje

Izvor: [12]

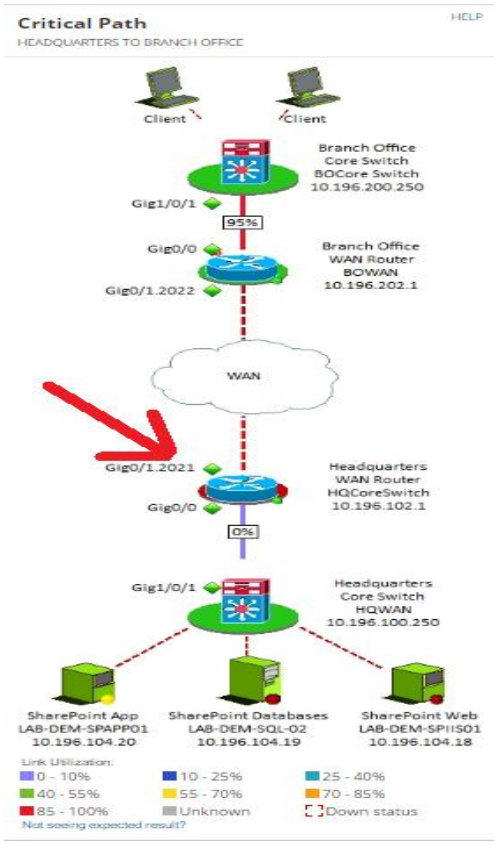
Sve alarme i događaje je potrebno upravljati, nije poželjno nadzirati apsolutno svi alarmi, nego samo oni koji su bitni za jedan sustav, organizaciju. Zato je unutar SolarWinds moguće podesiti alarme tako da odgovaraju potrebama mrežnog upravitelja i sukladni politci upravljanja. Slika 15. prikazuje popis svih alarma koji su dobiveni uz računalni program SolarWinds, a moguće je dodati i nove alarme, samo je potrebno odabrati alarme koji se žele pratiti, a postoji cijeli niz alarma i do šesnaest stranica različitih alarma. Također je sve te alarme potrebno kroz upravljanje pogreškama bilježiti radi budućih mogućih pogrešaka.



Slika 15. Prikaz alarma te što se njima prati i koji su odabrani za praćenje

Izvor: [12]

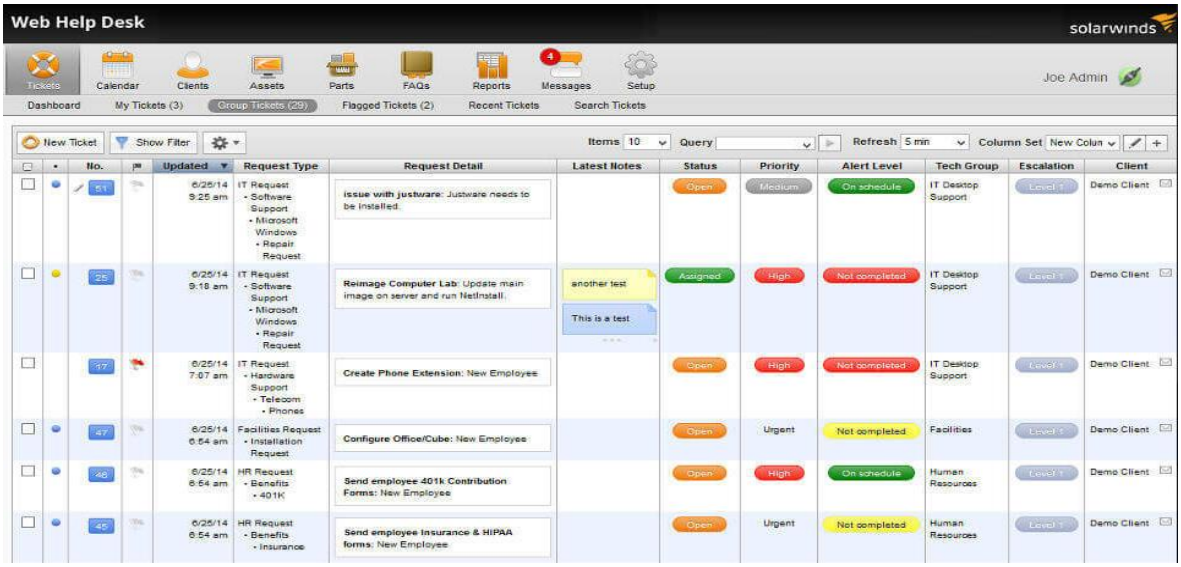
Sljedeći je cilj dijagnoza pogreške, zašto je do nje došlo, izvor i na kraju rješavanje same pogreške. Sučelje SolarWinds omogućava nadzorom jednostavan grafički prikaz mjesta gdje se dogodila pogreška kao što je prikazano na slici 16. (označeno crvenom strelicom). Nakon što je nađen izvor nadzorom, potrebno je kroz upravljanje, tj. mrežni upravitelj mora razriješiti nastalu pogrešku. Sa slike je vidljivo da je jedan usmjerivač u neoperativnom stanju i da komunikacijska veza između usmjerivača glavnog sjecišta i preklopnika glavnog sjedišta nije u funkciji. Dakle mrežni upravitelj mora udaljeno pristupiti (SSH ili telnet) usmjerivaču i preklopniku te ustvrditi koji od njih dvoje je odgovoran za pogrešku u komunikaciji. Mora provjeriti koja komponenta nije u funkciji, da li je to sučelje, ventilator uređaja, nestanak struje, požar ili nemogućnost komunikacije dijelova mreže zbog loših konfiguracija.



Slika 16. Grafički prikaz dijagnoze gdje je nastala pogreška

Izvor: izradio autor

Zadnje, a vezano za upravljanje je prijavljivanje problema, tj. *ticketa*. Za *ticketiranje* se koristi dodatak SolarWinds-u, također njihov alat, ali nije dio ovoga koji je prije prikazivan kroz završni rad. Zove se Web Help Desk i nudi pregledan prikaz svih *ticketa* sa vrstom zahtjeva od strane korisnika, statusom, prioritetom i kojoj grupi pripada, kao što je prikazano na slici 17. Ovim putem mrežni upravitelj može lako upravljati i nadzirati sve prijavljene probleme i koji je njihov status.



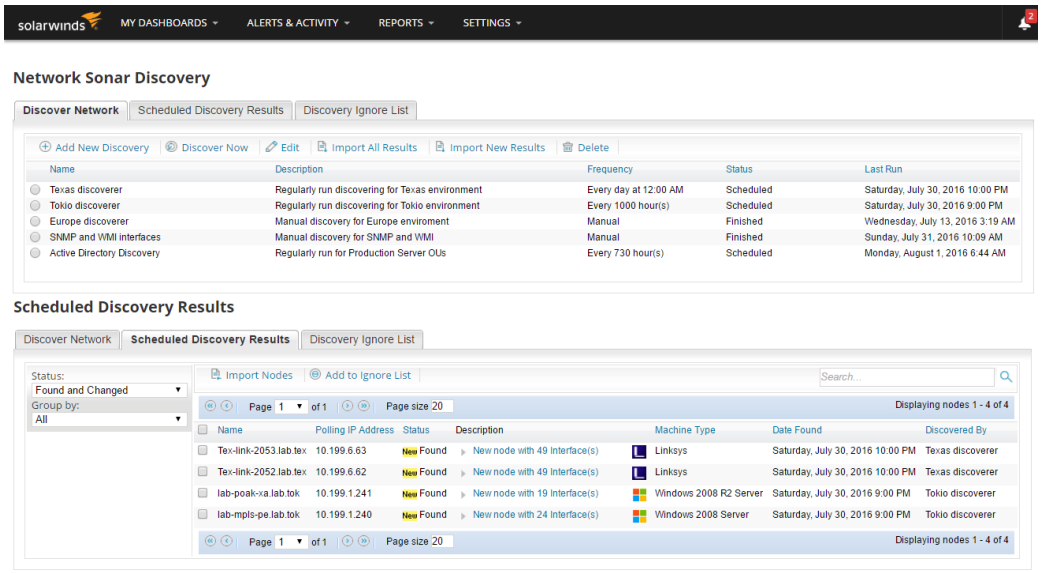
Slika 17. Prikaz alata za detaljno upravljanje *ticketima*

Izvor: [15]

Usporednom analizom sustava za upravljanje i nadzor pogrešaka je vidljivo da je nadzor samo jedan dio upravljanja, on omogućava nadzor udaljenih računala i u obliku alarma šalje upozorenja o mogućim kvarovima, a i javlja nastale pogreške. Nakon toga dolazi upravljanje, kao prvo bilježi alarme, zatim ih dijagnozira i nastoji sanirati, ispraviti. Također se time stječu bitne informacije i moguće je poboljšati kvalitetu računalne mreže, sprječavajući pogreške iste vrste ili se omogućava njihovo brže saniranje. Konkretni rezultati dobiveni ovom analizom su postavljanje alarma kroz upravljanje (slika 15.), zatim nadzor WAN mreže i pogreške koje se događaju na njoj (slika 9.) te pronalazak mjesta pogreške i na koji način se rješavaju pogreške (slika 16.). Potrebno je udaljeno pristupiti mrežnom uređaju i nizom komandi ustanoviti razlog nastale pogreške.

6.2 Usporedna analiza sustava za upravljanje i nadzor konfiguracijama (C)

U nastavku završnog rada dana je usporedna analiza sustava za upravljanje i nadzor konfiguracija kroz računalni program SolarWinds. Ciljevi upravljanja konfiguracijama su uspostavljanje i održavanje dosljednosti performansi, zatim (automatsko) otkrivanje mreže, sinkronizacija opreme, upravljanje rezervnim inačicama računalnih programa za uređaje u svrhu obnove u slučaju kvarova i na kraju upravljanje *patchevima*[32]. Prvo će se prikazati sve vezano za otkrivanje mreže s obzirom da SolarWinds posjeduje tu opciju. Kao što je prikazano na slici 18. vide se opcije za otkrivanje novih uređaja na mreži. Vidljivo je koje su mreže kroz upravljanje podešene za otkrivanje novih uređaja i koliko često, neke su postavljene da same otkrivaju nove elemente unutar svoje mreže u zadanim intervalima, a neke su namještene za ručno otkrivanje mreže. Druga stvar koja se može vidjeti na slici 18. je izvještaj rezultata planiranih otkrivanja i vidljivo je da su dodana dva nova uređaja na dvije različite lokacije. Na jednoj su to dva preklopnika s 48 *portova*, a na drugoj lokaciji su to dva Windows servera.

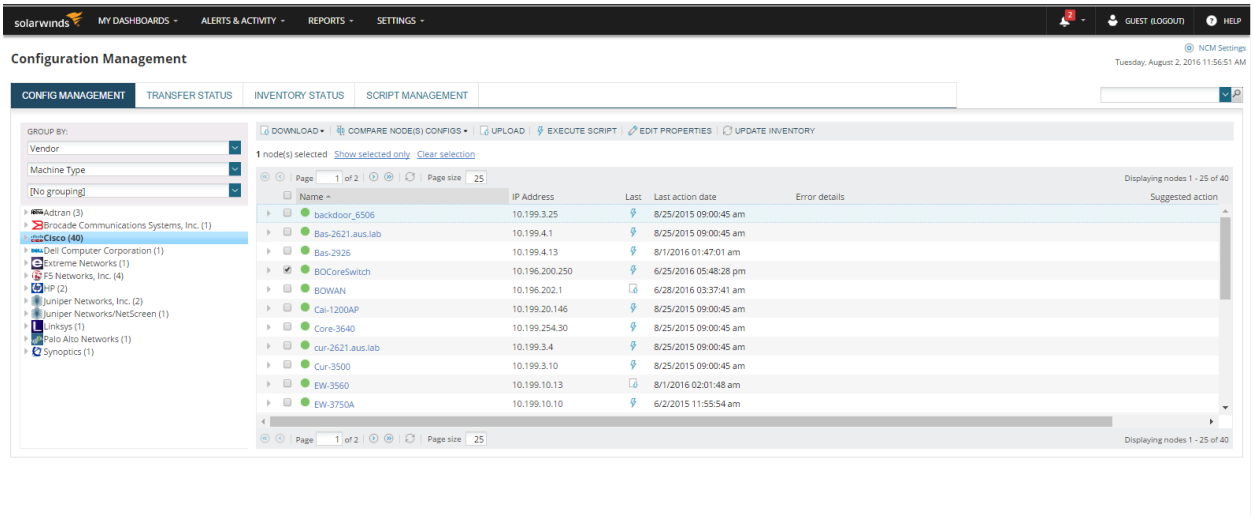


Slika 18. Prikazuje opcije vezane za upravljanje otkrivanjem mreže

Izvor: [12]

[32] *patch* – je dio softvera dizajniran za nadogradnju računalnih programa, operativnih sustava s ciljem popravka ili unaprjeđenja funkcionalnosti računalnog programa

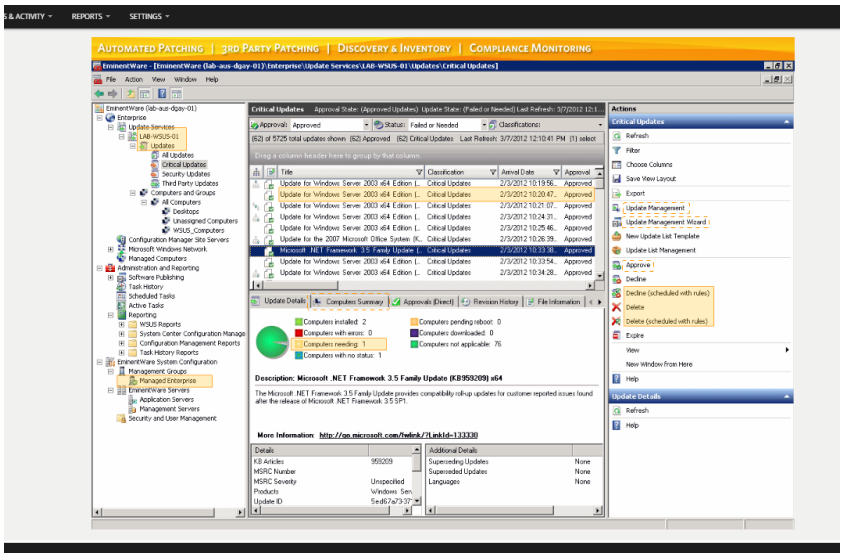
Sljedeće vezano za upravljanje konfiguracijama je prikaz svih konfiguriranih uređaja, gdje se mogu grupirati uređaji po proizvođaču i selektirati svaki pojedino kako bi se moglo upravljati njihovim konfiguracijama. Kao što je prikazano na slici 19. moguće je preuzeti trenutnu konfiguraciju uređaja, odabere se uređaj i preuzme trenutna konfiguracija ili početna konfiguracija. Moguće je još uspoređivati konfiguracije s ostalim čvorištima te učitati konfiguracije, pokrenuti ih, urediti i ažurirati inventar.



Slika 19. Prikaz upravljanja konfiguracijama i popis opreme po proizvođačima

Izvor: [12]

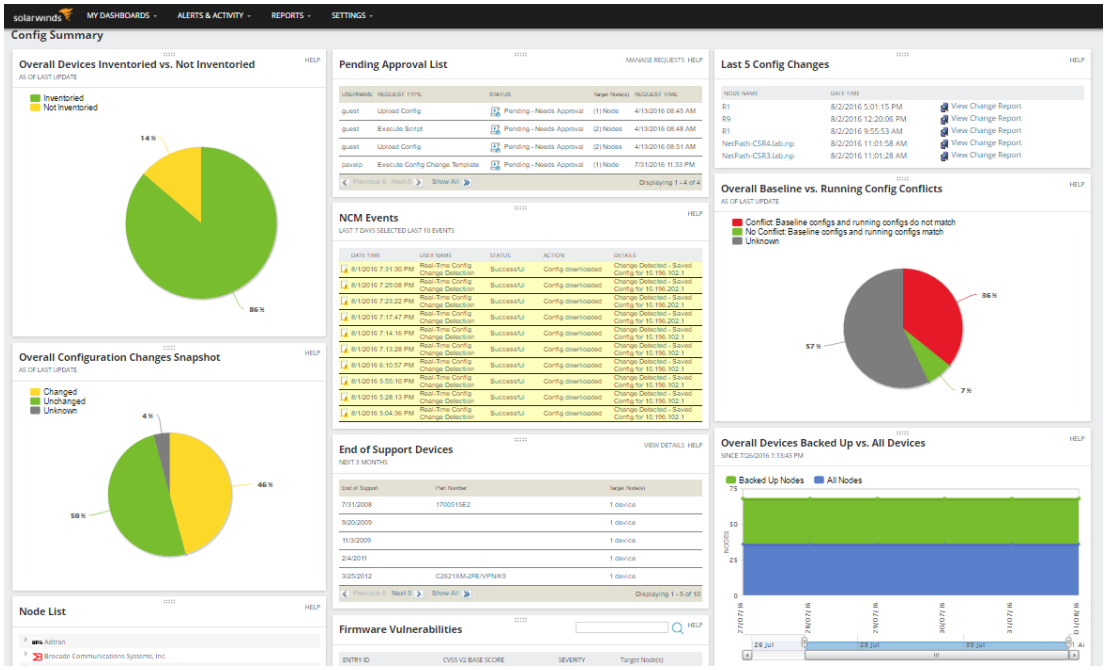
Zadnje vezano za upravljanje konfiguracijama se odnosi na upravljanje *patchevima*, a postoji alat implementiran unutar SolarWinds-a koji omogućava pregled organizacije s grupiranim cjelinama te su izdvojeni uređaji kojima je potrebna kritična nadogradnja sustava, aplikacija, operativnog sustava te drugih alata korištenih u organizaciji. Kao što je prikazano na slici 20. može se vidjeti popis računala kojima je potrebna nadogradnja te je moguće odobriti nadogradnju, odbiti ili izbrisati s liste za nadogradnju. Kako bi sve radilo sinkronizirano, potrebno je sustavno nadograđivanje cjelokupne računalne mreže, a ne samo pojedine komponente mreže. To vodi ka ne sinkroniziranosti mreže i mogućim problemima.



Slika 20. Prikaz alata za upravljanje *patchevima* i vođenja evidencije nadogradnji

Izvor: [17]

Kod nadzora konfiguracija, najbitnije je praćenje promjene konfiguracija i nadogradnja na samim uređajima. Još kada se u 5. poglavlju spominjao nadzor pojedinog uređaja, jedan od nadziranih elemenata je bilo zadnjih pet napravljenih konfiguracija, to je iznimno korisna informacija u slučaju pojave pogreške na uređaju, nedavno nakon promjene konfiguracije. Slika 21. prikazuje sve moguće mjere vezane za nadzor konfiguracijama te je vidljivo kako zaista ima pregledne mjere u obliku grafikona različitih boja, popis konfiguracija koje čekaju odobrenje za izvršenje, zadnjih pet promjena konfiguracija i na kojem čvorištu. Nadalje, popis događaja vezanih za konfiguracije te jesu li uspješno izvedene i kada, s opcijom da se preuzme konfiguracija. Koristan grafikon koji prikazuje koliko je računalna mreža interoperabilna i da li postoji konflikta između trenutno pokrenutih konfiguracija, daje temeljne informacije kako bi se re-konfigurirali pojedini mrežni uređaji i poboljšala kvaliteta mreže. Grafikon dobiven nadzorom koji prikazuje koliko čvorišta ima sigurnosnu kopiju konfiguracije, upozorava na potencijalnu opasnost od gubitka konfiguracija pojedinih uređaja na mreži. Dobiveni podaci nadzorom koji su prikazani na slici 21., govore koliko je kvalitetno obavljeno upravljanje konfiguracijama na računalnoj mreži te ukazuje da je potrebno re-konfigurirati pojedine dijelove mreže ili promijeniti politiku upravljanja konfiguracijama.



Slika 21. Prikaz svih nadzornih elemenata vezanih za konfiguraciju na mreži

Izvor: izradio autor

Vidljivo je da je nadzor, iako nije bio previše opisan u 4.1.2, koristan za upravljanje konfiguracijama. Moguće je u kratkom rok vidjeti promjene napravljene na udaljenim uređajima te preuzeti konfiguracije i vidjeti kakva je interoperabilnost, da li postoji konflikta na pokrenutim konfiguracijama. Naravno da je upravljanje konfiguracijama bitnije od nadzora, jer je nadzor samo jedan dio upravljanja konfiguracijama, ali daje bitne informacije na raspolaganje upravitelju mreže. Upravljanje konfiguracijama bez nadzora je moguće, postave se početne konfiguracije, zabilježi kada je napravljena promjena u notes s nadanjima da će biti funkcionalni s ostatkom mreže. Bez nadzora konfiguracija nije moguće brzo pronaći pogreške, ne vode se bilješke kada su mijenjane konfiguracije kroz program koji objedinjuje sve bilješke, tko je mijenjao, da li postoji konflikta u interoperabilnosti s ostalim uređajima i konfiguracijama. Konkretni rezultati dobiveni kroz upravljanje i nadzor WAN mreže su ti da je potrebno posjedovati bazu za upravljanje konfiguracijama (CMDB), kao što je prikazano na slici 19. CMDB je najbitniji dio upravljanja konfiguracijama, pomoću koje je jednostavno preuzeti trenutne konfiguracije s uređaja i postaviti nove konfiguracije te kroz nadzor pratiti promjene konfiguracija i interoperabilnost novih konfiguracija s ostatkom mreže (slika 21.). Potrebno je također odraditi kvalitetno upravljanje i sustavno nadograđivanje računalne mreže, radi bolje funkcionalnosti i veće pouzdanosti.

6.3 Usporedna analiza sustava za upravljanje i nadzor politike naloga (A)

Mjerenje prometa kojeg stvaraju korisnici mreže (ostvareni promet) je osnovna mjera za upravljanje i nadzor politike naloga. Kod usporedne analize sustava za upravljanje i nadzor politike naloga će se najviše govoriti o prometu, koliko je iskorištenost resursa na pojedinim dijelovima mreže te obratiti pozornost na mjesta gdje je najveća opterećenost prometom i sanirati to optimizacijom prometa. U ovom slučaju prvo će se objasniti nadzor politike naloga, jer se podaci dobiveni mjerenjima kroz nadzor koriste za poboljšanje i optimizaciju iskorištenosti mreže. Potrebno je raspodijeliti resursi, mjeriti količina prometa i na kraju naplata usluge. Kroz SolarWinds je moguće nadzirati sve te mjere i to kroz mrežni protokol NetFlow. Slika 22. prikazuje sve što se može mjeriti nadzorom politike naloga i pokriva sva područja politike naloga. Moguće je postaviti sučelja za nadzor kroz upravljanje resursima te se može vidjeti koliko prometa ulazi u mrežu i koliko prometa izlazi iz mreže, a mjerne jedinice su Mbps, kbps, što znači da se mjeri propusnost. Ovo je iznimno važan podatak, kada se želi mjeriti iskorištavanje pojedinih sučelja na čvorištima ili potrošnja propusnosti koju dodjeljuje pružatelj internet usluge. Jedan od sljedećih grafikona sa slike 22., pokazuje koje aplikacije generiraju najviše prometa (WWW, DNS, SNMP itd.) i prikazuje se u gigabajtima (GB), megabajtima (MB), kilobajtima (kB) kao mjernim jedinicama, dakle ne pokazuje trenutnu generaciju prometa, nego sveukupni promet kroz zadani period promatranja. Također se mogu nadzirati pojedini korisnici unutar mreže te koliko prometa generiraj. Ovo je iznimno bitno za nadzor za analizu korisnika i koji korisnici najviše iskorištavaju resurse mreže, ujedno će se tom korisniku najviše i naplatiti usluga. Sama mreža ne vrši naplatu, nego davatelj usluge, međutim ako netko zlorabi ili iskorištava privilegije kroz organizaciju, moguće je upozoriti i limitirati toga korisnika kroz upravljanje politikom naloga. Kroz SolarWinds je moguće vidjeti koje aplikacije je korisnik zlorabio i upozoriti korisnika te kroz upravljanje, ako je nužno i limitirati mu korištenje usluga, kako ne bi napravio veliku novčanu štetu za organizaciju.



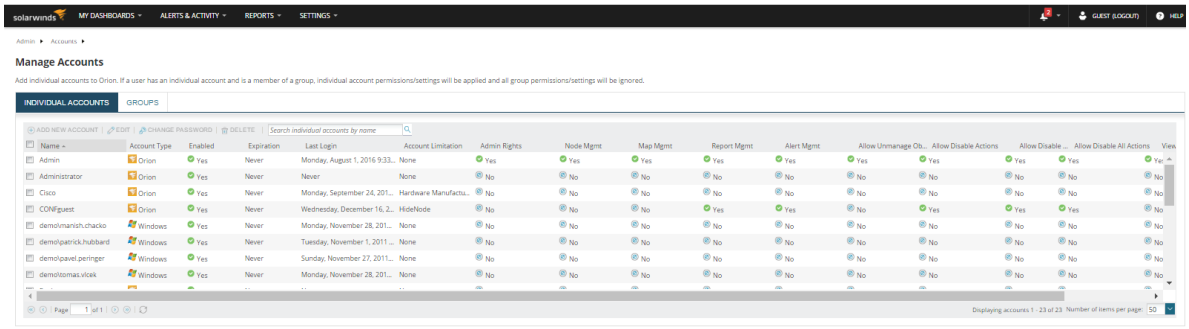
Slika 22. Prikaz grafikona koji prikazuju koliko prometa kreiraju pojedini korisnici, aplikacije, čvorovi

Izvor: izradio autor

SolarWinds nudi i alat za praćenje korisnika koji se prijavljuju na mrežu, zatim da li su njihovi korisnički računi promijenjeni, kao i računi za uređaje. Koliko se korisnika prijavilo udaljenim pristupom, koji se korisnici nisu uspjeli prijaviti itd. Zaista cijeli niz nadzornih mjera je pokriveno i nudi sve informacije za različite potrebe organizacije i prioriteta mrežnih upravitelja. Što se tiče IP SLA, nadziru se operacije od uslužnih servisa i je li sve funkcionalno te vrlo bitno, da li pružatelj usluge poštuju ugovorene stavke.

Nakon nadzora dolazi upravljanje politikom naloga, iako je nadzor spomenut kao bitniji dio, jer mjeri promet i iskorištavanje mreže, radi optimizacije i raspodjele resursa, potrebno je kreirati početne upravljačke funkcije i politiku upravljanja nalozima. Pri tome se u današnje vrijeme koriste standardi za upravljanje politikom naloga na već prije isprobanim računalnim mrežama i to se zove najbolja praksa (engl. *Best practice*). Naravno da najbolja praksa ponekad ne odgovara svim potrebama mreže, jer svaka je mreža različita, tako da se kroz nadzor može dobiti realno stanje na mreži i zatim kroz upravljanje ponovno napraviti revizija raspodjele resursa i kapaciteta, eventualna ograničenja pojedinih korisnika unutar mreže. Prvo će se spomenuti upravljanje korisničkim računima, a SolarWinds nudi i tu opciju kao što je prikazano na slici 23.

Dakle vidljivo je ime korisnika, koja prava su mu odobrena, da li će dobivati ikakve notifikacije i alarme vezane za upravljanje i nadzor, čvorišta. Moguće je i dodati nove korisničke račune, urediti postojeće, promijeniti lozinku i naravno ukloniti korisnički račun.



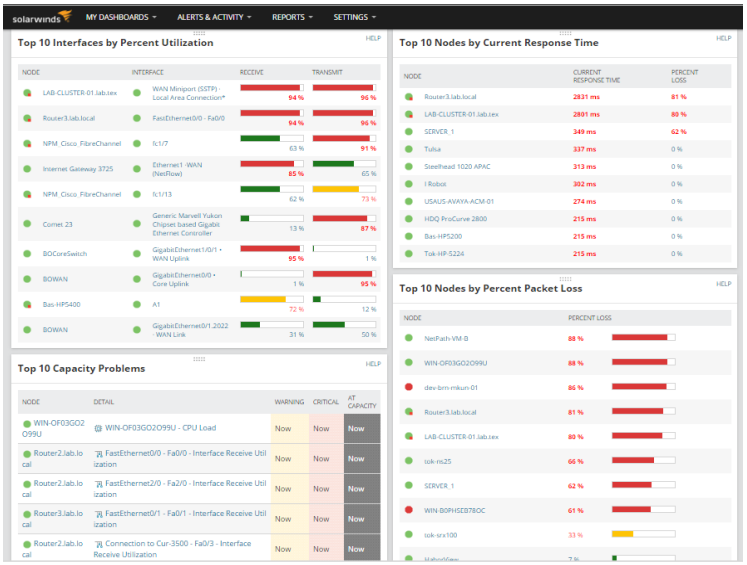
Slika 23. Prikazuje upravljanje korisničkim računima s pravima koje posjeduju

Izvor: [12]

Kod upravljanja je najbitnije mjeriti promet i kolika je opterećenost pojedinih dijelova mreže koji se dobije nadzorom te na temelju tih informacija moguće je odraditi mrežno planiranje i prometno inženjerstvo. Prometno inženjerstvo je praktički nemoguće odraditi bez nadzora, jer je nemoguće predvidjeti kako će se promet informacija odvijati, ne postoji osnovni uzorak. Naravno potrebno je i mjeriti generirani promet kako bi se mogla izvršiti adekvatna naplata i provjeriti da li se naplata podudara s izmjerenim prometom. Rezultati koji se dobiju upravljanjem i nadzorom politike naloga je upravljanje korisničkim računima, kako bi se mogli identificirati objekti na mreži i napraviti analiza korisnika računalne mreže. Koliki promet generiraju pojedini korisnici, kroz koje aplikacije te se temeljem toga mogu adekvatno naplatiti korištene usluge. Zbog toga se nadzire računalna mreža, tj. njeni korisnici kroz alate za nadzor (NetFlow) koji se postave kod krajnjih korisnika. Ti podaci mogu biti od velike važnosti i za upravljanje prometom unutar mreže te spriječiti preveliki protok podataka kroz mrežu.

6.4 Usporedna analiza sustava za upravljanje i nadzor performansi (P) i sigurnosti (S)

Kod performansi osnovne mjere kojima se procjenjuje računalna mreža su propusnost, kašnjenje, pouzdanost i iskorištavanje. Kao što je prikazano na slici 8., gdje se prikazuju mjere performansi po pojedinom čvorištu (uređaju), gdje je moguće očitati prosječno vrijeme odaziva, gubitak paketa, kašnjenje paketa, iskorištenje kapaciteta računalnih mreža i naravno zdravlje opreme (prosječno opterećenje procesora, memorije, funkcionalnost ventilatora itd.) i statistika koliko o dostupnosti čvora (uređaj). Prvo će se objasniti nadzor performansi sustava, zato što su podaci dobiveni nadzorom iznimno bitniji za upravljanje računalne mreže. Nakon što se odradi početno upravljanje i konfiguriranje mreže, potrebno je nadzirati mrežu za dobivanje podataka o performansama računalnih mreža. Upravljanje performansama mreže je nezamislivo bez nadzora i prikupljanja statističkih podataka o interakciji terminalnih uređaja na i van računalne mreže. Svaki pojedini čvor ima svoje mjere vezane za performanse koje se nadziru, kao što je prikazano na slici 8. Dakle kroz nadzor se dobiju statistički podaci o performansama čvorova i zatim bilježe, a SolarWinds zatim daje mogućnost pregleda „top 10“ čvorova na mreži po kritičnosti, tj. lošijim performansama za svaku mjernu performansu prije spomenutu. Slika 24. prikazuje tu statistiku performansi i daje jednostavan i brz prikaz čvorova i sučelja koji imaju poteškoća s performansama. Ovim putem je moguće proaktivno reagirati i vidjeti kroz upravljanje gdje je problem te ga sanirati prije nego li dođe do ozbiljnih problema unutar mreže.



Slika 24. Prikaz „top 10“ mjernih performansi na uređajima i sučeljima

Izvor: izradio autor

Nakon što se statistički podaci prikupe, moguće se njima služiti za ocjenjivanje kvalitete računalnih mreža, kvaliteta iskustva od strane korisnika tih mreža te podaci o performansama mreže s ciljem poboljšanja upravljanja računalnih mreža. Mjerenjem mrežnih performansi se potiče reaktivna usluga, dakle dobiveni podaci iz nadzora se proučavaju i ako su negativni dobiveni podaci, onda se vrši postupak ispravljanja. To je zadatak upravljanja performansama računalne mreže, međutim ubacivanjem kvalitete usluge za nadzor, moguće je i proaktivno djelovati. Da bi se postigla proaktivna usluga potrebno je nadzirati gubitak paketa, kašnjenje i *jitter*. Bitno je kod upravljanja postaviti da se izvlačenje podatak s uređaja putem SNMP *trapova* ne vrši stalno, zbog prevelikog iskorištavanja mrežnih kapaciteta (memorije, procesorske snage, mjesta na tvrdim diskovima[33]). Dakle potrebno je kroz nadzor ustvrditi performanse računalnih mreža, kompatibilnost uređaja na njoj, koliko je kašnjenje, gubitak paketa, vrijeme odaziva, zdravlje opreme i zatim napraviti dodatno upravljanje performansama na mreži i po potrebi napraviti analizu prometa i rekonstruirati samu mrežu ili zamijeniti pojedinu opremu, kako bi se poboljšao rad računalne mreže [5].

Konkretni rezultati dobiveni usporednom analizu su ti da je prvo potrebno postaviti parametre performansi koji će kroz nadzor prikazivati pojedine performanse uređaja i sveukupne performanse mreže. Te mjere su: kašnjenje, gubitak paketa, vrijeme obilaska paketa, dostupnost, kapacitete koje posjeduje mreža, propusnost (tablica 1.) i omogućava proaktivne usluge (primjer, kapaciteti mreže se popunjavaju, tako da je potrebno napraviti ekspanziju mreže, dodatni tvrdi diskovi, brisanje nepotrebnih podataka, itd.).

Zadnje područje gdje će se napraviti usporedna analiza između upravljanja i nadzora računalne mreže je sigurnost. Ovo područje se u današnje vrijeme sve više aktualizira i pridonosi joj se velika pozornost. Kod sigurnosti je prvo potrebno postaviti politiku upravljanja prometom za odnos jedne zasebne računalne mreže (primjer računalna mreža poduzeća) prema ostalim mrežama, tj. Internetu. Najbitniji dio zaštite računalne mreže je u obliku vatrozida (neovisno da li je to specijalizirani uređaj sa računalnim programom ili samo računalni program na operativnom sustavu) koji je postao neizostavan dio računalnih mreža. Vatrozid vrši dubinsku analizu svakoga paketa koji se šalje iz mreže i koji dolazi na mrežu. Potrebno je kroz politiku upravljanja odrediti koji promet će se dozvoliti, koje internetske stranice neće biti dostupne korisnicima te koja je procedura za izmjenu sigurnosnih postavki. Svaki terminalni uređaj mora imati svoj vatrozid u obliku računalnog programa. Potrebno je napomenuti kako SolarWinds ne nudi najbolje rješenje upravljanja sigurnošću, već se u praksi za veću sigurnost koristi vatrozid i njegov softver. Kako bi se postavile karakteristike selektiranja prometa i koja razina sigurnosti, koristi se računalni program od proizvođača vatrozida. Kroz taj softver je moguće podesiti sve vezano za zaštitu mreže i da se slaže za politikom upravljanja.

[33] tvrdi disk - sekundarna je jedinica za pohranu podataka u računalima.

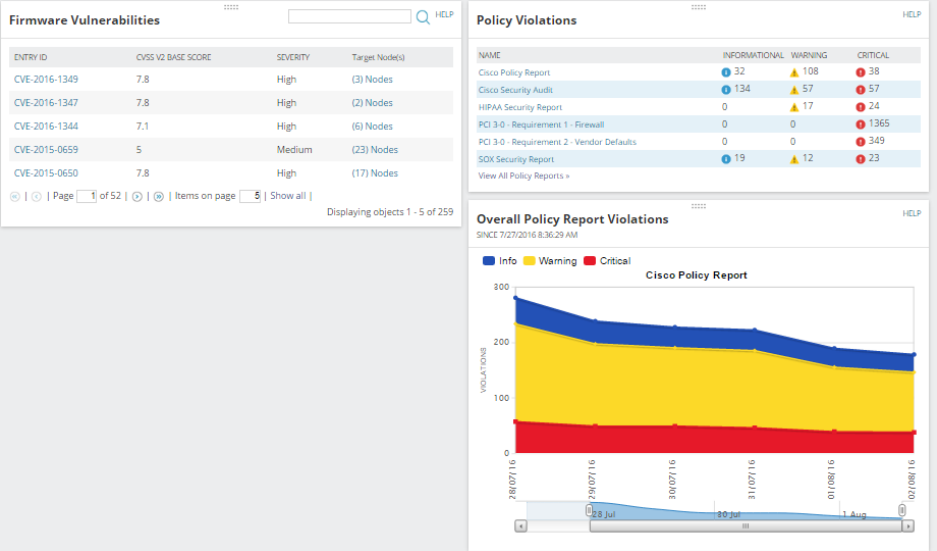
Primjer jednog takvog podešavanja upravljanja prometa putem vatrozida je prikazano na slici 25.



Slika 25. Prikaz softvera Fortinet vatrozida i njegovih postavka za upravljanje sigurnosti

Izvor: [16]

Nakon što se postavi politika upravljanja sigurnošću i prometom, dolazi na red nadzor sigurnosti. Što se tiče nadzora sigurnosti, SolarWinds nudi rješenja u obliku grafova s interaktivnim podataka koji prikazuje gdje se dogodilo kršenje politike upravljanja sigurnošću. Na slici 26. je moguće vidjeti tri primjera gdje se mjeri i nadzire kršenje načela, tj. politike upravljanja, kao i ranjivosti pojedinih softvera na uređajima. Na grafikonu je za primjer odabran proizvođač Cisco i njegovi mrežni uređaji te je vidljivo koliko je pridošlo poruka (informativnih, upozorenja i kritičnih) od strane tih terminalnih uređaja. U ostalim tablicama su prikazane poruke od strane drugih uređaja, vatrozida te koji su softveri na terminalnim uređajima ranjivi na napade.



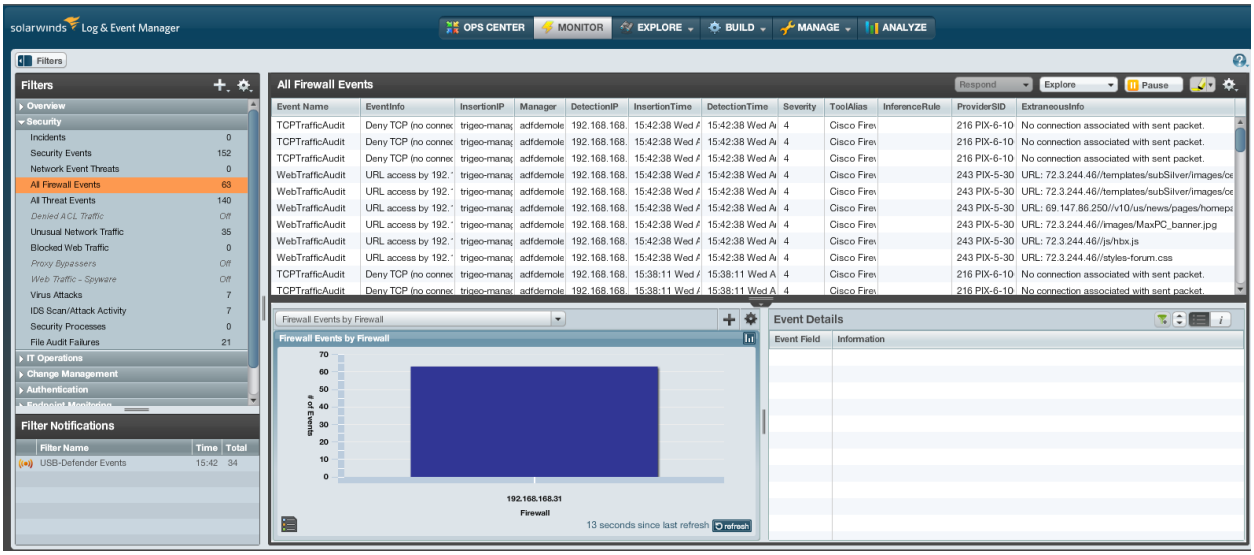
Slika 26. Prikaz prijava o kršenju politike upravljanja i ranjivosti softvera

Izvor: izradio autor

Dodatni alat SolarWinds-a koji nudi detaljniju analizu prometa koji prolazi kroz vatrozid, ali ne samo kroz vatrozid, nego i promet unutar mreže koji je sumnjiv. Ima prikaz incidenata koji su se dogodili na mreži, sigurnosnih događaja vezanih za mrežu te sigurnosni događaji na vatrozidu, neobičan promet, blokirani *web* promet, pa čak i prikazuje napade na mrežu. Napadi u obliku virusa (najpoznatiji je trojanaca[34]) se također bilježe sa svim detaljima kada se dogodio napad, gdje i preko kojeg alata. Sve ove funkcionalnosti se mogu vidjeti na slici 27. Konkretni rezultati dobiveni upravljanjem i nadzorom sigurnosti su upravljanje i postavljanje vatrozida i njegovih funkcionalnosti kao osnova sigurnosti računalnih mreža. Politikom upravljanja je potrebno odrediti kako filtrirati promet, tj. pakete na nepoželjne i odgovarajuće za računalnu mrežu, kao što je prikazano na slici (25.). Nakon što su se definirali početni parametri sigurnosti, nadzire se mreža i kroz alate prati koji uređaji, korisnici se ne pridržavaju tih parametra (slika 27.). Prvo su se postavili parametri, zatim nadzor i upravljanje dobivenih podataka nadzorom, to se odnosi na prikupljanje podataka i njihovo bilježenje te otklanjanje sigurnosnih poteškoća od strane uređaja ili korisnika. To se postiže trenutnim blokiranjem korisnika ili uređaja i zatim se vrši analiza da li je odgovorni korisnik namjerno ili nenamjerno (kroz nepoćudne poruke, web stranice, aplikacije) oštetio računalnu mrežu. Uređaj koji je

[34] trojanac - je maliciozni je računalni program koji se koristi da bi inficirao ciljani sustav terminalnih uređaja i uzrokovao na njemu zlonamjerne aktivnosti. Obično se takvi programi koriste za krađu osobnih podataka, širenje drugih virusa ili jednostavno remećenje performansi terminalnih uređaja

sigurnosno eksponiran potrebno je ponovno konfigurirati, a ako niti to ne pomaže, potrebno ga je zamijeniti.



Slika 27. Prikaz dodatnog SolarWinds alata za praćenje događaja vezanih za sigurnost mreže

Izvor: [14]

Tablica 3. prikazuje koja je razlika između upravljanja i nadzora, što omogućava nadzor, a što upravljanje, po akcijama bitnim za računalne mreže. S obzirom da je upravljanje neizostavni dio svake mreže, barem kroz početne konfiguracije, smatra se da upravljanje mreže mora postojati. Naravno kako bi se obavilo kvalitetno upravljanje, potreban je sustav za upravljanje u obliku računalnog programa, a kroz te računalne programe se implementiraju i alati za nadzor, koji računalne mreže čine sustavom za upravljanje i nadzor računalnih mreža.

Tablica 3. Usporedna analiza upravljanja i nadzora računalne mreže

Područje FCAPS modela	Akcije	Upravljanje računalne mreže	Nadzor računalne mreže
Pogreške (F)	Postavljanje i selekcija bitnih alarma	+	-
Pogreške (F)	Vođenje bilješka o alarmima, događajima	+	-
Pogreške (F)	Alarm je aktiviran (uređaj je prestao raditi)	-	+
Pogreške (F)	Izvor pogreške	-	+
Pogreške (F)	Saniranje pogreške	+	-

Konfiguracije (C)	Prijavljivanje problema (*ticket*)	+	-
Konfiguracije (C)	Prikaz svih konfiguriranih uređaja	+	-
Konfiguracije (C)	Učitati konfiguracije, preuzeti ih, pokrenuti ih, urediti i ažurirati inventar	+	-
Konfiguracije (C)	Nadogradnja sustava, aplikacija, operativnog sustava	+	-
Konfiguracije (C)	Praćenje promjena konfiguracija	-	+
Konfiguracije (C)	Konflikti između trenutno pokrenutih konfiguracija	-	+
Konfiguracije (C)	Koliko čvorišta ima sigurnosnu kopiju konfiguracije	-	+
Politika naloga (A)	Koliko prometa ulazi i izlazi iz mreže	-	+
Politika naloga (A)	Iskorištavanje pojedinih sučelja na čvorištima ili potrošnja propusnosti	-	+
Politika naloga (A)	Praćenje korisnika koji se prijavljuju na mrežu (uspješno, neuspješno), promjene korisničkih računa	-	+
Politika naloga (A)	Koliko prometa generiraju pojedine aplikacije i pojedini korisnici	-	+
Politika naloga (A)	Ograničenja pojedinih korisnika	+	-
Politika naloga (A)	Upravljanje korisničkim računima (AAA) i njihova prava	+	-
Politika naloga (A)	Mrežno planiranje i prometno inženjerstvo	+	-
Performanse (C)	Prikaz iskorištenosti sučelja	-	+
Performanse (C)	Koliko je odaziv, gubitak paketa, kapacitet mreže, kašnjenje	-	+

Performanse (C)	Trenutna opterećenost procesora i memorije	-	+
Performanse (C)	Proaktivne akcije	+	-
Performanse (C)	Prometna analiza, rekonstrukcija mreže, planiranje raspodjele kapaciteta	+	-
Performanse (C)	Briga oko kvalitete usluge (QoS) i kvalitete iskustva (QoE)	+	-
Sigurnost (S)	Koji promet će se dozvoliti	+	-
Sigurnost (S)	Procedura za izmjenu sigurnosnih postavki	+	-
Sigurnost (S)	Prikaz sigurnosnih incidenata koji su se dogodili na mreži	-	+
Sigurnost (S)	Prikaz napada na mrežu	-	+
Sigurnost (S)	Neobičan promet, blokirani web promet	-	+

Izvor: izradio autor

Ovime je završena usporedna analiza i zadnjeg područja FCAPS modela, gdje se vidi kako upravljanje i nadzor funkcioniraju simultano i jedno bez drugoga se u praksi ne implementiraju. Moguće je provesti samo upravljanje, bez nadzora, konfiguracijom opreme prema politici upravljanja, ali to bi u kratkom roku dovelo do kolapsa mreže i ne bi se znali izvori kvarova (zašto postoje problemi na mreži, da li je itko neovlašten pristupio mreži i otuđio podatke te brojne druge stavke koje su objašnjene, a dobivaju se nadzorom računalne mreže). Tablica 3. prikazuje koliko su upravljanje i nadzor računalnih mreža međusobno povezani, s različitim funkcijama, ali pridonose jedno drugome za kvalitetniji rad računalnih mreža.

7. Zaključak

Sustavi za upravljanje i nadzor računalnih mreža predstavljaju okosnicu svih kvalitetnih računalnih mreža. Bez kvalitetnog sustava za upravljanje i nadzor računalnih mreža i organizacija koje se profesionalno bave upravljanjem i nadzorom računalnih mreža, pouzdanost i dostupnost računalnih mreža ne bi bila zagarantirana. Sve je veći broj računalnih mreža kojima je u cilju biti dostupne korisnicima i zahtijevaju određenu kvalitetu usluge te zbog tih zahtjeva, sustavi za upravljanje i nadzor računalnih mreža imaju veliku ulogu kod računalnih mreža. Završni rad se može podijeliti na dva dijela. Prvi dio rada je teoretski i koncentriran je na upoznavanje s računalnom mrežnom i njenih značajki. To obuhvaća mrežni hardver (PAN, LAN, MAN i WAN računalne mreže) gdje se karakteriziraju računalne mreže po njihovom opsegu. Nakon mrežnog hardvera se predstavlja mrežni softver, koji opisuje načine unaprjeđenja mrežnog hardvera kroz softverska rješenja. To se postiže protokolnom hijerarhijom koja točno definira pojedine slojeve referentnih modela i načine komuniciranja između slojeva. Kod mrežnog softvera je bitno i dizajniranje slojeva, a najbitnija pitanja koja se postavljaju kod dizajniranja slojeva su pouzdanost mreže i mehanizmi koji to garantiraju, zatim pronalazak valjanog puta za podatke koji putuju kroz mrežu. Sljedeće pitanje dizajna je raspodjela resursa unutar mreže i mehanizmi kojima se to postiže i zadnje je pitanje sigurnosti, a mehanizmi koji osiguravaju sigurnost su povjerljivost, cjelovitost i dostupnost. Referentni modeli su zadnji koji će se objasniti pod značajkama računalne mreže. Dva modela koja se koriste kod računalnih mreža su referentni model OSI i model TCP/IP.

Nakon postavljenih temelja za završni rad, obrađuje se upravljanje i nadzor računalnom mrežom. Za upravljanje računalnim mrežama predstavio se model FCAPS, kao politika za upravljanje računalnih mreža. Prvo su se predstavili osnovni protokoli za upravljanje računalnim mrežama (ICMP i SNMP), radi jednostavnijeg razumijevanja daljnjeg sadržaja. Nakon osnovnih protokola se predstavlja model politike upravljanja, tj. FCAPS model i detaljno se objašnjavaju sva njegova područja. Nakon detaljnog opisa FCAPS modela kod upravljanja, isti taj model se detaljno objašnjava s aspekta nadzora računalne mreže. Osim toga kod nadzora računalne mreže se govori o nadzoru pojedine mreže (najčešći način nadzora) i nadzora Interneta kao mreže svih mreža. Za kraj se opisuju dodatne tehnike i protokoli koji su neizostavni dio nadzora računalnih mreža, neki od njih su *telnet*, *syslog* i *log*.

Detaljnim opisima upravljanja i nadzora računalne mreže, moguće je opisati jedan takav sustav kroz računalni program za upravljanje i nadzor računalnih mreža. U funkciji završnog rada koristio se računalni program SolarWinds te su se predstavile njegove funkcionalnosti i analizirala sva područja FCAPS modela.

Drugi dio završnoga rada se bazira na praktičnoj primjeni obrađene teorije kroz završni rad. Cilj i tematika završnog rada je provesti usporednu analizu sustava za upravljanje i nadzor računalnih mreža kroz alate za upravljanje i nadzor računalne mreže. Kako bi se došlo do toga cilja, analizirao se cijeli FCAPS model i sva njegova područja na temelju jednog računalnog programa za upravljanje i nadzor računalne mreže, SolarWinds. Usporedna analiza se provela na WAN računalnoj mreži i time stekla znanja kako upravljati i nadzirati računalnu mrežu velikog opsega, kao i razlike između upravljanja i nadzora te kakva je problematika upravljanja i nadzora WAN mreže (upravljanje i nadzor drugih vrsta računalnih mreža nema velikih razlika, WAN je najveća među njima). Vidljivo je iz završnog rada, što je sve potrebno nadzirati na WAN mreži da bi se dobili bitni mjerljivi podaci kojima je svrha poboljšanje rada i kvalitete računalne mreže kroz upravljanje. Kvalitetna računalna mreža je pouzdana s rijetkim pogreškama, posjeduje potrebne mrežne performanse, dostupna 99 % vremena, sigurna i posjeduje kapacitete za razvoj (skalabilnost). Kod izrade završnoga rada, postavljene su granice promatranja za definiranje svih bitnih stavki za postizanje cilja, bez dubljih analiza pojedinih područja FCAPS modela. Promatrano područje je toliko opširno da njihova analiza prelazi opseg i veličinu završnog rada.

Usporedna analiza je bitna jer segmentira upravljanje i nadzor računalnih mreža na dvije odvojene cjeline te analizira njihovu povezanost i razlike. Provedenom usporednom analizom moguće je dobiti znanja korisna za organizaciju zaduženja unutar računalne mreže (na osoblje koje će se baviti upravljanjem i/ili nadzorom). Također što se tiče kvalitetnih alata za upravljanje i nadzor računalnih mreža, potrebno je posjedovati pristup većoj računalnoj mreži ili većem broju mrežnih računala za kvalitetnu i opsežnu usporednu analizu. SolarWinds je kao i ostali kvalitetni računalni programi iznimno teško podesiti (konfigurirati) na terminalnim uređajima slabijih performansi te su ograničene funkcije i nije moguće iskoristiti njegov puni potencijal, bez komercijalne verzije SolarWinds-a. Nedavno je kreiran interaktivni program za testiranje SolarWinds-a (demo verzija), s kvalitetnom WAN mrežom i podacima u stvarnom vremenu. Nažalost, također korištenjem demo verzije nije moguće postići puni potencijal programa, naime limitirane su njegove dodatne funkcije te je za to potrebno imati licencirani računalni program SolarWinds za detaljniju usporednu analizu upravljanja i nadzora računalnih mreža.

Literatura

[1] Tanenbaum, A., Wetherall, D.: *Computer Networks 5th edition*, Pearson, Boston, SAD; 2010. (kolovoz 2016.)

[2] Foroughi, A.: *Network Management, Chapter 20*, University of Southern Indiana, Indiana, USA; 2008., internetski izvor: http://www.usi.edu/business/aforough/Chapter%2020.pdf (kolovoz 2016.)

[3] Nacionalni CERT: SNMP protokol, Zagreb, Hrvatska; 2010.

internetski izvor: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-09-313.pdf

(kolovoz 2016.)

[4] Kurose, J.F., Ross, K.W.: *Computer Networking: A Top-Down Approach*, *6th edition*, Pearson, New Jersey, USA; 2012. (kolovoz 2016.)

[5] Bakhshi, B.: *FCAPS Network Management*, Amirkabir University of Technology, Iran; 2015., internetski izvor: http://slideplayer.com/slide/4870460/ (kolovoz 2016.)

[6] Wong, E.: *Network Monitoring Fundamentals and Standards*, Washington University in St. Louis, USA; 1997., internetski izvor: www.cse.wustl.edu/~jain/cis788-97/ftp/net_monitoring.pdf (kolovoz 2016.)

[7] Clemm, A.: *Network Management Fundamentals.* Indianapolis, USA, Cisco Press; 2006., internetski izvor: http://sirpabs.ilahas.com/ebooks/Computer%20&%20Technology/Cisco.Press.Network.Management.Fundamentals.Nov.2006.pdf (kolovoz 2016.)

[8] Cisco Systems: *Traffic Accounting Scenarios*, USA, 2004.,

internetski izvor: http://www.cisco.com/networkers/nw04/presos/docs/NMS-2031.pdf (kolovoz 2016.)

[9] Moceri, P.: *SNMP and Beyond: A Survey of Network Performance Monitoring Tools*, Washington University in St. Louis, USA; 2006.,

internetski izvor: http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors2.pdf (kolovoz 2016.)

[10] Adato, L.: *Monitoring 101.*,

internetski izvor: https://thwack.solarwinds.com/servlet/JiveServlet/previewBody/187523-102-2-28123/1510_SWI_monitoring-101-eBook_20151211.pdf (kolovoz 2016.)

[11] Brad Hale.: *Network Management – Back to the Basics*.,

internetski izvor: http://web.swcdn.net/creative/pdf/Whitepapers/Network_Management_-_Back_to_the_Basics.pdf (kolovoz 2016.)

[12] Interaktivni računalni program:

http://oriondemo.solarwinds.com/Orion/SummaryView.aspx?ViewID=119 (kolovoz 2016.)

[13] Jackson J., Guzman, G. - *Operations Management and Open Source Tools*., internetski izvor: https://www.mcnc.org/sites/default/files/MCNC-Operations-Management-Using-Open-Source-Tools.pdf (kolovoz 2016.)

[14] Interaktivni računalni program: http://lem.demo.solarwinds.com/lem/index.jsp (kolovoz 2016.)

[15] Slika na internetu: http://www.solarwinds.com/help-desk-software (kolovoz 2016.)

[16] Fortinet - *FortiOS Handbook - Security Profiles for FortiOS 5.0*.,

internetski izvor: http://docs.fortinet.com/uploaded/files/1082/fortigate-security_profiles-50.pdf (kolovoz 2016.)

[17] Interaktivni računalni program:

http://oriondemo.solarwinds.com/Orion/External.aspx?Title=SolarWinds%20Orion%20Demo&URL=http://demo.solarwinds.com/flashdemo/spm/orion-demo-embedded.aspx (kolovoz 2016.)

Popis kratica i akronima

Kratica	Značenje kratice
AAA	*Authentication, Authorization and Accounting* Autentifikaciju, autorizaciju i politiku naloga pojedinih
ARPANET	*Advanced Research Projects Agency Network* Prva računalna mreža na svijetu
ASCII	*American Standard Code for Information Interchange* Američki standardni znakovnik za razmjenu obavijesti
ASN.1	*Abstract Syntax Notation One* Standard apstraktnih zapisa
BGP	*Border Gateway Protocol* Protokol za razmjenu podataka usmjernika
CMDB	*Configuration Management Database* Baza za upravljanje konfiguracijama
DDOS	*Distributed Denial of service* Distribuirano uskraćivanje usluge
DLP	*Data leakage/Loss protection/Prevention* Sustav za prevenciju curenja podataka i zaštitu od gubitka podataka
DNS	*Domain Name System* Protokol za davanje imena mrežnim adresama
DOS	*Denial of service* Uskraćivanje usluge
FCAPS	*Fault, Configuration, Accounting, Performance, Security management/monitoring* Model za upravljanje i nadzor računalne mreže
FTP	*File transfer protocol* Protokol za prijenos podataka

HTTP	*HyperText Transfer Protocol* Protokol za prijenosa informacija na Webu
ICMP	*Internet Control Message Protocol* komunikacijski protokol koji kontrolira poruke
IEEE	*Institute of Electrical and Electronics Engineers* Institut udruženja elektrotehničara za definiranje standarda
IPS	*Intrusion Prevention System* Sustav za prevenciju napada
ISO	*International Standards Organization* Međunarodna organizacija za normizaciju
ISP	*Internet Service Provider* Pružatelj Internet usluga
LAN	*Local Area Networks* Lokalna računalna mreža
MAC	*Media Acces Control* Pristupni protokol za utvrđivanje pristup fizičkom mediju
MAN	*Metropolitan Area Network* Mreža na području grada
MIB	*Management Information Base* Baza upravljačkih informacija
OSI	*Open Systems Interconnection* Referentni model za otvoreno povezivanje sustava
P2p	*point-to-point* Veza između dva krajnja uređaja
PAN	*Personal Area Networks* Mreža uskim područjem spajanja
QoE	*Quality of Experience* Kvaliteta iskustva korisnika
QoS	*Quality of Service* Kvaliteta usluge

RMON	*Remote monitoring* Protokol za nadzor udaljenih uređaja
RTP	*Real-time Transport Protocol* Protokol za dostavu medija u stvarnom vremenu
RTT	*Round-trip time* Vrijeme obilaska
SLA	*Service Level Agreement* Ugovorne usluge kroz ugovor
SMI	*Structure of Management Information* Standard za izgradnju MIB baze se zove
SMON	*Switched network monitoring* Nadzor preklopničke mreže
SMTP	*Simple Mail Transfer Protocol* Protokol za elektroničku poštu
SNMP	*Simple Network Management Protocol* Jednostavni mrežni protokol za nadzor i upravljanje
SONET	*Synchronous Optical Networking* Sinkrone optičke mreže
SSH	*Secure Shell* Protokol za pristup udaljenom računalu
TCP/IP	*Transmission Control Protocol/Internet Protocol* Model za otvoreno povezivanje sustava, baziran na TCP i IP protokolu
Telnet	*TELephone NETwork* Protokol za upravljanje uređaja na daljinu
VLAN	*Virtual Local Area Network* Virtualna lokalna mreža
VPN	*Virtual Private Network* Virtualna privatna mreža
VoIP	*Voice over Internet Protocol* prijenos zvuka preko Internet protokola

UDP	*User Datagram Protocol* Bespojni protokol prijenosne razine, baziran na *datagramima*
WAN	*Wide Area network* Široko područna mreža
WiMAX	*Worldwide Interoperability for Microwave Access* Svjetska interoperabilnost za mikrovalni pristup
WWW	*World Wide Web* ili kratko Web je mreža svih mreža

Popis slika

Slika 1. Prikazuje vrste mreže po opsegu 4
Slika 2. Prikaz žičane LAN mreže s preklopnikom 6
Slika 3. Prikaz načina rada MAN mreže 8
Slika 4. Rezultati *ping* testiranja 17
Slika 5. Sustav za upravljanje mrežom 19
Slika 6. Primjer mogućih kvarova vezanih za pregrijavanje uređaja 21
Slika 7. Prikaz proizvođača i njihove opreme u mreži 42
Slika 8. Prikaz podataka i dobivenih mjera nadzorom uređaja 43
Slika 9. Prikazuje sve alarme pridošle od strane objekata 44
Slika 10. Prikazani sažetak događaja 45
Slika 11. Sažeti prikaz nadzora mreže po različitim područjima FCAPS modela 46
Slika 12. Prikaz svih glavnih postavki unutar računalnog programa SolarWinds 47
Slika 13. Prikazuje sučelje za praćenje svih događaja na mreži i nadzor krajnjih korisnika 49
Slika 14. Centar za poruke s opcijama za filtriranje 50
Slika 15. Prikaz alarma te što se njima prati i koji su odabrani za praćenje 50
Slika 16. Grafički prikaz dijagnoze gdje je nastala pogreška 51
Slika 17. Prikaz alata za detaljno upravljanje *ticketima* 52
Slika 18. Prikazuje opcije vezane za upravljanje otkrivanjem mreže 53
Slika 19. Prikaz upravljanja konfiguracijama i popis opreme po proizvođačima 54
Slika 20. Prikaz alata za upravljanje *patchevima* i vođenja evidencije nadogradnji 55
Slika 21. Prikaz svih nadzornih elemenata vezanih za konfiguraciju na mreži 56
Slika 22. Prikaz grafikona koji prikazuju koliko prometa kreiraju pojedini korisnici, aplikacije, čvorovi 58
Slika 23. Prikazuje upravljanje korisničkim računima s pravima koje posjeduju 59
Slika 24. Prikaz „top 10“ mjernih performansi na uređajima i sučeljima 60
Slika 25. Prikaz softvera Fortinet vatrozida i njegovih postavka za upravljanje sigurnosti 62
Slika 26. Prikaz prijava o kršenju politike upravljanja i ranjivosti softvera 63
Slika 27. Prikaz dodatnog SolarWinds alata za praćenje događaja vezanih za sigurnost mreže 64

Popis tablica

Tablica 1. Pokazuje koje su najbitnije mjere vezane za nadzor performansi s klasifikacijom i njihovim opisom 35
Tablica 2. Definira RMON ciljeve i njihova objašnjenja 37
Tablica 3. Usporedna analiza upravljanja i nadzora računalne mreže 64

METAPODACI

Naslov rada: Usporedna analiza sustava za upravljanje i nadzor računalnih mreža

Student: Valentino Vizner

Mentor: doc. dr. sc. Ivan Grgurević

Naslov na drugom jeziku (engleski): Comparative Analysis of Management and Monitoring Systems of Computer Networks

Povjerenstvo za obranu:

- Prof. dr. sc. Zvonko Kavran predsjednik
- Doc. dr. sc. Ivan Grgurević mentor
- Dr. sc. Ivan Forenbacher član
- Izv. prof. dr. sc. Dragan Peraković zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: Informacijsko komunikacijski promet

Vrsta studija: Preddiplomski

Studij: Promet

Datum obrane završnog rada: 13. rujna 2016.