Tehnike za nadzor i analizu mrežnog prometa

Dodig, Ana

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Ana Dodig

TEHNIKE ZA NADZOR I ANALIZU MREŽNOG PROMETA

ZAVRŠNI RAD

Zagreb, 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 10. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Tehnologija telekomunikacijskog prometa I**

ZAVRŠNI ZADATAK br. 6519

Pristupnik: **Ana Dodig (0135241413)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Tehnike za nadzor i analizu mrežnog prometa**

Opis zadatka:

Objasniti ulogu i značaj nadzora i analize mrežnog prometa u komunikacijskim mrežama. Analizirati tehnike za nadzor i analizu mrežnog prometa bazirane na ruteru.
Prikazati značajke aktivnih, pasivnih i kombiniranih tehnika za nadzor i analizu prometa te analizirati njihove prednosti i nedostatke.

Mentor:

Š. Mrvelj

prof. dr. sc. Štefica Mrvelj

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

TEHNIKE ZA NADZOR I ANALIZU MREŽNOG PROMETA

NETWORK TRAFFIC MONITORING AND ANALYSIS TECHNIQUES

ZAVRŠNI RAD

Mentorica: prof. dr. sc. Štefica Mrvelj

Studentica: Ana Dodig

JMBAG: 0135241413

Zagreb, rujan 2021

SAŽETAK

Mrežni promet se odnosi na ukupnu količinu mrežnih paketa koji prolaze kroz računalnu mrežu. Sama analiza mrežnog prometa je postupak kojim se mrežni paketi presreću i podliježu analizi. Pod presretanjem paketa misli se na čitanje paketa putem aplikacije kojoj paket nije originalno namijenjen. Nadzor mrežnog prometa je temelj rada mrežnih administratora koji vode brigu o tome da sustav cijelo vrijeme bude dostupan, ali i kako bi čim brže otklonili problem ukoliko bi se on pojavio. Budući da broj korisnika Interneta izuzetno brzo raste dolazi do preopterećenosti mreže. Kako bi se to spriječilo nužno je cijelo vrijeme nadzirati i analizirati mrežni promet te odrediti skup pravila prioriteta prometa za dostupni kapacitet. U ovome radu će se analizirati i objasniti tehnike za nadzor i analizu mrežnog prometa, njihovu ulogu i svrhu služenja prilikom praćenja i analize mrežnog prometa. Koriste se pojedini aktivni, pasivni ili kombinirani alati kako bi takav sustav mogao uspješno funkcionirati.

KLJUČNE RIJEČI: ***nadzor mrežnog prometa, analiza mrežnog prometa, aktivne tehnike za nadzor i analizu mrežnog prometa, pasivne tehnike za nadzor i analizu mrežnog prometa, kombinirane tehnike za nadzor i analizu mrežnog prometa***

SUMMARY

Network Traffic refers to the total amount of network packages that passes through a computer network. The analysis of the network traffic is procedure when network packages are intercepted and subjected to analysis. Package interception refers to reading packages through applications that are not originally for that package. Network traffic monitoring is foundation for the network administrators that take care of system availability and allows them to remove the problem if it appears. Since the number of Internet users is growing really fast network congestion occurs. To prevent that it is important to monitor and analyse network traffic all the time and to set the rules of the traffic priorities for available capacity. In this thesis will be analysed and explained control and analyse techniques for the network traffic, their role and purpose during the tracking and analysing of the network traffic. Active, passive or combined tools are used in order for such a system to work successfully.

KEY WORDS: network traffic monitoring, network traffic analysis, active techniques for network traffic monitoring and analysis, passive techniques for network traffic monitoring and analysis, combined techniques for network traffic monitoring and analysis

SADRŽAJ

1. UVOD

Velika kompliciranost mrežne infrastrukture u korporacijama stavlja sve veći teret na mrežne administratore koji se o njoj brinu. U takvim korporacijama postoje lokacije gdje je nužno analizirati i nadzirati mrežni promet. Na svakoj lokaciji bi se nalazio jedan uređaj za nadzor mrežnog prometa. Budući da se u mrežama nalaze uređaji različitih proizvođača, jednostavno je nemoguće održavati sustav bez posebnih alata. Mrežni administratori se nalaze pred velikim izazovima kako bi pronašli odgovarajuću aplikaciju koja bi mogla pružiti promptnu i točnu informaciju o stvarnom stanju mreže. Danas su na tržištu dostupni brojni alati koji mogu pomoći administratorima da nadziru i analiziraju mrežni promet. Neki alati su besplatni, a oni od svjetski poznatih kompanija su skuplja rješenja.

Predmet ovog završnog rada su tehnike za nadzor i analizu mrežnog prometa. Cilj ovog rada je objasniti pojam i značenje mrežnog prometa, prikazati i opisati osnovne postupke koji su vezani za nadzor i analizu mrežnog prometa te prikazati i objasniti neke alate za nadzor i analizu mrežnog prometa.

Naziv završnog rada je TEHNIKE ZA NADZOR I ANALIZU MREŽNOG PROMETA i sastoji se od sedam poglavlja:

1. Uvod
2. Uloga i značaj nadzora i analize mrežnog prometa
3. Tehnike za nadzor i analizu mrežnog prometa bazirane na routeru
4. Aktivne i pasivne tehnike za nadzor i analizu prometa
5. Kombinirane tehnike za nadzor i analizu mrežnog prometa
6. Komparativna analiza značajki tehnika za nadzor i analizu prometa u mreži
7. Zaključak.

U drugom dijelu rada govori se općenito o ulozi nadzora i analize mrežnog prometa, što je to nadzor mrežnog prometa, koje su prednosti nadzora i analize mrežnog prometa. Govori se o mrežnim protokolima, a posebno se definiraju tri najbitnija sloja za nadzor mrežnih transakcija, a to su: podatkovni sloj, mrežni sloj i transportni sloj.

U trećem dijelu rada su prikazane tehnike nadzora mrežnog prometa koje su temeljene na usmjerivaču odnosno routeru. Detaljno se objašnjava SNMP protokol – jednostavni mrežni

protokol za upravljanje, Netflow i RMON – nadzor na udaljenoj lokaciji. Predstavljene su njihove prednosti i nedostatci.

U četvrtom dijelu rada definiraju se aktivne i pasivne tehnike za nadzor i analizu prometa te objašnjavaju razlike između te dvije tehnike.

Peto poglavlje objašnjava kombinirane tehnike za nadzor i analizu mrežnog prometa, opisane su tehnike nadgledanje resursa s ruba mreže (WREN) i samokonfigurirajući nadzornik mreže (SCNM).

U šestom dijelu rada je napravljena komparativna analiza značajki tehnika za nadzor i analizu prometa u mreži, definirani su uređaji za nadzor i analizu mrežnog prometa te je prikazano nekoliko trenutno najboljih uređaja za nadzor i analizu mrežnog prometa na tržištu.

2. ULOGA I ZNAČAJ NADZORA I ANALIZE MREŽNOG PROMETA

Mrežni promet je poznat i kao podatkovni promet, a odnosi se na količinu podataka koji se kreću mrežom u određenom trenutku. Mrežni podatci su upakirani u mrežne pakete koji rade dosta veliko opterećenje na mreži. Mrežni promet glavna je sastavnica za mjerenje mrežnog prometa, kontrolu i njegovu simulaciju. Pravilna organizacija mrežnog prometa pomaže u osiguravanju kvalitete usluge u određenoj mreži [1].

Iz količine i vrste mrežnog prometa se mogu doznati informacije o namjeri i korištenju same računalne mreže. Ako se priča o računalnoj sigurnosti, mrežni promet može otkriti dosta informacija o samoj mreži, načinu njezina korištenja ali i podatcima koji se putem nje prenose. Nadzorom i analizom mrežnog prometa moguće je otkriti napade na internetske servise i web aplikacije, napade uskraćivanjem usluga i slično.

Kako bi nadgledanje mrežnog prometa poslužilo za otkrivanje zlonamjernih aktivnosti na računalnoj mreži jako je bitno znati vrstu informacije koja se traži. Takva informacija obično se može uklopiti u uobičajeno funkcioniranje računalne mreže.

Pravilna analiza mrežnog prometa pruža sljedeće prednosti:

- Prepoznavanje mrežnih „uskih grla“ – mogu postojati korisnici i aplikacije koji troše jako velike količine propusnosti.
- Sigurnost mreže – neobična količina prometa u nekoj konekciji može biti znak napada. Izvješća o mrežnom prometu pružaju mogućnost da se takvi napadi na vrijeme spriječe.
- Mrežni inženjering – poznavanje razina upotrebe mreže omogućava analizu budućih zahtjeva.

Nadzor mrežnog prometa odnosi se na aktivnosti povezane s upravljanjem mrežnim prometom i korištenjem propusne širine, a sve to s ciljem sprječavanja „uskih grla“ i neočekivanih skokova prometa. Nadzor mrežnog prometa može pomoći kompanijama da unaprijed predvide razne skokove prometa i identificiraju snopove propusnosti i na taj način im omogućava da spriječe nastanak problema [2]. Analiza mrežnog prometa uključuje analizu trendova prometne komunikacije kako bi se pravovremeno identificirali i otklonili mogući problemi. Analiza prometa omogućava način praćenja aktivnosti i dostupnosti mreže pa kompanije na vrijeme mogu uočiti određene nepravilnosti kao što su operativni ili sigurnosni problemi [2].

Praćenje mrežnog prometa obično uključuje mjerenje načina na koji mrežni promet dolazi do odredišta. Mrežni paketi se presreću i podvrgavaju analizi. Pod presretanjem paketa se misli na čitanje paketa od strane aplikacije kojoj paket nije originalno namijenjen. Uhvaćeni paket se nakon hvatanja primitka i lokalnog zapisivanja prosljeđuje na odredište odnosno mrežni promet se samo snima bez ikakvih izmjena ili blokiranja komunikacije [3].

Mrežnim administratorima svakako trebaju sofisticiraniji alati za nadzor i analizu mrežnog prometa kako bi bili u korak s povećanjem opterećenosti računalne mreže. Nadzor je potreban ne samo kako bi se na vrijeme uspjeli otkloniti mrežni problemi već i da bi se uspjelo pravovremeno spriječiti kvar na mreži, kako bi se otkrile unutarnje i vanjske prijetnje te izabrale dobre odluke vezano za mrežno planiranje [4].

Neke od prednosti praćenja mrežnog prometa su [4]:

- izbjegavanje „uskog grla“
- smanjenje troškova na način da se kupi propusnost prema stvarnom opterećenju mreže
- jednostavno rješavanje mrežnih problema
- mogućnost da se utvrdi koje aplikacije i koji korisnici koriste maksimalnu širinu i drugo.

2.1. MREŽNI PROTOKOLI

Da bi se mrežni promet mogao analizirati nužno je poznavati mrežne protokole i standarde na kojima se bazira računalna mreža koja se planira analizirati. Svi oni podatci koji putuju računalnom mrežom, prenose se u paketima. Svaki taj paket ima svoje zaglavlje gdje se nalaze svi potrebni podatci o tom paketu. Oni uključuju mrežnu adresu polazišta i mrežnu adresu odredišta, polazišni i odredišni mrežni port kao i ostale bitne podatke. Kako bi računalni sustavi mogli neometano međusobno komunicirati, taj sam proces odvijanja komunikacije bi trebao biti unificiran. U tom smislu unificiranja računalnih mreža je kreiran OSI (engl. *Open Systems Interconnection*) referentni model.

On određuje principe koje računalni sustavi moraju pratiti da bi mogli međusobno komunicirati s ostalim računalnim sustavima. OSI model se dijeli na sedam slojeva [5]:

1. Fizički sloj – ovo je najniži sloj koji služi samo za uspostavljanje fizičkog kanala između računalnih sustava koji međusobno komuniciraju

2. Podatkovni sloj – on je taj koji omogućava da se podatci prenose između računalnih sustava koji komuniciraju, zajedno sa kontrolom prijenosa
3. Mrežni sloj – služi kako bi usmjerio i adresirao mrežne pakete
4. Transportni sloj – ovaj sloj omogućava prijenos podataka u mrežnim paketima
5. Sjednički sloj – služi za ostvarivanje i održavanje sjednice između mrežnih aplikacija
6. Prezentacijski sloj – mrežnoj aplikaciji predaje podatke u njoj razumljivom obliku
7. Aplikacijski sloj – odnosi se na samu mrežnu aplikaciju.

Svaki od spomenutih sedam slojeva ima svoju funkciju i namjenu, a svi zajedno omogućavaju standardizirane mreže komunikacije. Za nadzor mrežnih transakcija su najbitnija tri sloja koja će biti detaljnije analizirana, a to su: podatkovni, mrežni i transportni sloj.

2.1.1. Podatkovni sloj

Podatkovni sloj služi kako bi se podatci prenosili između računalnih sustava i kako bi se izvršavala kontrola prijenosa podataka između tih sustava. Na ovom sloju se nalazi i Ethernet protokol. U Ethernet mreži, svako računalo ima svoju 48 bitnu MAC adresu na osnovi koje se podatci usmjeravaju prema pojedinim računalima [5].

Najčešće korišteni protokoli podatkovnog sloja su SLIP i PPP koji će u nastavku detaljnije biti objašnjeni [6].

2.1.1.1.SLIP

SLIP (engl. *Serial Line Internet Protocol*) je jednostavan protokol. Napravljen je za rad preko serijskog porta i veza putem usmjerivača prometa. SLIP nema mogućnost adresirati i razmijeniti informacije o adresama. On može podržavati samo jedan skup protokola koji mora biti istovjetan na obje strane. Ne može obavljati detekciju niti korekciju pogreške. Za takve stvari se SLIP oslanja na protokole gornjeg sloja [7].

2.1.1.2.PPP

PPP (engl. *Point-to-Point Protocol*) je protokol koji omogućava autentikaciju, kompresiju podataka, detekciju greške i balansiranje opterećenja preko više kanala. Sastoji se od dva dijela: protokola za nadzor veze, LCP (engl. *Link Control Protocol*) koji uspostavlja, konfigurira i testira vezu te protokola za nadzor mreže NCP (engl. *Network Control Protocol*) koji dogovara prijenos različitih protokola mrežne razine.

2.1.2. Mrežni sloj

Mrežni sloj prvenstveno služi za prijenos paketa i njihovo usmjeravanje, ali je u principu funkcija ovog mrežnog sloja puno šira i kompleksnija. Mrežni sloj je najniži sloj koji se brine za prijenos podataka s jednog kraja mreže na drugi kraj. Zadatak mrežnog sloja je omogućiti uspostavljanje, održavanje i raskid veza. Najvažnija funkcija je svakako usmjeravanje (engl. *routing*). Algoritmi za usmjeravanje dio su softvera mrežnog sloja i odgovorni su za donošenje odluke o putu kojim se paketi planiraju prenositi. Usmjeravanje obavljaju uređaji koji se zovu usmjernici (engl. *routeri*). Na ovom sloju je svakako najpopularniji protokol IP protokol koji spaja računalne mreže različitih tehnologija, topologija i primjene. Unutar mrežnog sloja, još se koristi i ICMP protokol. On uglavnom služi za otkrivanje aktivnih računala na mreži te dijagnostiku različitih grešaka na mreži [5], [8].

Mrežni sloj bi trebao voditi računa o tome da ne dođe do zagušenja mreže koje se javlja onda kada je dolazni promet veći od kapaciteta izlaznih linija pa je u podmreži previše paketa i neki se počinju gubiti. Podmrežom se smatraju prva tri sloja. Kontrola zasićenja povezana je sa usmjeravanjem jer je upravo to i glavni razlog zasićenja. Ako su kojim slučajem polazišna i odredišna stanica u različitim mrežama, mrežni sloj je taj koji mora riješiti probleme koji zbog toga nastaju.

Ciljevi prilikom stvaranja usluga mrežnog sloja su :

- usluge moraju biti neovisne o tehnologiji podmreže
- na prijenosni sloj ne smije utjecati broj, tip i topologija mreža
- mrežne adrese za prijenosni sloj moraju imati jedinstveni način označavanja i kroz LAN i kroz WAN.

Dva su načina unutarnje organizacije mrežnog sloja i to: jedna koja koristi veze sa spajanjem, a druga koristi veze bez spajanja [6], [9].

2.1.2.1.Virtualni kanal

Virtualni kanal se uglavnom koristi kod usluga sa spajanjem veza. Kod samog uspostavljanja veze se odabere jedan put od pošiljatelja prema primatelju i on se koristi kroz cijelo vrijeme trajanja veze odnosno svi paketi idu samo tim putem. Svaki usmjernik treba zapamtiti gdje treba predati pakete za svaki od trenutačno otvorenih virtualnih kanala koji prolaze kroz njega. Onoga trenutka kada paket dođe do usmjernika, usmjernik pomoću broja virtualnog kanala koji se nalazi u zaglavlju paketa, točno zna gdje treba proslijediti paket. Korištenje privremenog virtualnog kanala čini tri faze komunikacije [6], [10]:

- uspostavljanje veze
- prijenos podataka
- raskidanje veze.

2.1.2.2.Datagrami

One mreže koje koriste veze bez spajanja koriste datagrame i imaju sljedeća svojstva [6], [11]:

- Računalo koje šalje podatke, može ih poslati bilo kada i bilo gdje jer će usmjernik odmah proslijediti datagram.
- Kada računalo pošalje datagram, ono ne zna je li mreža sposobna dostaviti ga do odredišta te je li odredište uopće aktivno.
- Svaki datagram se šalje neovisno, točnije, dva uzastopna datagrama mogu različitim putevima doći do odredišta.
- Ukoliko postoji mogućnost da se nađe drugi put do odredišta, kvar usmjernika ili veze ne utječe na komunikaciju.

2.1.3. Transportni sloj

Ovaj sloj obavlja jako puno funkcija, uključujući i nekoliko razina prepoznavanja grešaka, ponovne uspostave rada nakon ispadanja sustava, upravljanje virtualnim kanalima i multipleksiranje. Transportni sloj je granica između viših i nižih slojeva. Oslobađa više slojeve od brige o učinkovitosti prijenosa podataka. Ovaj sloj na najvišoj razini može otkriti greške, ponekad ih čak i ispraviti, identificirati skupove podataka koji su poslani u ispravnom redoslijedu, a ukoliko su poslani krivim redoslijedom, on ih može presložiti u ispravan redoslijed. Transportni sloj također podržava pouzdan prijenos između dva krajnja čvora na komunikacijskoj mreži [6], [12]. Na ovom sloju se nalaze TCP i UDP protokoli. Kada se podatci prenose, TCP protokol uspostavlja sjednicu između klijenta i poslužitelja dok se UDP protokol bazira na prijenos paketa, bez kontrole prijenosa na razini samog protokola. Osnovne karakteristike TCP protokola [5], [13]:

- pouzdanost – svaki paket koji je poslan ima svoj potvrdni broj, a paketi za koji nije dobiven potvrdni broj, ponovno se šalju
- potpuna duplex komunikacija – mogućnost istovremenog primanja i slanja podataka
- sigurnost – neovlašteni korisnik ne može ubacivati lažirane pakete u otvorenu sjednicu ukoliko nema ovlaštenje nadgledati tu sjednicu.

UDP protokol je puno jednostavniji protokol, ali je zato i manje pouzdan.

3. TEHNIKE ZA NADZOR I ANALIZU MREŽNOG PROMETA BAZIRANE NA RUTERU

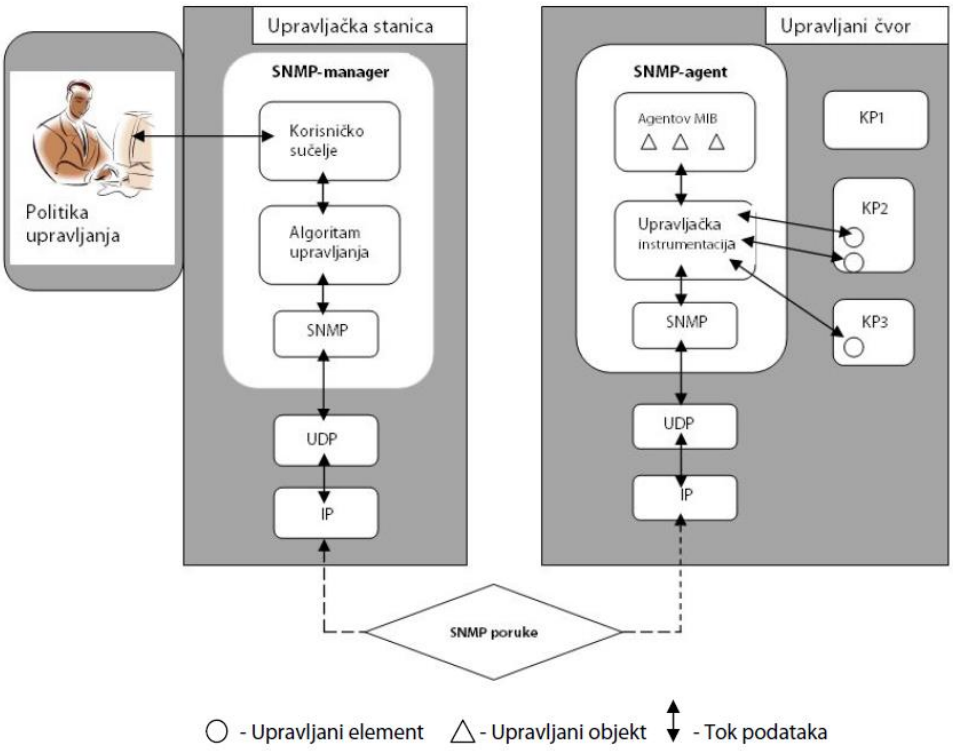
Tehnike nadzora mrežnog prometa koje su temeljene na usmjerivaču odnosno routeru su sljedeće [14]:

1. SNMP protokol
2. NETFLOW
3. RMON

3.1. SNMP PROTOKOL – JEDNOSTAVNI MREŽNI PROTOKOL ZA UPRAVLJANJE

Simple Network Management Protocol je najzastupljeniji protokol predviđen za rad na TCP/IP mrežama. Prilično je jednostavan, ali i fleksibilan kako bi omogućio kvalitetno upravljanje velikim brojem različitih tipova uređaja. On za funkciju ima prikupiti i analizirati primljene informacije o stanju računalne mreže. Ovaj protokol mrežnom administratoru omogućava da nadgleda performanse te pronalazi i rješava probleme na mreži. Ovaj protokol je dio sustava za upravljanje mrežom (Network Management System – NMS).

NMS je sastavljen od jedne ili više upravljačkih stanica na kojima se izvode upravljačke aplikacije te od upravljačkih čvorova na kojima se izvode upravljački agenti. Prikazano je to na slici 1 [15].



Slika 1: Sustav za upravljanje mrežom u okviru SNMP protokola

Izvor: [15]

Kao što je vidljivo iz slike 1, ovaj protokol služi za povezivanje upravljačkih stanica sa SNMP agentima koji su instalirani na mrežnoj opremi korisnika, a sve skupa se može povezati kao usluga za olakšano upravljanje i nadziranje pojedinih dijelova mrežnog sustava na sljedećim područjima [16]:

- prepoznavanje i dojava grešaka u sustavu
- upravljanje konfiguracijom
- upravljanje performansama
- upravljanje sigurnošću
- upravljanjem uslugama
- upravljanje obračunavanjem troškova.

U prvoj polovici osamdesetih godina prošlog stoljeća, u mrežama koje koriste TCP/IP protokole nisu bili implementirani protokoli upravljanja mrežnom opremom već se koristio protokol ICMP (Internet Control Message Protocol). On je omogućavao prijenos upravljačkih poruka između računala i upravljanih mrežnih uređaja. Koristeći ICMP i različita zaglavlja i različita

zaglavlja IP paketa moguće je razviti jednostavne i moćne alate za upravljanje mrežom, ali čak ni oni ne pružaju dovoljno učinkovitu funkcionalnost za upravljanje složenim mrežama. Iz tog razloga je 1987. godine razvijen protokol SGMP (Simple Gateway Monitoring Protocol) koji je namijenjen nadzoru usmjerivača. Zahtjevi koji su rasli i jako brz razvoj ionako složenih TCP/IP mreža, mrežno upravljanje su činili otežanim. Sve to je dovelo do poboljšanja protokola SNMP. Od njegovog predstavljanja 1988. godine, SNMP je postao najpopularniji protokol za upravljanje umreženim računalima i uređajima.

SNMP zahtijeva da svi agenti u NMS-u moraju podržavati jedinstveni OSI referentni model zasnovan na protokolima UDP i IP. Takav pristup onemogućava primjenu SNMP upravljanja u uređajima kao što su npr. neki mostovi i modemi koji ne podržavaju TCP/IP OSI referentni model. Isto tako, postoje brojni manji sustavi u kojima nisu ugrađeni protokoli TCP/IP OSI modela. Zbog ograničenih procesnih mogućnosti nije preporučljivo u takve sustave ugrađivati podršku za SNMP. Kako bi se spomenuti problemi otklonili, uveden je posrednik u upravljanju mrežom odnosno agent zastupnik.

Verzije SNMP protokola koje su danas u upotrebi su:

- SNMPv1 – u upotrebi od 1988. godine
- SNMPv2 – u upotrebi od 1995. godine
- SNMPv3 – u upotrebi od 1998. godine

SNMPv1 protokol je prihvaćen kao standard u TCP/IP mrežama od 1988. godine. Još i danas se dosta koristi bez obzira na poznate sigurnosne nedostatke. Kod ovog protokola se sigurnost temelji na korištenju tzv. zajedničkih znakovnih nizova. To je ustvari niz tekstualnih ASCII znakova i podsjeća na tradicionalne lozinke koje se koriste u operacijskim sustavima. Koriste se za izmjenu SNMP poruka između upravljačke jedinice i upravljanog uređaja. Problem je u tome što se ne koristi nikakav oblik enkripcije pa neovlašteni korisnici mogu snimanjem IP paketa koji se prenose mrežom pročitati sadržaj poruka, a samim time i zajedničke znakovne nizove. Znajući za taj podatak, zlonamjerni korisnici mogu pristupiti upravljačkim informacijama nekog mrežnog uređaja i promijeniti njegovu konfiguraciju.

SNMPv2 je donijela određena poboljšanja, ali su problemi što se tiče sigurnosti i dalje ostali prisutni. Godine 1993. inačica 2.0 je postala standard i nudila je dodatne mogućnosti kao što su sigurnost i autentikacija. SNMPv2 predstavlja proširenje protokola SNMPv1 i podržava tri načina pristupa upravljačkoj informaciji [15], [17]:

1. upravljač – agent zahtjev – odgovor

   SNMPv2 upravljač šalje zahtjev agentu, a agent odgovara slanjem traženih upravljačkih informacija. Koristi se dohvaćanje i modificiranje upravljačkih informacija.
2. upravljač – upravljač zahtjev – odgovor

   Jedan SNMPv2 upravljač šalje zahtjev drugom upravljaču, a drugi odgovara slanjem traženih upravljačkih informacija.

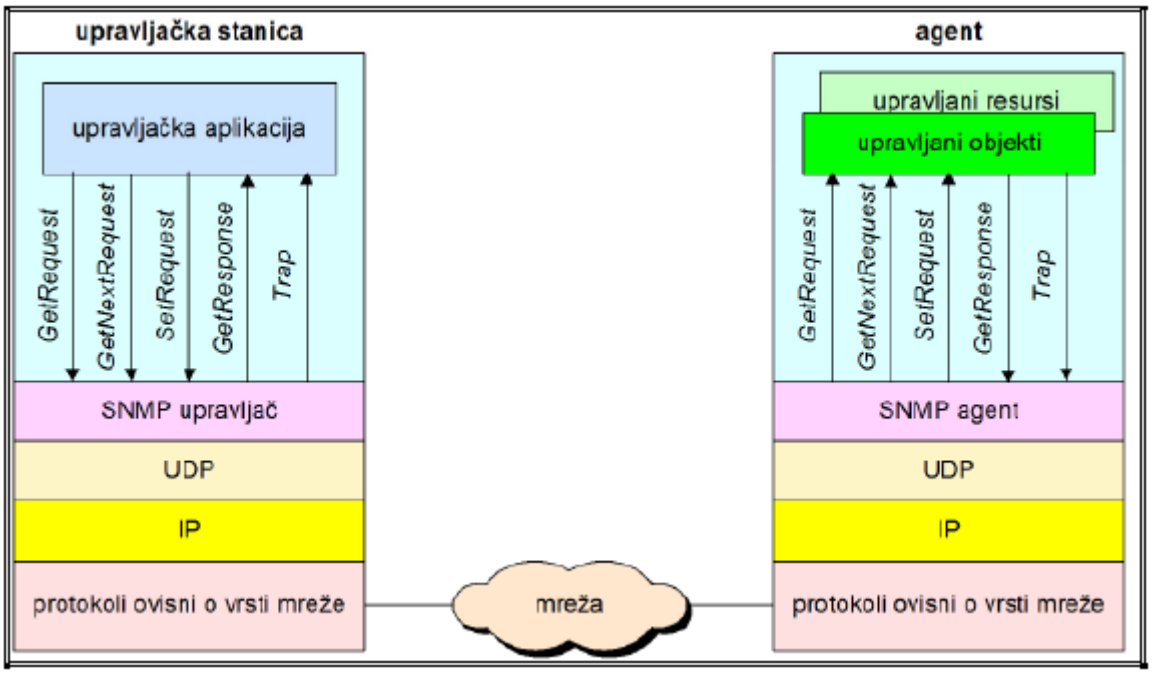
3. agent – upravljač bez potvrde

   SNMPv2 šalje poruku „*Trap*“ upravljaču.

SNMPv3 posjeduje bitno poboljšanje sigurnosti. Ovaj protokol sadrži provjeru vjerodostojnosti korisnika i zaštitno kodiranje SNMP poruka odnosno enkripciju. SNMPv3 može koristiti korisničku autentikaciju ili se provjera vjerodostojnosti korisnika može obaviti bez slanja lozinki u čitljivom obliku. Takva provjera se temelji na upotrebi algoritma. Najvažnija promjena u ovom protokolu je napuštanje koncepta NMS-a koji se temelji na upravljačima i agentima.

Tri osnovne funkcionalnosti koje protokol SNMP pruža sustavu upravljanja mrežom su mogućnost slanja sjedećih poruka [15], [18]:

1. *Get* (dohvati) – upravljačkoj stanici omogućava dohvaćanje vrijednosti upravljanih objekata koji su sadržani u upravljačkoj bazi informacija (MIB, engl. Management Information Base). Slanje ovakvih poruka agentima naziva se prozivanje. Upravljač agente najčešće proziva ciklički. Unutar nekog zadanog vremenskog intervala upravljač prozove redom sve agente i nakon toga započinje novi ciklus prozivanja. Frekvenciju prozivanja je moguće konfigurirati u SNMP upravljaču.
2. *Set* (postavi) – upravljačkoj stanici omogućava postavljanje vrijednosti upravljanih objekata u MIB-ovima agenata. Aplikacija obično vrši operaciju *set* tako da upravljačkoj stanici preda naziv agenta i jedan ili više identifikator objekata (OID, engl. Object Identifiers) zajedno s pripadajućim inačicama te novu vrijednost. Agent prosljeđuje zahtjev i dodjeljuje nove vrijednosti MIB varijabli. Ako dođe do pogreške nova vrijednost neće biti dodijeljena.
3. *Trap* (privuci pažnju) – omogućava agentu da obavijesti upravljačku stanicu o važnim događajima koji se zbivaju u komunikacijskoj okolini agenta.



Slika 2: Razmjena SNMP poruka

Izvor: [15], [19]

Na slici 2 se vidi kako izgleda razmjena poruka jednostavnog mrežnog protokola za upravljanje.

U SNMP NMS-u upravljačka informacija se između upravljača i agenata prenosi u obliku SNMP poruka. Svaka SNMP poruka sadrži tri polja [15], [20]:

- inačica protokola SNMP
- naziv zajednice (zajednički znakovni niz)
- SNMP PDU.

Po nazivima polja vidi se odstupanje od OSI terminologije po kojoj bi se cijela SNMP poruka trebala zvati SNMP PDU (engl. *Packet Data Unit*). Polje inačice sadrži jednu od tri moguće vrijednosti:

- 1 za SNMPv1
- 2 za SNMPv2
- 3 za SNMPv3 poruku.

Zajednički znakovni niz se koristi za potrebe sigurnosti SNMP komunikacije u upravljačkim sustavima. Polje zajednice je u stvari niz tekstualnih znakova koji podsjeća na tradicionalne lozinke. Najveći problem je u tome što neovlašteni korisnik snimanjem IP paketa koji se prenosi

mrežom može pročitati sadržaj SNMP poruke te tako saznati zajednički znakovni niz. Kobna posljedica navedenog je da bilo koji korisnik, ako poznaje znakovni niz, može pristupiti upravljačkim informacijama nekog mrežnog uređaja i promijeniti mu konfiguraciju. U svakom agentu se konfiguriraju tri zajednička znakovna niza:

1. *read-only*
2. *read-write*
3. *trap.*

Read-only znakovni niz omogućava isključivo čitanje vrijednosti podataka iz MIB-ova.
Read-write niz omogućava čitanje i upisivanje vrijednosti u MIB-ove.
Trap niz omogućava upravljačima prijem poruka *Trap*.

Većina proizvođača mrežne opreme isporučuje mrežne uređaje s unaprijed postavljenim *read-only i read-write* zajedničkim nizovima: *public,* odnosno *private*. Na primjer, u polju zajednice u SNMP poruci koja je namijenjena modificiranju određene vrijednosti u MIB-u agenta mora biti upisan tekst *private*. Naravno, administratori bi trebali svakako promijeniti zajedničke nizove prilikom početne instalacije mrežnih uređaja. U NMS-u koji se oslanja na SNMPv1 ili SNMPv2 poželjno je korištenje vatrozida koji će upravljanu mrežu zaštititi od ugrožavanja sigurnosti kroz mehanizme protokola SNMP. Druga mogućnost poboljšanja sigurnosti mreže prilikom korištenja zajedničkih znakovnih nizova su virtualne privatne mreže (*Virtual Private Network* - VPN).

3.2. NETFLOW

Netflow je mrežni protokol koji je stvorio Cisco i koji skuplja aktivni IP mrežni promet dok teče prema nekom sučelju ili izvan njega. *Netflow* podatci se zatim analiziraju te čine sliku protoka i volumena mrežnog prometa. Ovaj protokol koriste informatički profesionalci za analizu mrežnog prometa kako bi mogli odrediti polaznu točku, odredište, volumen kao i puteve kroz mrežu. *Netflow* slijedi jednostavan proces prikupljanja podataka, sortiranja i analize. Glavne komponente uključuju [14], [21]:

- *IP Flow* – sastoji se od grupe paketa koji sadrže iste atribute paketa. Kako se paket prosljeđuje putem routera, on se pregledava na set određenih atributa.

- *Netflow Cache* – to je baza skupljenih informacija gdje su podatci sačuvani kad se paketi pregledavaju.
- *Command Line Interface* – ovo je jedna od dvije metode pristupa *Netflow* podatcima i daje trenutačni uvid u mrežni promet.
- *Netflow Collector* – je druga metoda pristupa podatcima, a to je izvoz podataka na *Netflow* kolektor odnosno server koji prikuplja i procesuira promet i izvezene podatke tako da ih je lako analizirati.

Ovaj protokol nazivaju standardnom industrijom za praćenje prometa. Predstavlja alat za ocjenu procesa mreže. Ako se pojavi bilo koja nepravilnost u mreži, *Netflow* analizator će se uskladiti s tom aktivnosti. *Netflow* se sastoji od tri komponente i to: predmemorije protoka (engl. *Netflow Accounting*), sakupljača tokova (engl. *Netflow Flow Collector*) i analizatora podataka (engl. *Netflow Data Analyzer*).

Prva komponenta predmemorija analizira i prikuplja IP podatke koji ulaze u sučelje i te podatke priprema za slanje dalje u mrežu. Informacije koje se mogu dobiti iz *Netflow* paketa su [22]:

- adresa izvora i odredišta
- brojevi sučelja ulaza i izlaza
- protokol četvrte razine
- broj paketa u toku
- ukupni bajtovi u toku
- vremenska oznaka u toku
- izvorni i odredišni broj autonomnog sustava (AS)
- TCP Flag
- vrsta usluge (ToS).

Analizator podataka je odgovoran za prezentaciju podataka. Prikupljeni podatci mogu se koristiti za različite svrhe, osim za nadgledanje mreže, kao što su planiranje mreže, terećenje i naplata. U odnosu na metode praćenja kao što su SNMP i RMON, prednost *Netflowa* je ta što postoje brojni softverski paketi za analizu prometa koji služe za povlačenje podataka iz *Netflow* paketa i njihovo prezentiranje na način koji je puno lakši za korisnike.

Korištenjem alata *Netflow Analyzer* moguće je izvući potrebne informacije iz *Netflow* paketa kako bi se stvorili grafikoni koje administrator može proučiti kako bi održao razumijevanje njihove mreže. Jedna od najvećih koristi kod upotrebe *Netflowa* u kombinaciji s drugim alatima

je ta što postoji mogućnost da se stvore različiti brojni grafikoni koji će detaljno opisivati mrežne aktivnosti u nekom trenutku.

Usmjerivači koji imaju omogućenu značajku *Netflow*, generiraju *Netflow* zapise. Ti generirani zapisi se izvoze, odnosno usmjeravaju iz usmjerivača i sakupljaju se pomoću *Netflow* sakupljača (engl. *Collector*). Nakon sakupljanja, *Netflow* sakupljač kreće sa obrađivanjem podataka kako bi se mogla obaviti analiza prometa i prezentacija u korisničkom formatu.

3.3. RMON – NADZOR NA UDALJENOJ LOKACIJI

RMON – Remote Monitoring definira mehanizme nadzora mreže na udaljenoj lokaciji i bez stalnog sudjelovanja upravljačke stanice u tom procesu. Osnovna ideja na kojoj se ovaj standard temelji jeste da se u upravljani mrežni uređaj ugradi RMON sonda koja će prikupljati potrebne podatke te ih slati upravljaču. RMON sonde se koriste u svim vrstama mreža koje se danas koriste u praksi, podržavajući rad kroz sve vrste usmjerivača i mostova za što su odgovorni proizvođači mrežne opreme. Na taj način prikuplja komunikacijsku statistiku u okolini mrežnog uređaja. Podatci se spremaju u bazu upravljačkih informacija u uređaju upravljanom od strane SNMP managera. On ima mogućnost pristupa i dohvata svih željenih podataka. Takav je sistem izuzetno učinkovit u slučaju pada veze koja povezuje upravljačku stanicu i upravljani uređaj na mreži. RMON sonda može u bilo kojem trenutku obavijestiti stanicu o nastupu nekog važnog događaja u okolini upravljanog uređaja na mreži. RMON je poznat po tome da se jednostavno ugradi u sve vrste mreža [14], [23].

RMON funkcije i njihov način rada smanjuju potrebu za individualnim agentima koji svojim radom opterećuju krajnje sustave, a prometom cjelokupnu mrežu. Upravljačka stanica u kojoj je instalirana aplikacija za upravljanje mrežom, može prozivati SNMP agenta i tada govorimo o eksternom prozivanju. Ako sonda lokalno poziva npr. operacijski sustav IOS u mrežnom uređaju iz kojeg prikuplja komunikacijske podatke, govorimo o internom prozivanju. Ukoliko prilikom prozivanja dođe do bilo kakve pogreške, agent RMON sonde može o tome poslati obavijest upravljaču pomoću poruke.

RMON1 - postoji ukupno devet različitih grupa SNMP varijabli unutar prve verzije RMON standarda. Svaka od ovih grupa, osim onih statističkih, imaju podatkovne i kontrolne tablice. Kontrolne tablice kontroliraju koji se podatci skupljaju i kako često dok se unutar podatkovne tablice ti podatci spremaju. RMON kompatibilni uređaji su upravljani preko RMON MIB-a.

RMON MIB sadrži statističke podatke skupljene od promatranog uređaja te se mogu promatrati kao tablice kako bi lakše koristili potrebne informacije. Ove tablice su podijeljene u dvije skupine: kontrolne tablice (engl. *Control Tables*) i podatkovne tablice (engl. *Data Tables*), svaka sa integriranim sigurnosnim sustavom i kontrolom pristupa. Kontrolne tablice se mijenjaju u skladu sa potrebnim kontrolama i potrebnim podatcima koje očekujemo od uređaja dok podatkovne tablice te podatke spremaju [24].

RMON2 je nadopuna standarda RMON koja se fokusira na više slojeve te dozvoljava praćenje prometa na svim slojevima mreže. To je glavna razlika u odnosu na RMON standard koji je pratio promet samo na MAC ili nižim slojevima. Zbog tog razloga je RMON2 dizajniran za korištenje sa strane aplikacija za nadzor mreže, a ne za korištenje sa strane ljudskih korisnika. Svaki promatrani objekt mora imati ime, sintaksu, nivo pristupa te implementacijski status. Ime ima tip i instancu objekta te se koristi kao identifikator promatranog objekta. Nivo pristupa označava dozvole pristupa za promatrani objekt odnosno ima li dozvolu čitanja, pisanja ili oba. Implementacijski status je status objekta i može imati jednu od četiri vrijednosti:

- obavezno
- izborno
- zastario
- odbačeno.

RMON2 objekti su također podijeljeni u deset grupa koje nadopunjuju one već definirane u RMON1 standardu. Kao i u RMON1, u RMON2 postoje dvije vrste tablica sa istim osobinama kao i u prvoj verziji [24].

4. AKTIVNE I PASIVNE TEHNIKE ZA NADZOR I ANALIZU PROMETA

Nadzor mreže je izuzetno zahtjevan zadatak za mrežnog administratora. Oni se cijelo vrijeme trude omogućiti da mreže rade bez ikakvih smetnji ili zastoja. Ponekad zbog pada mreže dolazi do kolapsa u cijelom poduzeću i ugrožena je sigurnost pružanja njihovih usluga. Iz tog razloga administratori mreže moraju nadzirati kretanje prometa u cijeloj mreži i voditi računa o tome da se nigdje na mreži ne pojavljuju sigurnosni propusti [24].

Tehnike za nadzor i analizu mrežnog prometa koje nisu bazirane na usmjerivaču odnosno routeru mogu ponuditi puno veću fleksibilnost od tehnika za nadzor koje su bazirane na usmjerivaču jer su one još uvijek dosta ograničene u svojim mogućnostima i opcijama. Mogu se podijeliti na:

- aktivno praćenje
- pasivno praćenje

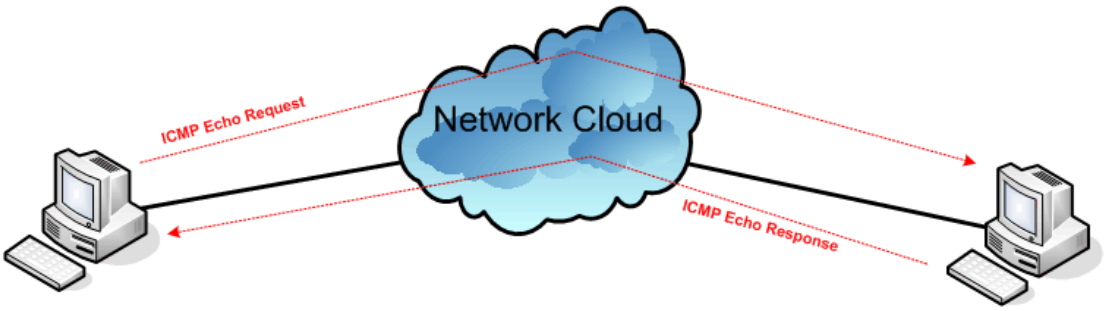
4.1. AKTIVNO PRAĆENJE

Aktivno praćenje prikuplja podatke između najmanje dvije točke u mreži. Bave se mjernim podatcima kao što su [24]:

- mjerenje dostupnosti
- mjerenje rute
- kašnjenje paketa
- preuređivanje paketa
- gubitak paketa
- mjerenje kapaciteta i protoka podataka.

Jedan od uobičajenih paketa koji mjere kašnjenje i gubitak paketa je *Ping*. To je alat za rješavanje problema koji administratori sustava koriste za ručno testiranje povezanosti mrežnih uređaja, ali i za mrežno kašnjenje ili gubitak paketa. Koristi se još i *Traceroute* koji pomaže u određivanju topologije mreže. Oba spomenuta alata šalju ICMP pakete uređaju u mreži odnosno primatelju i čekaju da primatelj odgovori pošiljatelju.

Na slici 3 može se vidjeti kako izgleda primjer ping naredbe.



Slika 3: ICMP ping naredba

Izvor: [24]

4.2. PASIVNO PRAĆENJE

Pasivno praćenje ne mijenja promet koji je već na mreži i prikuplja podatke o samo jednoj točki u mreži. Po tome se razlikuje od aktivnog praćenja koji prikuplja podatke o najmanje dvije točke u mreži. [24]

Na slici 4 je prikazano postavljanje pasivnog sustava praćenja gdje je monitor postavljen na jednu vezu između dvije krajnje točke i nadzire promet kako putuje preko veze.

Slika 4: Postavljanje pasivnog praćenja

Izvor: [24]

Pasivna praćenja su bazirana na tome da prikupljaju informacije odnosno prate točnu brzinu paketa, vrijeme dolaska paketa i drugo. Pasivno praćenje se može koristiti uz pomoć bilo kojeg

analizatora paketa. Ovaj način praćenja nema velikih troškova, ali ima određenih nedostataka. Kod ovakvog načina praćenja, mjerenja se mogu analizirati samo izvan mreže, a ne redom kako se i prikupljaju. To mrežnim administratorima pričinjava itekako velik problem jer moraju obraditi jako puno skupova podataka koji su prikupljeni [24].

5. KOMBINIRANE TEHNIKE ZA NADZOR I ANALIZU MREŽNOG PROMETA

Kombinirane tehnike za nadzor i analizu mrežnog prometa su svakako bolji i precizniji odabir od korištenja samo jedne tehnike za nadzor i analizu mrežnog prometa. Dvije kombinirane tehnike za nadzor i analizu mrežnog prometa su WREN (engl. Watching Resources from the Edge of the Network) – Nadgledanje resursa s ruba mreže i SCNM (engl. Self Configuring Network Monitor) – Samokonfigurirajući nadzornik mreže.

5.1. Nadgledanje resursa s ruba mreže – WREN

Nadgledanje resursa s ruba mreže koristi kombinaciju aktivnih i pasivnih tehnika praćenja, aktivno obrađuje podatke kada je prometno opterećenje maleno i pasivno prati promet za vrijeme velikog prometnog opterećenja. On prati promet i na izvoru i na odredištu prometa što omogućava preciznija mjerenja. WREN koristi praćenje paketa koji generira aplikacija za mjerenje raspoložive širine pojasa (kapaciteta). WREN je podijeljen na dvije razine: funkcionalnosti na razini paketa za praćenje jezgre i analiziranje paketa na korisničkoj razini [24].

Funkcionalnosti za praćenje paketa na razini jezgre odgovorne su za skupljanje informacija povezanih s dolaznim i odlaznim paketima.

Incoming Packets				**Outgoing Packets**			
timestamp	seq #	ack #	TCP cwnd	timestamp	seq #	ack #	data size

Slika 5:Podatci prikupljeni praćenjem paketa na razini jezgre

Izvor: [24]

Slika 5. prikazuje podatke koji se prikupljaju za svaki paket. Međuspremnik je dodan jezgri i njemu se pristupa putem dva sistemska poziva. Jedan poziv počinje praćenje i pruža potrebne informacije za prikupljanje značajki, a drugi poziv dohvaća trag iz jezgre. Objekt za praćenje paketa sposoban je koordinirati mjerenja između različitih uređaja. Jedan uređaj će pobuditi drugi uređaj postavljanjem zastavice u zaglavlje odlaznog paketa kako bi započeo praćenje istog niza paketa koji se prati. Drugi uređaj će pratiti sve pakete koji imaju istu zastavicu

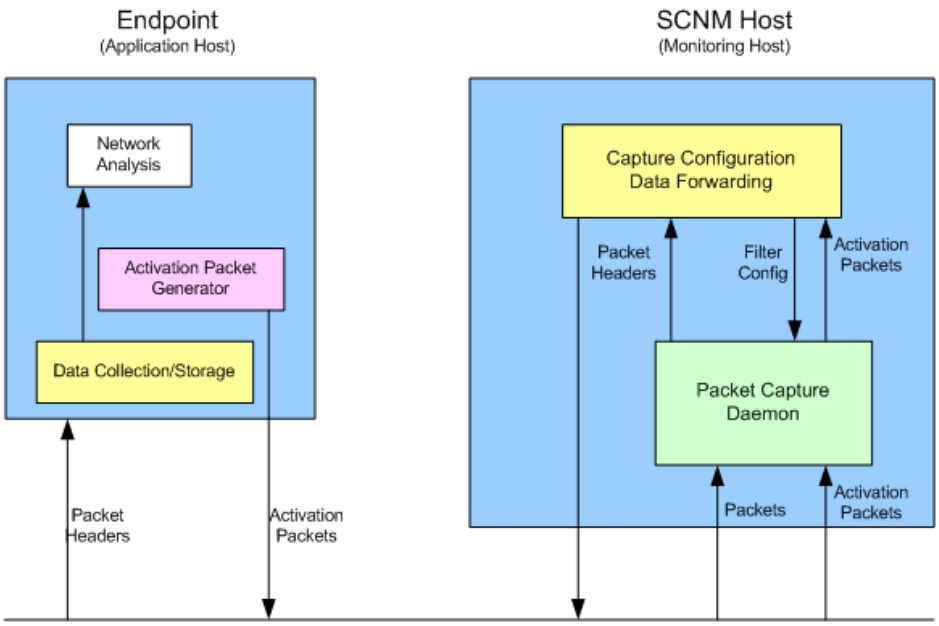
postavljenu u zaglavlju paketa. Takav način rada omogućava da se podatci s istim paketima spremaju na svakoj krajnjoj točki neovisno o tome što se između njih događa.

Analiziranje paketa na korisničkoj razini druga je razina u WREN okruženju. Ovdje se započinje praćenje bilo kojeg paketa i prikupljaju se i obrađuju podatci koji su vraćeni iz objekta praćenja na razini jezgre. Kod analiziranja paketa na korisničkoj razini ne moraju se cijelo vrijeme pratiti informacije iz objekta za praćenje paketa. Mogu se analizirati odmah nakon završetka nadzora ili se podatci spremaju za kasniju analizu. Kada nema puno prometa, WREN uvodi promet u mrežu kako bi mogao održati kontinuirani tijek mjerenja protoka. WREN korisnici mogu pratiti i promet aplikacija drugih korisnika, ali s nepotpunim informacijama. Mogu primati samo brojeve sekvenci i potvrda, ali ne mogu primati stvarne dijelove podataka iz paketa. WREN je vrlo koristan alat koji koristi sve prednosti aktivnog i pasivnog praćenja [24].

5.2. Samokonfigurirajući nadzornik mreže – SCNM

Samokonfigurirajući nadzornik mreže je alat za praćenje koji koristi kombinaciju aktivnih i pasivnih tehnika praćenja. Okruženje samokonfigurirajućeg nadzornika mreže se sastoji od hardverskih i softverskih komponenti. Hardver je instaliran na kritičnim mjestima na mreži i odgovoran je za prikupljanje zastavica u zaglavlju paketa. Softver radi na krajnjim točkama mreže.

Na slici 6 su prikazane softverske komponente samokonfigurirajućeg nadzornika mreže.



Slika 6: SCNM softverske komponente

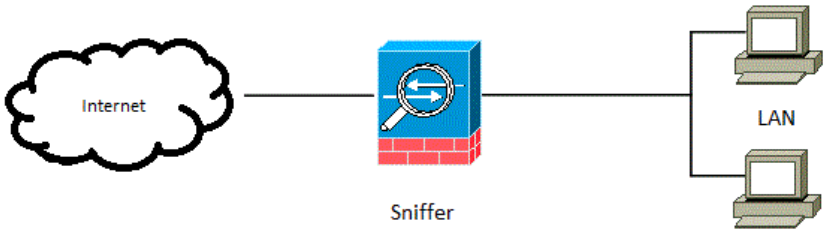
Izvor: [24]

Softver je odgovoran za stvaranje i slanje paketa koji se koriste za početak praćenja mreže. Korisnici pošalju aktivacijski paket na mrežu, a taj paket sadržava detalje o paketima koje želi nadzirati i prikupljati. Na temelju podataka unutar aktivacijskog paketa, postavlja se filter na krajnju točku. Prikupljaju se zastavice sa zaglavlja paketa mrežnog i transportnog sloja koje odgovaraju filteru. Filter nakon određenog vremena automatski istekne, osim ako u međuvremenu ne primi još jedan aktivacijski paket.

6. KOMPARATIVNA ANALIZA ZNAČAJKI TEHNIKA ZA NADZOR I ANALIZU PROMETA U MREŽI

Velik broj proizvođača komunikacijske opreme u svoje uređaje je ugradio mogućnost kontrole prometa. Procjena prometa se može konfigurirati na usmjernicima i preklopnicima, ali sama identifikacija prometa ipak nije toliko precizna na posebno specijaliziranim uređajima. Kod velikih korporacija i u jako velikim mrežnim sustavima potrebno je konfigurirati veliki broj pravila koji zahtijevaju veliku procesorsku snagu usmjernika ili preklopnika što je u konačnici jako skupo, a zbog velikog broja pravila na odlaznim sučeljima usmjernika mogućnost pogreške se povećava kao i vrijeme otklanjanja pogreške u pravilima. [25]

Analiza mrežnog prometa je postupak kojim se mrežni paketi podvrgavaju analizi. Presretanje paketa podrazumijeva njihovo čitanje uz primjenu odgovarajuće aplikacije. Dohvaćeni paket se nakon njegovog snimanja i lokalnog registriranja prosljeđuje na odredište. Programska rješenja za analizu mrežnog prometa se nazivaju se snifferi odnosno analizatori paketa. Ti alati mogu prikazati paket u obliku koji je lako razumljiv, točnije oni dekodiraju informacije specifične za protokol danog paketa. Analizatori paketa su u mogućnosti promet snimati putem pasivnog osluškivanja više odredišnih poruka (kao što je bežični mrežni promet) ili putem presretanja poruka. Na slici 7 je prikazano gdje se nalazi analizator paketa unutar mreže.



Slika 7: Pozicija analizatora paketa unutar mreže

Izvor: [3], [26]

Dodatne mogućnosti pojedinih alata su:

- automatsko uočavanje pogreške u prijenosu
- otkrivanje uzroka pogreške

- prikaz podataka u grafičkom obliku
- kreiranje ispitnih paketa koji mogu biti ispravni ili neispravni.

Alati mogu biti hardverska ili softverska rješenja. Hardverska rješenja se ugrađuju u telekomunikacijsku opremu te su sposobna vrlo brzo analizirati promet protokola nad kojim su izgrađeni. Softverska rješenja su šire namjene od hardverskih i u mogućnosti su analizirati puno više protokola. Koriste se u trenutku kada se želi otkriti uzrok nekog problema.

Kada se odredi mjesto u informatičkoj infrastrukturi gdje je potrebno nadzirati mrežni promet, unutarnja strana mreže se spoji na unutarnje sučelje, npr. preklopnik, a vanjska strana se spoji na vanjsko sučelje, npr. usmjernik. Svaki uređaj sadrži pasivnu komponentu za premoštenje, integriran u postojeći uređaj ili kao zaseban uređaj. Ukoliko se uređaj pokvari, nestane struje ili se dogodi nekakva greška u programu, komponenta za premoštenje osigurava nesmetan prolazak prometa kroz uređaj. Sav promet koji prolazi kroz uređaje pripada u nepoznati promet. Proučavajući taj promet možemo saznati koja računala i serveri razmjenjuju podatke na unutarnjoj i vanjskoj strani uređaja [24], [27].

6.1. NEKI OD NAJBOLJIH UREĐAJA ZA NADZOR I ANALIZU MREŽNOG PROMETA

Alati za nadzor mrežnog prometa olakšavaju kontrolu mrežnog prometa i pomažu da se postigne potpuna vidljivost, poboljša kvaliteta usluge te da se mogu predvidjeti i spriječiti „uska grla“ u potpunosti [2], [28].

Praćenjem mrežnog prometa služe se:

- Sistemski administratori kako bi mogli analizirati probleme u mreži, spriječiti ili uočiti napade tamo gdje nema IDS sustava te unaprijedili performanse sustava.
- *Cyber* kriminalci kako bi prikupili podatke koji putuju mrežom, dobili uzorke o prometu koji putuje određenom mrežom te dobili informaciju o tome koji su protokoli najranjiviji.

Neki od primjera korištenja sniffera su:

- uočavanje mrežnih pogreški

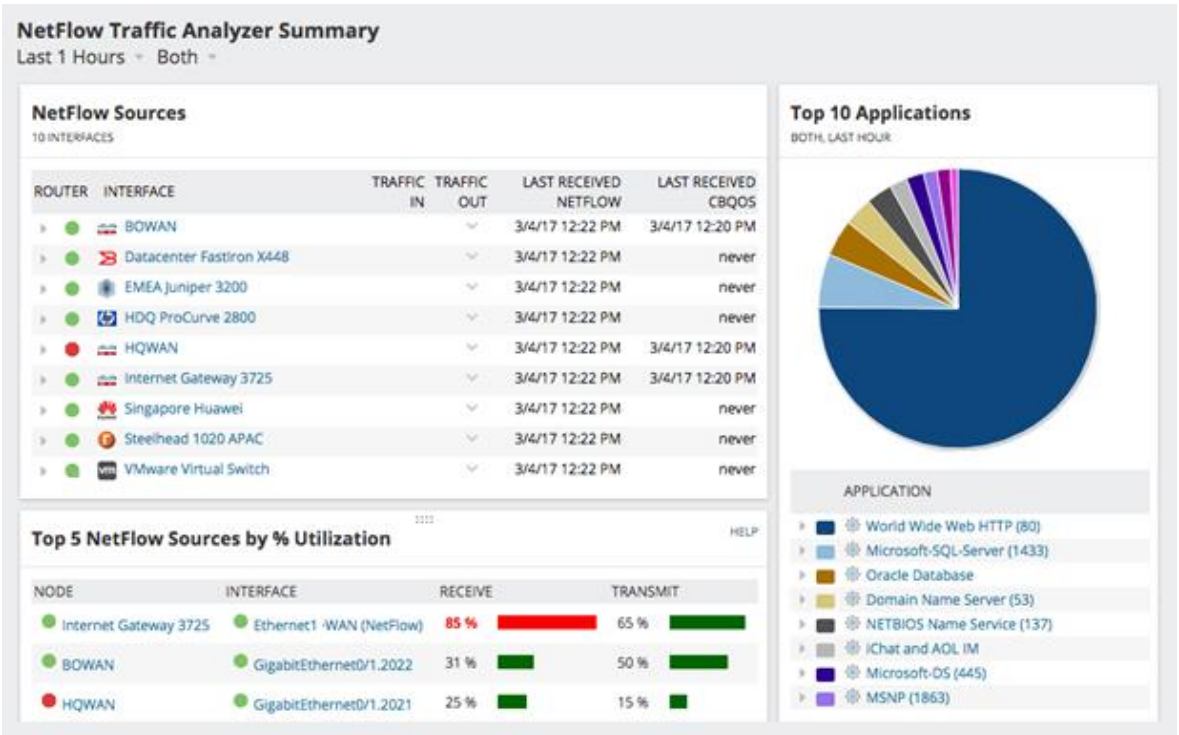
- uočavanje pokušaja upada na sustav
- izolacija sustava sa mrežnim kvarom
- nadzor podataka u prijenosu mrežom
- prikupljanje statistike mrežnog prometa.

U nastavku će biti prikazani neki od najboljih alata za nadzor i analizu mrežnog prometa.

6.1.1. SolarWinds NetFlow Traffic Analyzer

Ovaj specijalizirani alat omogućava analizu mrežnog prometa, upozorenja o prometu aplikacija, napredno prepoznavanje aplikacija i drugo. Ova aplikacija isto tako omogućava da se napravi analiza trendova i obrazaca u mrežnom prometu u različitim vremenskim intervalima. Podatci u ovoj aplikaciji se prikazuju putem internetskog preglednika i na taj način omogućavaju da joj se pristupi s bilo kojeg uređaja, u bilo koje vrijeme i s bilo kojeg mjesta putem internetske veze.

Na slici 8 se može vidjeti kako izgleda sučelje ovog analizatora prometa.



Slika 8: NetFlow Traffic Analyzer

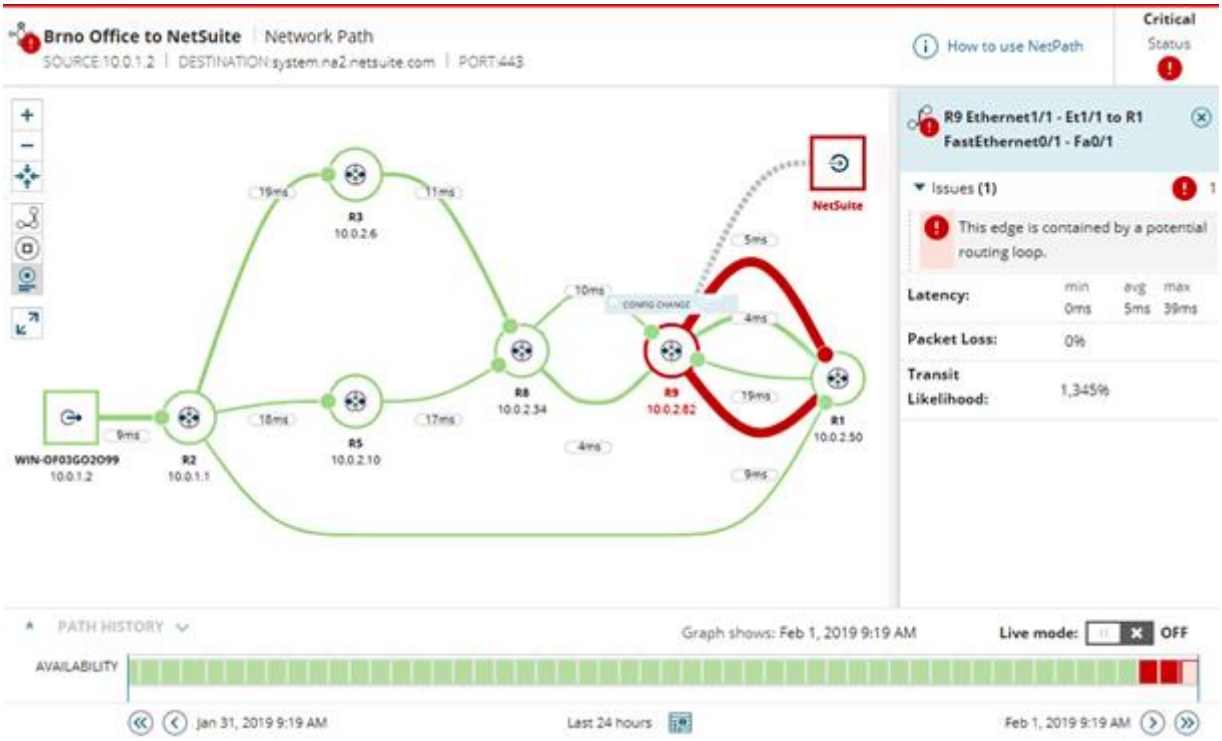
Izvor: [2], [29]

Ova aplikacija ima i sofisticiran sustav upozorenja napravljen na način da upozori ukoliko promet naglo skoči ili padne. To korisnicima svakako omogućava izuzetno brze akcije kako bi se problemi čim prije otklonili.

6.1.2. SolarWinds Network Performance Monitor (NPM)

SolarWinds je vodeći proizvođač alata za nadzor i upravljanje infrastrukturom i ima jako veliko i dugogodišnje iskustvo sa Cisco uređajima. Alat radi na principu da pregleda mrežu prije instalacije i otkriva sve uređaje koji su na njega priključeni. To dovodi do automatske generacije mrežne topološke karte. Mrežni nadzor performansi svakih pet minuta ispituje njihove registrirane uređaje na njihove statuse. Rezultati provjere statusa budu prikazani na nadzornoj ploči alata [2], [30].

Na slici 9 je prikazano kako izgleda analizator prometa SolarWinds.



Slika 9: SolarWinds monitor performansi mreže

Izvor: [2], [29]

6.1.3. Paessler PRTG Network Monitor

Ovaj uređaj za nadzor mrežnog prometa je zapravo skup uređaja koji se nazivaju senzorima. Koristi se senzorski pristup praćenju mreže i može nadzirati mreže, poslužitelje i aplikacije. Statusi svih mrežnih uređaja prikazani su na nadzornoj ploči. Razumijevanje podataka je maksimalno olakšano radi toga što su podatci prikazani u obliku grafikona u različitim bojama. PRTG nudi niz senzora za praćenje mrežnog prometa.

Slika 10 prikazuje kako izgleda sučelje PRTG analizatora paketa.

Slika 10: PRTG mrežni monitor

Izvor: [2], [29]

6.1.4. Wireshark

Wireshark je besplatan alat otvorenog koda za analizu mrežnog prometa. Radi se o alatu koji hvata podatke koji u paketima putuju mrežom i prikazuje ih na najdetaljniji mogući način. Wireshark je mrežni alat što znači da može raditi na različitim platformama. Neke od mogućnosti ovog alata su [30]:

- hvatanje podatkovnih paketa s mrežnog sučelja
- prikazivanje paketa s vrlo detaljnim informacijama o mrežnom protokolu
- otvaranje i spremanje paketa

- uvoz i izvoz podataka u druge slične programe
- pretraga i filtriranje paketa po raznolikim kriterijima
- kreiranje različitih statistika.

Podatke unutar mrežnih paketa Wireshark može očitati s više različitih vrsta mreža, a najpoznatije koje podržava su:

- Ethernet – najučestalija LAN tehnologija koja se s 10 gigabitnom izvedbom, koristi i kao WAN tehnologija. Ethernet šalje pakete od pošiljatelja prema jednom (Unicast) ili više (Multicast/Broadcast) prijamnika.
- IEEE 802.11 – skup standarda za bežičnu računalnu komunikaciju (WLAN) na frekvencijskim pojasevima od 2.4, 3.6 i 5 GHz. Razvijen je od strane IEEE LAN/MAN Standards Committee (IEEE 802).
- PPP – (eng. Point-to-Point Protocol) protokol koji se koristi za izravno povezivanje dvaju čvorova računalne mreže. Omogućava povezivanje računala serijskim, telefonskim ili optičkim kabelom, pomoću mobilnih telefona te posebno oblikovanom radio ili satelitskom vezom.
- Loop-back – virtualno mrežno sučelje koje je implementirano softverski.

Ovaj alat, baš poput i svih drugih alata za analizu mreže ima određene sigurnosne propuste i nepravilnosti. Sigurnosni propust se očituje u neovlaštenim odnosno nedopuštenim radnjama koje itekako mogu naštetiti mreži i svim njenim korisnicima. Wireshark sprječava sigurnosne propuste na način da analizira moguće probleme i radnje koje bi mogle stvoriti probleme. Zadatci analize unutar ovog alata dijele se na preventivne i reaktivne.

Preventivne metode uključuju mrežne metode za očitavanje trenutnog statusa mreže i aplikacije. Preventivne metode se koriste za detektiranje problema na mreži i prije nego ih korisnik mreže primijeti.

Reaktivne metode se koriste tek onda kada se uoče greške prilikom rada mreže. Ako postoji problem s određenim poslužiteljem, Wireshark će prijaviti problem tek nakon pokušaja hvatanja paketa s mreže.

Ovo su neke od analiza koje korisnicima Wiresharka mogu poslužiti u funkciji sigurnosti [30]:

- pronalaženje korisnika s najviše prometa na mreži
- identifikacija protokola i aplikacija koje se trenutno koriste
- određivanje prosječnog broja paketa u sekundi
- prikaz svih korisnika komunikacijske mreže
- prepoznavanje najčešćih problema na mreži
- određivanje korisnika koji usporavaju promet na mreži
- identifikacija neuobičajenog pregleda prometa na mreži
- uočavanje neuobičajenih protokola i dr.

6.2. ANALIZA ANALIZATORA PAKETA

Analizatori paketa (engl. sniffers) su programski alati koji omogućavaju promatranje Ethernet mrežnog prometa te rade zabilješke svih važnih podataka kako bi se kasnije mogla napraviti analizu. Iz tog razloga su oni jako snažan alat za administratore mrežnih sustava jer jako brzo uočavaju greške na mrežnim sustavima. Isto tako brzo greške i otklone.

Ovaj alat isto tako može biti korišten od strane nelegalnih korisnika i korišten u nelegalne svrhe kako bi uspjeli doći do povjerljivih podataka korisnika računalne mreže kao što su njihova korisnička imena i lozinke. Za cilj imaju postati administratori sustava i ne biraju sredstva kako do toga doći [31].

6.2.1. Problemi sniffers alata

Za nekoga tko se ne zna koristiti ovim alatima, oni su opasni. Bitno je poduzeti sve što je nužno za sigurnost jer nelegalni korisnici mogu doći do jako bitnih podataka kao što su korisničko ime i lozinka administratora sustava. Ukoliko do tog podatka dođu, lako preuzimaju kontrolu nad cijelim sustavom. Kako se analizom mrežnog prometa može doći do povjerljivih podataka kao što su korisnička imena i lozinke te im se na taj način omogućava administracija sustava, postoji mogućnost da se na taj način dovede u pitanje sigurnost raznih mrežnih uređaja. Na isti način je upitna sigurnost i svih mrežnih protokola na višim mrežnim slojevima [31].

Većina korisnika koji su manje iskusni, ignoriraju takve mogućnosti i koriste različite aplikacije i protokole koji nisu baš najsigurniji pa se otkrivaju razne povjerljive informacije korisnika. Do toga dolazi jer se te sve informacije računalnom mrežom šalju bez ikakve zaštite odnosno u istom onom obliku u kojem ih je korisnik unio.

6.2.2. Sigurnosni rizik i pravovremene mjeren

Danas postoje kvalitetni mehanizmi koji mogu zaštititi od neželjenog promatranja mrežnog prometa. Kao najjednostavnije rješenje nameće se korištenje jednokratnih lozinki koje će se koristiti za samo jedno prijavljivanje u sustav. Poslije toga je nemoguće opet se prijaviti s istom lozinkom. Za svaki sljedeći ulazak u sustav, dobije se nova lozinka. Oni korisnici koji su nešto manje iskusni mogu predložiti da se isključi onaj modul koji omogućava analizu i promatranje mrežnog prometa. Ali to nikako nije preporučljivo iz razloga što se na taj način mogu uočiti eventualni pokušaji napada na mrežni sustav [31].

6.2.3. Detekcija upada nadzorom mrežnog prometa

Jedini ispravan način koji može spriječiti ili smanjiti rizik od utjecaja prijetnji je omogućavanje detaljnog uvida u mrežni promet i aktivnosti unutar lokalne mreže. Velika većina tvrtki se pouzdaje u zastarjele IT sustave koji imaju sigurnosne kontrole samo na krajnjim točkama sustava (engl. *endpoint security*). Na takav način se svjesno zanemaruje ono što je između te dvije krajnje točke, a to je jednostavno nedopustivo budući da u današnje vrijeme preko 70% napada dolazi iz lokalne mrežne okoline.

Da bi se tako nešto moglo spriječiti, trebao bi se koristiti alat za nadzor mrežnog prometa ali u kombinaciji s točno određenim algoritmima.

Sustavi za detekciju upada dijele se na NIDS i HIDS sustave odnosno sustave za detekciju mrežnih upada i upada na lokalno računalo [32].

NIDS sustavi nadziru mrežni sloj operacijskog sustava kako bi uspjeli detektirati zlonamjerne uzorke mrežnog prometa, npr. pretraživanje mrežnih priključaka, iznenadni skok mrežnog prometa i slično. Najčešće se promatraju osjetljivi dijelovi mreže kao što je dio mreže koji najviše komunicira s vanjskim svijetom, a sadrži web ili mail poslužitelje.

HIDS sustavi nadziru aplikacijske zapise, izmjene u sustavu i drugo.

Postoji još jedna podjela sustava za detekciju, a to je podjela po načinu same detekcije. Tako imamo sustave koji pronalaze upade pomoću :

- statističke analize odnosno detekcije anomalija – sustavi koji na temelju bilješki koje su prikupili pri normalnom radu sustava detektiraju neobične događaje
- usporedbe potpisa – sustavi koji događaje uspoređuju s definiranim obrascima napada.

Oba navedena sustava imaju svoje prednosti i mane. Mana detekcije anomalija odnosno prvog spomenutog načina jeste da sustav mora duže vrijeme „učiti“ normalno ponašanje sustava, pri čemu postoji i mogućnost krivog učenja. Prednost mu je što može otkriti prethodno nezabilježene vrste napada.

Mana drugog načina je ta da obrazac napada mora biti poznat kako bi se njegov potpis mogao usporediti sa trenutnim događajima na sustavu. Prednost ovog načina rada jest pouzdanost detekcije (manji broj je lažnih detekcija).

Metode kojima se koriste dijelovi sustava za sprječavanje upada (nakon što je isti detektiran) brojne su, a neke od temeljnih su blokiranje prometa iz smjera napada, podizanje alarma, zaključavanje dijela sustava pod napadom i sl. [32].

7. ZAKLJUČAK

Nadzorom i analizom mrežnog prometa se dolazi do dosta informacija o mreži i svim aktivnostima na mreži. U ovom završnom radu je prikazano nekoliko alata i različitih tehnika nadzora i analize mrežnog prometa pomoću kojih je moguće detaljnije analizirati aktivnosti na računalnoj mreži. Važno je spomenuti kako i legalni i nelegalni korisnici mogu koristiti alate za nadzor i analizu mrežnog prometa, ali razlika je u tome što nelegalni korisnici te alate koriste isključivo kako bi saznali korisnička imena i lozinke koje nisu nikako zaštićene, a putuju računalnom mrežom.

Kako komunikacijska i mrežna infrastruktura iz godine u godinu postaju sve veće i kompleksnije nužno je na određenim lokacijama nadzirati i analizirati mrežni promet. Računi se plaćaju putem interneta, sve je više web trgovina koje omogućavaju kupovinu „iz fotelje“, svi uređaji koji se koriste u kućanstvima su umreženi. Sve navedeno dovodi do toga da je izuzetno bitna velika propusnost.

Svi ovi uređaji koji su opisani u radu, a odnose se na nadzor i analizu prometa na prilično jednostavan način omogućavaju da se mrežni promet nadzire i ukoliko je potrebno – ograniči. Ukoliko i dođe do „uskog grla“ i dođe do preopterećenosti, mrežni promet se snima i na taj način je moguće dobiti informaciju koji promet je kriv za preopterećenost. Nekada se čini da nema kraja tom procesu, ali proizvođači uređaja i alata za nadzor i analizu prometa stalno rade na unaprjeđenju svojih proizvoda kako bi bili u korak sa zahtjevima tržišta i potrošača.

Bez alata za nadzor i analizu mreže jednostavno se ne bi mogla jamčiti kakvoća i efikasnost računalnih mreža. Svaki alat za nadzor ima svoje performanse i svaki korisnik na temelju toga može odabrati koji je za njega najbolji odnosno najisplativiji.

Budući da su u ovome završnom radu opisane neki od najboljih alata za nadzor i analizu mreže na tržištu, moguće je vidjeti i jasne razlike među njima. Ako se za primjer uzme SolarWinds NPM, on ima mogućnost skeniranja računalne mreže i može dohvatiti sve čvorove u mreži te prikazati njihove parametre, dok kod PRTG Network Monitor-a to nije slučaj.

Jedan od najčešće korištenih alata za analizu mrežnog prometa je svakako Wireshark. To je zaslužio iz nekoliko razloga. Wireshark podržava sve važnije mrežne protokole i ima mogućnost implementacije za nove protokole. Rad s paketima je kod ovog alata je prilagođen grafičkom sučelju Wiresharka pa je potreban minimalan trud, znanje i vrijeme kako bi se uspjele savladati osnovne funkcionalnosti. Kad je sigurnost u pitanju, Wireshark ima malih

problema i poteškoća, ali se one polako otklanjaju i svaka nova verzija Wiresharka je sve sigurnija.

Na kraju se ipak dolazi do zaključka kako svi alati nemaju nikakvih odstupanja kod nadzora prometa jer ih izvode točno, ali ipak, pojedini alati čine to s puno većim sposobnostima te samim time pružaju puno kvalitetniji pregled mreže.

Svrha nadzora i analize mrežnog prometa svakako je pokušati spriječiti „uska grla“ i preopterećenost mreže te ojačati i povećati iskoristivost mreže. Na taj način se postaje konkurentniji na tržištu i može se održavati kakvoća usluge na nivou.

LITERATURA

[1]Techopedia. *Network Traffic Analiysis*. Preuzeto s: https://www.techopedia.com/definition/29917/network-traffic [Pristupljeno: srpanj 2021].

[2] Staff Contributor. *Best Network Traffic Monitoring Tools*. Preuzeto s: https://www.dnsstuff.com/network-traffic-monitors [Pristupljeno: srpanj 2021].

[3] Centar informacijske sigurnosti. *Praćenje mrežnog prometa*. Preuzeto s: https://www.cis.hr/sigurnosni-alati/pracenje-mreznog-prometa.html [Pristupljeno: srpanj 2021].

[4] Application Performance Management. *Network Traffic Monitor*. Preuzeto s:

https://www.applicationperformancemanagement.org/network-monitoring/network-traffic-monitor/ [Pristupljeno: srpanj 2021].

[5] CARNet Hrvatska akademska i istraživačka mreža. *Analiza mrežnog prometa*. [Prezentacija] Preuzeto s: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-09-90.pdf [Pristupljeno: srpanj 2021].

[6] Androić D. *OSI referentni model*. [Predavanje] Prirodoslovno – matematički fakultet Zagreb. Preuzeto s: https://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_2.pdf [Pristupljeno: srpanj 2021].

[7] Wikipedia, the free encyclopedia. *Serial Line Internet Protocol*. Preuzeto s: https://en.wikipedia.org/wiki/Serial_Line_Internet_Protocol [Pristupljeno: kolovoz 2021].

[14] Uma M, Padmavathi G. *An Efficient Network Traffic Monitoring for Wireless Networks*. International Journal of Computer Applications 2012; 53(9): 51-59.

[15] CARNet Hrvatska akademska i istraživačka mreža. *SNMP protokol.* [Prezentacija] Preuzeto s: https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-09-313.pdf [Pristupljeno: srpanj 2021].

[16] Bažant A, *Osnovne arhitekture mreža*. Element Zagreb, Zagreb. 2003.

[22] Chakchai So – In. *A Survey of Network Traffic Monitoring and Analysis Tools*. Preuzeto s: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3.pdf [Pristupljeno: kolovoz 2021].

[24] Cecil A. *Summary of Network Traffic Monitoring and Analysis Techniques* Preuzeto s: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring.pdf [Pristupljeno: srpanj 2021].

[25] Maksimović M, Perinović V, Žigman D. *Uređaji za analizu i kontrolu mrežnog prometa*. Polytechnic & Design 2014; 2(2): 269-273.

[31] CARNet Hrvatska akademska i istraživačka mreža. *Analiza alata Wireshark.* [Prezentacija] Preuzeto s: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-09-312.pdf [Pristupljeno: srpanj 2021].

[32] CARNet Hrvatska akademska i istraživačka mreža. *Analiza sniffing alata i zaštite*. [Prezentacija] Preuzeto s: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2001-11-06.pdf [Pristupljeno: srpanj 2021].

[33] Centar informacijske sigurnosti. *IPS / IDS.* Preuzeto s: https://www.cis.hr/sigurnosni-alati/ips-ids.html [Pristupljeno srpanj 2021].

POPIS ILUSTRACIJA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad (vrsta rada) isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Tehnike za nadzor i analizu mrežnog prometa, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

U Zagrebu 7.9.2021.

Studentica:
Ana Dodig
(potpis)