PLATFORMA ZA ANALIZU PERFORMANSI MREŽE KORIŠTENJEM ALATA perfSONAR

Trutin, Martina

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Stručni diplomski studij elektrotehnike

MARTINA TRUTIN

ZAVRŠNI RAD

Platforma za analizu performansi mreže korištenjem alata perfSONAR

Split, rujan 2024.

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Stručni diplomski studij elektrotehnike

Predmet: Sigurnost mreža i usluga

ZAVRŠNI RAD

Kandidat: Martina Trutin

Naslov rada: Platforma za analizu performansi mreže korištenjem alata perfSONAR

Mentor: Marko Meštrović, mag. ing. el., pred.

ODOBRENO ZA OBRANU

Split, rujan 2024.

SADRŽAJ

Sažetak

Platforma za analizu performansi mreže korištenjem alata perfSONAR

Zadatak ovog diplomskog rada je implementirati sustav za mjerenje mrežnih performansi zasnovan na sustavu otvorenog koda perfSONAR. U uvodu je opisana potreba za mjerenjima mrežnih performansi. U sljedećem poglavlju je opisan OSI model koji čini osnovu za standardizirani pristup mrežnim sustavima te omogućava razdvajanje pojedinih mrežnih funkcija. U trećem i četvrtom poglavlju opisani su često korišteni mrežni protokoli te alati za mjerenje njihovih performansi. U petom poglavlju opisan je perfSONAR sustav koji se koristi u akademskim i istraživačkim institucijama poput GÉANT-a i CERN-a. U šestom poglavlju prikazana je instalacija i konfiguracija perfSONAR sustava te način pokretanja mrežnih mjerenja.

Ključne riječi: perfSONAR, performance, network

Summary

Performance service-oriented network monitoring architecture perfSONAR

The task of this final paper is to implement a network performance measurement system based on the open-source system perfSONAR. The need for network performance measurements is described in the introduction. The OSI model, which forms the basis for a standardized approach to network systems and allows for the separation of individual network functions, is discussed in the next chapter. Frequently used network protocols and tools for measuring their performance are described in the third and fourth chapters. The perfSONAR system, used in academic and research institutions such as GÉANT and CERN, is covered in Chapter 5. In the sixth chapter, the installation and configuration of the perfSONAR system are described, along with the steps to start network measurements.

Keywords: perfSONAR, performance, network

1. UVOD

Povezivanje i razmjena podataka između računala, uređaja i sustava diljem svijeta omogućava gotovo sve aspekte modernog života, od poslovnih operacija i financijskih transakcija do obrazovanja i zabave. Mjerenja performansi računalnih mreža ključan su faktor za optimizaciju mrežnih operacija, osiguravanje kvalitete usluge (QoS) i održavanja zadovoljstva korisnika. Mjerenja performansi uključuju metrike poput kašnjenja (engl. latency), propusnosti (engl. throughput), varijacije kašnjenja (engl. jitter) i gubitka paketa (engl. packet loss).

Za pravilno provođenje mrežnih mjerenja potrebno je razumjeti OSI model, koji služi kao podloga za organizaciju mrežnih funkcija u slojevima. OSI model je standard koji dijeli mrežne procese u sedam slojeva počevši od najnižeg, fizičkog sloja do najvišeg, aplikacijskog sloja. Ovaj model omogućuje da različiti uređaji i sustavi međusobno komuniciraju na standardiziran način, što je važno za stabilnost i pouzdanost mreža. Svaki sloj modela ima svoje funkcije i protokole koji pomažu u upravljanju mrežnim resursima i održavanju efikasnosti mreže.

Mrežni protokoli su pravila koja uređaji koriste za komunikaciju unutar mreže. Protokoli kao što su IP, TCP, UDP, HTTP i FTP definiraju kako se podaci prenose i osiguravaju međusobnu komunikaciju između različitih uređaja. Na primjer, TCP osigurava pouzdan prijenos podataka, dok UDP omogućuje brži prijenos, ali s manje pouzdanosti. Znanje o različitim mrežnim protokolima važno je za učinkovito upravljanje mrežom.

Alati za mrežna mjerenja i analizu kao što su iperf, ping ili traceroute omogućuju praćenje performansi mrežnog prometa. Pomoću ovih alata mogu se identificirati uska grla, optimizirati brzina mreže i poboljšati sigurnost. Zbog toga su mrežna mjerenja, zajedno s poznavanjem OSI modela i mrežnih protokola, nužna za uspješno upravljanje modernim računalnim mrežama.

Jedan od alata otvorenog koda koji omogućuje objedinjavanje različitih mrežnih mjerenja te vizualizaciju i analizu rezultata je sustav perfSONAR. Taj sustav je zamišljen kao centralno mjesto koje objedinjava skupove mrežnih uređaja i orkestrira izvođenje mjerenja među njima. Preko grafičkog sučelja dostupna je vizualizacija rezultata uz mogućnosti jednostavnog dodavanja i konfiguracije novih mjerenja.

2. OSI MODEL

OSI (engl. Open Systems Interconnection) model je konceptualni okvir koji standardizira funkcije komunikacijskog sustava ili računalne mreže dijeleći ih u sedam različitih slojeva. Razvijen je od strane Međunarodne organizacije za standardizaciju (ISO) i služi kao referentni model za projektiranje i razumijevanje mrežnih protokola i komunikacijskih procesa. Važnosti OSI modela su da omogućava standardizirani pristup dizajnu mrežnih sustava, olakšava razvoj i integraciju različitih mrežnih tehnologija, te omogućava različitim mrežnim uređajima i protokolima da međusobno komuniciraju, bez obzira na proizvođača. Također, pomaže u razdvajanju složenih mrežnih funkcija u manje, upravljive dijelove, te svaki sloj ima svoju specifičnu funkciju i može se ažurirati neovisno o drugima. OSI model pomaže u dijagnosticiranju i rješavanju mrežnih problema identificiranjem u kojem sloju se problem nalazi. Omogućuje standardizaciju, interoperabilnost i modularnost. Njegova struktura od sedam slojeva pomaže boljem razumijevanju načina na koji različiti dijelovi mreže funkcioniraju i međusobno komuniciraju, olakšavajući razvoj, implementaciju i rješavanje problema u mrežnim sustavima. Slojevi OSI modela su:

- Fizički sloj (engl. Physical Layer)
- Sloj podatkovne veze (engl. Data Link Layer)
- Mrežni sloj (engl. Network Layer)
- Transportni sloj (engl. Transport Layer)
- Sloj sesije (engl. Session Layer)
- Prezentacijski sloj (engl. Presentation Layer)
- Aplikacijski sloj (engl. Application Layer)

Slika 1.1. OSI model

2.1. Fizički sloj

Temelj je svih mrežnih komunikacija jer se bavi prijenosom električnih signala preko fizičkog medija. Njegova glavna uloga je osigurati fizičke karakteristike veze između mrežnih uređaja, omogućavajući slanje i primanje sirovih podataka (bitova) kroz različite prijenosne medije. Fizički sloj upravlja načinom na koji se bitovi kodiraju i prenose između uređaja i pretvara digitalne podatke u signale koji mogu putovati preko fizičkog medija. Ovi signali mogu biti u obliku električnih impulsa, svjetlosnih signala ili radio valova, ovisno o korištenom mediju. Fizički sloj definira karakteristike i specifikacije fizičkog prijenosa medija, a to uključuje vrste kablova (bakreni, optički), bežične tehnologije, te konektore i sučelja. Ovaj sloj također određuje i fizički raspored uređaja u mreži, poznat kao topologija mreže, a primjeri topologija uključuju zvjezdastu, prstenastu i mrežnu topologiju. Definira način na koji se signali generiraju, kodiraju i moduliraju za prijenos podataka. To može uključivati različite tehnike modulacije, kao što su AM (engl. amplitude modulation), FM (engl. frequency modulation) i PM (engl. phase modulation). Fizički sloj osigurava pravilno vrijeme prijenosa bitova između uređaja, koristeći tehnike sinkronizacije kako bi primatelj točno odredio kada počinje i završava svaki bit. Definira brzinu prijenosa podataka preko fizičkog medija, mjerenu u bitovima po sekundi (bps). Elementi fizičkog sloja su: kablovi i konektori, bežične tehnologije, aktivni i pasivni uređaji, te standardi i protokoli. Postoje bakreni kablovi u koje spadaju koaksijalni kablovi, UTP (engl. Unshielded Twisted Pair) i STP (engl. Shielded Twisted Pair) kablovi koji su najčešće korišteni u lokalnim mrežama, zatim optička vlakna koja koriste svjetlosne signale za prijenos podataka, pružajući veće brzine prijenosa i dulje udaljenosti bez gubitka signala i različiti tipovi konektora kao što su RJ45 za UTP/STP kablove, te različiti konektori za optičke kabele. U bežične tehnologije spadaju radio valovi koji se koriste za bežične mreže poput Wi-Fi, Bluetooth i mobilnih mreža, te infracrveni koji se koriste u specifičnim aplikacijama za bežični prijenos podataka. U aktivne i pasivne uređaje ubrajamo repetitore (uređaji koji pojačavaju ili regeneriraju signale kako bi se omogućio prijenos na većim udaljenostima), hubove (centralne točke u mreži koje prosljeđuju podatke svim uređajima u mreži, bez usmjeravanja) i konvertere (uređaji koji omogućavaju komunikaciju između različitih tipova fizičkih medija). Od standarda i protokola imamo IEEE 802.3 (Ethernet) koji definira standard za žičane mreže, IEEE 802.11 (Wi-Fi) koji definira standard za bežične mreže i SONET/SDH (engl. Synchronous Optical Networking/ Synchronous Digital Hierarchy) standardi za optičke mreže. Fizički sloj postavlja temelje za sve ostale slojeve

mrežne komunikacije i razumijevanje ovog sloja je ključno za projektiranje, implementaciju i održavanje učinkovitih i pouzdanih mrežnih sustava.

2.2. Sloj podatkovne veze

Ovaj sloj je ključan za osiguravanje pouzdanog prijenosa podataka preko fizičkog sloja. Djeluje kao most između fizičkog i mrežnog sloja, upravljajući prijenosom okvira podataka i rješavanjem grešaka koje se mogu pojaviti tijekom prijenosa. Funkcije sloja podatkovne veze su formiranje okvira (engl. Framing), kontrola pristupa mediju (MAC-Media Access Control), otkrivanje i ispravljanje grešaka, kontrola toka podataka i fizičko adresiranje. Sloj podatkovne veze segmentira podatke u manje dijelove nazvane okviri (engl. frames). Okviri sadrže korisne podatke i kontrolne informacije potrebne za prijenos i imaju zaglavlje (engl. header) i završetak (engl. trailer) koji sadrže kontrolne informacije poput MAC adresa, kontrole grešaka i oznaka početka i kraja okvira. Različiti MAC protokoli koriste različite metode za kontrolu pristupa, uključujući CSMA/CD (engl. Carrier Sense Multiple Access with Collision Detection) za Ethernet i CSMA/CA (engl. Carrier Sense Multiple Access with Collision Avoidance) za Wi-Fi. Sloj podatkovne veze koristi metode za otkrivanje pogrešaka poput kontrolnih zbrojeva (engl. checksum) i CRC (engl. Cyclic Redundancy Check). Koristi MAC adrese za jedinstvenu identifikaciju uređaja na lokalnoj mreži. MAC adrese su ugrađene u mrežne kartice i jedinstvene su za svaki uređaj. Protokoli i tehnologije sloja podatkovne veze su:

- *Ethernet* (IEEE 802.3) koji je najčešće korišten žičani LAN standard i koristi CSMA/CD za upravljanje pristupom mediju. Ethernet okviri sadrže MAC adrese izvora i odredišta, tip protokola i podatkovni dio.
- *Wi-Fi* (IEEE 802.11) koji je standard za bežične mreže i koristi CSMA/CA za izbjegavanje kolizija u bežičnom prijenosu. Wi-Fi okviri imaju dodatna polja za upravljanje bežičnim prijenosom, uključujući SSID (engl. Service Set Identifier) i informacije o sigurnosti.
- *Token Ring* (IEEE 802.5) koji koristi pristup baziran na tokenima gdje uređaji mogu slati podatke samo kad posjeduju token. Ovaj pristup sprječava kolizije, ali je manje učinkovit u modernism mrežama u usporedbi s Ethernetom.

- *Frame Relay* koji se koristi za prijenos podataka u WAN (engl. Wide Area Network) mrežama. Omogućuje prijenos podataka visoke brzine preko virtualnih veza. Koristi minimalno otkrivanje i ispravljanje grešaka kako bi se postigle velike brzine prijenosa.
- *Point-to-Point Protocol* (PPP) koji omogućuje izravnu vezu između dva mrežna uređaja. Koristi se u dial-up vezama i širokopojasnim pristupnim tehnologijama. Pruža autentifikaciju, kompresiju i enkapsulaciju podataka.

Ključne komponente sloja podatkovne veze su mrežne kartice (NIC-Network Interface Cards) i mrežni preklopnici. Mrežne kartice omogućavaju fizičku vezu između uređaja i mreže. Svaka mrežna kartica ima jedinstvenu MAC adresu. Obavljaju funkcije sloja podatkovne veze, uključujući formiranje okvira i kontrolu pristupa mediju. Mrežni preklopnici su uređaji koji povezuju više uređaja unutar jedne mreže. Koriste MAC adrese za usmjeravanje okvira prema odredišnom uređaju. Sloj podatkovne veze OSI modela ključan je za osiguravanje pouzdanog i učinkovitog prijenosa podataka preko fizičkog sloja.

2.3. Mrežni sloj

Mrežni sloj odgovoran je za usmjeravanje paketa podataka kroz mrežu. Njegova glavna funkcija je omogućiti komunikaciju između različitih mrežnih segmenata, upravljati adresiranjem i usmjeravanjem podataka te osigurati da paketi podataka stignu do svog odredišta. Funkcije mrežnog sloja su logičko adresiranje, usmjeravanje (engl. Routing), fragmentacija i ponovno sastavljanje paketa te enkapsulacija i de-enkapsulacija paketa. Mrežni sloj dodjeljuje jedinstvene logičke adrese svakom uređaju u mreži. Najpoznatiji protokol za logičko adresiranje je Internet Protocol (IP) na kojem praktično počiva čitav internet. Logičke adrese omogućuju jedinstvenu identifikaciju svakog uređaja i njegovu lokaciju unutar mreže. Također, mrežni sloj osigurava prijenos podataka između različitih mrežnih segmenata. Usmjerivači (engl. routeri) analiziraju IP adrese i koriste usmjerivačke tablice za određivanje najbolje rute za prijenos paketa. Usmjeravanje može biti statičko (ručno konfigurirane rute) ili dinamičko (korištenje dinamičkih usmjerivačkih protokola poput OSPF, BGP, RIP). Paketi podataka mogu biti preveliki za prijenos kroz određeni prijenosni medij. Mrežni sloj fragmentira velike pakete u manje dijelove koji se mogu prenijeti kroz medij. Primateljski uređaj ponovno sastavlja fragmente u izvorni paket. Mrežni sloj dodaje zaglavlje (engl. header) svakom paketu podataka, koje sadrži kontrolne informacije poput IP adrese izvora i odredišta. Kada paket stigne na

odredište, mrežni sloj uklanja zaglavlje i prosljeđuje podatke višem sloju. Mrežni sloj bavi se upravljanjem prioritetima mrežnog prometa kako bi se osigurale odgovarajuće performanse za različite tipove prometa, kao što su glasovni i video prijenosi.

Ključni protokoli mrežnog sloja su:

1) *Internet Protocol (IP)*
   a) IPv4- Najrašireniji protokol za logičko adresiranje i usmjeravanje. Koristi 32-bitne adrese, omogućujući oko 4,3 milijarde jedinstvenih adresa.
   b) IPv6- Dizajniran da zamijeni IPv4 zbog ograničenog broja adresa. Koristi 128-bitne adrese, omogućujući praktički neograničen broj jedinstvenih adresa.
2) ICMP (engl. Internet Control Message Protocol)- Koristi se za dijagnostičke i kontrolne svrhe, kao što su prijava grešaka, testiranje dostupnosti uređaja (ping) i mrežna dijagnostika (traceroute).
3) IGMP (engl. Internet Group Management Protocol)- Koristi se za upravljanje multicast grupama, omogućujući uređajima da se pridruže ili napuste multicast grupe.
4) Routing protokoli
   a) RIP (engl. Routing Information Protocol)- Jedan od najstarijih routing protokola, koristi udaljenost (broj skokova) kao metriku za određivanje najbolje rute.
   b) OSPF (engl. Open Shortest Path First)- Link-state protokol koji koristi troškovnu metriku za određivanje najbolje rute. Omogućuje brzu konvergenciju i skalabilnost.
   c) BGP (engl. Border Gateway Protocol)- Koristi se za usmjeravanje između autonomnih sustava na internetu. Ključan je za rad interneta, omogućavajući razmjenu routing informacija između različitih mreža.

2.4. Transportni sloj

Ključan je za osiguranje pouzdanog prijenosa podataka između aplikacija koje se nalaze na različitim računalima u mreži. Funkcije transportnog sloja su:

- osiguravanje pouzdane komunikacije između izvornog i odredišnog računala,
- segmentacija i ponovno sastavljanje podataka što znači da razbija podatke iz viših slojeva na manje segmente kako bi se mogli efikasno prenijeti kroz mrežu,

- kontrola toka tako da kontrolira brzinu prijenosa podataka između izvornog i odredišnog računala kako bi se izbjeglo preopterećenje mreže ili prijemnika,
- otkrivanje i ispravljanje grešaka koje se mogu pojaviti tijekom prijenosa podataka pri čemu se koriste razne metode za otkrivanje i ispravljanje grešaka poput kontrolnih zbrojeva (engl. checksum) ili mehanizama za ponovno slanje segmenata s greškom (engl. retransmission),
- *multiplexing* i *demultiplexing*, odnosno omogućavanje istovremenog korištenja mreže od strane više aplikacija na jednom računalu.

Segmenti podataka su označeni portovima koji identificiraju izvorne i odredišne aplikacije. Ključni protokoli transportnog sloja su TCP (engl. Transmission Control Protocol) i UDP (engl. User Datagram Protocol). TCP je pouzdan, orijentiran na vezu, protokol koji osigurava ispravan prijenos podataka između aplikacija. Pruža usluge kao što su pouzdana isporuka, kontrola protoka, i redoslijed podataka. TCP zaglavlje sadrži polja poput izvornog i odredišnog porta, redni broj, potvrdni broj, kontrolne bitove, veličinu prozora, kontrolni zbroj i urgent pointer. UDP je nepouzdan, neorijentiran na vezu, protokol koji pruža brži prijenos podataka bez garancije isporuke. Pogodan je za aplikacije koje zahtijevaju brzinu i mogu tolerirati gubitak podataka, poput video streaminga i online igara. UDP zaglavlje sadrži polja poput izvornog i odredišnog porta, dužinu i kontrolni zbroj. Portovi se koriste za identifikaciju specifičnih aplikacija na izvornom i odredišnom računalu. Standardizirani portovi su rezervirani za poznate usluge (npr. port 80 za HTTP, port 443 za HTTPS), dok su dinamički portovi dodijeljeni aplikacijama koje ih zahtijevaju. Utičnice su kombinacija IP adrese i broja porta, koriste se za uspostavljanje i održavanje komunikacije između izvornog i odredišnog računala. Kontrola toka osigurava da brzina prijenosa podataka ne preopterećuje mrežu ili prijemnik. Mehanizmi kontrole toka uključuju sliding window protokol, gdje veličina prozora određuje količinu podataka koji se mogu poslati prije nego što se primi potvrda. Kontrola zagušenja sprječava preopterećenje mreže kontroliranjem količine podataka koji se šalju. Algoritmi kontrole zagušenja, poput TCP Tahoe, TCP Reno i TCP Vegas, prilagođavaju brzinu prijenosa podataka prema stanju mreže.

2.5. Sloj sesije (engl. Session Layer)

Sloj sesije odgovoran je za upravljanje i održavanje sesija između dva komunikacijska uređaja i aplikacije. Sesija je logička veza između aplikacija koja omogućava razmjenu podataka i koordinaciju aktivnosti. Ovaj sloj pruža mehanizme za uspostavljanje, održavanje i prekidanje sesija. Uspostavljanje znači da inicira vezu između dva krajnja uređaja ili aplikacije, postavljajući parametre komunikacije i osiguravajući da su obje strane spremne za prijenos podataka. Nadgleda i održava aktivnu sesiju upravljajući prijenosom podataka i osiguravajući kontinuitet komunikacije. Ispravno zatvara sesiju kada više nije potrebno osiguravajući da su svi podaci ispravno preneseni i da nema gubitka podataka. U slučaju prekida prijenosa podataka komunikacije se može nastaviti od posljednje kontrolne točke, a ne od početka, što povećava učinkovitost i pouzdanost prijenosa. Razumijevanje funkcija i protokola sloja sesije neophodno je za dizajniranje i implementaciju složenih mrežnih sustava koji zahtijevaju stabilnu i koordiniranu komunikacije između svojih dijelova.

2.6. Sloj prezentacije (engl. Presentation Layer)

Sloj prezentacije odgovoran je za transformaciju podataka između aplikacijskog sloja i sloja sesije. Njegova glavna funkcija je osiguravanje da Podaci preneseni između različitih aplikacija budu u formatu koji obje strane mogu razumjeti. Ovaj sloj djeluje kao prevoditelj podataka i omogućava njihovu pravilnu interpretaciju i prikaz. Upravlja formatiranjem podataka kako bi se osigurala njihova pravilna interpretacija. Osigurava podatke šifriranjem na strani pošiljatelja i dešifrira na strani primatelja kako bi se podaci zaštitili od neovlaštenog pristupa tijekom prijenosa. Smanjuje veličinu podataka radi učinkovitijeg prijenosa i pohrane.

2.7. Aplikacijski sloj (engl. Application Layer)

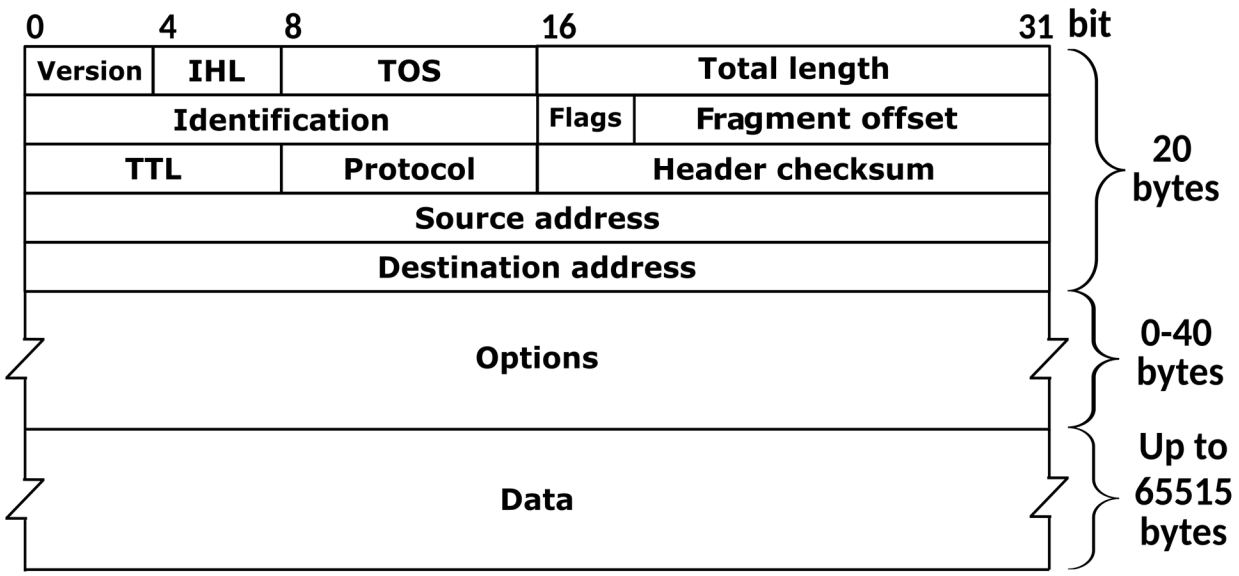
Njegova glavna funkcija je omogućiti mrežne usluge koje koriste aplikacije, kao što su web preglednici, e-mail klijenti, FTP klijenti i druge mrežne aplikacije. Aplikacijski sloj pruža razne mrežne usluge direktno aplikacijama i upravlja njihovim mrežnim potrebama. Omogućava različite mrežne usluge koje aplikacije koriste za komunikacije preko mreže. Upravlja načinom na koji aplikacije komuniciraju s mrežom uključujući uspostavljanje, održavanje i prekidanje veze. Osigurava sigurnost komunikacije kroz provjeru identiteta korisnika i kontrolu pristupa resursima. Pruža podršku za različite aplikacijske protokole koji definiraju kako aplikacije komuniciraju preko mreže.

3. MREŽNI PROTOKOLI

3.1. IP protokol

Internet protokol je osnovni protokol koji omogućava komunikacije između računala preko mreže. Svaki uređaj koji je povezan na internet ima jedinstvenu IP adresu. IP adresa je brojčani Identifikator koji omogućava uređajima da komuniciraju međusobno. Postoje dvije glavne verzije IP adresa, IPv4 i IPv6. IPv4 koristi 32-bitne adrese što omogućava ukupno oko 4,3 milijarde jedinstvenih adresa. IPv6 je uveden zbog ograničenog broja IPv4 adresa. Koristi 128-bitne adrese što omogućava ogroman broj jedinstvenih adresa. IP omogućava da se veliki podaci fragmentiraju u manje dijelove, odnosno pakete, kako bi se efikasno prenosili preko mreže. Svaki paket sadrži IP zaglavlje u kojem su informacije o adresi pošiljatelja i primatelja, te informacije o redoslijedu paketa. Paketi se preusmjeravaju kroz mrežu od izvora do odredišta pomoću usmjernika koji analiziraju IP zaglavlja paketa i odlučuju o najboljoj putanji za prijenos paketa.

3.1.1. IPv4

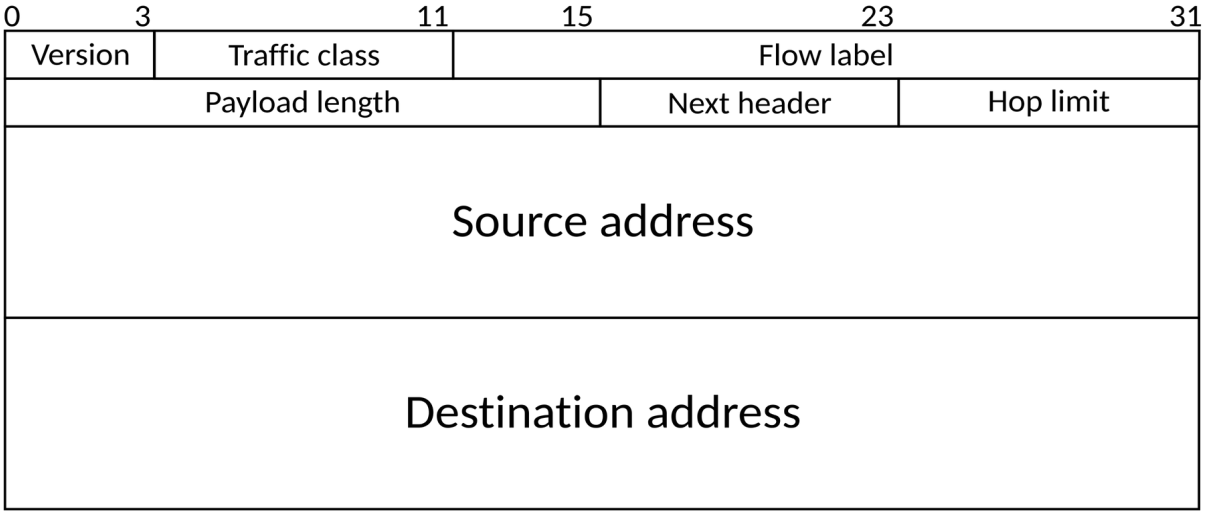


Slika 3.1. IPv4 protokol

IPv4 zaglavlje je osnovni dio svakog IPv4 paketa i ima fiksnu minimalnu dužinu od 20 bajtova, ali može biti produženo do 60 bajtova. Polja IPv4 zaglavlja su:

- verzija koje označava da je riječ o IPv4 protokolu.
- polje dužine zaglavlja (IHL) specificira ukupnu dužinu zaglavlja u 32-bitnim riječima, s minimalnom vrijednošću od 5 (što odgovara 20 bajtova)
- polje TOS (vrsta usluge) omogućava specificiranje prioriteta i vrste usluge koju paket zahtijeva, kao što su kašnjenje ili propusni opseg
- polje ukupna dužina, predstavlja ukupnu dužinu IP paketa, uključujući i zaglavlje i podatke, izraženu u bajtovima.
- polje identifikacija je jedinstveni identifikator koji se koristi za prepoznavanje fragmenata originalnog IP paketa. Povezano s ovim, polje flagovi sadrži bitove koji određuju različite kontrolne informacije, kao što su DF (engl. Don't Fragment) i MF (engl. More Fragments).
- Polje pomak fragmentacije označava poziciju fragmenta u odnosu na početak originalnog datagrama, omogućavajući rekonstrukciju originalnog paketa
- vrijeme života (TTL) polje je nužno za kontrolu trajanja paketa na mreži. Ovo polje se smanjuje za jedan pri svakom prolasku kroz usmjernik, a kada dostigne nulu, paket se odbacuje, što sprječava beskonačno kruženje paketa po mreži.
- polje protokol označava koji transportni protokol se koristi (npr. TCP ili UDP).
- polje kontrolni zbroj zaglavlja koristi se za osiguranje integriteta zaglavlja (provjerava se je li prenešeno zaglavlje ispravno)
- IP adrese izvora i odredišta specificiraju jedinstvene adrese uređaja koji šalju i primaju paket.
- polje opcije omogućava dodatne specifične funkcionalnosti kao što su sigurnost i specifično usmjeravanje, dok glavni dio paketa čine podaci koji se prenose.

3.1.2. IPv6



Slika 3.2. IPv6 protokol

IPv6 zaglavlje je dizajnirano da bude jednostavnije i efikasnije u odnosu na IPv4. Fiksne je veličine od 40 bajtova i ne uključuje opcije koje produžuju osnovno zaglavlje. Osnovna razlika je u efikasnosti i skalabilnosti, jer IPv6 eliminira potrebu za fragmentacijom u rutama, umjesto toga se oslanjajući na izvore da upravljaju veličinom paketa. Polja IPv6 zaglavlja su:

- verzija (4 bita) određuje verziju IP protokola, za IPv6 ovaj broj je 6.
- prioritet saobraćaja (engl. Traffic Class, 8 bita) koristi se za određivanje prioriteta paketa unutar mreže. Uključuje kontrole za određivanje razine usluge, kao što su kvalitet usluge (QoS) i vrsta usluge (ToS).
- oznaka protoka (engl. Flow Label, 20 bita) koristi se za označavanje paketa koji zahtijevaju poseban tretman od strane usmjerivača, omogućujući brži prolaz kroz mrežu.
- duljina tereta (engl. Payload Length, 16 bita) označava veličinu podataka u paketu, isključujući zaglavlje
- sljedeće zaglavlje (engl. Next Header, 8 bita) identificira vrstu zaglavlja koje dolazi neposredno nakon IPv6 zaglavlja. Ovo može biti zaglavlje višeg sloja (kao što su TCP ili UDP) ili dodatno IPv6 zaglavlje (kao što su zaglavlja opcija).

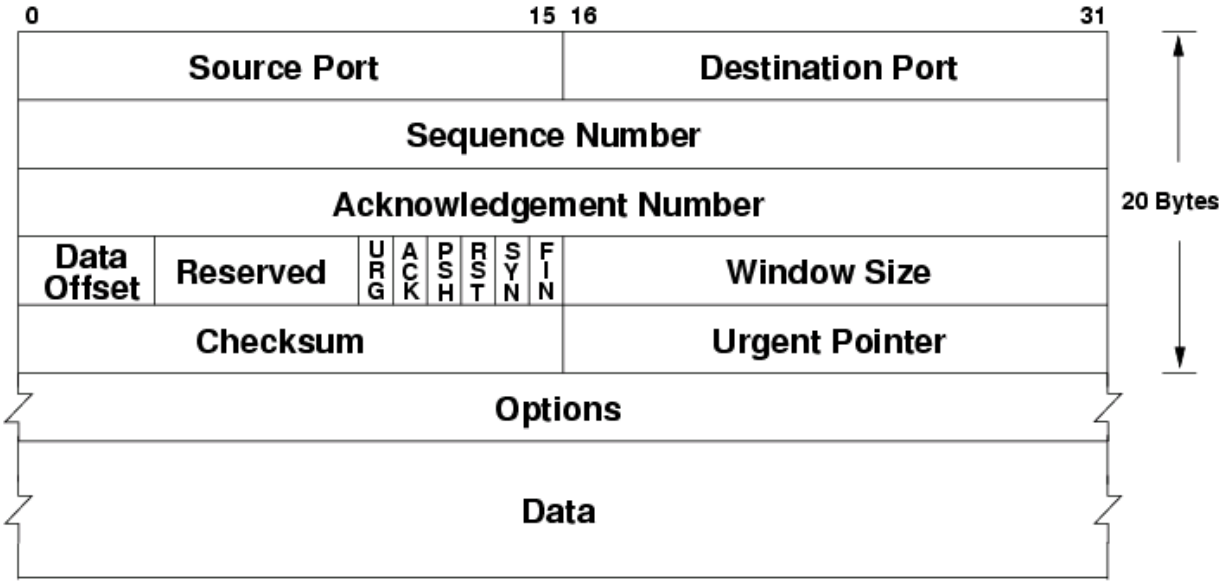
- Ograničenje skoka (engl. Hop Limit, 8 bita) zamjenjuje polje TTL (engl. Time To Live) iz IPv4 i smanjuje se za 1 na svakom usmjerivaču kroz koji paket prolazi. Kada dostigne nulu, paket se odbacuje.
- Izvorna adresa (128 bita): IPv6 adresa pošiljatelja paketa.
- Odredišna adresa (128 bita): IPv6 adresa primatelja paketa.

3.2. TCP protokol

TCP protokol (engl. Transmission Control Protocol) jedan je od najvažnijih i najraširenijih protokola u TCP/IP skupu protokola, koji omogućuje pouzdanu i sigurnu komunikaciju na internetu. TCP je dizajniran da osigura da podaci, koji se šalju između dva uređaja, stignu točno i u ispravnom redoslijedu. Ovaj protokol je temelj za mnoge internetske aplikacije, uključujući web preglednike, e-poštu i prijenos datoteka. Njegovi mehanizmi za pouzdanu isporuku, kontrolu protoka i zagušenja, kao i fleksibilnost za različite aplikacije, čine ga nezamjenjivim za mnoge svakodnevne mrežne aktivnosti.

Jedan od ključnih aspekata TCP-a je njegova sposobnost da osigura pouzdanu isporuku podataka. TCP koristi složene mehanizme za osiguranje da svi podaci stignu do svog odredišta neoštećeni i u pravilnom redoslijedu. Ova pouzdanost postiže se korištenjem brojeva sekvenci i potvrda. Kada uređaj šalje podatke preko TCP-a, svaki segment podataka označen je jedinstvenim brojem sekvence. Prijemnik koristi te brojeve kako bi potvrdio primitak svakog segmenta, šaljući natrag potvrdu s brojem sekvence sljedećeg očekivanog segmenta. Ako pošiljatelj ne dobije potvrdu u razumnom vremenskom periodu, on će ponovno poslati neprimljene segmente, osiguravajući tako potpunu isporuku podataka.

Kontrola toka još je jedan vitalni aspekt TCP-a. TCP koristi mehanizam poznat kao *windowing* kako bi osigurao da pošiljatelj ne preplavi prijemnik s više podataka nego što on može obraditi. Prozor, odnosno *window size*, određuje koliko podataka može biti poslano prije nego što se mora primiti potvrda. Ovaj mehanizam omogućuje prilagođavanje kapaciteta pošiljatelja i prijemnika, čime se izbjegavaju zagušenja na mreži.



Slika 3.3. TCP protokol

TCP zaglavlje sadrži sve informacije potrebne za upravljanje vezom i osiguranje pouzdanosti. Polja TCP zaglavlja su:

- Izvorni port (16 bita) identificira izvorni port na uređaju koji šalje podatke.
- Odredišni port (16 bita) identificira port na uređaju koji prima podatke.
- Broj sekvence (engl. Sequence Number, 32 bita) se koristi za kontrolu redoslijeda paketa kako bi se osiguralo da se podaci rekonstruiraju u pravilnom redoslijedu na primateljevoj strani.
- Broj potvrde (engl. Acknowledgment Number, 32 bita): Ako je postavljena zastavica za potvrdu (ACK flag), ovaj broj ukazuje na sljedeći očekivani broj sekvence koji pošiljatelj treba primiti.
- Duljina zaglavlja (engl. Data Offset, 4 bita) označava veličinu TCP zaglavlja u 32-bitnim riječima. Ovo ukazuje gdje podaci počinju unutar TCP segmenta.
- Polje rezervirano (6 bita) je rezervirano za buduću upotrebu i uvijek bi svi bitovi trebali biti postavljeni na nulu.

- Zastavice (engl. Control Flags, 6 bita) sadrže bitove koji kontroliraju stanje veze, uključujući:
    - URG (engl. Urgent Pointer): Označava da su podaci u paketu hitni.
    - ACK (engl. Acknowledgment): Potvrđuje prijem paketa.
    - PSH (engl. Push Function): Traži od primatelja da što prije proslijedi podatke aplikaciji.
    - RST (engl. Reset): Resetira vezu.
    - SYN (engl. Synchronize): Uspostavlja vezu.
    - FIN (engl. Finish): Zatvara vezu.
- Veličina prozora (Window Size, 16 bita) određuje količinu podataka koju druga strana može poslati prije nego što je potrebna potvrda.
- Kontrolna suma (Checksum, 16 bita) se koristi se za provjeru integriteta zaglavlja i podataka.
- Pokazatelj hitnosti (Urgent Pointer, 16 bita): Ako je URG zastavica postavljena, ovaj broj ukazuje na poziciju posljednjeg hitnog podatka unutar paketa.
- Opcije (Variable) je opcionalno polje koje se može koristiti za različite dodatne svrhe, poput određivanja maksimalne veličine segmenta, skaliranja prozora, i drugih opcija koje poboljšavaju performanse ili funkcionalnost.

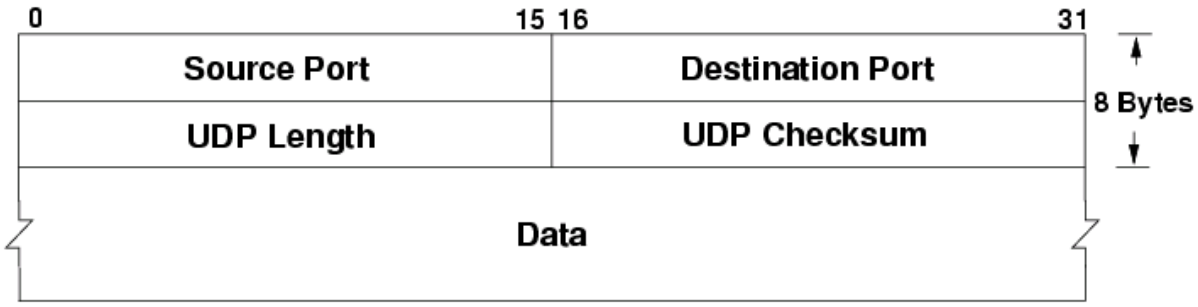
Proces uspostavljanja TCP veze poznat je kao „three-way handshake”. Kada klijent želi uspostaviti vezu sa serverom, prvo šalje postavljenu SYN zastavicu, predlažući početni broj sekvence. Server odgovara s postavljenim SYN-ACK zastavicama, potvrđujući primitak i predlažući svoj početni broj sekvence. Na kraju, klijent odgovara s postavljenom ACK zastavicom, potvrđujući primitak serverovog SYN-ACK segmenta, čime se veza uspostavlja. Ovaj proces osigurava da su obje strane spremne za komunikaciju i da su početni brojevi sekvenci pravilno postavljeni.

TCP je nezamjenjiv za aplikacije koje zahtijevaju visoku razinu pouzdanosti i točnosti. Web preglednici, koji koriste HTTP i HTTPS protokole, oslanjaju se na TCP za isporuku web stranica.

E-mail protokoli kao što su SMTP, POP3, i IMAP koriste TCP kako bi osigurali da se elektronička pošta isporuči točno i bez gubitaka. FTP (engl. File Transfer Protocol) koristi TCP za siguran i pouzdan prijenos datoteka, dok protokoli kao što je SSH (engl. Secure Shell) omogućuju sigurnu udaljenu prijavu i upravljanje serverima preko TCP-a.

3.3. UDP protokol

UDP protokol (engl. User Datagram Protocol) je dizajniran za aplikacije koje zahtijevaju brzinu i učinkovitost više od pouzdanosti i točnosti isporuke podataka. Ovaj protokol se koristi u situacijama gdje je potrebno minimizirati kašnjenje, kao što je streaming video sadržaja, online igre i VoIP (engl. Voice over IP) aplikacije. UDP je poznat po svojoj jednostavnosti. Njegovo zaglavlje sadrži samo osnovne informacije potrebne za prijenos podataka, čineći ga mnogo manjim i bržim za obradu u usporedbi s TCP-om.



Slika 3.4. UDP protokol

UDP zaglavlje sastoji se od samo četiri osnovna polja:

- Izvorni port (16 bita) identificira izvorni port na uređaju koji šalje podatke.
- Odredišni port (16 bita) identificira port na uređaju koji prima podatke.
- Duljina (16 bita) ukazuje na ukupnu duljinu UDP paketa, uključujući i zaglavlje i podatke. Minimalna duljina je 8 bajtova (veličina zaglavlja).
- Kontrolna suma (*Checksum*, 16 bita) je opcionalno polje u IPv4, ali obavezno u IPv6 te služi za provjeru integriteta podataka i zaglavlja.

UDP ne osigurava isporuku paketa, njihov ispravan redoslijed ili zaštitu od dupliciranja. Ako se paket izgubi ili ošteti tijekom prijenosa, UDP ga neće ponovno poslati, niti će prijemnik obavijestiti pošiljatelja o gubitku. Ovaj nedostatak pouzdanosti omogućava postizanje većih brzina i niže latencije. Primjerice, VoIP aplikacije koriste UDP jer korisnici preferiraju kontinuirani prijenos glasa s minimalnim kašnjenjem, čak i ako to znači da će neki dijelovi razgovora biti izgubljeni. Još jedna prednost UDP-a je njegova podrška za multicast prijenos. Multicast omogućava slanje jednog paketa podataka grupi prijemnika, što je korisno za aplikacije poput IPTV-a ili webinara.

Budući da ne postoji mehanizam za kontrolu protoka ili zagušenja, aplikacije koje koriste UDP uobičajeno implementiraju vlastite metode za kontrolu prijenosa podataka prilagođavajući ih specifičnim potrebama aplikacije. Na primjer, aplikacija može koristiti vlastite algoritme za kontrolu protoka kako bi osigurala optimalnu brzinu prijenosa podataka u realnom vremenu.

4. MREŽNA MJERENJA I ALATI

U radu mreže može nastati čitav niz problema poput problema s hardverom, mrežnim kablovima, neispravnim mrežnim uređajima, pogrešnim konfiguracijama, zagušenjima u mrežnom prometu itd. Kako bi se rano identificirali potencijalni problemi, optimizirali resursi te mogli planirati budući kapaciteti, potrebno je kontinuirano vršiti mjerenja mrežnih performansi. Osim navedenih razloga, mjerenja mrežnih performansi služe i za poboljšanje korisničkog iskustva te detekciju sigurnosnih problema na mreži poput DdoS napada ili neovlaštenih pristupa. U sljedećim poglavljima bit će objašnjena najvažnija mrežna mjerenja te alati koji se korite u praksi.

4.1. Mrežna mjerenja

Latencija, gubitak paketa, propusnost, i jitter samo su neki od parametara koji se analiziraju tijekom mrežnih mjerenja. Bez točnih podataka o ovim parametrima, teško je utvrditi jesu li mrežni resursi optimalno iskorišteni te postoje li problemi koji bi mogli utjecati na pravilan rad mreže. Analizom mrežnih podataka mogu se identificirati uska grla, preopterećene veze ili neučinkovita distribucija resursa, te se na temelju tih informacija mogu donijeti odluke o nadogradnji mrežne opreme, promjeni mrežne topologije ili uvođenju novih tehnologija koje će povećati ukupnu učinkovitost mreže.

4.1.1. Latencija

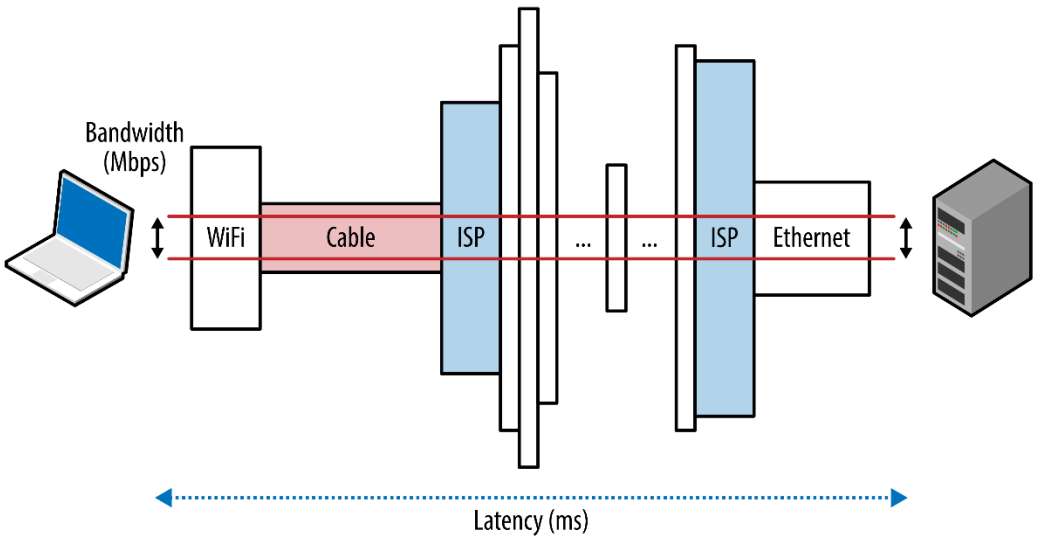
Latencija ili kašnjenje predstavlja vrijeme koje je potrebno da jedan paket podataka stigne od izvora do odredišta. To vrijeme, iako se mjeri u milisekundama, može značajno utjecati na način na koji doživljavamo mrežne usluge i aplikacije. Mreža može imati vrlo visoku propusnost, odnosno sposobnost prijenosa velike količine podataka u sekundi, ali ako latencija između dva krajnja uređaja na mreži nije dovoljno niska, korisnici mogu doživjeti kašnjenja ili zastoje u radu aplikacija. Posebno je kritična u aplikacijama koje zahtijevaju trenutnu reakciju poput online igara ili video komunikacija. Glavni uzrok latencije je fizička udaljenost između izvora i odredišta. Što je udaljenost veća, to je vrijeme potrebno da podaci putuju između točaka također veće. Osim toga, mrežni uređaji kroz koje podaci prolaze, poput usmjernika i preklopnika, također mogu pridonijeti latenciji zbog vremena potrebnog za obradu i prosljeđivanje paketa. Također, zagušenja na mreži mogu uzrokovati povećanje latencije. Kada previše podataka prolazi kroz određenu točku u mreži, dolazi do usporavanja i povećanja vremena čekanja, jer

mrežni uređaj mora obraditi svaki paket prije nego što ga proslijedi dalje. To se posebno može dogoditi tijekom vršnih opterećenja, kada mnogi korisnici istovremeno koriste istu mrežnu infrastrukturu.

Latencija također ima utjecaj na algoritme za kontrolu toka, poput TCP kontrole toka, koji su dosta osjetljivi su na veličinu latencije. Visoka latencija može smanjiti brzinu prijenosa, čak i ako mreža ima visoku propusnost, jer sustavi moraju čekati potvrdu da su prethodni podaci uspješno stigli prije nego što mogu poslati nove. Korisnici mogu primijetiti latenciju na mnogo načina poput sporog učitavanja web stranica, videozapisa koji se prekidaju ili preskaču dijelove komunikacije te kašnjenja koje ometa razgovor kod glasovnih poziva. Kroz optimizaciju mrežnih ruta, korištenje bržih mrežnih uređaja i tehnologija te smanjenje zagušenja, moguće je značajno smanjiti latenciju i poboljšati korisničko iskustvo.

Latenciju se u mrežnim mjerenjima uobičajeno mjeri na dva načina:

- *one way delay* – jednosmjerna latencija os izvora do odredišta. Ova vrsta testa mjeri kašnjenje odvojeno za svaki smjer putanje. Uobičajeno se kao alat za mjerenje koristi OWAMP klijent
- *two way delay – Round Trip Time* (RTT) je jedan od pokazatelja performansi mreže koji mjeri ukupno vrijeme potrebno da paket stigne od izvora do odredišta i natrag do izvora.

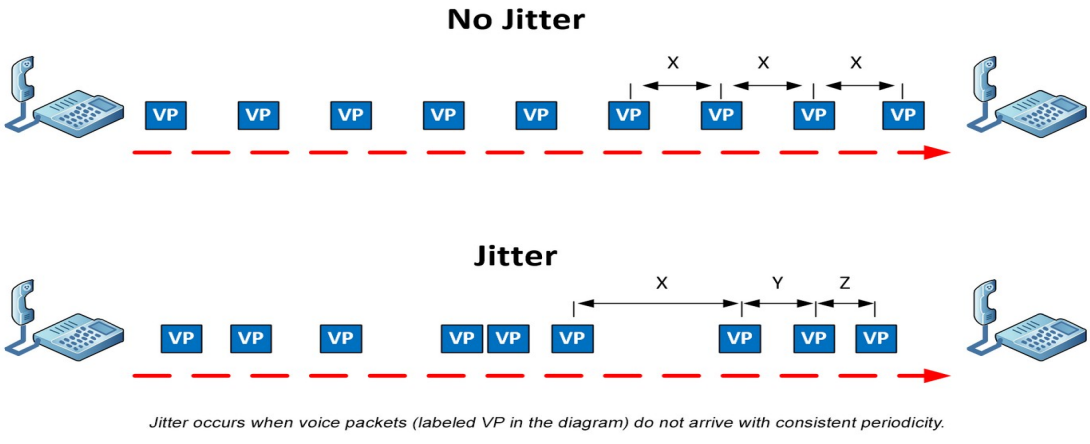


Slika 4.1. Grafički prikaz latencije

4.1.2. Jitter

Jitter (varijacija kašnjenja) se odnosi na varijacije u vremenu dolaska podatkovnih paketa unutar iste sesije. Paketi bi, u idelanom slučaju, od izvora do odredišta trebali stići u pravilnim vremenskim razmacima, jedan za drugim, kako bi se podaci mogli ispravno rekonstruirati na odredištu. Međutim, paketi često ne stižu u istom vremenskom intervalu zbog različitih mrežnih uvjeta, poput zagušenja, promjenama ruta kroz mrežu ili problema s mrežnim uređajima. Ova nepravilnost u vremenu dolaska paketa se naziva jitterom. Za mnoge mrežne aplikacije, mali jitter neće predstavljati problem. No, za aplikacije koje zahtijevaju pravodobnu isporuku podataka, poput VoIP-a, video konferencija ili online igranja, jitter može imati neželjene posljedice. Ako paketi ne stignu na vrijeme, može doći do prekida u zvuku, smrzavanja slike, ili čak gubitka podataka.

Postoje razne tehnike kojima se može umanjiti jitter, poput korištenja QoS (engl. Quality of Service) postavki koje daju prioritet prometu osjetljivom na kašnjenje ili korištenja jitter buffer-a. Jitter buffer je privremeno spremište na prijemnoj strani komunikacije koje prikuplja pakete i isporučuje ih u pravilnim intervalima, smanjujući tako učinak jittera na kvalitetu usluge. Međutim, preveliki jitter buffer može sam po sebi uzrokovati kašnjenja pa je ključno pravilno balansirati između smanjenja jittera i održavanja niske latencije. Jitter također može biti izazov u bežičnim mrežama, gdje su uvjeti prijenosa još promjenjiviji. Interferencije, udaljenost između uređaja i prepreke u prostoru mogu uzrokovati fluktuacije u vremenu dolaska paketa. Stoga su bežične mreže često osjetljivije na probleme s jitterom u usporedbi s žičanim mrežama.

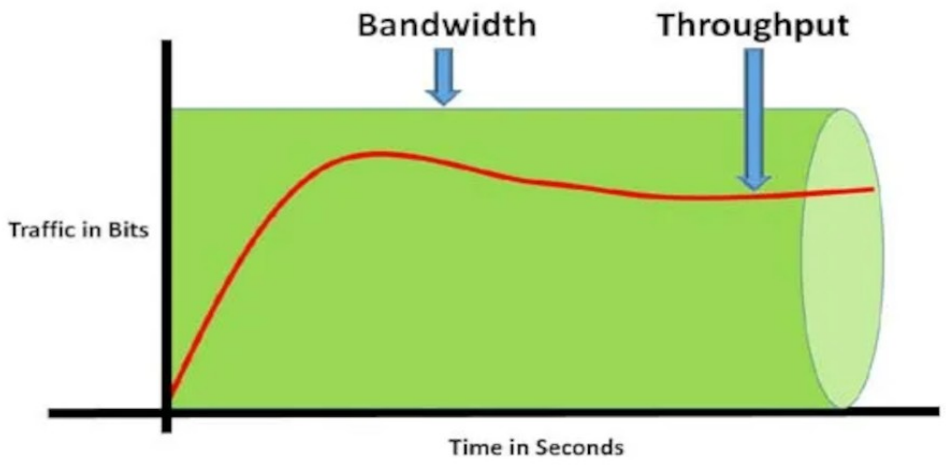


Slika 4.2. Grafički prikaz jittera

4.1.3. Propusnost

Propusnost (engl. throughput) predstavlja količinu podataka koja se može prenijeti s jednog mjesta na drugo unutar mreže u određenom vremenskom razdoblju, obično izražena u bitovima po sekundi (bps). Dok latencija i jitter služe za razumijevanje vremenskih aspekata prijenosa podataka propusnost nam govori koliko se podataka može prenijeti kroz mrežu. Propusnost je često prva stvar koju korisnici primjećuju kada procjenjuju kvalitetu svoje internetske veze. Kada preuzimamo datoteke, gledamo video sadržaje ili igramo online igre veća propusnost omogućava brži prijenos i bolju kvalitetu usluge. Primjerice, streaming visoko kvalitetnog videa zahtijeva značajnu količinu podataka da bi se osiguralo neprekinuto iskustvo gledanja. Ako propusnost nije dovoljno visoka, video može biti isprekidan, niske kvalitete ili čak potpuno prekinut. U poslovnim okruženjima, gdje se veliki volumeni podataka svakodnevno prenose između udaljenih lokacija, visoka propusnost je presudna za učinkovito poslovanje. Na primjer, u financijskim institucijama gdje se transakcije moraju obavljati u realnom vremenu, visoka propusnost osigurava da se podaci mogu brzo i sigurno prenijeti, minimizirajući kašnjenja. Propusnost mreže ovisi o više faktora. Fizička infrastruktura mreže, poput optičkih kabela, bakrenih žica ili bežičnih antena, postavlja fizičke granice na brzinu prijenosa podataka. Optički kabeli omogućuju mnogo veću propusnost u usporedbi s bakrenim kablovima zbog svoje sposobnosti prijenosa podataka putem svjetlosnih impulsa, što omogućuje prijenos na vrlo velike udaljenosti bez gubitka signala. Osim fizičke infrastrukture, mrežni protokoli i tehnologije također igraju ulogu u određivanju propusnosti. Moderni protokoli i tehnologije, poput 5G u mobilnim mrežama ili najnovijih Wi-Fi standarda, dizajnirani su za povećanje propusnosti i omogućavanje bržeg prijenosa podataka.

Kada previše korisnika pokušava koristiti iste mrežne resurse istovremeno, propusnost se dijeli između njih, što može uzrokovati usporavanja. Kada propusnost postane ograničavajući faktor, mrežni administratori mogu primijeniti različite tehnike za upravljanje prometom, poput prioritizacije prometa osjetljivog na kašnjenje ili korištenja tehnika kompresije podataka kako bi se maksimizirala iskorištenost dostupne propusnosti. Stalna mjerenja propusnosti nužna su za planiranje budućih razvoja mrežne infrastrukture i povećanje kapaciteta mreže.

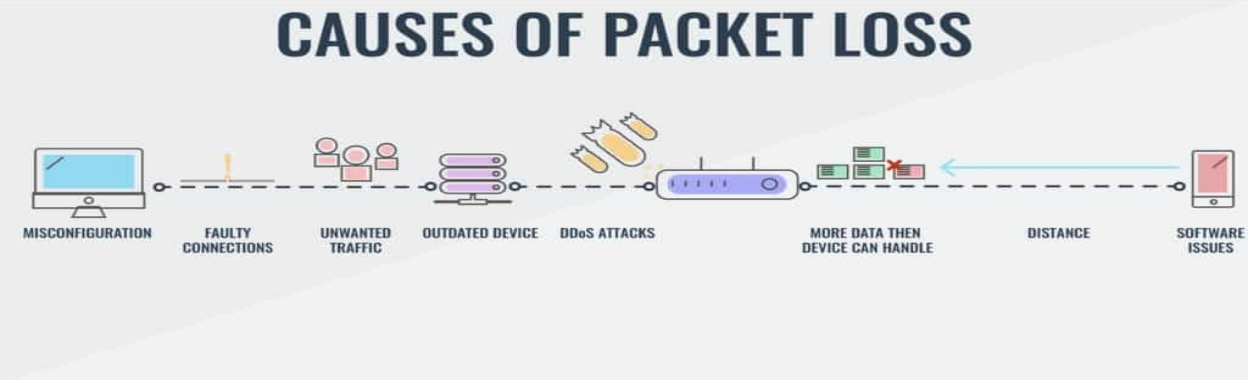


Slika 4.3. Grafički prikaz propusnosti

4.1.4. Gubitak paketa

Gubitak paketa (engl. packet loss) nastaje kada jedan ili više paketa ne uspije doći do svog odredišta tijekom prijenosa kroz mrežu. To može izazvati ozbiljne smetnje u različitim vrstama mrežnih aplikacija. Kada mreža funkcionira ispravno paketi dolaze do svog odredišta u pravilnom redoslijedu i bez gubitaka. Gubitak paketa može nastati iz više razloga. Jedan od najčešćih uzroka je zagušenje mreže. Kada previše podataka pokušava proći kroz istu mrežnu vezu, mrežni uređaji poput usmjernika i prekidača mogu postati preopterećeni i jednostavno odbaciti neke pakete kako bi se rasteretili. Osim zagušenja, gubitak paketa može nastati zbog oštećenih kabela, problema s hardverom ili softverom, ili interferencija u bežičnim mrežama.

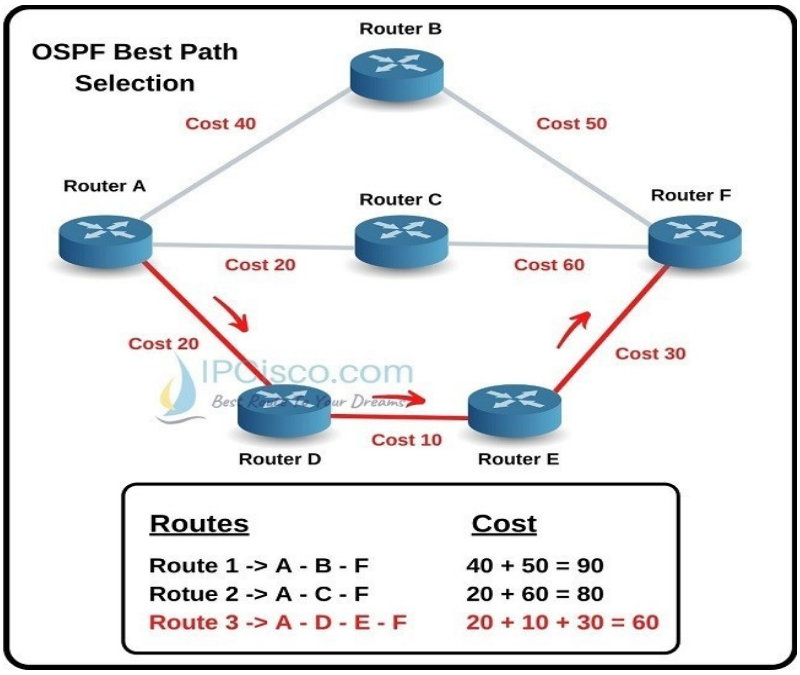
Kako bi se ublažio utjecaj gubitka paketa, koriste se različite tehnike. Jedna od osnovnih metoda je ponovno slanje izgubljenih paketa, što omogućava da primatelj ipak dobije sve potrebne podatke, iako uz nešto veće kašnjenje. Međutim, ova metoda nije uvijek prikladna za aplikacije koje zahtijevaju nisku latenciju, poput *real-time* video prijenosa ili online igranja. U tim slučajevima, koriste se tehnike poput ispravljanja pogrešaka ili *forward error correction* (FEC), gdje se dodatni podaci šalju zajedno s glavnim paketima kako bi se omogućilo rekonstrukciju izgubljenih informacija bez potrebe za ponovnim slanjem. Gubitak paketa također može poslužiti kao pokazatelj većih problema unutar mreže. Redovito praćenje i analiziranje gubitka paketa može pomoći mrežnim administratorima da prepoznaju i riješe potencijalne probleme prije nego što oni ozbiljno utječu na korisnike.



Slika 4.4. Grafički prikaz gubitka paketa

4.1.5. Put paketa kroz mrežu

Svaki paket sadrži dio podataka iz korisničkog zahtjeva, kao i informacije potrebne za njegovo usmjeravanje, poput IP adrese izvora i odredišta. Usmjernici na mreži analiziraju IP adresu odredišta unutar paketa i koriste tablice usmjeravanja kako bi odlučili gdje će poslati sljedeći paket. Taj proces usmjeravanja ponavlja se na svakom čvoru mreže kroz koji paket prolazi, a svaki usmjernik na putu donosi odluku o tome koja je najbolja ruta za paket prema odredištu. Put paketa nije uvijek linearan ili jednostavan. Paketi mogu putovati različitim rutama do odredišta, ovisno o trenutnim uvjetima u mreži, poput zagušenja ili kvarova. Mrežni uređaji koriste dinamičke protokole za usmjeravanje, poput BGP-a (engl. Border Gateway Protocol), kako bi se prilagodili promjenama u mreži i odabrali najefikasniji put. To znači da, iako paketi koji čine jednu cjelinu mogu biti poslani u istom trenutku, oni ne moraju nužno putovati istim putem i mogu stići na odredište u različito vrijeme. Nakon što su prošli kroz sve potrebne mrežne uređaje i segmente mreže, paketi stižu do odredišnog poslužitelja ili uređaja. Tu se ponovno sastavljaju u originalnu poruku ili podatke koje je korisnik poslao bilo da se radi o prikazu web stranice, isporuci e-pošte ili preuzimanju datoteke. Ako neki od paketa ne stigne na odredište ili je oštećen, protokoli poput TCP-a (engl. Transmission Control Protocol) mogu zahtijevati ponovno slanje tih paketa, osiguravajući cjelovitost podataka.



Slika 4.5. Grafički prikaz puta paketa kroz mrežu

4.2. Alati

4.2.1. Ping

Ping je osnovni mrežni alat koji se koristi za provjeru povezanosti između dva uređaja na mreži. Ime "*ping*" dolazi iz analogije sa sonarom, gdje se zvučni valovi šalju i čekaju povratak reflektiranog signala kako bi se izmjerila udaljenost do objekta. Na sličan način, ping šalje mrežni paket i mjeri vrijeme koje je potrebno da taj paket dođe do odredišta i vrati se nazad. Ovo vrijeme se naziva "round-trip time" (RTT).

Ping koristi Internet Control Message Protocol (ICMP) za slanje "*ECHO_REQUEST*" paketa od izvorišnog uređaja prema odredišnom uređaju. Kada odredišni uređaj primi *ECHO_REQUEST* on odgovara s "*ECHO_REPLY*" paketom koji se vraća natrag izvorišnom uređaju. Ping mjeri vrijeme potrebno za povratak paketa, tj. round-trip time (RTT). Ovo vrijeme daje korisnicima uvid u latenciju, odnosno kašnjenje u mrežnoj komunikaciji između dva uređaja.

Ako ping ne primi odgovor u određenom vremenskom razdoblju prijavljuje se gubitak paketa. Ping izvještava o postotku izgubljenih paketa tijekom testa, što može ukazivati na mrežne probleme poput zagušenja ili neispravnih mrežnih uređaja. Jednostavan je za korištenje, što ga

čini dostupnim i korisnim alatima za sve razine korisnika, od početnika do iskusnih mrežnih administratora. Prvi je alat koji se obično koristi za dijagnostiku mrežnih problema. Ako računalo ne može pristupiti određenoj mrežnoj adresi, ping može pomoći u utvrđivanju je li problem u povezivosti.

Evo nekoliko primjera kako se koristi:

- testiranje povezanosti s lokalnim mrežnim uređajem:
  ping 192.168.1.1
- testiranje povezanosti s web poslužiteljem:
  ping google.com
- kontinuirano pinganje dok se ne prekine (korisno za dugotrajni monitoring):
  ping -t google.com

4.2.2. Iperf3

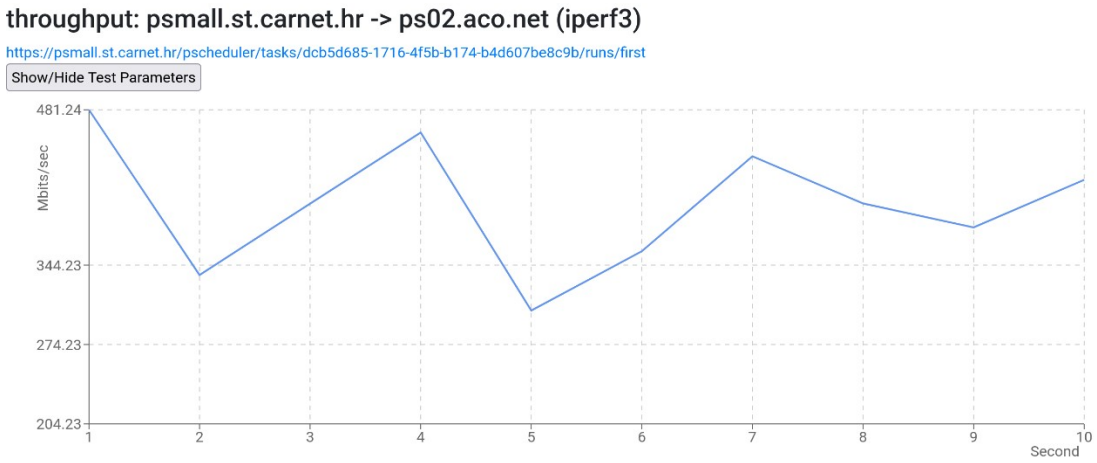
IPerf3 je alat za mjerenje i testiranje mrežnih performansi koji omogućuje korisnicima preciznu analizu propusnosti (engl. throughput) između dva krajnja uređaja na mreži. Često se koristi u različitim mrežnim okruženjima zbog svoje preciznosti i fleksibilnosti, a značajnu primjenu ima i u okviru PerfSONAR-a.

IPerf3 omogućuje mjerenje maksimalne propusnosti mreže između dva uređaja. Propusnost se mjeri u megabitima ili gigabitima po sekundi. Može testirati mrežnu propusnost u oba smjera: od klijenta prema poslužitelju i obrnuto. Podržava mjerenje propusnosti pomoću TCP i UDP protokola. TCP testovi su korisni za procjenu pouzdanosti veze, dok su UDP testovi korisni za testiranje kvalitete usluga osjetljivih na kašnjenje, kao što su VoIP i video streaming.

IPerf3 generira detaljna izvješća koja uključuju informacije o kašnjenju, jitteru (varijabilnosti kašnjenja), gubitku paketa i drugim relevantnim mrežnim metrikama. Omogućuje pokretanje više paralelnih mrežnih tokova (engl. streams) unutar jednog testa, što je korisno za simulaciju stvarnih mrežnih opterećenja i testiranje kapaciteta mreže. Također, omogućuje i postavljanje ograničenja na širinu pojasa tijekom testova, što može biti korisno za simulaciju specifičnih mrežnih uvjeta.

IPerf3 koristi jednostavnu poslužitelj-klijent arhitekturu. Jedan uređaj se pokreće u načinu rada poslužitelja (iperf3 -s), dok drugi uređaj djeluje kao klijent (iperf3 -c <IP-adresa poslužitelja>).

Klijent šalje podatke prema poslužitelju, a poslužitelj mjeri brzinu prijenosa. Kada klijent započne test, iPerf3 prenosi podatke između klijenta i poslužitelja i mjeri propusnost veze. Nakon završetka testa, iPerf3 prikazuje rezultate u prikladnom formatu.



Slika 4.6. *Troughput* mjeren pomoću iperf3

4.2.3. Nuttcp

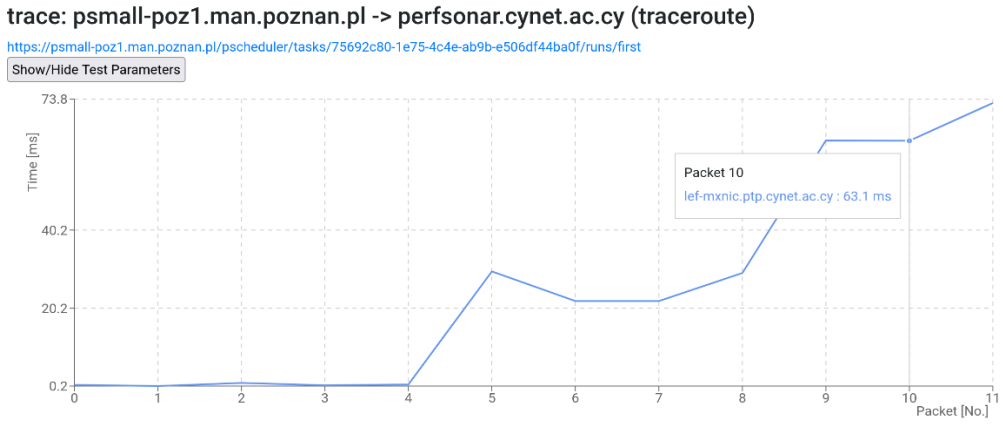
Nuttcp je mrežni alat za mjerenje propusnosti (engl. throughput) između dva uređaja na mreži. Slično kao i drugi mrežni alati, poput iPerf-a, nuttcp omogućuje preciznu analizu performansi mrežne veze uključujući prijenos podataka putem TCP ili UDP protokola. Alat je dizajniran za rad u okruženju komandne linije i često se koristi u svrhu dijagnostike mrežnih problema, testiranja mrežnih performansi, te optimizacije mrežnih resursa.

4.2.4. Traceroute

Traceroute je mrežni alat koji se koristi za praćenje puta (rute) kojim podatkovni paketi prolaze od izvorišnog do odredišnog uređaja. Ovaj alat je vrlo koristan za dijagnostiku mrežnih problema jer omogućuje korisnicima da vide svaku međutočku (čvor ili usmjerivač) kroz koju paket prolazi na putu do odredišta zajedno s vremenom koje je potrebno za prijenos paketa između tih točaka. Traceroute šalje niz ICMP (engl. Internet Control Message Protocol) ili UDP (User Datagram Protocol) paketa s niskim vremenskim ograničenjem (TTL - *Time To Live*). TTL određuje koliko "skokova" (engl. hops) paket može napraviti prije nego što bude odbačen. Svaki put kad paket stigne do rutera, TTL se smanjuje za 1. Kada TTL dosegne nulu, ruter odbacuje paket i vraća ICMP poruku o grešci (engl. Time Exceeded) natrag na izvorišni uređaj. Traceroute bilježi ovu poruku i tako određuje koji ruter je paket prošao. Traceroute započinje s TTL=1 i

postupno povećava TTL za svaki sljedeći paket. Na taj način svaki paket stigne jednu međutočku dalje nego prethodni, sve dok ne dosegne krajnje odredište. Na kraju, *traceroute* prikazuje popis svih rutera kroz koje je paket prošao, zajedno s vremenskim kašnjenjem za svaki skok. *Traceroute* mjeri vrijeme za svaki skok (obično u milisekundama), što omogućuje uvid u kašnjenje između svake međutočke. Ako postoji značajno povećanje kašnjenja ili prekid u ruti, to može ukazivati na problem u mreži.

Traceroute se često koristi za identificiranje točke na mreži gdje dolazi do problema, kao što su zagušenja, prekidi veze ili povećana latencija. Mrežni administratori mogu koristiti traceroute kako bi analizirali putove kojima podaci prolaze kroz mrežu, što može biti korisno za optimizaciju mrežne infrastrukture. Ako se ne može doći do određenog poslužitelja ili web stranice, *traceroute* može pomoći u otkrivanju gdje se točno gubi veza, bilo da je to na lokalnoj mreži, na strani davatelja internetskih usluga ili negdje drugdje. Usmjerivači mogu biti konfigurirani da ne odgovaraju na ICMP ili UDP pakete što znači da neće biti prikazani u rezultatima traceroute-a. Osim toga, put kojim podaci prolaze prema odredištu može se razlikovati od puta natrag do izvora, što također može otežati analizu. *Traceroute* može biti spor za mreže s mnogo skokova ili gdje postoji visoka latencija.



Slika 4.7. Mjerenje traceroute-a između Poljske i Cipra

4.2.5. Tracepath

To je mrežni alat sličan traceroute-u, ali s nekoliko ključnih razlika. Oba alata koriste se za praćenje puta koji podatkovni paketi prolaze od izvorišnog uređaja do odredišnog uređaja, prikazujući sve međutočke (čvorove ili usmjerivače) na tom putu.

Tracepath je dizajniran da bude jednostavniji za upotrebu i da ne zahtijeva administratorske privilegije što ga čini pristupačnijim za prosječne korisnike. *Tracepath* šalje UDP (engl. User Datagram Protocol) pakete prema odredištu s postepenim povećanjem vrijednosti TTL sličnim načinom kao i traceroute. TTL ograničava koliko "skokova" (engl. hops) paket može napraviti prije nego što bude odbačen. Jedna od posebnosti tracepath-a je automatsko podešavanje MTU-a (engl. Maximum Transmission Unit). Alat pokušava otkriti najmanju veličinu paketa koju svi čvorovi na putu mogu proslijediti bez fragmentacije. To je korisno za identificiranje mjesta gdje dolazi do fragmentacije paketa što može uzrokovati smanjenje mrežnih performansi.

Tracepath prikazuje sve međutočke na putu do odredišta, uključujući kašnjenje (latenciju) između svake točke. Ovaj prikaz pomaže korisnicima da vide gdje može doći do zastoja ili gubitka paketa. Tracepath može pomoći u prepoznavanju gdje dolazi do problema na mreži, bilo da se radi o visokoj latenciji, zagušenju ili fragmentaciji paketa.

4.2.6. Paris-traceroute

Paris-traceroute je napredni mrežni alat razvijen za praćenje rute kojom paketi prolaze kroz mrežu, ali s ciljem prevladavanja određenih ograničenja tradicionalnog traceroute alata. Iako oba alata imaju istu osnovnu funkciju – identificiranje međutočaka između izvorišnog i odredišnog uređaja – *Paris-traceroute* uvodi inovacije koje omogućuju točnije i pouzdanije praćenje rute u složenim mrežnim okruženjima, posebno onima s asimetričnim usmjeravanjem i složenim mrežnim topologijama. U modernim mrežama, posebno onima koje koriste složene mehanizme usmjeravanja standardni traceroute alat može prikazati netočne ili nepotpune rezultate. To se događa zbog načina na koji različite mrežne tehnologije, primjerice *load balancing*, obrađuju promet. Na primjer:

- Asimetrične rute**:** Traceroute može pokazati različite rute za pakete u dolaznom i odlaznom smjeru, što može zbuniti korisnike.
- *Load balancing***:** Mnoge mreže koriste load balancing (raspodjelu opterećenja) kako bi različiti paketi iz iste sesije mogli prolaziti različitim rutama, što može uzrokovati da traceroute prikazuje pogrešne ili promjenjive rute.

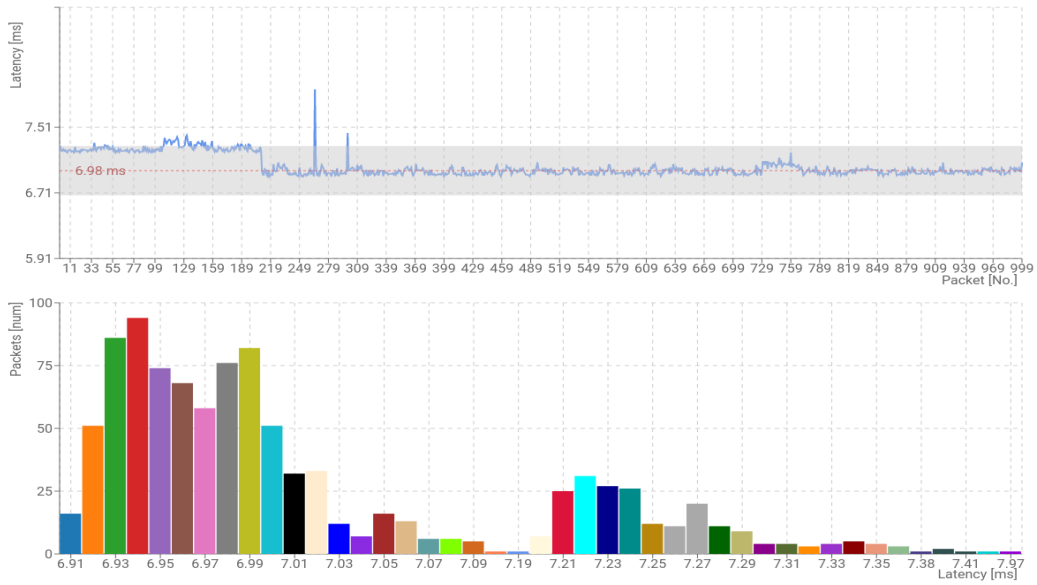
Paris-traceroute je razvijen kako bi se riješili ovi problemi omogućujući preciznije praćenje puta podataka kroz mrežu. Koristi specifične tehnike za održavanje dosljednosti putanje paketa

kroz mrežu. To se postiže očuvanjem konzistentnosti kodova koji se koriste u procesu odlučivanja rute, kao što su IP adresa izvora i odredišta, portovi, te ostali parametri. Alat osigurava da svi paketi koji pripadaju istom traceroute testu slijede istu rutu kroz mrežu, čak i u prisutnosti load balancing-a, što omogućuje precizno mapiranje rute. Paris-traceroute pruža detaljniji i točniji prikaz mrežne rute, minimizirajući mogućnost prikaza lažnih ili promjenjivih ruta.

4.2.7. Owping

Owping (engl. One-Way Ping) je mrežni alat koji se koristi za mjerenje jednosmjerne latencije, gubitka paketa i drugih ključnih mrežnih performansi između dva krajnja uređaja na mreži. Za razliku od standardnog ping alata koji mjeri obostranu (engl. round-trip) latenciju (vrijeme potrebno da paket stigne do odredišta i vrati se natrag), owping je dizajniran za mjerenje vremena koje je potrebno da paket stigne do odredišta u jednom smjeru. To omogućuje precizniju analizu mrežnih performansi, posebno u asimetričnim mrežama gdje latencija u jednom smjeru može biti značajno različita od latencije u suprotnom smjeru. Owping mjeri vrijeme potrebno da paket putuje od izvorišnog uređaja do odredišnog uređaja bez potrebe da se vraća nazad. Ovo je ključno za mreže gdje su uvjeti u jednom smjeru različiti od uvjeta u drugom, poput različitih putova za dolazni i odlazni promet. Alat također bilježi koliko se paketa gubi tijekom prijenosa između dva uređaja, što je važno za dijagnosticiranje problema s mrežom poput zagušenja ili nepravilnog usmjeravanja. Da bi owping precizno mjerio jednosmjernu latenciju, potrebno je da su satovi na izvorišnom i odredišnom uređaju vrlo precizno sinkronizirani. U tu svrhu, često se koristi Network Time Protocol (NTP) za usklađivanje vremena između uređaja.

Osim latencije i gubitka paketa owping može pružiti dodatne podatke kao što su varijabilnost kašnjenja (jitter)



Slika 4.8. Mjerenje kašnjenja paketa

4.2.8. Curl

Curl (engl. Client URL) je popularan alat za prijenos podataka putem različitih mrežnih protokola. Razvijen od strane Daniela Stenberga, curl je izuzetno koristan za rad s web resursima jer omogućuje korisnicima slanje zahtjeva prema web poslužiteljima i preuzimanje podataka izravno iz komandne linije. Alat je otvorenog koda i dostupan je na većini operativnih sustava, uključujući Linux, macOS i Windows.

Curl podržava širok spektar mrežnih protokola, uključujući HTTP, HTTPS, FTP, FTPS, SCP, SFTP, SMTP, POP3, IMAP i druge, što ga čini izuzetno fleksibilnim alatom za razmjenu podataka. Koristi se iz komandne linije što omogućuje jednostavno slanje zahtjeva prema web poslužiteljima i preuzimanje odgovora.

Curl naredbe su relativno jednostavne i lako se integriraju u skripte za automatizaciju zadataka. Podržava sve uobičajene HTTP metode, kao što su *GET, POST, PUT, DELETE, PATCH, HEAD, i OPTIONS*. To omogućuje njegovu integraciju s *RESTful API-jima* i drugim web servisima na različite načine. Podržava sigurne veze putem SSL/TLS protokola.

Curl pruža detaljne informacije o svakom koraku prijenosa podataka, što je korisno za debugiranje i analizu mrežnih problema. Alat može prikazati podatke o vremenu odgovora, statusnim kodovima, veličini preuzetih podataka i drugim važnim detaljima. *Curl* se često koristi

za preuzimanje datoteka s web poslužitelja. Jednostavnom naredbom, korisnici mogu preuzeti datoteku s bilo kojeg URL-a na svoj lokalni sustav:

```
-curl -O https://primjer.com/file.zip
```

Curl je koristan alat za testiranje *RESTful API-ja*. Omogućuje slanje zahtjeva različitih vrsta (*GET, POST, PUT*) s prilagođenim podacima i zaglavljima:

```
-curl -X POST -H"Content-Type: application/json"-
d'{"name":"Martina"}'https://api.primjer.com/users
```

Curl se često koristi u skriptama za automatizaciju zadataka, poput preuzimanja podataka iz web aplikacija, slanja e-mailova, ili ažuriranja podataka na udaljenim poslužiteljima. Curl se može koristiti za provjeru povezanosti s web poslužiteljem ili za ispitivanje odgovora poslužitelja:

```
-curl -I https://primjer.com
```

Curl omogućuje rad s HTTP kolačićima, što je korisno za sesijske operacije ili održavanje stanja aplikacije:

```
-curl -c cookies.txt https://primjer.com
```

5. perfSONAR SUSTAV ZA MJERENJE MREŽNIH PERFORMANSI

perfSONAR (engl. Performance focused Service Oriented Network monitoring ARchitecture) je distribuirani sustav za mjerenje mrežnih performansi koji se koristi za rješavanje mrežnih problema i optimizaciju mrežne infrastrukture ponajviše u istraživačkim i obrazovnim mrežama, ali i u raznim organizacijama i institucijama širom svijeta. Razvijen kroz međunarodnu suradnju nekoliko istraživačkih organizacija, perfSONAR omogućava korisnicima da prikupe, analiziraju i dijele podatke o performansama mreže na sustavan i standardiziran način.

5.1. Osnovne Karakteristike i Funkcionalnosti

perfSONAR se sastoji od nekoliko komponenti koje zajedno pružaju cjelovito rješenje za praćenje i analizu mrežnih performansi. Ove komponente uključuju alate za mjerenje poput nuttcp za mjerenje propusnosti, alata za testiranje latencije OWAMP, te ostale alate za mjerenje gubitka paketa i mrežna kašnjenja. Uz navedeno, perfSONAR podržava standardizirane protokole za prikupljanje i razmjenu podataka, što omogućava interoperabilnost između različitih mreža i sustava.

Jedna od ključnih prednosti perfSONAR-a je njegova distribuirana priroda. Mrežni administratori mogu postaviti perfSONAR čvorove na različitim dijelovima mreže kako bi kontinuirano pratili performanse između tih točaka. Ovo omogućava otkrivanje problema u realnom vremenu, poput povećane latencije ili gubitka paketa, te pruža detaljne uvide u performanse mreže kroz povijesne podatke. Ti podaci se zatim mogu koristiti za optimizaciju mrežne infrastrukture, planiranje kapaciteta, te brzo rješavanje problema kada se pojave.

5.2. Primjene i Prednosti

PerfSONAR se široko koristi u akademskim i istraživačkim mrežama, kao što su GEANT u Europi, Internet2 u SAD-u, te slične mreže u drugim regijama. Njegova sposobnost da pruži precizne i detaljne podatke o mrežnim performansama, te činjenica da je besplatan, čini ga idealnim alatom za mrežne inženjere i istraživače u akademskim krugovima koji trebaju održavati visoku kvalitetu usluge i osigurati neprekidan i brz prijenos podataka.

Na primjer, u znanstvenim istraživanjima koja uključuju ogromne količine podataka, kao što su fizika visokih energija (koristi se na CERN-u), perfSONAR omogućava istraživačima da brzo identificiraju i riješe probleme s povezivanjem koji bi mogli ometati prijenos podataka između

udaljenih lokacija. U obrazovnom kontekstu, sveučilišta koriste perfSONAR kako bi osigurali pouzdanu internetsku vezu za svoje studente i osoblje, posebno u slučajevima kada je potrebna veza s udaljenim resursima ili partnerima u istraživanju.

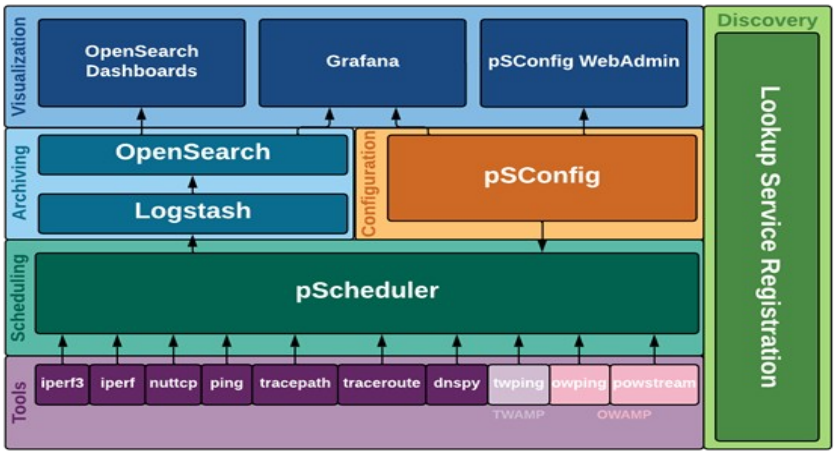
Osim akademskih primjena, perfSONAR se može koristiti i u komercijalnim mrežama, gdje može pomoći tvrtkama u praćenju i optimizaciji performansi svojih mrežnih infrastruktura. Tvrtke mogu koristiti perfSONAR kako bi pratili kvalitetu mrežnih usluga, otkrili uska grla ili identificirali probleme prije nego što oni negativno utječu na poslovanje.

Jedan od značajnih korisnika perfSONAR-a je i američko ministarstvo energetike (Esnet) koje povezivost svojih udaljenih lokacija prati upravo putem tog sustava.

5.3. Tehnička arhitektura i implementacija

PerfSONAR je izgrađen na modularnoj arhitekturi, koja omogućava lako proširenje i prilagodbu sustava specifičnim potrebama korisnika. Osnovna arhitektura uključuje različite tipove čvorova: mjerni čvorovi, arhivski čvorovi i klijentske aplikacije. Mjerni čvorovi su odgovorni za izvođenje različitih testova performansi mreže, dok arhivski čvorovi pohranjuju rezultate tih testova za kasniju analizu. Klijentske aplikacije omogućavaju korisnicima pristup i vizualizaciju podataka o performansama.

Jedna od ključnih značajki perfSONAR-a je njegova sposobnost integracije s drugim alatima i sustavima za upravljanje mrežama. To omogućava korisnicima da perfSONAR uključe u svoje postojeće sustave za nadzor i upravljanje, čime se dodatno povećava vrijednost podataka o mrežnim performansama.



Slika 5.1. Arhitektura perfSONAR sustava

Arhitektura perfSONAR-a može se podijeliti u šest elemenata:

- Alati
- Planiranje rasporeda mjerenja
- Arhiviranje
- Konfiguracija
- Vizualizacija
- Otkrivanje čvorova

5.3.1. Alati

Brojni pomoćni programi odgovorni su za izvođenje mrežnih mjerenja te čine temeljni sloj perfSONAR-a. Ovi alate se ne pozivaju izravno, već se koristi naredba pscheduler iz sloja planiranja rasporeda. Zadani alati koji dolaze s perfSONAR-om uključuju:

owamp - skup alata koji se koriste za mjerenje gubitka paketa i jednosmjernog kašnjenja; uključuje naredbu owping za pojedinačne kratkotrajne testove i naredbu powstream za dugotrajne pozadinske testove

twamp - alat koji se koristi za mjerenje gubitka paketa i dvosmjernog kašnjenja; ima veću točnost u odnosu na alate kao što je ping, a bez zahtjeva za sinkronizacijom sata kao što ih ima owamp

iperf3 – prerađen klasični iperf alat koji se koristi za mjerenje mrežne propusnosti i pridruženih metrika

iperf2 - uobičajeni alat koji se koristi za mjerenje propusnosti mreže koji postoji već mnogo godina

nuttcp - alat za mjerenje propusnosti s nekim korisnim opcijama kojih nema u drugim alatima

traceroute - alat za praćenje paketa koji se koristi za identifikaciju mrežnih putova

tracepath - alat za praćenje puta paketa na mreži koji također mjeri i MTU

paris-traceroute - alat za praćenje paketa koji pokušava identificirati put paketa na mreži u slučaju prisutnosti balansera opterećenja

ping – alat za određivanje dostupnosti, povratnog vremena (RTT) i gubitka paketa

Također, perfSONAR ima arhitekturu dodataka (plugina) koja podržava mnoge druge alate kao što su alati za mjerenje performansi DNS-a i HTTP-a.

5.3.2. Planiranje rasporeda mjerenja

pScheduler je servis koji je odgovoran za izvođenje mrežnih mjerenja ili općenito zadataka u perfSONAR-u. Kada treba pokrenuti mrežno mjerenje u perfSONAR sustavu, putem pscheduler klijenta iz naredbenog retka ili putem pScheduler API-ja zatraži se od pScheduler poslužitelja da u rasporedu mjerenja pronađe vremenski odsječak u kojem će se izvršiti traženo mjerenje (zadatak).

Poslužitelj pScheduler će koordinirati izvršenje i, po želji, pohranjivanje traženog zadatka. Alati koje pScheduler izvršava mogli bi se pokrenuti neovisno o njemu, ali pScheduler pruža dodane vrijednosti poput:

Integritet mjerenja - pScheduler održava raspored svih mjerenja koja se trebaju izvoditi i neće dopustiti da se mjerenja koja međusobno mogu negativno utjecati izvode istovremeno. Na primjer, dva testa propusnosti se neće izvoditi u isto vrijeme jer bi mogli utjecati na međusobne rezultate. Nasuprot tome, dva testa latencije se mogu pokrenuti u isto vrijeme jer niska potrošnja resursa ne utječe značajno na rezultate paralelnih testova.

Pojednostavljena koordinacija - pScheduler pojednostavljuje koordinaciju tijekom izvršenja zadatka, a nakon što pristigne rezultat, pScheduler će kontaktirati obje strane i po potrebi pokrenuti sve radnje.

Kontrola pristupa - pScheduler ima sustav ograničenja koji omogućuje definiranje pravila o tome tko može izvoditi koju vrstu mjerenja.

Dijagnostika - pScheduler nudi uvid u raspored koji održava, što znači da se može odrediti kada je zadatak bio pokrenut, je li trenutno pokrenut ili kada će se pokrenuti. Također, neko vrijeme čuva informacije o ishodu zadatka, uključujući i to je li rezultat bio neuspješan, što može biti korisno za dijagnosticiranje problema u infrastrukturi.

Proširivost – Plug-in arhitektura omogućuje pisanje dodataka za nove testove, alate i programe za arhiviranje.

5.3.3. Arhiviranje

perfSONAR sloj za arhiviranje je komponenta koja pohranjuje rezultate mjerenja kao podatke vremenske serije. Može biti integrirana unutar samog mjernog čvora ili postavljena kao jedna središnja instanca za više mjernih čvorova.

Prijašnje verzije perfSONAR-a su az arhiviranje koristile bazu esmond, a novijim razvojem perfSONAR-a uvedeno je pohranjivanje podataka u dobro poznati paket OpenSearch što je znatno proširilo mogućnosti istraživanja podataka, analiza i traženja korelacija.

5.3.4. Konfiguracija

Konfiguracijski sloj je mjesto gdje je moguće definirati željena mjerenja zajedno s uputama o tome gdje će se pohraniti njihovi rezultati. Primarna komponenta u ovom sloju zove se pSConfig. To je predložak za opisivanje i konfiguriranje topologije zadataka. Pri upravljanju s više perfSONAR čvorova (distribuirana zajednica perfSONAR mjernih čvorova), neki konfiguracijski zadaci mogu brzo postati nezgrapni. Primjerice, zakazivanje zadataka koje trebaju biti pokrenuti na svakoj lokaciji ili održavanje komponenti vizualizacije za prikaz rezultata mjerenja s više čvorova. pSConfig osigurava sljedeće agente za automatizaciju svakog od gore navedenih zadataka:

- pSconfig pScheduler Agent je agent odgovoran za čitanje predloška i konfiguriranje zadataka definiranih u pScheduleru.
- pSConfig Grafana Agent je agent odgovoran za čitanje predloška i konfiguriranje Grafane za prikaz rezultata definiranih zadataka na nadzornoj ploči.

5.3.5. Vizualizacija

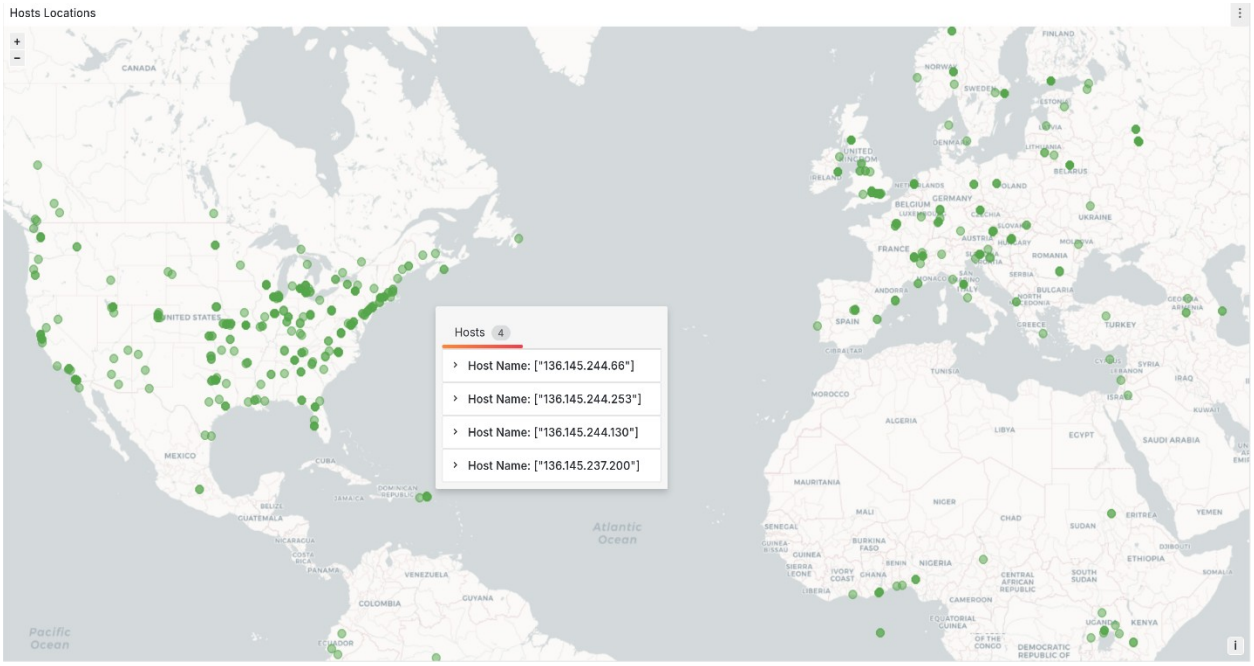
perfSONAR sustav uključuje komponente za vizualizaciju podataka koje pružaju uvid u podatke i služe kao primarni način za analizu i identifikaciju mrežnih problema. Primarni alati koje pruža perfSONAR su:

- Grafana – poznati programski okvir za izradu nadzornih ploča; prikazuje različita mjerenja tijekom vremena i pruža korisne informacije o uključenim čvorovima

- OpenSearch Dashbaords - sučelje za OpenSearch koje omogućuje pregled podataka

5.3.6. Otkrivanje čvorova (Lookup service)

Svaki perfSONAR čvor može pokrenuti komponentu koja se zove Lookup Service (LS) Registration Daemon. Ta komponenta prikuplja informacije o svakom perfSONAR sloju kao i o čvoru na kojem se izvodi te registrira svoje postojanje u javnoj i/ili privatnoj usluzi pretraživanja.



Slika 5.2. Primjer *Lookup* servisa

6. INSTALACIJA SUSTAVA I PRIMJERI MJERENJA

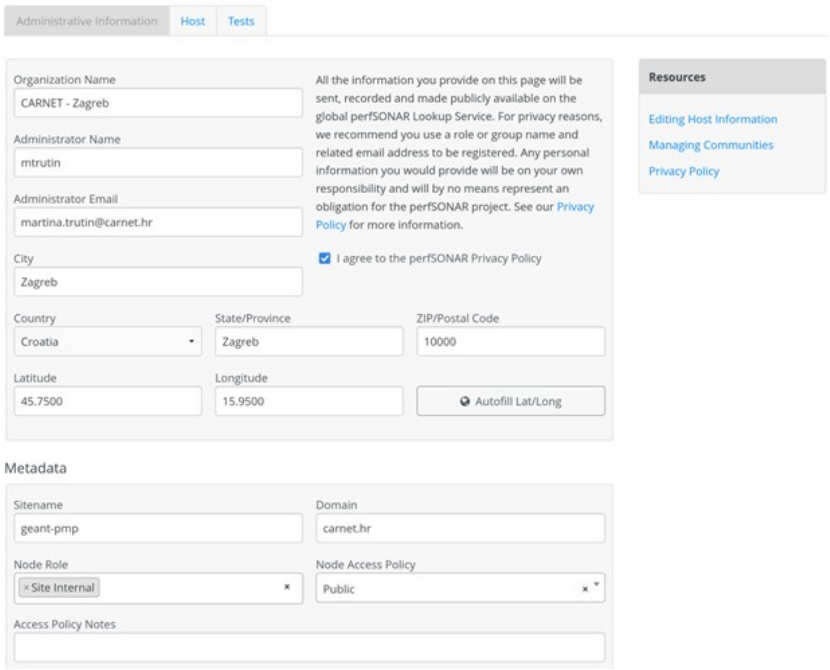
Za potrebe diplomskog rada izvršena je instalacija perfSONAR sustava.

6.1. Instalacija

PerfSONAR se najčešće instalira na serverima s Linux operativnim sustavom, a službeno podržane distribucije su Alma i Rocky linux te Debian i Ubuntu. Prije same instalacije, potrebno je osigurati da je operativni sustav ažuriran te da su svi potrebni paketi i ovisnosti pravilno instalirani. Također je potrebno osigurati stabilnu mrežnu vezu i dovoljno resursa na serveru, jer perfSONAR zahtijeva značajnu procesorsku snagu i memoriju. Nakon pripreme okruženja, slijedi instalacija softvera. Postupak uključuje dodavanje perfSONAR-ovih repozitorija, instalaciju osnovnih paketa i konfiguraciju sustava. Konfiguracija uključuje postavljanje osnovnih parametara poput mrežnih sučelja koja će se koristiti za testiranje, definiranje testova koji će se provoditi (poput *latency* testa, *throughput* testa i sl.), te konfiguraciju rasporeda testiranja.

6.2. Konfiguracija

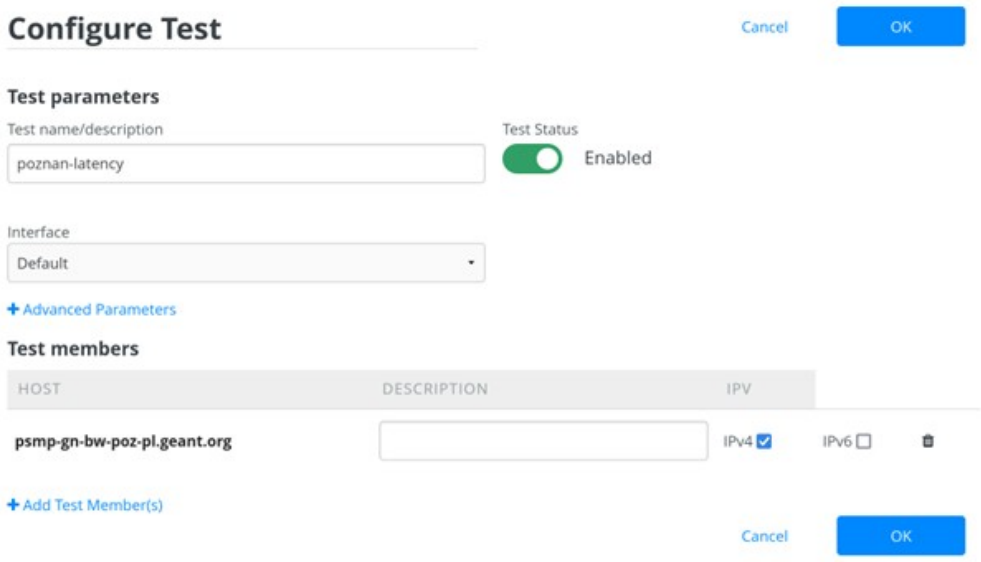
Konfiguracija je relativno jednostavna i radi se dodavanjem nekoliko osnovnih podataka o računalu na kojem se izvršava program. Dodaju se parametri poput imena računala, domene, geolokacije računala te organizacije i administratora.



Slika 6.1. Primjer administratorske konfiguracije perfSONAR sustava

Osnovna funkcija perfSONAR sustava je dodavanje mjerenja koja se periodički izvršavaju u raspored izvršavanja (pScheduler). Mjerenja je moguće dodati putem grafičkog sučelja. Pri dodavanju mjerenja potrebno je definirati sljedeće parametre:

- Vrsta mjerenja
- Naziv mjerenja
- mrežno sučelje s kojeg će se izvršavati mjerenje
- Mrežni čvor koji je uključen u mjerenje
- Verziju IP protokola (IPv4 ili IPv6)
- ostale nužne parametre vezane za pojedinu vrstu mjerenja



Slika 6.2. Primjer konfiguracije mjerenja latencije između poslužitelja i mrežnog čvora

6.3. Primjeri mjerenja

PerfSONAR omogućava konfiguraciju i postavljanje rasporeda mjerenja putem grafičkog korisničkog sučelja. Osim tog načina dozvoljeno je i direktno pokretanje mjerenja iz komandne linije. U sljedećim poglavljima navedeni su primjeri pokretanja pojedinih mjerenja.

6.3.1. Primjeri mjerenja iz komandne linije

Mjerenja iz komandne linije pomoću perfSONAR alata omogućuju korisnicima da provode razne mrežne testove izravno s terminala, pružajući fleksibilnost i preciznu kontrolu nad postupkom testiranja. Ova metoda omogućuje brzu prilagodbu parametara testa, praćenje rezultata u stvarnom vremenu, te lakoću automatizacije i integracije testova u složenije mrežne skripte i procese. Time se korisnicima omogućuje učinkovita dijagnostika i optimizacija mrežnih performansi bez potrebe za grafičkim sučeljima ili dodatnim alatima.

6.3.1.1. RTT mjerenje između instaliranog sustava i čvora u Irskoj

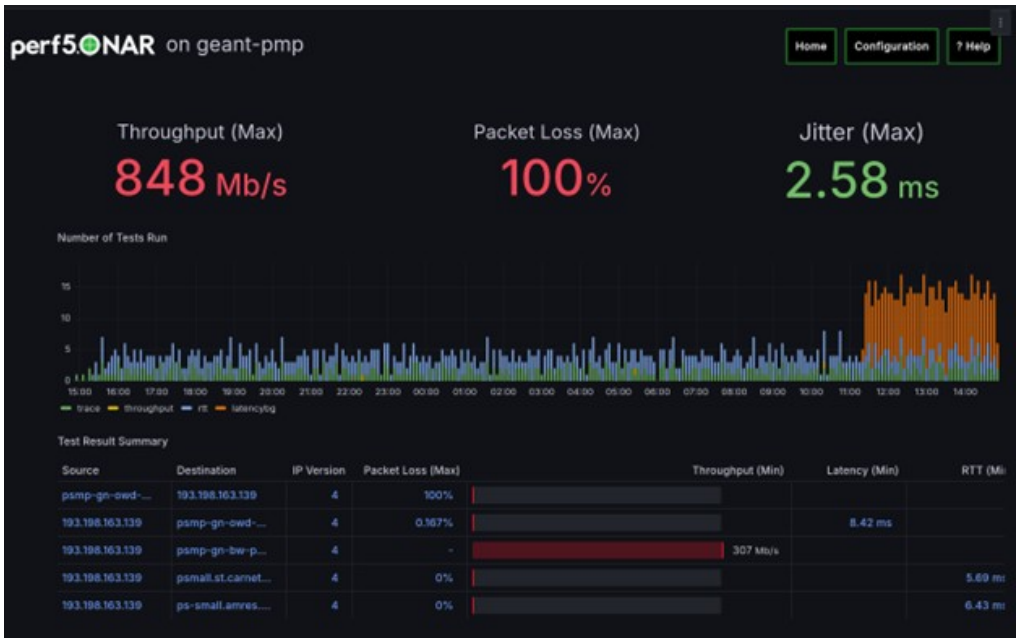
```
mtrutin@geant-pmp:~$ pscheduler task rtt --dest bob.heanet.ie
Submitting task...
Task URL:
https://geant-pmp/pscheduler/tasks/a8c7bd53-a8a4-4ca3-8c65-de50e92d2e9f
Running with tool 'ping'
Fetching first run...

Next scheduled run:
https://geant-pmp/pscheduler/tasks/a8c7bd53-a8a4-4ca3-8c65-de50e92d2e9f/runs/
216470fe-4e4a-4733-9f5b-06a7b2ba2d52
Starts 2024-08-26T18:16:24+02:00 (~3 seconds)
Ends   2024-08-26T18:16:34+02:00 (~9 seconds)
Waiting for result...

1       bob.heanet.ie (193.1.33.6)  64 Bytes  TTL 50  RTT 41.7000 ms
2       bob.heanet.ie (193.1.33.6)  64 Bytes  TTL 50  RTT 41.2000 ms
3       bob.heanet.ie (193.1.33.6)  64 Bytes  TTL 50  RTT 41.1000 ms
4       bob.heanet.ie (193.1.33.6)  64 Bytes  TTL 50  RTT 41.1000 ms
5       bob.heanet.ie (193.1.33.6)  64 Bytes  TTL 50  RTT 41.1000 ms

0% Packet Loss  RTT Min/Mean/Max/StdDev = 41.0930/41.2390/41.7040/0.2330 ms

No further runs scheduled.
```

6.3.1.2. Mjerenje propusnosti između instaliranog sustava i čvora u Gruziji

```
mtrutin@geant-pmp:~$ pscheduler task throughput --dest perfsonar.grena.ge
Submitting task...
Task URL:
https://geant-pmp/pscheduler/tasks/dba079b9-648e-49f2-89e0-c6c9cd75185f
Running with tool 'iperf3'
Fetching first run...

Next scheduled run:
https://geant-pmp/pscheduler/tasks/dba079b9-648e-49f2-89e0-c6c9cd75185f/runs/
ac9c8522-14ed-4ce5-95ab-eaf5ca3b7603
Starts 2024-08-26T18:21:41+02:00 (~6 seconds)
Ends   2024-08-26T18:22:00+02:00 (~18 seconds)
Waiting for result...

* Stream ID 5
Interval       Throughput     Retransmits    Current Window
0.0 - 1.0      53.42 Mbps     1333           241.80 KBytes
1.0 - 2.0      34.60 Mbps     0              249.60 KBytes
2.0 - 3.0      33.55 Mbps     19             133.90 KBytes
3.0 - 4.0      23.07 Mbps     0              153.40 KBytes
4.0 - 5.0      23.07 Mbps     0              200.20 KBytes
5.0 - 6.0      34.60 Mbps     0              321.10 KBytes
6.0 - 7.0      35.65 Mbps     90             193.70 KBytes
7.0 - 8.0      23.07 Mbps     0              224.90 KBytes
8.0 - 9.0      34.60 Mbps     0              323.70 KBytes
9.0 - 10.0     34.56 Mbps     102            224.90 KBytes

Summary
Interval       Throughput     Retransmits    Receiver Throughput
0.0 - 10.0     33.02 Mbps     1544           30.75 Mbps

No further runs scheduled.
```

6.3.2. Primjeri mjerenja iz grafičkog sučelja

Rezultati mjerenja dostupni su putem grafičkog sučelja Grafana. Primjer rezultata mjerenja konfiguriranih na poslužitelju prikazan je na sl.**6.3.**



Slika 6.3. Primjer uvida u rezultate mjerenja kroz grafičko sučelje Grafana

Grafana je program otvorenog koda koji se koristi za vizualizaciju i analizu podataka iz različitih izvora. Grafana korisnicima omogućava kreiranje prilagođenih nadzornih ploča (dashboards) s grafovima, kartama i drugim vizualnim elementima kako bi se moglo pratiti performanse sustava ili aplikacija. Grafana podržava širok raspon baza podataka, uključujući Prometheus, InfluxDB, Elasticsearch i Opensearch koji se koristi u perfSONAR-u. Intuitivna sučelja i jednostavna integracija s mnogim alatima za monitoring čine je popularnim alatom za praćenje metrika u stvarnom vremenu i postavljanje upozorenja na temelju definiranih praga performansi.

perfSONAR sustav unutar Grafane donosi unaprijed pripremljene nadzorne ploče prilagođene rezultatima mrežnih mjerenja. Osim tih unaprijed pripremljenih grafova korisnik može konfigurirati svoja sučelja prema specifičnim potrebama koristeći neke od stotina dostupnih grafova, dijagrama, panela iz Grafane.

7. ZAKLJUČAK

perfSONAR sustav je sustav otvorenog koda, lako dostupan i jednostavan za instalaciju i konfiguraciju. Objedinjuje niz alata za mjerenje mrežnih performansi uz pravljenje rasporeda mjerenja te spremanje rezultata mjerenja. Vizualizacija rezultata omogućava administratorima jednostavnu analizu te alarmiranje u slučaju problema u radu mreže. Sve te karakteristike učinile su da perfSONAR postane jedan od prvih izbora za mrežne nadzorne sustave na velikom broju akademskih i istraživačkih institucija.

U ovom radu prikazana je instalacija i konfiguracija perfSONAR sustava te su demonstrirani razultati mjerenja prikazani kroz grafičko sučelje. Pri izradi ovog rada pokazalo se da je sustav zaista jednostavan za instalaciju i korištenje, ali da istovremeno ima sve ono potrebno što ga čini nadzornim alatom koji se može koristiti u poslovnom okruženju.

LITERATURA

[1] User Guide for perfSONAR 5.1.2, https://docs.perfsonar.net/index.html (10.07.2024.)

[2] Open systems Interconnection: Basic reference model ISO/IEC 7498-1:1994

[3] IPv4 zaglavlje, https://en.wikipedia.org/wiki/IPv4 (15.07.2024.)

[4] IPv4 zaglavlje, https://en.wikipedia.org/wiki/IPv6 (15.07.2024.)

[5] TCP, https://en.wikipedia.org/wiki/Transmission_Control_Protocol (20.07.2024.)

[6] UDP, https://en.wikipedia.org/wiki/User_Datagram_Protocol (20.07.2024.)

[7] iperf3, https://iperf.fr/ (23.07.2024.)

[8] curl, https://curl.se/ (28.07.2024.)

[9] latencija, https://hpbn.co/primer-on-latency-and-bandwidth/ (01.08.2024.)

[10] propusnost, https://aymensekhri.medium.com/throughput-versus-bandwidth-in-brief-cff52313f87 (01.08.2024.)

[11] gubitak paketa, https://www.ir.com/guides/what-is-network-packet-loss (02.08.2024.)

[12] put paketa kroz mrežu, https://ipcisco.com/lesson/ospf-cost-and-spf-algorithm/ (02.08.2024.)

[13] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, 1981

[14] Eddy, W., Ed., "Transmission Control Protocol (TCP)", STD 7, RFC 9293, DOI 10.17487/RFC9293, 2022

[15] Postel, J., "User Datagram Protocol", STD 6, RFC 768, DOI 10.17487/RFC0768, 1980