PANEVROPSKI UNIVERZITET APEIRON, BANJA LUKA
FAKULTET INFORMACIONIH TEHNOLOGIJA

Redovne studije
Smjer : "Inženjering Informacionih Tehnologija"

Predmet:
Napredne računarske mreže

Network Automation and Intent-Based Networking

(Seminarski rad)

Predmetni nastavnik
Doc.dr Dražen Marinković

Student: Pavlović Ivan
Br. Indeksa : 92-20/RITP-S

Banja Luka, Februar 2025

SADRŽAJ

UVOD

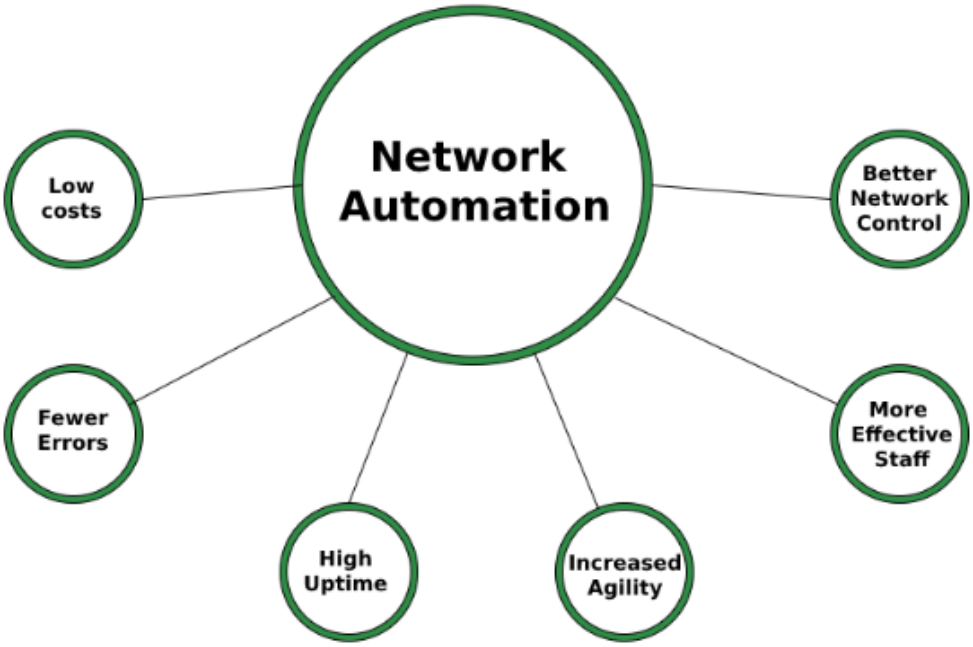
Savremene mreže postaju sve složenije uslijed rasta broja povezanih uređaja, povećanja obima saobraćaja i zahtijeva za visokom dostupnošću i sigurnošću. Tradicionalni pristupi upravljanja mrežom, koji se oslanjaju na manuelnu konfiguraciju i reaktivno rješavanje problema, postaju neodrživi u dinamičnim i skalabilnim okruženjima. Zbog toga se sve veći značaj pridaje mrežnoj automatizaciji, koja omogućava automatizovano upravljanje mrežnim resursima, minimiziranje ljudskih grešaka i poboljšanje efikasnosti rada.

Jedan od naprednih koncepata u oblasti mrežne automatizacije je Intent-Based Networking (IBN). Ovaj pristup transformiše način na koji se mreže konfigurišu i održavaju, omogućavajući mrežnim administratorima da definišu svoje ciljeve na visokom nivou, dok sistem automatski implementira i prilagođava konfiguracije u skladu sa zadatim parametrima. Integracijom vještačke inteligencije (AI) i mašinskog učenja (ML), IBN omogućava prediktivnu analizu, optimizaciju mrežnih performansi i proaktivno upravljanje mrežom.

U ovom seminarskom radu istražujemo ključne koncepte mrežne automatizacije i IBN-a, uključujući alate i tehnologije, razlike u odnosu na tradicionalne metode upravljanja mrežom, kao i sigurnosni aspekti i izazovi implementacije ovih sistema.

1. Mrežna automatizacija i Intent-Based Networking (IBN)

„Mrežna automatizacija odnosi se na upotrebu softverskih alata i skripti za automatizaciju konfiguracije, upravljanja, testiranja, implementacije i rada mrežnih uređaja i usluga. Cilj je smanjenje ljudske intervencije u obavljanju ovih zadataka, što rezultira povećanom efikasnošću, smanjenjem grešaka i bržim vremenom odaziva na promjene u mrežnom okruženju“ [1].



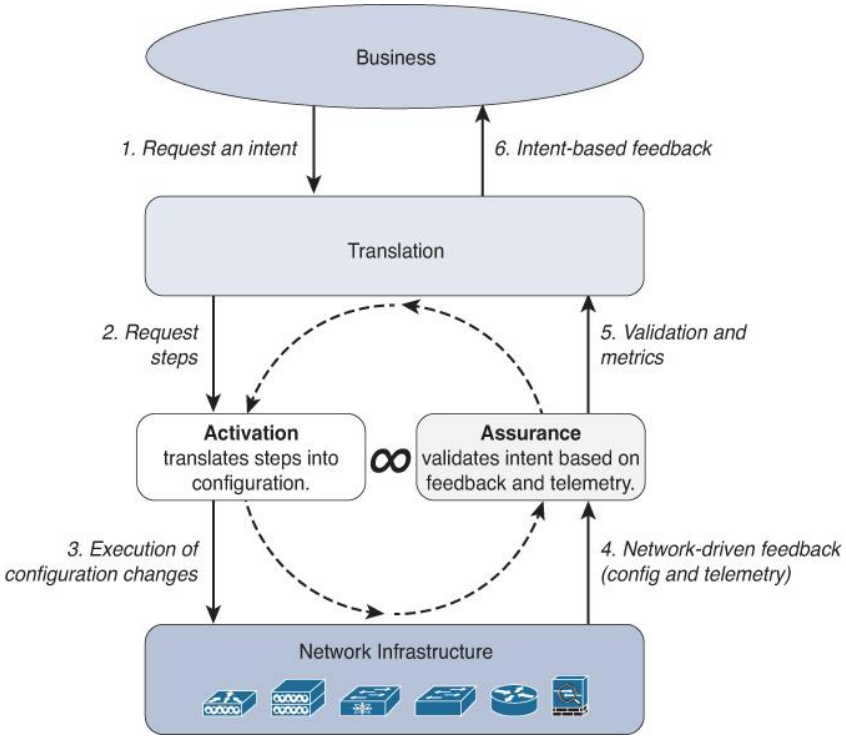
Slika 1 - Prednosti mrežne automatizacije

„Intent-Based Networking (IBN) predstavlja napredniji pristup upravljanju mrežama, gdje se fokus pomjera sa manuelne konfiguracije pojedinačnih uređaja na definisanje željenih ishoda ili poslovnih ciljeva, poznatih kao "intencije". Umijesto da administratori specificiraju tačne komande za konfiguraciju mreže, oni definišu visoko-nivojske intencije, a mreža se dinamički prilagođava kako bi ispunila te zahtijeve. IBN pojednostavljuje upravljanje složenim mrežama osiguravajući da mrežna infrastruktura bude usklađena sa željenim operativnim ciljevima. Administrator može navesti da želi sigurnu komunikaciju između dva segmenta mreže sa određenim nivoom propusnosti, a IBN sistem će automatski konfigurisati potrebne parametre kako bi ispunio tu intenciju“ [1].

„Ovaj pristup smanjuje potrebu za detaljnom manuelnom konfiguracijom i omogućava mreži da se automatski prilagođava promijenama u poslovnim zahtijevima ili uslovima rada. IBN koristi softverski omogućen proces automatizacije koji primjenjuje visoke nivoe inteligencije, analitike i orkestracije kako bi poboljšao rad mreže i njenu dostupnost“ [1].

„Kada operateri opišu poslovne ishode koje žele da postignu, mreža te ciljeve prevodi u potrebnu konfiguraciju bez potrebe za manuelnim kodiranjem i izvršavanjem pojedinačnih zadataka. Nakon toga, sistem pruža kontinuirane provjere između željenog i operativnog stanja mreže, koristeći zatvorenu petlju validacije kako bi neprestano verifikovao ispravnost konfiguracije“ [1].

IBN predstavlja evoluciju u odnosu na tradicionalno upravljanje mrežama, omogućavajući organizacijama da definišu svoje poslovne ciljeve na visokom nivou, dok mreža sama upravlja detaljima implementacije, što rezultira efikasnijim i agilnijim mrežnim operacijama.



Slika 2 - IBN sistematski pristup mreži

1.1. Razlozi za automatizaciju mreža

„Automatizacija mreža postaje ključna komponenta modernih IT sistema zbog sve veće kompleksnosti mrežnih infrastruktura i zahtijeva za bržim, sigurnijim i efikasnijim upravljanjem. Njene glavne prednosti uključuju“ [2]:

> „**Smanjenje ljudskih grešaka** - ručna konfiguracija mrežnih uređaja često dovodi do nenamjernih grešaka koje mogu uzrokovati ozbiljne probleme, uključujući sigurnosne ranjivosti i prekide u radu. Automatizovani sistemi osiguravaju doslijednost u konfiguraciji i smanjuju mogućnost pogrešnih unosa, što poboljšava pouzdanost mreže“ [2].
>
> „**Povećanje efikasnosti** - implementacija automatizacije omogućava brže izvršavanje mrežnih operacija, poput konfiguracije rutera i sigurnosnih politika. Time se smanjuje vrijeme potrebno za održavanje i omogućava IT timovima da se fokusiraju na strateške zadatke umjesto na rutinske operacije“ [3].
>
> „**Bolja skalabilnost** - kako organizacije rastu, njihova mrežna infrastruktura postaje sve složenija. Automatizacija omogućava upravljanje velikim mrežama bez proporcionalnog povećanja manuelnog rada. Na primjer, automatizovane skripte mogu istovremeno primjeniti konfiguracione promjene na stotine uređaja, umijesto da se svaka promjena unosi pojedinačno“ [2].

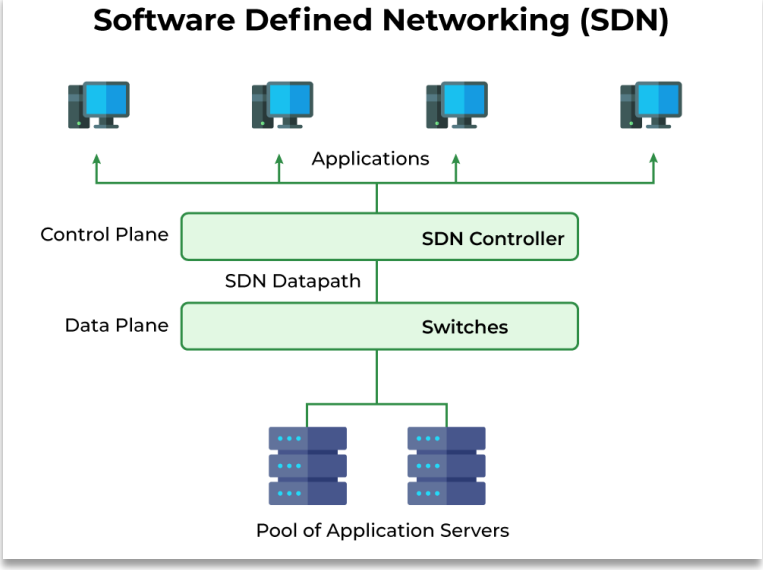
„**Brže rešavanje problema** - automatizovani sistemi mogu proaktivno pratiti performanse mreže i automatski otkrivati probleme prije nego što izazovu ozbiljne posljedice. Korištenjem analitike i viještačke inteligencije, mreže mogu predvidjeti potencijalne kvarove i odmah primjeniti korektivne mjere“ [2].

„**Smanjenje operativnih troškova** - optimizacijom radnih procesa i smanjenjem potrebe za manuelnim intervencijama, organizacije mogu značajno smanjiti troškove održavanja mrežne infrastrukture. Automatizacija također smanjuje potrebu za velikim timovima mrežnih administratora, jer se većina zadataka može izvršiti automatski“ [2].

1.2. Infrastruktura za mrežnu automatizaciju

Infrastruktura za mrežnu automatizaciju obuhvata skup tehnologija i alata koji omogućavaju automatizovano upravljanje i konfiguraciju mrežnih resursa. Ove tehnologije omogućavaju bolje praćenje, kontrolu i optimizaciju mrežnih performansi, smanjujući potrebu za manuelnim radom i ljudskim greškama. Ključne komponente infrastrukture uključuju:

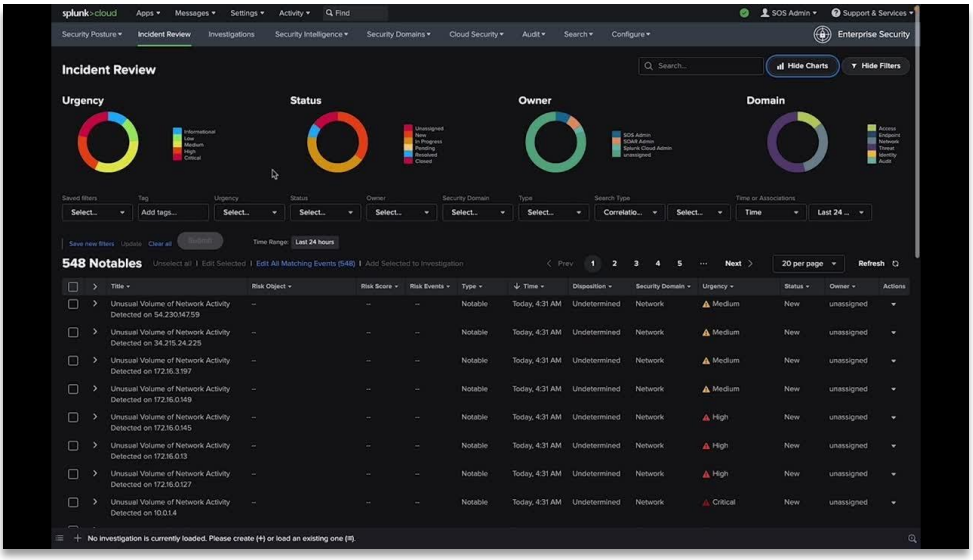
- „**Software-Defined Networking (SDN)** - SDN omogućava centralizovano upravljanje mrežom putem softverskog interfejsa, čime se omogućava dinamičko, fleksibilno upravljanje mrežnim resursima bez potrebe za promjenom fizičke infrastrukture“ [4].



Slika 3 - Prikaz SDN upravljanja mreže u praksi

- „**API-driven mreže** - korištenjem API-ja (Application Programming Interface), mrežni uređaji i aplikacije mogu se integrisati i automatski komunicirati, omogućavajući dinamičko i automatsko podešavanje mrežnih politika i konfiguracija“ [5].

- „**Monitorisanje** - omogućavaju prikupljanje podataka u stvarnom vremenu o stanju mreže, performansama i greškama. Monitoring omogućava proaktivno otkrivanje problema, dok monitoring pomaže u kontinuiranom praćenju i analizi mrežnih resursa“ [6].



Slika 4 - Vizuelni prikaz "Splunk" softvera za monitorisanje sistema

1.3. Evolucija mrežne automatizacije kroz vrijeme

Mrežna automatizacija se razvijala kako bi odgovorila na rastuće zahtijeve modernih IT infrastruktura. U početku, mreže su se upravljale manuelno, što je dovodilo do grešaka, nesigurnosti i velike složenosti, posebno u velikim organizacijama. Sa razvojem tehnologije, počelo je uvođenje automatizacije, koja je omogućila efikasnije upravljanje mrežama.

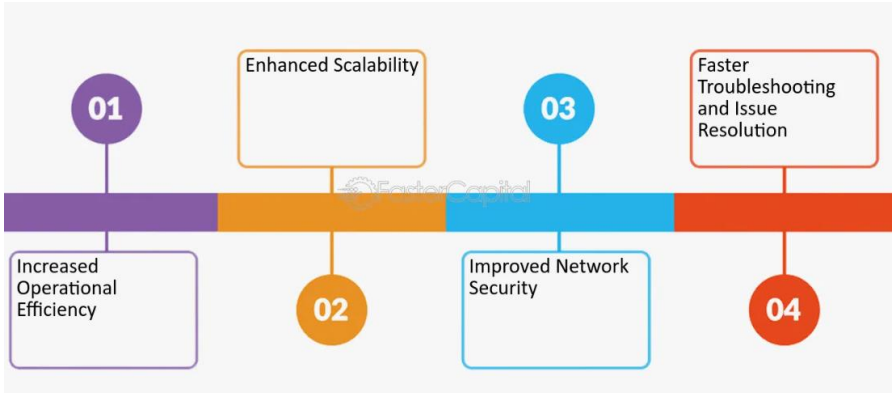
„Početci mrežne automatizacije kreću od 2000-ih godina, kada su uvođeni prvi alati za automatizaciju, kao što su script-based sistemi i programi zasnovani na komandnoj liniji, koji su omogućavali administrativnim timovima da upravljaju mrežama na daljinu, smanjujući potrebu za manuelnim podešavanjima. Ove tehnologije su omogućile bržu i precizniju konfiguraciju mreža, ali su i dalje zavisile od pojedinca za svaku promjenu i implementaciju“ [4].

„Naredna faza u razvoju bila je popularizacija Software-Defined Networking (SDN), koja je omogućila centralizovano upravljanje mrežnim resursima putem softverskog interfejsa. SDN se pojavljuje kao odgovor na složenost tradicionalnih mreža i omogućava jednostavniju, bržu i skalabilniju konfiguraciju, kao i bolju integraciju sa cloud tehnologijama i virtualizovanim mrežama. Kako je SDN evoluirao, tako su se razvijali i alati za upravljanje mrežom u realnom vremenu“ [5].

„Danas, sa pojavom Intent-Based Networking (IBN), mrežna automatizacija je postala još naprednija. IBN koristi AI i machine learning tehnologije kako bi omogućio autonomno odlučivanje u mreži, čineći je proaktivnom, dinamičnom i samopopravljajućom. Ove tehnologije omogućavaju mrežama da prepoznaju greške i automatski riješe probleme prije nego što utiču na performanse mreže“ [6].

2. Mrežna automatizacija

„Mrežna automatizacija podrazumijeva upotrebu softverskih rješenja za automatizaciju konfiguracije, upravljanja, testiranja, implementacije i rada mrežnih uređaja i usluga. Ovaj pristup omogućava mrežnim operaterima da efikasnije upravljaju mrežama uz smanjenje manuelnih zadataka, što rezultira smanjenjem ljudskih grešaka i povećanjem operativne efikasnosti“ [7] [8].

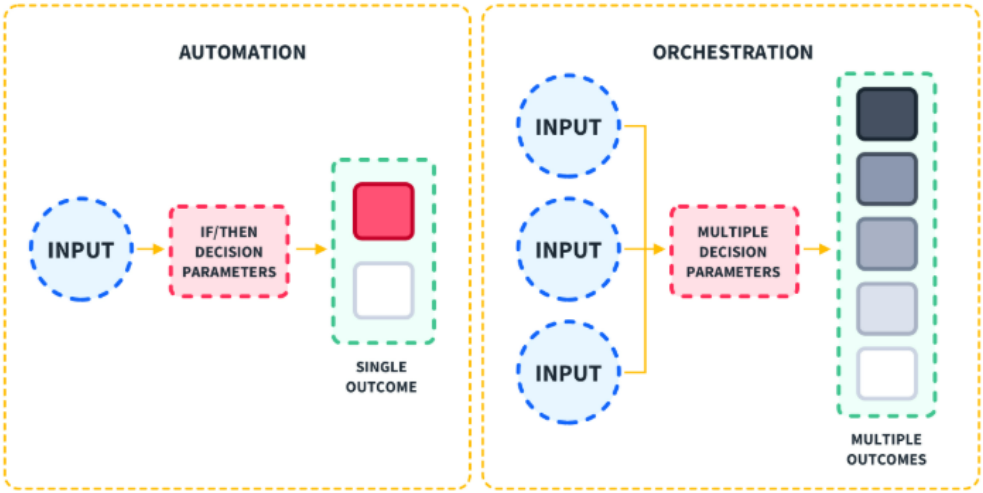


Slika 5 - Prednosti mrežne automatizacije

„Mrežna automatizacija obuhvata nekoliko ključnih koncepata i ciljeva koji omogućavaju efikasno i pouzdano upravljanje savremenim mrežama. Među njima se ističu orkestracija, konfiguracija i monitoring“ [7].

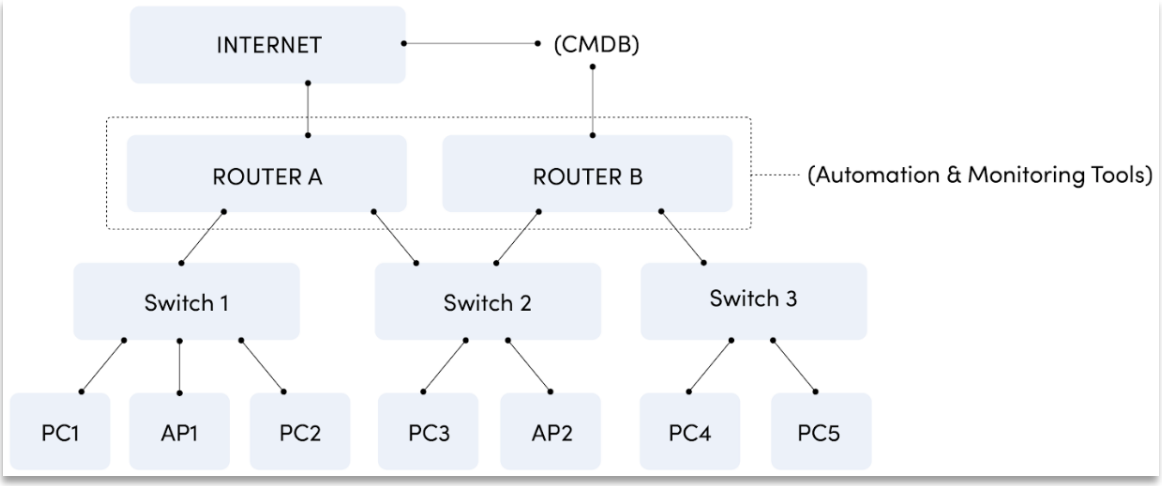
„Orkestracija predstavlja proces automatizacije koordinacije i upravljanja složenim mrežnim operacijama i uslugama. Cilj je integrisati različite mrežne komponente i procese kako bi se obezbijedilo njihovo usklađeno funkcionisanje“ [8].

„Orkestracija omogućava automatizovano upravljanje radnim tokovima, što smanjuje potrebu za manuelnim intervencijama i povećava operativnu efikasnost“ [9].



Slika 6 - Razlika između Automatizacije i orkestracije

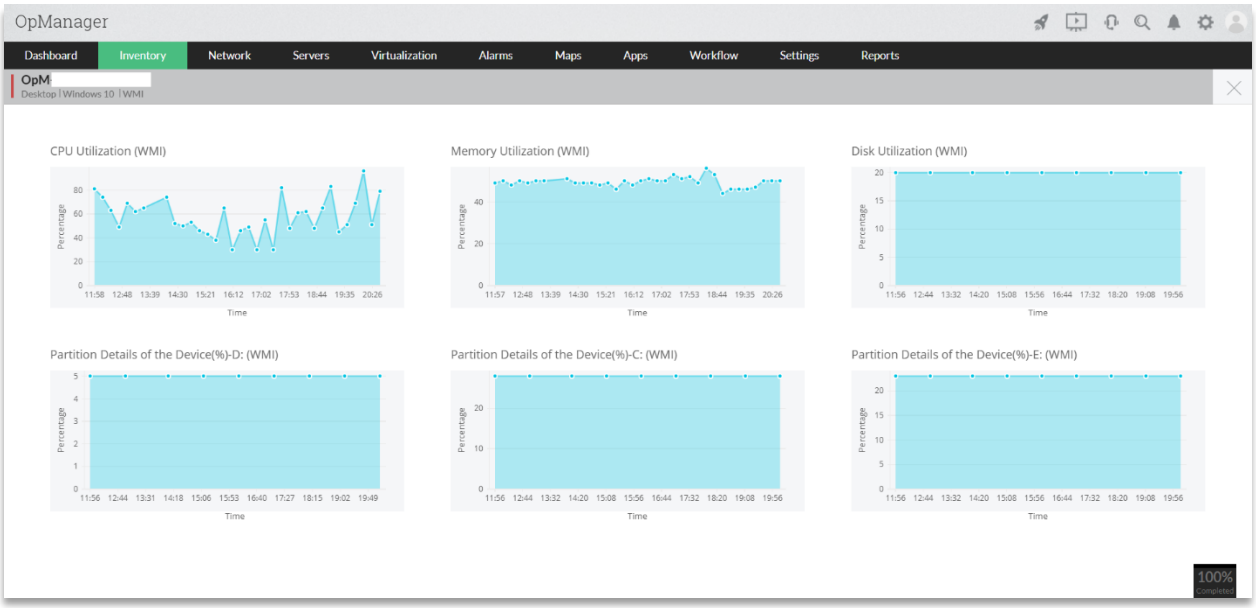
„Konfiguracija se odnosi na proces postavljanja i podešavanja mrežnih uređaja i servisa prema unaprijed definisanim parametrima. Automatizacija konfiguracije smanjuje rizik od ljudskih grešaka i omogućava brže implementacije promjena u mreži“ [10].



Slika 7 - Automatizovano dodjeljivanje mrežnih resursa

„Korištenjem alata za automatizaciju konfiguracije, administratori mogu dosljedno primjeniti standardizovane postavke na više uređaja istovremeno“ [11].

„Monitoring podrazumijeva kontinuirano praćenje performansi i stanja mrežnih komponenti. Automatizovani sistemi za monitoring prikupljaju podatke u realnom vremenu, omogućavajući proaktivno otkrivanje problema i brzu reakciju na potencijalne prijetnje ili anomalije [6]. Ovi sistemi često koriste napredne analitičke alate za predviđanje i prevenciju problema prije nego što utiču na korisnike“ [5].

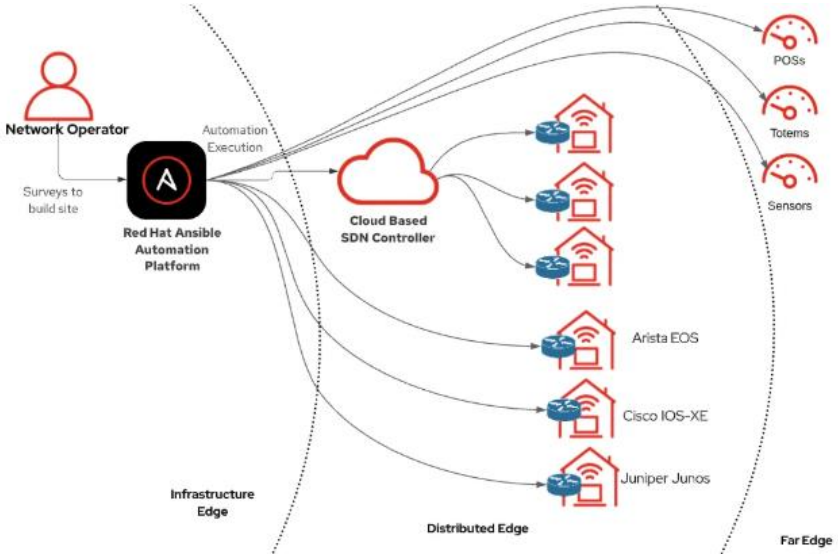


Slika 8 - Monitoring alat za praćenje u realnom vremenu

2.1. Alati i tehnologije za mrežnu automatizaciju

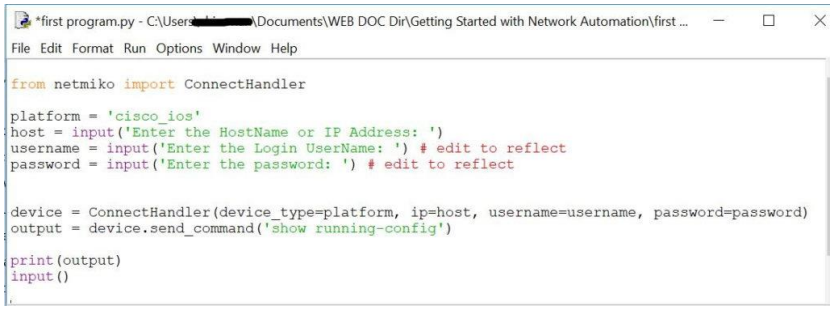
„Mrežna automatizacija se oslanja na različite alate i tehnologije koji omogućavaju efikasnije upravljanje mrežnim resursima, smanjenje manuelnog rada i povećanje sigurnosti i skalabilnosti mreža. Ključni alati koji se često koriste u mrežnoj automatizaciji uključuju **Ansible**, **Python**, **Netmiko** i **Napalm**“ [7].

„**Ansible** je alat otvorenog koda koji se koristi za automatizaciju konfiguracije mrežnih uređaja. Omogućava administratorima da definišu konfiguracione zadatke pomoću YAML playbook datoteka, čime se olakšava primjena konfiguracija na više uređaja istovremeno. Budući da ne zahtijeva instalaciju klijenta na mrežnim uređajima, Ansible se često koristi za orkestraciju velikih mrežnih infrastruktura“ [7].



Slika 9 - Primjena Ansible alata u automatizaciji mrežne konfiguracije

„**Python** je jedan od najčešće korišćenih programskih jezika za mrežnu automatizaciju. Pomoću Python skripti moguće je automatizovati različite mrežne operacije, poput prikupljanja podataka o mrežnim uređajima, konfigurisanja interfejsa ili upravljanja sigurnosnim politikama. Python se integriše s različitim mrežnim bibliotekama, omogućavajući fleksibilnost i proširivost automatizovanih rješenja“ [12].



Slika 10 - Primjer automatizacije mreže u Python-u sa jednostavnom skriptom za početnike

„**Netmiko** je Python biblioteka koja pojednostavljuje interakciju s mrežnim uređajima putem **SSH** protokola. Omogućava automatizaciju zadataka kao što su slanje komandi, dobijanje podataka o statusu mreže i ažuriranje konfiguracije. Netmiko podržava širok spektar mrežnih operativnih sistema, uključujući Cisco IOS, Juniper JunOS i Arista EOS“ [13].

```
1.  import netmiko
2.  from netmiko import ConnectHandler
3.
4.  iosv_l2 = {
5.      'device_type': 'cisco_ios',
6.      'ip':   '192.168.1.50',
7.      'username': 'cisco',
8.      'password': 'cisco',
9.      'secret': 'cisco',
10.
11. }
12.
13. net_connect =ConnectHandler(**iosv_l2)
14. net_connect.enable()
15. output =net_connect.send_command('show ip int brief')
16. print(output)
17.
18. config_commands = [ 'int loop 0', 'ip addre 1.1.1.1 255.255.255.0', 'no sh']
19. output = net_connect.send_config_set(config_commands)
20. print (output)
21. output =net_connect.send_command('show ip int brief')
22. print (output)
```

Slika 11 - Korištenje Netmiko arhitekture i kako koristi SHH za povezivanje sa mrežnim uređajima

„**Napalm** (*engl. Network Automation and Programmability Abstraction Layer with Multivendor support*) je još jedna Python biblioteka koja omogućava jednostavno upravljanje mrežnim uređajima nezavisno od vendora. Napalm pruža ujednačen API za interakciju sa uređajima različitih proizvođača, čime se pojednostavljuje implementacija mrežne automatizacije u heterogenim mrežnim okruženjima“ [14].

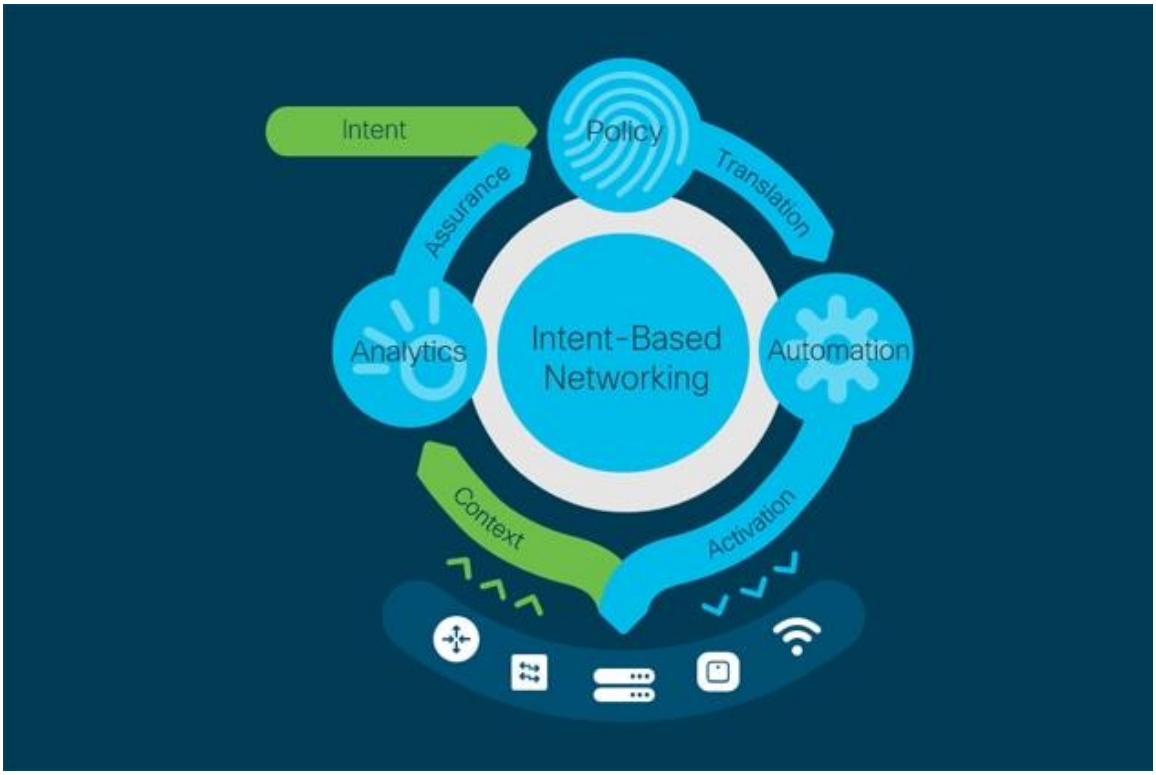
3. Intent-Based Networking (IBN)

„Intent-Based Networking (IBN) predstavlja napredan koncept mrežne automatizacije koji koristi vještačku inteligenciju (AI) i mašinsko učenje (ML) za automatsku implementaciju i upravljanje mrežama na osnovu unaprijed definisanih ciljeva („intenata“). Glavni cilj IBN-a je da smanji manuelne intervencije i omogući mreži da sama analizira, prilagođava i optimizuje svoje operacije u realnom vremenu.

Osnovne komponente IBN sistema uključuju:

- **Prepoznavanje namjere** (Intent Recognition) - korisnik definiše poslovne ciljeve koje mreža treba da ispuni, a IBN sistem prevodi te ciljeve u tehničke mrežne politike.

- **Automatska primjena politika** (Policy Application) - sistem primjenjuje mrežne konfiguracije na osnovu prepoznatih intenata, koristeći automatizaciju i orkestraciju.
- **Kontinuirani monitoring i analiza** (Continuous Validation & Assurance) - IBN neprestano analizira mrežno stanje, koristi telemetriju i AI za detekciju problema i automatsko prilagođavanje konfiguracija.
- **Samoprilagođavanje** (Self-Optimization) - IBN mreže su sposobne da uče iz istorijskih podataka i automatski optimizuju svoje performanse bez ljudske intervencije.



Slika 12 - Ilutracija IBN-a i njegovih prednosti

Implementacija IBN sistema omogućava kompanijama veću agilnost, sigurnost i efikasnost u upravljanju mrežama, uz smanjenje operativnih troškova i ljudskih grešaka“ [15].

3.1. Osnovni princip rada IBN-a

„Intent-Based Networking (IBN) je napredni model mrežne automatizacije koji omogućava mrežama da autonomno tumače poslovne ciljeve i prilagođavaju svoje konfiguracije bez potrebe za manuelnim intervencijama. Za razliku od tradicionalnih mreža, koje zahtijevaju ručnu konfiguraciju i nadzor, IBN koristi vještačku inteligenciju (AI), mašinsko učenje (ML) i automatizaciju kako bi transformisao način upravljanja mrežama“ [16].

„Osnovni princip rada IBN-a zasniva se na sljedećim koracima:

- Definisanje namjere (Intent Definition) - korisnik unosi poslovne ciljeve i zahtijeve mreže u obliku visoko-nivoznih politika, umijesto tehničkih komandi. Na primjer, može se definisati da određena aplikacija mora imati minimalnu latenciju ili prioritet u saobraćaju.
- Prevođenje namjere u mrežne politike (Translation to Policies) - IBN sistem koristi AI i automatizovane procese da prevede korisničke zahtjeve u specifične mrežne konfiguracije.
- Primjena i automatizacija (Automated Implementation) - sistem automatski primjenjuje mrežne politike na uređaje i infrastrukturu, smanjujući potrebu za manuelnim podešavanjem.
- Kontinuirano praćenje i analiza (Continuous Monitoring & Optimization) - Korištenjem telemetrije i analitike u realnom vremenu, IBN prati performanse mreže, detektuje nepravilnosti i automatski prilagođava konfiguracije radi optimizacije performansi i sigurnosti.
- Samoprilagođavanje (Self-Healing & Adaptation) - na osnovu istorijskih podataka i AI modela, mreža može prepoznati probleme prije nego što se manifestuju i proaktivno ih riješiti bez ljudske intervencije“ [17].

IBN donosi ključne prednosti, uključujući smanjenje operativnih troškova, povećanje mrežne sigurnosti i pouzdanosti, bržu implementaciju promjena i veću agilnost u upravljanju IT infrastrukturom. Implementacijom ovog modela, mreže postaju inteligentnije, autonomnije i sposobne za samostalno donošenje odluka u skladu sa unaprijed definisanim ciljevima.

3.2. Razlika između tradicionalnog upravljanja mreže i IBN-a

Tradicionalno upravljanje mrežom oslanja se na manuelnu konfiguraciju svakog uređaja pojedinačno, pri čemu mrežni administratori moraju ručno unositi konfiguracije putem CLI (Command Line Interface) komandi. Ovaj proces je složen, vremenski zahtijevan i podložan ljudskim greškama, što otežava skaliranje mreže i brzu adaptaciju na promjene u IT okruženju.

Sa druge strane, Intent-Based Networking (IBN) transformiše ovaj pristup automatizacijom i inteligentnim donošenjem odluka. U IBN modelu, administratori definišu poslovne ciljeve i politike mreže na visokom nivou, a sistem samostalno interpretira ove "intencije" i primjenjuje potrebne promene. IBN koristi tehnologije poput viješ̆tačke inteligencije (AI), mašinskog učenja (ML) i automatizovane analitike kako bi osigurao da mreža funkcioniše u skladu sa definisanim ciljevima.

Osnovne razlike između tradicionalnog upravljanja i IBN-a su slijedeće:

- **Konfiguracija** - tradicionalni model zahtijeva ručno konfigurisanje svakog uređaja, dok IBN automatski prevodi korisničke zahtijeve u mrežne politike i primjenjuje ih.
- **Reakcija na promjene** - u tradicionalnim mrežama, promjene se implementiraju ručno i zahtijevaju značajnu intervenciju, dok IBN automatski prilagođava mrežne parametre u realnom vremenu.

- **Praćenje i optimizacija** - tradicionalno upravljanje mrežom se oslanja na statične konfiguracije i reaktivno otklanjanje problema, dok IBN koristi napredne analitičke alate za proaktivno praćenje i optimizaciju mrežnih performansi.
- **Pouzdanost** - IBN minimizuje ljudske greške i povećava sigurnost mreže kroz automatizaciju i samoprilagođavanje, dok tradicionalni pristup često zahtijeva manuelne provjere i intervencije.

Implementacijom IBN-a, organizacije mogu postići veću agilnost, sigurnost i efikasnost u upravljanju mrežom, čime se smanjuju operativni troškovi i povećava stabilnost IT infrastrukture.

3.3. Ključne komponente IBN-a

„Intent-Based Networking (IBN) se sastoji od nekoliko ključnih komponenti koje omogućavaju automatizovano, inteligentno upravljanje mrežom u skladu sa poslovnim ciljevima organizacije. Ove komponente uključuju Intent, Translation, Validation i Assurance, koje zajedno omogućavaju mreži da dinamički odgovore na promjene i optimizuje performanse“ [18].

„Intent (srp. namjera) – predstavlja definisanje poslovnih ciljeva mreže na visokom nivou. Umjesto da administratori ručno konfigurišu svaki uređaj, oni unose svoje zahtijeve u obliku politike, poput „prioritizuj VoIP saobraćaj“ ili „obezbijedi end-to-end enkripciju“. IBN sistem zatim automatski razumije ovu intenciju i prevodi je u konkretne mrežne akcije“ [19].

„Translation (srp. prevođenje) – nakon što sistem primi definisanu intenciju, slijedeći korak je prevođenje poslovnih zahtijeva u tehničke konfiguracije koje se mogu primjeniti na mrežne uređaje. Ovaj proces podrazumijeva analizu zadatih pravila i njihovo prilagođavanje specifičnoj infrastrukturi organizacije, koristeći modele zasnovane na automatizaciji i vještačkoj inteligenciji“ [19].

„Validation (srp. provjera ispravnosti) - nakon što su politike prebačene u mrežnu konfiguraciju, IBN sistem vrši proaktivnu validaciju. Ova faza osigurava da su implementirane promjene u skladu sa zadatim ciljevima, prije nego što ih primjeni na mrežne uređaje. Validacija uključuje simulacije i analize kako bi se spriječile greške i nekompatibilnosti“ [20].

„Assurance (srp. neprekidno praćenje i prilagođavanje) – IBN mreža kontinuirano prati performanse, identifikuje odstupanja i ako je potrebno, prilagođava konfiguraciju kako bi osigurala da mreža radi optimalno. Koristeći analitiku i mašinsko učenje, sistem može predvidjeti potencijalne probleme i automatski ih rješiti prije nego što utiču na korisnike“ [21].

Zahvaljujući ovim komponentama, IBN omogućava visoku automatizaciju, smanjuje ljudske greške i poboljšava sigurnost i pouzdanost mreže, čime se postiže efikasnije upravljanje mrežom i brža prilagodljivost poslovnim potrebama.

3.4. Uloga vještačke inteligencije i mašinskog učenja u IBN sistemima

„Viješ tačka inteligencija (AI) i mašinsko učenje (ML) igraju ključnu ulogu u Intent-Based Networking (IBN) sistemima, omogućavajući im da analiziraju podatke, donose odluke i automatizuju mrežne operacije na način koji prevazilazi tradicionalne metode upravljanja mrežom“ [22].

AI i ML doprinose IBN sistemima kroz slijedeće aspekte:

- „Analiza podataka i donošenje odluka – IBN mreže koriste AI i ML algoritme za analizu velikih količina mrežnih podataka u realnom vremenu. Na osnovu analize saobraćaja, performansi i sigurnosnih događaja, sistem može predviđati potencijalne probleme i automatski ih rješavati.

- Automatizacija mrežnih operacija – umijesto manuelnog podešavanja, IBN uz pomoć AI-a prilagođava konfiguraciju uređaja u skladu sa unaprijed definisanim ciljevima (intent-ima). To smanjuje potrebu za ljudskom intervencijom i ubrzava prilagođavanje mreže promjenama u radnom okruženju“ [22].

- „Prediktivna analiza i proaktivno otkrivanje problema – AI modeli omogućavaju mreži da prepozna obrasce koji prethode kvarovima ili napadima. Ovi modeli koriste istorijske podatke kako bi identifikovali anomalije i spriječili potencijalne incidente prije nego što oni negativno utiču na korisnike.

- Optimizacija mrežnih resursa – mašinsko učenje omogućava IBN sistemima da dinamički prilagođavaju raspodjelu mrežnih resursa. Na primjer, može se optimizovati protok podataka u skladu sa opterećenjem mreže ili prioritetima aplikacija, poboljšavajući kvalitet usluge“ [23].

- „Unaprijeđena sigurnost – AI može automatski detektovati i odgovarati na prijetnje, identifikovati neovlaštene aktivnosti i prilagoditi sigurnosne politike u realnom vremenu. Kombinovanjem ML modela sa sigurnosnim analitikama, IBN može prepoznati napredne sajber prijetnje i smanjiti vrijeme odgovora na incidente“ [24].

Integracija AI i ML tehnologija u IBN omogućava mrežama da postanu autonomnije, efikasnije i sigurnije, čime se postiže visoka automatizacija i prilagodljivost poslovnim potrebama.

3.5. Primjena i slučajevi upotrebe IBN-a

Intent-Based Networking (IBN) donosi napredne mogućnosti automatizacije i inteligentnog upravljanja mrežom u različitim okruženjima, omogućavajući efikasnije konfiguracije, proaktivno rješavanje problema i optimizaciju resursa.

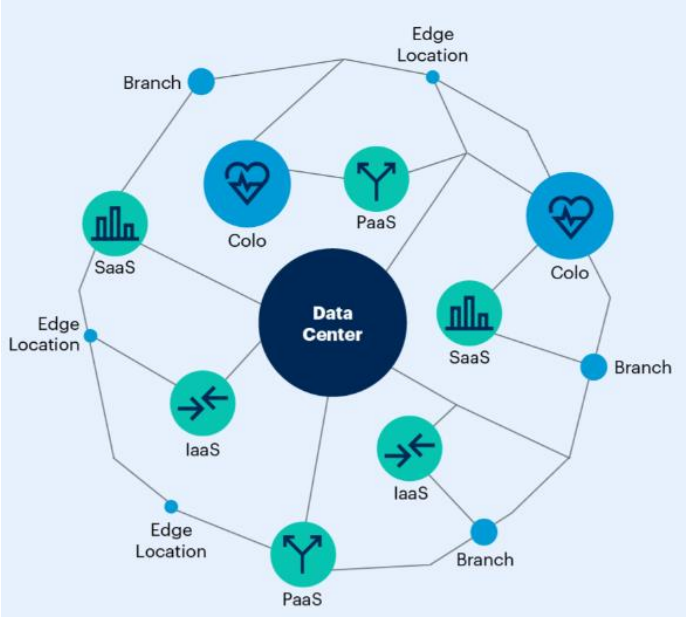
IBN pojednostavljuje i ubrzava proces konfiguracije mrežnih uređaja tako što interpretira intencije administratora i automatski implementira potrebne promjene. Tradicionalni pristup zahtijeva manuelno konfigurisanje svakog uređaja pojedinačno, dok IBN omogućava centralizovanu i

doslijednu primjenu politika kroz cijelokupnu mrežnu infrastrukturu. Ovo smanjuje mogućnost grešaka i poboljšava sigurnost mreže.

„IBN koristi viješ tačku inteligenciju i mašinsko učenje za analizu mrežnih podataka u realnom vremenu. Prediktivni algoritmi detektuju potencijalne probleme prije nego što utiču na performanse mreže, omogućavajući pravovremene korektivne mjere. Ova sposobnost smanjuje vrijeme zastoja i poboljšava korisničko iskustvo, posebno u velikim mrežnim okruženjima“ [22].

Primjena IBN-a u različitim okruženjima:

- „Data centri – automatizacija resursa za cloud servise. U modernim data centrima, IBN omogućava automatsku konfiguraciju mrežnih resursa u skladu sa potrebama aplikacija i opterećenjem servera. Na primjer, može dinamički prilagoditi mrežne politike kako bi optimizovao performanse cloud servisa, istovremeno održavajući sigurnost i usklađenost sa propisima“ [23].



Slika 13 - Dijagram automatizacije resursa u cloud okruženju

- „IoT mreže – optimizacija velikog broja uređaja sa minimalnom latencijom. IBN pomaže u efikasnom upravljanju velikim brojem IoT uređaja tako što automatski prilagođava mrežne parametre kako bi smanjio latenciju i poboljšao pouzdanost komunikacije. Ovaj pristup je posebno važan u industrijama kao što su pametne fabrike, pametni gradovi i zdravstvena zaštita, gdje IoT uređaji generišu ogromne količine podataka“ [24].

- Cloud infrastruktura – integracija sa hibridnim i multi-cloud okruženjima. IBN omogućava organizacijama da pojednostave upravljanje složenim mrežama koje uključuju on-premises, hibridne i multi-cloud resurse. Automatski prilagođava mrežnu konfiguraciju kako bi optimizovao saobraćaj između različitih cloud provajdera, povećavajući efikasnost i sigurnost podataka.

IBN transformiše način na koji organizacije upravljaju mrežama, uvodeći visok nivo automatizacije, inteligencije i prilagodljivosti u različitim IT okruženjima.

4. Sigurnosni aspekti i izazovi IBN-a

Mrežna automatizacija donosi brojne sigurnosne prednosti, ali i izazove koji zahtijevaju pažljivo upravljanje kako bi se minimizirali potencijalni rizici. Automatizacija smanjuje mogućnost ljudskih grešaka, koje su često uzrok sigurnosnih incidenata. Korištenjem automatizovanih skripti i orkestracije, mrežni administratori mogu primjenjivati sigurnosne politike na velikom broju uređaja bez potrebe za ručnom konfiguracijom. Međutim, pogrešna implementacija automatizovanih procesa može dovesti do masovnih sigurnosnih propusta, pa je neophodno vršiti detaljno testiranje prije primjene u produkcionom okruženju.

Jedan od ključnih izazova u sigurnosti mrežne automatizacije jeste zaštita konfiguracionih podataka i pristupa mrežnim uređajima. Ako napadač uspije da kompromituje sistem za automatizaciju, može dobiti pristup cijeloj mrežnoj infrastrukturi. Zbog toga se preporučuje upotreba enkriptovanih kanala za komunikaciju, kao i stroga kontrola privilegija korisnika koji imaju pristup automatizovanim alatima.

4.1. Upravljanje pristupom i autentifikacija

Upravljanje pristupom i autentifikacija ključni su aspekti zaštite automatizovanih mrežnih sistema. Zero Trust model, koji podrazumijeva provjeru identiteta svih korisnika i uređaja bez obzira na to gdje se nalaze u mreži, postaje standard u sigurnosnim strategijama. Ovaj model funkcioniše na principu "nikome ne vjeruj, sve provjeri", čime se značajno smanjuje mogućnost neovlaštenog pristupa mrežnim resursima.

Pored toga, dvofaktorska autentifikacija (2FA) i enkriptovani kanali za komunikaciju spriječavaju presretanje podataka i neovlašten pristup, osiguravajući da samo verifikovani entiteti mogu izvršavati mrežne operacije [29]. Korištenje savremenih protokola kao što su Transport Layer Security (TLS) i IPsec dodatno poboljšava sigurnost prenosa podataka u mrežnoj automatizaciji.

4.2. Automatizacija sigurnosnih politika

Implementacija sigurnosnih politika kroz mrežnu automatizaciju omogućava organizacijama da brzo primjenjuju zaštitne mjere na svim uređajima. Korištenjem alata poput Ansible, Cisco ACI i Palo Alto Panorama, administratori mogu definisati pravila pristupa, segmentacije i detekcije prijetnji, koja se zatim automatski primjenjuju na mrežnu infrastrukturu. Automatizacija sigurnosnih politika također igra ključnu ulogu u detekciji i odgovoru na prijetnje. Savremeni sistemi za mrežnu sigurnost koriste viješ̆tačku inteligenciju i mašinsko učenje kako bi analizirali saobraćaj u realnom vremenu i prepoznali potencijalne napade prije nego što izazovu štetu [31]. Na primjer, Next-Generation Firewall (NGFW) rješenja omogućavaju dinamičko prilagođavanje sigurnosnih politika na osnovu prepoznatih obrazaca prijetnji.

ZAKLJUČAK

Mrežna automatizacija i IBN predstavljaju ključne tehnološke pravce koji omogućavaju efikasnije, sigurnije i fleksibilnije upravljanje savremenim mrežama. Automatizacija smanjuje potrebu za manuelnim intervencijama, čime se smanjuje rizik od ljudskih grešaka i povećava operativna efikasnost. Istovremeno, implementacija IBN-a omogućava mrežama da se prilagođavaju promjenjivim uslovima rada kroz inteligentno donošenje odluka.

Integracija AI i ML tehnologija dodatno unapređuje IBN sisteme, omogućavajući prediktivnu analitiku i proaktivno otkrivanje problema prije nego što oni utiču na performanse mreže. Ovi napredni sistemi već pronalaze primjenu u različitim oblastima, uključujući data centre, IoT mreže i cloud infrastrukturu.

Međutim, uprkos brojnim prednostima, implementacija mrežne automatizacije i IBN-a donosi i određene izazove, posebno u pogledu sigurnosti i upravljanja pristupom. Kako bi se obezbijedila uspješna primjena ovih tehnologija, neophodno je usvojiti standardizovane sigurnosne prakse, uključujući Zero Trust modele i enkriptovane komunikacione kanale.

Budući razvoj mrežnih tehnologija vjerovatno će dodatno unaprijediti automatizaciju i inteligentno upravljanje mrežama, otvarajući nove mogućnosti za optimizaciju performansi, povećanje sigurnosti i smanjenje operativnih troškova. Stoga je istraživanje i implementacija ovih tehnologija ključni korak ka modernizaciji mrežnih infrastruktura i prilagođavanju sve složenijim zahtijevima digitalnog doba.

POPIS SLIKA

CITATNI IZVORI

[1] » Intent-Based Networking: The Future of Network Automation,« Cisco, [Mrežno]. Available: https://www.cisco.com/c/en/us/solutions/intent-based-networking.html. [Pokušaj pristupa 2 February 2025].

[2] Digitalna Inicijativa, »Zašto je automatizacija investicija, a ne trošak,« Digitalna Inicijativa, [Mrežno]. Available: https://digitalna-inicijativa.com/zasto-je-automatizacija-investicija-a-ne-trosak/. [Pokušaj pristupa 2 February 2025].

[3] Ecommerce Bridge, »AI i automatizacija u e-trgovini: Kompletan vodič,« Ecommerce Bridge, [Mrežno]. Available: https://www.ecommercebridge.co.ba/hub/ai-i-automatizacija-u-e-trgovini-kompletan-vodic. [Pokušaj pristupa 2 February 2025].

[4] Ascendant USA, »Software-Defined Networking (SDN),« Ascendant USA, 8 January 2025. [Mrežno]. Available: https://ascendantusa.com/2025/01/08/software-defined-networking-sdn/. [Pokušaj pristupa 2 February 2025].

[5] Layer 8 Packet, »Layer 8 Packet,« The Role of APIs in Network Automation: Transforming How Networks Operate, [Mrežno]. Available: https://www.layer8packet.io/home/the-role-of-apis-in-network-automation-transforming-how-networks-operate. [Pokušaj pristupa 2 February 2025].

[6] Splunk, »Network Telemetry,« Splunk, [Mrežno]. Available: https://www.splunk.com/en_us/blog/learn/network-telemetry.html. [Pokušaj pristupa 2 February 2025].

[7] J. Edelmal, S. Lowe i M. Oswalt, Network Programmability and Automation: Skills for the Next-Generation Network Engineer, 1st ed, O'Reilly Media, 2018.

[8] M. L. Gorodetsky, »Network Automation: State of the Art and Future Trends,« *IEEE Communications Magazine*, svez. 58, br. 4, pp. 12-18, 2020.

[9] Cisco, »Network Automation and Orchestration,« Cisco, [Mrežno]. Available: https://www.cisco.com/c/en/us/solutions/enterprise-networks/network-automation.html. [Pokušaj pristupa 4 February 2025].

[10] D. Geevarghese, Practical Network Automation: Leverage the Power of Python and Ansible to Optimize Your Network, 1st Edition, Packt Publishing, 2018.

[11] P. Goransson i C. Black, Software-Defined Networks: A Comprehensive Approach, 2nd Edition, Morgan Kaufmann, 2017.

[12] E. Chou, Mastering Python Networking, 3rd Edition, Packt Publishing, 2020.

[13] K. Bannister, »Automating Network Configuration with Netmiko,« *Network Computing Journal*, svez. 29, br. 3, pp. 45-50, 2021.

[14] D. Barroso, »Standardizing Network Automation with Napalm,« *IEEE Communications Magazine*, svez. 57, br. 8, pp. 22-30, 2019.

[15] D. Kreutz, F. M. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky i S. Uhlig, »Software-Defined Networking: A Comprehensive Survey,« *Proceedings of the IEEE*, svez. 103, br. 1, pp. 14-76, 2015.

[16] Cisco Systems, Intent-Based Networking: The Future of Enterprise Networks, White Paper, 2020.

[17] N. Feamster, J. Rexford i E. Zegura, »The Road to SDN: An Intellectual History of Programmable Networks,« *ACM SIGCOMM Computer Communication Review,* svez. 44, br. 2, pp. 87-98, 2014.

[18] Cisco, »The Evolution of Intent-Based Networking,« White Paper, 2020.

[19] N. McKeown, »Intent-Based Networking: An Overview,« *IEEE Communications Magazine,* svez. 58, br. 6, pp. 26-32, 2021.

[20] A. Clemm i R. R. Khandekar, »Intent-Based Networking – Concepts and Vision,« Springer, 2021.

[21] J. Strassner, »Artificial Intelligence for Self-Driving Networks,« *IEEE Network,* svez. 35, br. 3, pp. 14-20, 2021.

[22] M. Jarschel, »Machine Learning for Intent-Based Networking,« *IEEE Communications Surveys & Tutorials,* svez. 24, br. 2, pp. 110-128, 2022.

[23] A. Clemm, »AI-Powered Network Automation,« *IEEE Network,* svez. 36, br. 1, pp. 22-3', 2023.

[24] K. R. Liu, »Optimizing Network Traffic with Machine Learning,« *IEEE Transactions on Network and Service Management,* svez. 17, br. 4, pp. 980-994, 2021.