SOFTVERSKI DEFINISANE MREŽE/ SOFTWARE DEFINED NETWORKS

Armin Čelarević[1],
[1]Internacionalni univerzitet Travnik u Travniku, Aleja Konzula - Meljanac bb, Travnik, BiH,
e-mail: celarevicarmin@gmail.com

Pregledni članak

Sažetak

Softverski definisane mreže, nova su inovativna rješenja u svijetu računarstva kojim se mijenja način implementacije i upravljanja nad mrežom i mrežnim uređajima. Osnovne osobine ovih mreža su odvajanje kontrolne i podatkovne ravni, kao i uspostavljanje centralnog mjesta kontrole nad cjelokupnom mrežom u vidu SDN-kontrolera. Kontroler kao centralno mjesto u mreži nudi programsku sredinu za pristup aplikacijama, te se iste mogu koristiti za različite svrhe kao što su upravljanje prometom, upravljanje sigurnosnom politikom u mreži, optimizacijom mreže, itd. SDN omogućava dinamičku prilagodbu mrežnog okruženja trenutnim aplikativnim zahtjevima ili potrebama korisnika, te znatno jednostavnije upravljanje i povećavanje stalabilnosti mreže. SDN i OpenFlow arhitektura omogućava način implementacije programabilnih mrežnih arhitektura koje se mogu implementirati postepeno u već postojeću mrežu. Ovakav model mreža se razlikuje od tradicionalnih mreža koje koriste namjenske hardverske uređaje za kontrolu mrežnog saobrćaja. Softverski definisana mreža može kreirati i kontrolisati virtualnu mrežu ili kontrolisati tradicionalni hardver putem softvera. NFV budi mogućnost virtualizacije mrežnih funkcija zasnovanih na uređajima kao što su zaštitni zidovi i WAN-akceleratori. SDN donosi mnoge poslovne prednosti tako što olakšava IT-organizacijama automatizaciju mrežnih funkcija i smanjenje operativnih troškova.

Ključne riječi: *Softverski definisana mreža (SDN), OpenFlow, računarske mreže, SDN-kontroler.*

Abstract

Software-defined networks are new innovative solutions in the world of computing that change the way of implementation and management of networks and network devices. The basic features of these networks are the separation of the control and data planes, as well as the establishment of a central point of control over the entire network in the form of an SDN controller. The controller, as a central point in the network, offers a programming environment for accessing applications, which can be used for various purposes such as traffic management, network security policy management, network optimization, etc. SDN enables dynamic adaptation of the network environment to current application requirements or user needs, as well as significantly simpler management and increased network scalability. SDN and OpenFlow architecture provide a way to implement programmable network architectures that can be implemented gradually in an already existing network. This network model differs from traditional networks, which use dedicated hardware devices to control network traffic. A software-defined network can create and control a virtual network or control traditional hardware through software. NFV enables the virtualization of device-based network functions such as firewalls and WAN accelerators. SDN brings many business benefits by making it easier for IT organizations to automate network functions and reduce operational costs.

Keywords: *Software-Defined Network (SDN), OpenFlow, Computer Networks, SDN Controller.*

1. UVOD

Računarstvo u oblaku korisnicima omogućava pohranu podataka i instalaciju programske podrške na poslužitelje koji su povezani putem interneta. Uz pomoć web preglednika i posebnih klijenata, ove su usluge fleksibilne. Softverski definisana mreža je mreža, gdje je kontrola mreže odvojena od prosljeđivanja paketa, i ima mogućnost direktnog programiranja. Takva migracija kontrole, nekada čvrsto vezane za pojedinačni mrežni uređaj, u vanjske računarske uređaje omogućava osnovnoj infrastrukturi odvojenost od aplikacija i mrežnih usluga, koje mrežu mogu tretirati kao logički ili virtuani entitet. SDN omogućava dinamičku prilagodbu mrežnog okruženja aplikacijskim zahtjevima ili potrebama korisnika, te znatno pojednostavljuje upravljanje i povećanje skalabilnosti mreže, što se očituje jednostavnom implementacijom dodatnih mrežnih usluga. SDN-softver na sebe preuzima kontrolnu razinu koja se do sada nalazila na svakom pojedinačnom uređaju čineći time mrežne uređaje ispod sebe jednostavnim „radnicima“. Drugim riječima, u predhodnim metodama razvoja računarskih mreža glavnu ulogu imao je hardver, dok se danas teži standardizaciji mrežnih procesa i glavnu ulogu u mrežnom upravljanju preuzima softver. Kako SDN- kontroleri nisu mrežni uređaji, mogu iskoristi prednosti mjerila, pohrane podataka i dostupnosti savremenih resursa računarstva u oblaku. U današnje vrijeme SDN-kontroleri se izgrađuju na otvorenim platformama, koristeći otvorene standarde što im omogućava korištenje i upravljanje mrežne opreme različitih proizvođača. Sposobnost brže reakcije na probleme i prekide poboljšava dostupnost mreže, a programabilnost olakšava IT- organizacijama automatizaciju mrežnih funkcija smanjujući operativne troškove. Glavni cilje SDN-mreža je omogućavanje računarstva u oblaku, mrežnim inženjerima i administratorima brzu reakciju na promjenu poslovnih zahtjeva putem centralizirane upravljačke jedinice. Softverski definisane mreže obuhvataju više vrsta mrežnih tehnologija osmišljenih kako bi mreža bila fleksibilnija, te kako bi podržala virtualnu infrastruktuturu poslužitelja i zadovoljila potrebe aplikacija.

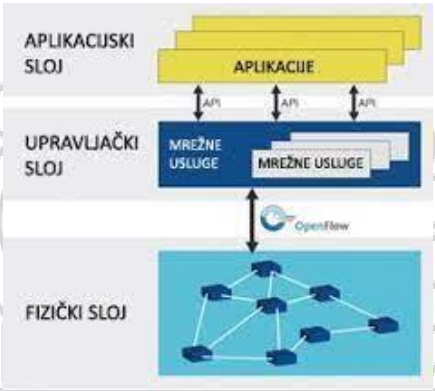
2. Arhitektura softverski definisanih mreža

SDN je mrežna arhitektura gdje je kontrola mreže odvojena od prosljeđivanja, te se može izravno programirati. Mreža pristupa aplikacijama kao jedan logički switch, te se time dobije kontrola nad cijelom mrežom s jedne logičke tačke, što pojednostavljuje dizajn mreže i same operacije unutar mreže. SDN pojednostavljuje rad samih mrežnih uređaja, jer više ne trebaju razumjeti i obraditi hiljade protokolnih standarda, već samo trebaju prihvatiti upute od SDN-kontrolera. Najvažnije je da administratori i mrežni operateri mogu programski konfigurirati ovu pojednostavljenu apstrakciju mreže i ne moraju ručno podesiti hiljade linija koda za konfiguraciju koji su razbacani među hiljadama uređaja. Uticajem centralizirane integracije SDN-kontrolera, moguće je promijeniti ponašanje mreže u realnom vremenu i implementirati nove aplikacije i usluge u nekoliko sati ili dana, a ne nekoliko sedmica ili mjeseci. U tradicionalnoj mreži svaki uređaj u sebi sadrži implementiranu upravljačku, kontrolnu i podatkovnu ravan. Svaka od tih mogućnosti vrši se distribuirano, odnosno svaki uređaj radi kalkulaciju za sebe, ne postoji centralna kontrola i administracija. Preklopnici i usmjerivači nalaze se na infrastrukturnom sloju, te u sebi imaju implementiranu samo podatkovnu ravan, a sve odluke o tome kada treba poslati paket određuje kontroler na kontrolnoj ravni i ta pravila zapisuje u tablice preklopnika. Aplikacije ostvaruju dvosmjernu komunikaciju s kontrolerom na norhbound okruženje, te tako mogu u realnom vremenu dobivati informacije o mreži. Centraliziranjem mrežnog stanja u kontrolnom sloju, SDN pruža mrežnim upraviteljima

fleksibilnost i konfiguriranju, upravljaju i optimiziraju mrežne resurse putem dinamičkih i automatiziranih SDN- programa.

Ključni principi SDN-arhitekture:

- konvencionalne aplikacije
- konvencijalne mreže



Slika 1. Arhitektura SDN mreža
Izvor: https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A180/datastream/PDF/view (13.05.2023.)

Arhitektura SDN-a mreža, može se posmatrati preko tri sloja:

- prosljeđivanje
- distribucija
- specifikacija

Aplikacijski sloj prosljeđivanja, potpuno neovisno o fizičkim karakteristikama mreže, obavlja ulogu izvršavanja i podrške aplikacijski prosljeđenim zahtjevima. Sloj distribucije, uz logički centraliziranu ulogu upravljanja mrežnim uređajima, te prikupljanja informacija o njihovom radu i međusobnoj povezanosti, stvara temelj za rad mrežnih aplikacija. Način na koji mrežne aplikacije realiziraju svoje primarne funkcije na fizičkoj razini, pripada apstrakcijskom sloju specifikacije koji ovakve zahtjeve riješava upotrebom virtualizacije, te programskih jezika.

Razlozi za korištenje SDN-domena uključuju:

- skalabilnost
- privatnost
- detaljna implementacija

2.1 OpenFlow

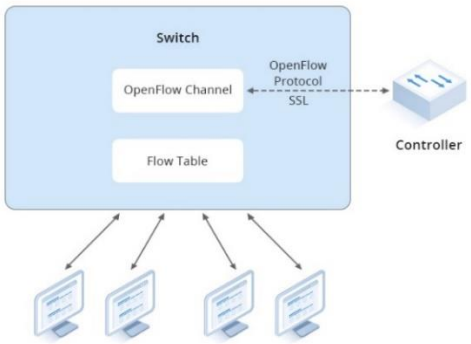
OpenFlow je standardni komunikacijski interfejs definisan između kontrolnog sloja i sloja za prosljeđivanje SDN-arhitekture. OpenFlow omogućava direktan pristup i manipulaciju uređaja koji se nalaze unutar ravni prosljeđivanja kao što su svičevi i ruteri, kako fizički, tako i virtuelni. Odsustvo otvorenog interfejsa prema ravni prosljeđivanja je vodilo ka karakterizaciji današnjih mrežnih uređaja. Posljednih nekoliko godina došlo je do

ogromnog povećanja mrežnog prometa, to je u velikoj mjeri uzrok eksplozivnom rastom upotrebe interakcijskih aplikacija i usluga s velikim brojem formata podataka, vrsta usluge i internetskih uređaja. Softverski definisano umrežavanje, pojavilo se kao odgovor industrije na suočavanje s tim izazovima. SDN omogućava mrežama da dinamički reaguju na promjene u obrascima i dostupnosti mrežnih resursa. Mrežne arhitekture mogu se odmah prilagoditi, odgovoriti na zahtjeve aplikacija i korisnika, a usluge se mogu uvesti daleko brže. SDN osigurava razdvajanje između upravljačke ravnine i funkcija podatkoven ravnine, odnosno prekidača mreža pomoću protokola koji mijenja tablice za prosljeđivanje u mrežnim prekidačima. Kontroler omogućava mrežama interakciju s aplikacijama i učinkovito se rekonfiguriraju po potrebi, omogućavajući im da implementiraju više logičkih mrežnih topologija. OpenFlow protokol je implementiran na obje strane interfejsa između mrežne infrastrukture i SDN kontrolnog softvera. OpenFlow koristi koncept toka kako bi identificirao mrežni saobraćaj na osnovu unaprijed definisanih pravila koja mogu biti statički ili dinamički programirana od strane SDN-kontrolnog softvera. Budući da OpenFlow omogućava programiranje mreže zasnovano na toku, OpenFlow bazirana SDN-arhitektura pruža izuzetno granlarnu kontrolu mreže kako bi odgovorila i primjenama na aplikacijskom, korisničkom i serijskom sloju u realnom vremenu. Ovaj protokol je ključan za omogućavanje SDN-mreža i trenutno je jedini standardizovani SDN-protokol koji omogućava direktnu manipulaciju mrežnih uređaja koji se nalaze unutar ravni za prosljeđivanje. Razvojem i popularizacijom OpenFlow-a kontinuirano se proširuju i njegova područja istraživanja i primjene, pokrivajući virtualizaciju mreže, sigurnost i kontrolu pristupa, te uravnoteženje opterećenja.

2.1.1 Rad OpenFlow-prekidača s kontrolerom

OpenFlow-prekidači imaju tri vrste priključaka: fizičke, logičke i rezervisane priključke. Fizički priključak odnosi se na priključak koji je povezan s hardverom. Na prekidaču OpenFlow odgovara ethernet priključku. Međutim, ti portovi ponekad ne odgovaraju tačno, jer OpenFlow-prekidači također mogu virtuelizirati fizičke portove. U ovom trenutku, fizički priključak OpenFlow-a je virtualni dio hardverskog priključka. Za razliku od fizičkog porta, logički port je apstraktni port visoke razine koji obično definišu drugi, kao što su grupe za agregaciju veza, povratni priključci, itd. Ako logički priključak primi paket i treba komunicirati s kontrolerom, šalje izvješće kontroleru s fizičkim donjim priključkom. OpenFlow rezervirani priključak uglavnom se odnosi na generičke operacije prosljeđivanja. Na OpenFlow-prekidačima postoji nekoliko obaveznih rezervisanih priključaka. Operacija prekidača OpenFlow mora imati tri osnovna elementa: tablica toka, kontroler i OpenFlow-protokol. Svaki Open Flow-prekidač uspostavlja neovisne veze s kontrolerom za prijenos i obradu tablice protoka, s jedinstvenim ID-om operativne podatkovne veze. Kontroler je spojen preko TCP/IP-a na upravljačkoj ravni prekidača. Kada kontroler uspostavi vezu s prekidačem, šalje naredbenu porku koja označeva uspješnu vezu, a zatim šalje navedenu određenu verziju OpenFlow-protokola skretnici. OpenFlow-prekidači podržavaju različite operacije protoka za prosljeđivanje OpenFlow-paketa. Prilikom postupka prosljeđivanja prometa prosljeđuje jednosmjerne ili višesmjerne pakete kroz fizički priključak na interfejs omogućeno za OpenFlow koji je regulator odredio za obradu. U ovom trenutku SDN-kontroler može postaviti put kroz mrežu za posebne optimizacije kao što su brzina. Na temelju programabilnih karakteristika OpenFlow-a na mreži, riješava razlike između mrežne opreme različitih proizvođača. Budući da je kontrolno pravo potupuno otvoreno,

može se postići bilo koje željeno usmjeravanje mreže, pravila prijenosa i pravila kroz prilagodbu.



Slika 2.: OpenFlow
Izvor: https://media.fs.com/images/community/upload/kindEditor/202205/18/connection-1652867902-jsa4H6RtzK.jpg (13.05.2023.)

U današnje vrijeme OpenFlow ima veliku aplikaciju u velikim podatkovnim centrima u oblaku. Podatkovni centri i implementacije u oblaku povećavaju potrebu za virtualizacijom. OpenFlow-prekidači mogu učinkovito riješiti problem zagušenja podataka koji proizilazi iz nepravilnog dodjeljivanja puta prijenosa u podatkovnim centrima, čime se poboljšava operativna učinkovitost podatkovnih centara. To se dešava zato što može dinamički dobiti informacije o prijenosu podataka i koristiti OpenFlow prometne unose za postizanje uravnoteženja prometa na svakoj stazi. Iz tog se može vidjeti da su u procesu kontinuiranog razvoja interneta OpenFlow i SDN-tehnologije donijele nove tehnološke inovacije i razvoj u tradicionalnu mrežu, te će se u budućnosti nastaviti ažurirati i poboljšavati kako bi doprinijele bržoj komunikaciji.

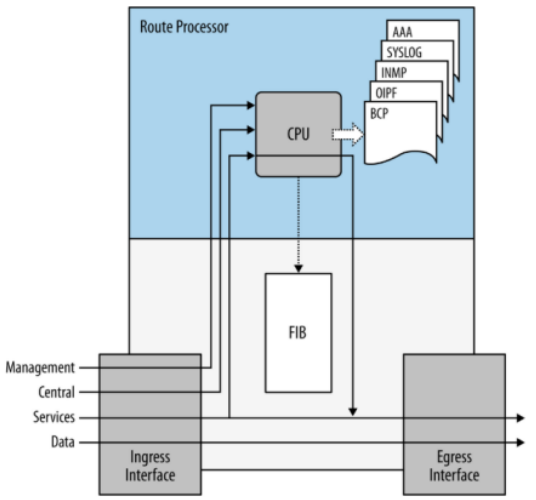
2.2 SDN-kontroler

Softverski definisani kontroler za umrežavanje, središnja je komponenta SDN-arhitekture. U umrežavanju postoji upravljačka ravan, upravljačka ravan i podatkovna ravan. SDN-kontroler pruža funkcije upravljačke ravnine i upravljačke ravnine za mrežne elemente u domeni kojom upravlja. To znači da SDN-kontroler, na temelju mrežnih informacija i skupa unaprijed definisanih pravila, upravlja mrežnim elementima i konfiguriše podatkovnu ravan, tj. usmjerava protok podataka kroz mrežu. Jedna od prednosti korištenja SDN-kontrolera je što omogućava učinkovitije upravljanje mrežom promjene u konfiguaciji mreže. Mogu se primjeniti sa središnjeg mjesta, a ne s ručnog konfigurisanja svakog pojedinog mrežnog elementa. Osim toga, SDN-kontroler može automatizirati određene zadatke, koa što su upravljanje prometom i sigurnost, što može pomoći u smanjenju rizika od ljudske pogreške i poboljšati ukupnu pouzdanost mreže. SDN-kontroleri pružaju API (eng. Application Programming Interface), poznati i kao sjeverno sučelje, putem kojeg vanjske aplikacije ili sistemi poput platformi za orkestraciju mogu komunicirati s mrežom. U takvim slučajevima SDN-kontroler prevodi zahtjeve slojeva aplikacija kao što je opis mrežne konfiguracije na visokoj razini. SDN-kontroleri mogu upravljati i fizičkim mrežnim uređajima i softverskim komponentama koje izvršavaju mrežne funkcije. Platforma SDN-kontrolera obično sadrži zbirku „pluggable“ modula koji mogu obavljati različite mrežne zadatke. Platforma kontrolera može biti iz društva koje se razlikuje od aplikacije, što omogućava interoperabilnost i fleksibilnost. Naprimjer, CISCO nudi platformu kontrolera koju je izgradio OpenDaylight. Ovaj kontroler otvorenog koda interoperabilan je sa nekoliko različitih vlasničkih aplikacija. Implementacija i integracija SDN kontrolera u mrežu može donijeti brojne prednosti:

- pruža jedinstveno sučelje koje mrežnim administratorima i vanjskim aplikacijama omogućava interakciju s mrežom,
- povećava brzinu automatizacije mreže,
- optimizira korištenje resursa,
- povrćava otpornost mreže,
- moguće upravljanje fizičkim mrežnim uređajima i softverskim mrežnim elementima.

2.3 Upravljačka i podatkovna ravan

Usmjerivači i preklopnici u tradicionalnoj mreži imaju kontrolnu i podatkovnu ravan implementiranu unutar sebe. SDN-naprave odvajaju kontrolnu i podatkovnu ravan za zasebne uređaje, te komunikaciju između njih ostvaruju upotrebom zasebnog SDN-protokola. Podatkovna ravan sadrži tablice u kojoj su definisana pravila za usmjeravanje paketa, a tablicu popunjava kontrolna ravan ovisno o kalkulacijama protokola više razine. Kada na portove stignu paketi koji nemaju definisana pravila, oni se automatski proslijeđivaju procesoru na daljnju obradu. Podatkovna ravan povezana je s centralnim procesorom preko brze internet sabirnice. Kako bi osigurala veću dostupnost, kontrolna ravan često se implementira kao redundantna jedinica. Sklopovi i programi kontrolne i podatkovne ravni u tradicionalnim mrežama distribuirane su naravi zbog brze komunikacije koju podatkovna i kontrolna ravan ostvarju preko internih sabirnica, te efikasnih ASIC-čipova razvijenih posebno za obavljanje određenih funkcija, ovakav oblik umrežavanja ima svojih prednosti kao što su brzina, pouzdanost i učinkovitost, ali i mane kao što su distribuirana kontrola, te zatvoreni razvoj čipova, što povećava cijenu uređaja, te usporava inovacije i razvoj.



Slika 3. Kontrolna i podatkovna ravan
Izvor: https://www.researchgate.net/figure/Software-Defined-Networking-framework-6_fig1_352986802 (14.05.2023.)

Kod SDN-mreže odgovornost kontrolne i podatkovne ravni odvojena je na zasebnim uređajima. Preklopnici i usmjerivači su pojednostavljeni, te oni više ne moraju sadržavati čitav niz kompleksnih kontrolnih jednica i kodova, a te funkcije nalaze se implementirane u SDN-kontroler s kojim komunikaciju ostvaruju na zasebnom upravljačkom interfejsu. Kontroler je zadužen za sve kompleksne kalkulacije i programiranje, te davanje instukcija preklopnicima u

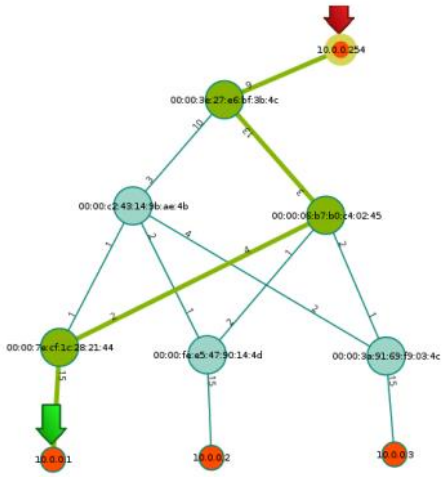
jednostavnom obliku. Kontroler sada može upravljati većim brojem preklopnika s jednog mjesta, a upravo za tu vrstu komunikacije najčešće se koristi OpenFlow-protokol.

2.4 Upravljanje prometom u SDN

Jedna od temeljnih prednosti koje SDN-mreža nudi je centralizirani i granularni pristup kontroli mrežnog prometa. SDN-aplikacije putem northbound interfejsa mogu proaktivno ili reaktivno uticati na rad same mreže. Aplikacije za kontrolu toka podataka mogu se svrstati u dvije grupe:

- aplikacijski kod kojih administratori ručno definišu željeni tok podataka u mreži na proaktivan način,
- aplikacije koje same dinamički definišu putanju prometa ovisno o stanju i zahtjevima mreže shodno analizi.

Kako bi se mogle prosljeđivati naredbe od strane aplikacije prema kontroleru, te dohvatati atribute i vrijednosti od strane kontrolera, potrebno je izvršiti inicijalnu autentifikaciju na kontroler putem RESET-interfejsa, prilikom čega kontroler na korištenje daje token koji vrijedi 24 sata. Token se koristi za autentifikaciju kod svih daljnjih poziva. Sama autentifikacija se obavlja putem Keystone Identity servisa, zasebnog autentifikacijskog eksternog modula koji je implementiran kao dio arhitekture Aruba VAN SDN kontrolera. Dobiveni token se sprema u zasebnu datoteku, te se poziva na nju prilikom svakog daljnjeg RESET-poziva. Za adekvatno upravljanje svim resursima koji se nalaze u OpenFlow-mreži kontroler putem RESET ful interfejsa nudi aplikacijama pristup svakom od njih, što uključuje mogućnost dohvata informacija kao što su logovi, metrike i statistike, autentifikacijski i autorizacijski podaci, podaci o OpenFlow i krajnjim uređajima. Svaki od ovih resursa može se primjeniti na zasebnom linku slanjem JSON-objekta s parametrima koji su definisani u samoj dokumentaciji Aruba VAN SDN kontrolera. Aruba VAN SDN omogućava usmjeravanje paketa u mreži koristeći internu aplikaciju Path Daemon koja izračunava najkraći put za sve pakete koje je proslijedio preklopnik uvidom u kompletnu topologiju mreže, te u mogućnosti spojnih preklopnika i njihovih sučelja. Uvijek će biti odabran najkraći put u mreži prema broju skokova, te brzini izlaznih sučelja preklopnika. Kada primi dolaznu poruku od preklopnika, Path Daemon na temelju izvršene kalkulacije vrši implementaciju flow-zapisa u tablicu preklopnika.



Slika 4. Putanja prometa paketa
Izvor: file:///C:/Users/deskt/OneDrive/Desktop/970012.7._Softverski_definirana_mrea_Valic_Gligora.pdf (15.05.2023.)

2.5 Primjena SDN-mreža

Softverski definisano umrežavanje nudi niz prednosti za organizacije koje se pokušavaju preseliti u virtualno okruženje. Postoji mnogo slučajeva upotrebe za različite organizacije, uključujući davatelje mobilnih usluga i usluga računarstva u oblaku, podatkovne centre. Za davatelje mobilnih usluga, softverski definisano umrežavanje nudi bandwith na zahtjev, što omogućava kontrolu veze mobilnih operatera i traženje dodatne širine pojasa kada je to potrebno. Razvojem SDx (eng. Software Defined Everthing) tehnologija, primjenjivi slučajevi upotrebe postaju sve važniji i za dobavljače i za krajnje korisnike. SDx-infrastruktura odgovorna je za potporu i povezivanje korisnika i uređaja s uslugama, što znači da su problemi s kojima se susrećemo u mreži, eksponencijalno veći od problema umrežavanja. Nova internetska infrastruktura zahtjeva različit hardver i softver namjenjen za pružanje usluga, automatizaciju i fleksibilnost koje zahtjevaju SDx-aplikacije i računarstvo u oblaku. Postavljanje široko razumljivih slučajeva upotrebe SDxl-pomoći će telekomuniacijskoj industriji postići produktivnije razgovore o potrebama korinsika, tehničkim zahtjevima i relevantnim poslovnim rješenjima za SDN i NFV. Ne samo da svi sudionici telekominikacijskog tržišta koriste drugačiju terminologiju kako bi opisali neznatno različite potrebe i potencijalne načine kako bi se te potrebe ispunile, također je potrebno kategorizirati određene slučajeve upotrebe.

Kombinacije SDN-a i NFV-a:

- Kontrolna pristupna mreža: postavljanje odgovarajućih povlastica za korisnike ili uređaje koji pristupaju mrežama, uključujući ograničenje kontrole pristupa i odgovarajuću kvalitetu usluga.
- Mrežna virtualizacja: stvaranje virtualne mreže na fizičkoj mreži, omogučavajući velikom broju mreža pokretanje preko fizičke mreže.
- Virtualna granica korisnika: virtualiziranje granica korisnika moguće je ili stvaranjem virtualne platforme na prostoru koje zauzima korisnik ili povlačenjem funkcija bliže jezgri mreže na virtualnoj multinacionalnoj platformi.
- Dinamičan međuodnos: izrađuju se dinamičke veze između lokacija, uključujući veze između podatkovnih centara, organizacija i drugih lokacija.
- Virtualne organizacijske mreže. Virtualiziraju se osnovni sistemi za davatelje usluga, uključujući mobilnu infrastrukturu.
- Optimizacija podatkovnog centra: optimizacija mreže pomoću SDN-a i NFV-a, u svrhu otkrivanja performansi aplikacija i uzimajući u obzir afinitete i skokove promjene opterećenja konfiguracije mreže.

Softverski definisana mreža specifičan je način primjene definisanog umrežavanja koja se primjenjuje na WAN-mreže, koja se koristi za povezivanje mreža na velikim geografskim udaljenostima. Poslovni korisnici zahtjevaju fleksibilnije, otvorene i WAN-tehnologije temeljene na računarstvu u oblaku, umjesto instaliranja specijalizirane WAN-tehnologije koja često uključuje skupe, fiksne sklopove ili posjedovanje hardverske opreme. Tehnologija virtualizacije može primjeniti tehnologiju sigurnosti i virtualne privatne mreže na širokopojasne internetske veze, što ih čini sigurnijima. Glavni cilj tehnologije SD-WAN je pružanje sigurne i jednostavne WAN-veze omogućene za računarstvo u oblaku i otvorene za softverske tehnologije. Vodeći proizvođači opreme su promijenili pristup tržištu nakon uočavanja performansi SD-WAN-a, kao što su CISCO i Riverbed, koje proizvode specijalizirane uređaje za WAN- povezivanje.

2.6 Sigurnost softverski definisanih mreža

Sigurnost mreže jedan je od najvažnijih faktora u današnjim organizacijama i upotrebi mreža. Stručnjaci zaduženi za sigurnost svaki dan poboljšavaju i razvijaju nove metode zaštite od postojećih kao i novih vrsta napada i neovlaštenih prisupa podacima. SDN se može koristiti za poboljšanje sigurnosnog položaja organizacije nadopunjavanjem sigurnosnih kontrola koje organizacijama omogućava praćenje, otkrivanje i odgovor na sigurnosne incidente. Prednosti sigurnosti SDN-a:

- Segmentacija mreže: segmentacija mreže uključuje stvaranje podmreža unutar veće mreže. Segmentacija može pomoći u razdvajanju i organiziranju mrežnog prometa organizacije ili ustanove. To omogućava učinkovitiju upotrebu propusnosti smanjenjem veličine domena emitovanja i smanjenjem nepotrebnog prometa na mreži.
- Lakše centralizirano daljinsko upravljanje: virtualiziranom mrežnom sigurnošću temeljenom na softveru lakše je upravljati s jedne centralizirane nadzorne ploče. To znači da mrežni i sigurnosni administratori mogu pristupiti i pregledati na daljinu. Uz softverski definisanu sigurnost stručnjaci za mrežnu sigurnost mogu pratiti sigurnost svih zaposlenika, bez obzira gdje se nalaze.
- Automatizacija: trenutne arhitekture vatrozida ne skaliraju se dobro, a to može ometati agilnost poslovanja. Vatrozid virtualne mreže omogućava da se iskoriste iste karakteristike kao i hardverski vatrozidi, ali dodaju više agilnosti, fleksibilnosti i skalabilnosti.
- Skalabilnost: velika prednost virtualizirane i softverski definirane mreže je skalabilnost. Mnogo je lakše sklairati virtualizirane procese i mrežne komponente jer ne zahtjevaju kupovinu novog hardvera. Ako sigurnost zahtjeva više sistemskih resursa dostavljač mu može dodijeliti nove usluge. Sigurnosni alati kao što je virtualni vatrozid može se implementirati po volji, što omogućava besprijekoran rast poslovanja.
- Manji fizički otisak: softverski definisana sigurnost hostirana je na virtualnim računarima. Virtualizirane funkcije mogu se povećati ili smanjiti ovisno o zahtjevima što omogućava smanjenje troškova za infrastrukturu i naknadu za usluge.

Organizacije mogu implementirati različite alate i procese kako bi osigurale sigurnost sa SDN-om. Jedna je višefaktorska provjera autentičnosti, metoda provjere autentičnosti u kojoj se korisniku odobrava pristup tek nakon što prikaže dva ili više dokaza mehanizmu autentifikacije. Osim toga, msp-ovi bi trebali provoditi periodične procjene kako bi otkrili i riješili probleme kao što su pogrešne konfiguracije i ranjivosti. Također, dobra je praksa nadopuniti sigurnosne kontrole SDN-a pomoću analitičkih rješenja za mrežnu sigurnost. Naprimjer, Bitdefenderova analiza mrežnog prometa, ključna komponenta proširenog otkrivanja i odgovora, primjenjuje inteligenciju prijetnji, mašinsko učenje i analitiku ponašanja na mrežni promet kako bi rano otkrila napredne napade i omogućila učinkovit odgovor na prijetnje.

2.7 Sigurnosni rizik SDN-a

Jedan od najznačajnijih faktora sigurnosnog rizika je mogućnost ugroženog napada SDN-kontrolera na sloj upravljačke ravni. Zbog centraliziranog dizajna SDN-a, SDN-kontroler postaje mozak SDN-arhitekture. Napadači se mogu usredotočiti na ugrožavanje SDN-kontrolera u pokušaju manipuliranja cijelom mrežom. Ako napadač uspješno dobije pristup, ugroženi SDN-kontroler može se koristiti za usmjeravanje mrežnih uređaja koje kontroliše da odustanu od svih dolaznih prometa ili pokrenu ozbiljne napade na druge ciljeve, poput slanja beskorisnig prometa žrtvi kako bi iscrpila svoje resurse.

Da bi se ublažio ovaj sigurnosni rizik ključno je očvrsnuti operativni sistem koji hostira SDN-kontroler i spriječiti neovlašteni pristup SDN-kontroleru. Sloj upravljačke ravni podložan je napadu distribuiranog uskraćivanja usluge, tj. DDoS napad. SDN-skretnice mogu uzrokovati da SDN-kontroler bude preplavljen mnogim upitima koji mogu uzrokovati kašnjenj ili pad mreže. Ako napadač komprimira SDN-kontroler, mogu hakirati SDN-aplikacije kako bi manipulisali sigurnosnim aplikacijama kako bi reprogramirali protok mrežnog prometa kroz SDN-kontroler. Na sloju podatkovne ravnine prekidači su osjetljivi i na napade uskraćivanja usluge. Zlonamjerni korisnik može preplaviti prekidače velikim korisnim teretom, uzrokujući ispuštanje legitimnih paketa kada se prekorači mogućnost međuspremnika prekidača. Postoji mnogo načina za rješavanje ovog napada, uključujući proaktivno predmemoriranje pravila, agregaciju pravila i smanjenje kašnjenja u komunikaciji prijelaza na SDN-kontroler. Također, povećanje mogućnosti međuspremnika prekidača može ublažiti rizik od DoS-napada. Komuniciranje poruka između sloja upravljačke ravnine i sloja ravni podataka podložno je napadima čovjeka u sredini. Napadač može potencijalno izmijeniti pravila s SDN-kontrolera u prekidače kako bi preuzeo kontrolu nad prekidačima. Jedno od najučinkovitijih rješenja za takve napade je šifrovanje poruka korištenjem korisnih digitalnih potpisa za osiguranje i provjeru integriteta i autentičnosti poruka. Programabilnost u stvarnom vremenu je otvorena za ozbiljnu ranjivost na sloju ravnine aplikacije. Konkretno, ako napadač može hakirati SDN-sigurnosne aplikacije, može manipulirati protokom mrežnog prometa kroz SDN-kontroler. Ako su SDN-aplikacije ugrožene, ugrožena je i cijela mreža. Kako bi se učinkovito ublažio takav sigurnosni rizik, ključno je da se prakse sigurnosnog kodiranja provode sveobuhvatnim postupcima upravljanja promjenama i provjere integritet kao dio životnog ciklusa razvoja softvera.

ZAKLJUČAK

SDN pruža novu, dinamičku mrežnu arhitekturu koja transformiše tradicionalne odnovne mreže bogate servisne platforme. Odjavljujući mrežni sloj i sloj podataka, OpenFlow bazirana SDN-arhitektura razdvaja temeljnu infrastrukturu od aplikacija koje je koristi, čime mreža postaje programabilna i upravlja na nivou računarske infrastrukture kojoj sve više nalikuje. Implementiranje SDN-rješenja zahtjeva dobro planiranje. Organizacije trebaju imati jasnu ideju o prednostima za koje misle da će ih realizirati implementacijom SDN-a. SDN potiče mrežnu virtualizaciju, omogućavajući administratorima upravljanje servisima, aplikacijama, skladištenjem i mrežama sa zajedničkim pristupom. Budućnost umrežavanja će se sve više oslanjati na softver, koji će ubrzati razvioj inovacija za mreže kao što je to u računarskim i domenima za skladištenje. SDN omogućava transformaciju današnje statičke mreže u jednu fleksibilnu, programabilnu platformu s integracijom dinamičkog alociranja sredstava. Najveći izazov pri implementaciji i konfiguriranju SDN-rješenja za administratore predstavljaju performanse mreže, skalabilnost, sigurnost i interoperabilnost. U konvencionalnoj mreži potreno je konfigurisati ručno svaki switch posebno što zahtjeva dostva više vremena i postupaka. Kod SDN-rješenja sve postupke, od konfiguriranja switch-eva i učenja mrežne topologije, prilikom prvog spajanja obavlja SDN-kontroler s jednog centraliziranog mjesta u vrlo kratkom vremenskom roku. Prema analizama i istraživanjima može se zaključiti da implementacija SDN-mreže može unaprijediti poslovanje jedne organizacije.

LITERATURA

1. Nadeau, T. D., Gray, K.: "SDN: Software Defined Networks", O'Reilly Media, Inc., 1. izdanje, California, 2013.
2. Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti, n.d. A Survey of Software-Defined Networking: Past,. s.l.:s.n.
3. Hartman, S., Wasserman, M., Zhang, D.: “Security Requirements in the Software Defined Networking Model”, Internet Engineering Task Force, Internet-Draft draft-hartman-sdnsec-requirements-01, April 2013.
4. J. Cassey; Introduction to SDN and Openflow;INE; (2015);
5. Lim, A.; “Security Risks in SDN and Other New Software Issues,” RSA Conference 2015, July 2015.
6. Underdahl, B.; G. Kinghorn; Software Defined Networking for Dummies, John Wiley & Sons, USA, 2015.
7. Kepes, B.: "SDN meets the real-world: Implementation benefits and
8. challenges", GIGAOM RESEARCH, 2014.
9. Dabbagh, M.; B. Hamdaoui; M. Guizani; A. Rayes; “Software-Defined Networking Security: Pros and Cons,” IEEE Communications Magazine, vol. 53, iss. 6, May 2015
10. MARGARET ROUSE, Generic Routing Encapsulation (GRE), 2011.
11. N. Freamster, J. Rexford, E. Zegura; The Road to SDN
12. Kim, H.; N. Feamster; “Improving Network Management With Software Defined Networking,” IEEE Communications Magazine, vol. 51, iss. 2, February 2013, p. 114-119