VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

Omrežja sodobnih podatkovnih centrov z arhitekturo CLOS

Kandidat: Luka Filipič

Vrsta študija: študent izrednega študija

Študijski program: Informatika

Mentor predavatelj: dr. Simon Žnidar, univ. dipl. inž. el.

Mentor v podjetju: mag. Damijan Markovič, univ. dipl. inž. rač.

Lektorica: dr. Aleksandra Gačić Belej, univ. dipl. prof. zgo. in slov.

Maribor, 2024

Sensitivity Classification: Internal

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Luka Filipič sem avtor diplomskega dela z naslovom Omrežja sodobnih podatkovnih centrov z arhitekturo CLOS, ki sem ga napisal pod mentorstvom dr. Simona Žnidarja, univ. dipl. inž. el., in mag. Damijana Markoviča, univ. dipl. inž. rač.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Celje, september 2024 Podpis študenta: Luka Filipič

Sensitivity Classification: Internal

ZAHVALA

Na tem mestu se iskreno zahvaljujem vsem, ki so me podpirali in mi pomagali pri pisanju tega diplomskega dela.

Najprej se zahvaljujem mentorju dr. Simonu Žnidarju za njegovo strokovno vodenje, neprecenljive nasvete skozi celoten proces priprave in pisanja diplomskega dela.

Iskreno zahvalo izrekam tudi sodelavcu mag. Damijanu Markoviču – Foxyu za njegovo pomoč, nasvete in podporo. Njegove usmeritve so bile ključne za uspešno dokončanje tega dela.

Posebna zahvala je namenjena mojemu dekletu Sari za njeno neizmerno razumevanje, potrpežljivost in podporo skozi celoten študij in pisanje diplomskega dela. Njena spodbuda mi je dala moč in motivacijo, da sem uspešno zaključil to pomembno poglavje v svojem življenju.

Diplomsko delo posvečam svojima pokojnima staršema, ki sta me ves čas skozi celotno življenje neizmerno spodbujala in verjela v moj uspeh.

Sensitivity Classification: Internal

POVZETEK

V zadnjih nekaj letih smo priča hitremu porastu uporabe aplikacij in storitev, ki so dostopne predvsem preko javnega oblaka. Na enak način se povečuje tudi zanimanje za dostopnost storitve znotraj posameznih organizacij, ki so gostovane v zasebnem ali hibridnem oblaku. Ta trend prinaša številne prednosti, kot so povečana agilnost, razširljivost, elastičnost in dostopnost do podatkov ter storitev od kjer koli in kadar koli. Vendar zahteva tudi ustrezno in robustno infrastrukturo podatkovnih centrov, ki lahko zagotovi nemoteno delovanje in varnost teh storitev.

Diplomsko delo je posvečeno opisu sodobnih konceptov, posameznih gradnikov in arhitekture omrežij sodobnega podatkovnega centra. V prvem delu se osredotočam na sodobne trende in vpliv pojava računalništva v oblaku na razvoj arhitekture omrežij podatkovnih centrov in zgodovinski pregled različnih arhitekturnih konceptov. V nadaljevanju sledi opis primernih protokolov in tehnologij za zagotavljanje učinkovitega delovanja oblačnih storitev, pri čemer je nujna moderna arhitektura podatkovnih centrov, kot je arhitektura CLOS. Ta arhitektura omogoča visoko zmogljivost, zanesljivost in razširljivost omrežij, kar je ključno za podporo velikim obremenitvam in hitro spreminjajočim se potrebam uporabnikov storitev. Poleg tega omogoča preprosto upravljanje omrežja in izboljšano varnost, kar je bistveno za zaščito podatkov ter zagotavljanje skladnosti z različnimi standardi in predpisi.

Vzpostavitev in vzdrževanje sodobne omrežne infrastrukture v podatkovnih centrih sta vse pomembnejša. To vključuje uporabo naprednih tehnologij, kot so navidezna okolja, avtomatizacija in orodja za nadzor, ki omogočajo učinkovito upravljanje in optimizacijo virov. S tem se zagotavljajo zanesljivost, varnost in visoka razpoložljivost storitev, kar je ključno za zadovoljstvo končnih uporabnikov. Predstavljena so teoretična izhodišča in možnosti uporabe umetne inteligence pri upravljanju in nadzorovanju omrežja.

V zadnjem delu diplomskega dela je predstavljen primer takšnega omrežja iz prakse, ki vsebuje vse lastnosti sodobne arhitekture podatkovnih centrov.

Ključne besede: podatkovni center, sodobna omrežja, CLOS, arhitektura Spine-Leaf, arhitektura podatkovnih centrov.

Sensitivity Classification: Internal

ABSTRACT

Networks of Modern Data Centers with CLOS Architecture

In recent years, we have witnessed a rapid increase in the use of applications and services that are primarily accessible through the public cloud. Similarly, interest in the availability of services within individual organizations hosted in private or hybrid clouds is also growing. This trend brings numerous advantages, such as increased agility, scalability, elasticity, and access to data and services from anywhere, at any time. However, it requires an appropriate and robust data center infrastructure to ensure the smooth operation and security of these services.

This thesis is dedicated to describing modern concepts, individual components, and the architecture of networks in modern data centers. The thesis focuses initially on modern trends and the impact of cloud computing on the development of data center network architecture, as well as a historical overview of various architectural concepts. Following this, there is a description of suitable protocols and technologies necessary for ensuring the efficient operation of cloud services, requiring a modern data center architecture such as the CLOS architecture. This architecture enables high performance, reliability, and scalability of networks, which is crucial for supporting heavy workloads and the rapidly changing needs of service users. Additionally, it allows for easy network management and improved security, which is essential for data protection and ensuring compliance with various standards and regulations.

The establishment and maintenance of modern network infrastructure in data centers are becoming increasingly important. This includes the use of advanced technologies such as virtual environments, automation, and monitoring tools that enable efficient management and resource optimization. This ensures the reliability, security, and high availability of services, which is crucial for end users' satisfaction. The theoretical foundations and possibilities of using artificial intelligence in network management and monitoring are also presented.

In the final section of this thesis, an example of such a network from practice is presented, encompassing all the features of modern data center architecture.

Keywords: data center, modern networks, CLOS, Spine-Leaf architecture, data center architecture

Sensitivity Classification: Internal

KAZALO VSEBINE

Sensitivity Classification: Internal

Sensitivity Classification: Internal

KAZALO SLIK

Sensitivity Classification: Internal

UVOD

V zadnjih petnajstih letih je prišlo do eksponentnega porasta uporabe aplikacij in storitev, ki gostujejo v različnih tipih podatkovnih centrov. Z naraščajočo priljubljenostjo računalništva v oblaku so se podatkovni centri razvili v zahtevne IKT-sisteme, ki morajo zagotavljati visoko zmogljivost, zanesljivost, razširljivost in varnost. Tradicionalne omrežne arhitekture pogosto ne zadoščajo več tem zahtevam, zato se uvajajo nove rešitve, kot je arhitektura CLOS (arhitektura, poimenovana po znanstveniku Charlesu Closu, ki jo je v letih po letu 1950 formaliziral), ki omogoča učinkovitejše delovanje in upravljanje podatkovnih centrov.

Arhitektura CLOS, prvotno razvita za potrebe telekomunikacijskih omrežij, je postala ključna tehnologija tudi v svetu podatkovnih centrov. Značilna je po svoji razširljivosti in zmožnosti obvladovanja velikih obremenitev ter podpiranju hitrega prilagajanja potrebam uporabnikov. Omrežja, zasnovana po tej arhitekturi, zagotavljajo nizko latenco in visoko prepustnost, kar je bistveno za sodobne aplikacije in storitve.

1.1 Opis področja in opredelitev problema

Področje raziskovanja obsega računalniška omrežja, natančneje in podrobneje se osredotoča na računalniške in telekomunikacijske protokole, tehnologije, uporabljene znotraj sodobnih podatkovnih centrov. Opravljena sta pregled razvoja in uporabljenih konceptov s prednostnimi in slabostmi ter primerjava s sodobnimi arhitekturami. Kljub prednostim, ki jih prinaša arhitektura CLOS, se organizacije pri implementaciji še vedno srečujejo s številnimi izzivi. Ena izmed glavnih težav je kompleksnost zasnove in upravljanja takšnih omrežij. Potrebno je poglobljeno razumevanje specifičnih tehnologij in protokolov, ki omogočajo učinkovito delovanje teh omrežij. Poleg tega je pomembno zagotoviti visoko raven varnosti, saj so podatkovni centri tarča številnih kibernetskih napadov. Vzpostavitev in vzdrževanje sodobne omrežne infrastrukture zahtevata tudi uporabo naprednih orodij za nadzor in optimizacijo virov, kar predstavlja dodatne izzive za organizacije.

1.2 Namen, cilji in osnovne trditve

Diplomsko delo se osredotoča na podrobno preučitev arhitekture CLOS in njenih prednosti ter izzivov pri implementaciji v sodobnih podatkovnih centrih. Namen je raziskati, kako lahko uporaba te arhitekture izboljša delovanje podatkovnih centrov, ter predstaviti praktične primere uporabe in primere dobrih praks za uspešno implementacijo.

Diplomsko delo vsebuje naslednje hipoteze:

- H1: Arhitektura »Spine-Leaf« (omenjena arhitektura predstavlja sodoben način izgradnje omrežij podatkovnih centrov) omogoča boljšo razširljivost podatkovnih centrov v primerjavi s tradicionalnimi topologijami.
- H2 Podatkovni centri, zgrajeni na topologiji »Spine-Leaf«, dosegajo nižjo omrežno latenco in so zanesljivejši v primerjavi s podatkovnimi centri, ki uporabljajo tradicionalne topologije.
- H3: Arhitektura »Spine-Leaf« omogoča večjo fleksibilnost pri upravljanju omrežja, kar vodi k hitrejšemu prilagajanju spreminjajočim se potrebam podatkovnega centra.
- H4: Arhitektura »Spine-Leaf« omogoča preprostejše upravljanje in s tem bolj optimalne stroške za delovanje omrežja podatkovnih centrov.
- H5: Zaradi preproste arhitekture »Spine-Leaf« omrežij je uvajanje v UI (umetne inteligence) preprostejše ter tako natančnejše in hitrejše odkrivanje nepravilnosti tako v konfiguracijah kot tudi delovanju omrežja.

1.3 Uporabljene raziskovalne metode

V nadaljevanju diplomskega dela bodo uporabljene naslednje raziskovalne metode:

- lastno pridobljeno znanje,
- primerjalna metoda,
- pregled obstoječe strokovne literature,
- analiza podatkov.

2 ARHITEKTURA PODATKOVNIH CENTROV

2.1 Uvod in trendi

S pospešenim razvojem računalništva v oblaku in z izkoriščanjem njegovih prednosti, kot so doseganje boljšega izkoristka strojne opreme in posledično zmanjševanje stroškov kapitala, hitrejša in boljša prilagodljivost uporabniškim zahtevam, učinkovito spremljanje uporabljenih virov, vsesplošna dostopnost itd., se vse več podjetij in organizacij odloča za selitev svojih storitev in aplikacij iz tradicionalnih podatkovnih centrov k ponudnikom oblačnega gostovanja.

Zaradi želje po izkoriščanju petih glavnih značilnosti računalništva v oblaku, ki so:

- samopostrežna storitev na zahtevo,
- širok dostop do omrežja,
- elastičnost združevanja virov,
- hitra elastičnost,
- izmerjena storitev,

je bilo treba tradicionalno arhitekturo podatkovnih centrov nadgraditi, da omogoča čim bolj optimalno nudenje storitev, aplikacij in vsebin. Nujno potrebno je, da zagotavlja visoko stopnjo kibernetske varnosti in večnajemnega modela, pri čemer je njegova glavna lastnost ta, da si več različnih uporabnikov deli skupne IKT (informacijsko-komunikacijske tehnologije) vire (omrežne, računske in shranjevalne).

Po navedbah svetovno znane organizacije za raziskave in analize trga na področju IKT Gartner Inc. bo v letu 2024 za 20,4 % več porabljenih sredstev za uporabo javnega oblaka v primerjavi z letom 2023, kar znaša 675,4 milijarde ameriških dolarjev. Spodnja tabela predstavlja predvideno rast porabljenih sredstev za storitve javnega oblaka do leta 2025.

	2023 Spending	2023 Growth (%)	2024 Spending	2024 Growth (%)	2025 Spending	2025 Growth (%)
Cloud Application Infrastructure Services (PaaS)	142,934	19.5	172,449	20.6	211,589	22.7
Cloud Application Services (SaaS)	205,998	18.1	247,203	20.0	295,083	19.4
Cloud Business Process Services (BPaaS)	66,162	7.5	72,675	9.8	82,262	13.2
Cloud Desktop-as-a-Service (DaaS)	2,708	11.4	3,062	13.1	3,437	12.3
Cloud System Infrastructure Services (IaaS)	143,302	19.1	180,044	25.6	232,391	29.1
Total Market	**561,104**	**17.3**	**675,433**	**20.4**	**824,763**	**22.1**

Slika 1: Prikaz porabljenih sredstev za storitve javnega oblaka

Vir: (Gartner, 2024)

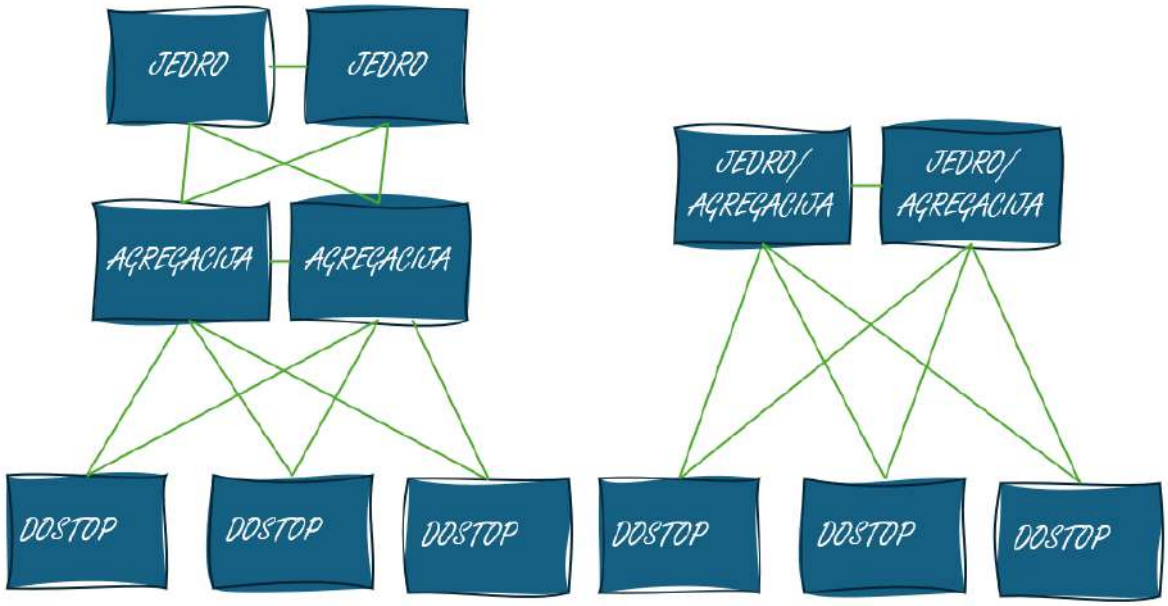
Takšna rast je posledica zelo intenzivnega uvajanja storitev umetne inteligence in modernizacije ter uvajanja novih aplikacij, ki so primerne za oblačno infrastrukturo. Prav to je vzrok za povišano rast storitev PaaS (angl. Platform as a Service) in IaaS (angl. Infrastructure as a Service), ki beležita največjo rast v zadnjih letih. Največji tržni delež še vedno pripada storitvam SaaS (angl. Software as a Service) (Gartner, 2024).

2.2 Arhitektura tradicionalnih podatkovnih centrov

Omrežna topologija tradicionalnih podatkovnih centrov temelji na hierarhični zasnovi, ki praviloma vključuje več plasti omrežnih naprav. Najbolj razširjen sta dva modela drevesne strukture, ki ju predstavlja spodnja slika, Slika 2. Takšna zasnova vključuje naslednje tri glavne plasti oziroma nivoje:

- dostopno plast,
- agregacijsko ali distribucijsko plast,
- jedrno plast.

V primeru manjših podatkovnih centrov se lahko jedrna in agregacijska plast združita v eno in tvorita tako imenovano arhitekturo združenega jedra.



Slika 2: Tradicionalni arhitekturi omrežja podatkovnega centra

Vir: (Lasten vir)

Naprave, uporabljene na dostopni plasti, so stikala, ki omogočajo protokol Ethernet in njihova vloga je priključitev strežnikov in servisnih naprav znotraj posamezne strežniške omare. Znotraj podatkovnega centra lahko namestimo dostopna stikala na konec vrste omar (angl. End of Rack) ali na vrh omare (angl. Top of Rack). Primeri dobrih praks narekujejo večdomni način priklopa končnih naprav in tudi povezovanje dostopnih stikal proti agregacijski plasti.

Stikala na agregacijski plasti ravno tako nudijo podporo protokolu Ethernet in so praviloma vzpostavljena v podvojeni postavitvi. Zagotavljajo neprekinjeno delovanje ob izpadu

posameznega stikala v danem trenutku. Naloga agregacijske plasti sta združevanje povezav dostopne ravni in povezava do jedrne plasti.

Naloga jedrne plasti oziroma Ethernet stikal sta usmerjanje prometa med različnimi omrežnimi segmenti znotraj podatkovnega centra in zagotavljanje povezljivosti s preostalimi logično zaključenimi deli omrežja npr. WAN (angl. Wide Area Network), MAN (angl. Metropolitan Area Network), Internet ipd.

Hitrosti povezav in tipi priključkov (optični, bakreni) so odvisni od posamezne postavitve. Praviloma velja nenapisano pravilo, da hitrosti in zmogljivosti uporabljenih stikal naraščajo od dostopne ravni proti jedrni.

Zagotavljanje varnosti v omrežju tradicionalnega podatkovnega centra je večplastno in razdeljeno na posamezno raven arhitekture. Delitev oziroma segmentacija omrežja v manjše enote je v splošnem zagotovljena s protokolom IEEE 802.1Q ter je odvisna posameznih potreb in strukture organizacije.

V nadaljevanju je naštetih nekaj najpogostejših načinov delitve:

- funkcionalna ali poslovna enota,
- geografska lokacija,
- glede na tipe naprav,
- glede na varnostno politiko,
- glede na vrsto prometa itd.

Dostopna raven nudi varnostne mehanizme, kot so na primer zaščita pred poplavljanjem okvirjev »unicast«, »multicast« in »broadcast«, različne varnostne funkcionalnosti zaščite protokola STP (angl. Spanning Tree Protocol) (BPDU Guard, Root Guard, Loop Guard ipd.), mehanizmi zaznavanja enosmerne komunikacije po optičnem vlaknu (angl. Unidirectional Link Detection) itd.

V tradicionalni omrežni arhitekturi podatkovnih centrov ima agregacijska raven ključno vlogo, saj deluje kot mejna točka med uporabo L2- in L3-protokolov. Na dostopni ravni omrežja se večinoma uporabljajo L2-protokoli, ki omogočajo preprosto preklapljanje in povezovanje končnih naprav. Vse naprave v isti skupini VLAN (angl. Virtual Local Area Network) na tej ravni lahko komunicirajo neposredno s pomočjo L2-protokolov in brez potrebe po usmerjanju.

Ko promet doseže agregacijsko raven, se običajno preklopi z L2- na L3-protokole. Agregacijska raven združuje promet iz več dostopnih stikal in nudi podporo usmerjevalnim protokolom.

Prav zaradi slednjih zagotavljanje varnostne politike temelji na filtrih oglaševanja in sprejemanja usmerjevalnih poti ter uporabe list dostopa na vmesnikih L3.

Opisana arhitektura se spopada z več pomembnimi slabostmi, ki vplivajo na delovanje, učinkovitost in razširljivost omrežja. Ena izmed glavnih slabosti je omejen obseg razširljivosti in lahko postane zelo nepraktična pri veliki količini prometa med posameznimi plastmi. To lahko predstavlja ozko grlo. Zaradi narave delovanja protokola vpetega drevesa (STP) so posamezne podvojene povezave iz strani algoritma postavljene v nedelujoče stanje in s tem preprečujemo možnost nastanka zank na L2-ravni. S tem izgubimo polovico pasovne širine, ki jo imamo na voljo. Sorazmerno visoka raven togosti arhitekture preprečuje hitro in enostavno vpeljavo novih storitev in aplikacij, kar upočasnjuje razvoj in prilagajanje poslovnim potrebam na trgu.

Opisane slabosti so podrobneje opisane in slikovno ponazorjene v naslednjih podpoglavjih.

2.2.1 Neuporabljene povezave, konvergenčni čas in neoptimalno posredovanje prometa

Vsem različicam protokola vpetega drevesa je skupno, da pri svojem delovanju zgradijo drevo in na podlagi blokiranih povezav preprečujejo nastanek zank v omrežju. Rezultat je, da so posamezne povezave med stikali v blokiranem stanju in s tem neizkoriščene za posredovanje prometa. Z višanjem števila sprememb na povezavah je večje število ponovnih izračunov vpetega drevesa in posledično višja poraba sistemskih virov stikal. Druga slabost je visok konvergenčni čas, ki se pojavi ob ponovnem izračunu drevesa. Delovanje protokola lahko optimiziramo na način, da spreminjamo privzete vrednosti časovnikov in s tem zagotovimo stabilno stanje po izpadu pod sekundo, vendar se ob uporabi povezav hitrosti od 10 Gb/s do 100 Gb/s lahko odraža v izpadu prometnih tokov.

Prometni tokovi med pošiljateljem in prejemnikom vedno potujejo skozi stikalo, ki ima vlogo vrha vpetega drevesa, navkljub temu, da lahko v omrežju obstaja krajša pot. Takšen način posredovanja prometa predstavlja neoptimalno delovanje.

2.2.2 Prometni tokovi v podatkovnih centrih

V podatkovnih centrih lahko prometne tokove razdelimo na dve vrsti glede na smer poteka. Prva je v smeri sever-jug, ki predstavlja promet med končnimi uporabniki v različnih delih omrežja proti različnim strežnikom in napravam znotraj podatkovnega centra. Primer dobrih praks narekuje, da se prometne tokove usmeri čez požarno pregrado in uveljavi predpisane varnostne politike.

Drug tip prometnih tokov je v smeri vzhod-zahod in poteka znotraj strežnikov v podatkovnem centru. Ti prometni tokovi so ključni za delovanje aplikacij, ki zahtevajo komunikacijo med različnimi strežniškimi komponentami, kot so na primer aplikacijski in podatkovni strežnik. Z večanjem števila aplikacij se drastično povečuje tudi količina opisanih prometnih tokov.

2.2.3 Poplavljanje okvirjev tipa »broadcast«

V pravilnem delovanju okvirji Ethernet, poslani iz izvornega stikala, ne smejo biti poslani nazaj na isto izvorno stikalo. Zaradi napake v nastavitvah stikal oziroma ne pravilnega delovanja se vseeno lahko zgodi scenarij, v katerem okvirji začnejo krožiti skozi stikala. Zaradi pomanjkanja varnostnega mehanizma pri okvirjih Ethernet se lahko slednji pošiljajo v nedogled. Takšen primer lahko v celoti ohromi delovanje omrežja podatkovnega centra.

Omrežni protokol IP ima varnostni mehanizem v obliki polja TTL (angl. Time to Live), čigar vrednost se zmanjša za ena vsakič, ko paket potuje skozi napravo tipa L3. Ob doseženi vrednosti nič se paket zavrže.

2.2.4 Mobilnost strežnikov in domena odpovedi

Razvoj virtualizacije strežnikov je prinesel marsikatero prednost in poenostavitev sistemske administracije. Mobilnost bremen v tradicionalnih podatkovnih centrih se spopada s pomembnimi omejitvami. Ena izmed glavnih slabosti je kompleksnost naslavljanja naslovov IP in konfiguracije omrežja pri premikanju naprav. Vsaka sprememba fizične lokacije navideznih strežnikov ali končnih naprav pogosto zahteva ročne prilagoditve omrežnih nastavitev, kar lahko povzroči napake. Zaželeno je, da se navidezni delovni stroji s selitvijo med različnimi podatkovnimi centri preselijo brez ponovnega zagona in ohranijo mrežne nastavitve.

Praviloma je v tradicionalnih podatkovnih centrih omogočeno seljenje navideznih delovnih naprav med različnimi geografskimi lokacijami na način, da se ohranijo vsi parametri omrežnih nastavitev. S takšno razširitvijo omrežnega segmenta čez različne fizične lokacije znatno povečamo domeno odpovedi. Ob morebitnih težavah, kot je na primer poplavljanje okvirjev L2, znotraj posameznega omrežnega segmenta, lahko povzročijo težave v delovanju celotnega podatkovnega centra.

2.2.5 Segmentacija omrežja

V tradicionalnih podatkovnih centrih je za delitev omrežja na manjša podomrežja praviloma uporabljen protokol IEEE 802.1Q, ki je princip delitve na skupine VLAN oziroma navidezna omrežja. Standard predpisuje polje TAG znotraj okvirja Ethernet v velikosti 12 bitov, kar pomeni, da je največje možno število VLAN skupin 4.096. V praksi je to število še nekoliko manjše, kajti proizvajalci omrežne opreme in standard predvidevajo nekaj rezerviranih skupin VLAN, ki niso splošno namenske.

Opisani način ima tri poglavitne slabosti. Prva je število možnih skupin VLAN, ki se lahko uporabijo za delitev. Druga je posledica prve, kajti večanje števila skupin se odraža v povečani obremenjenosti kontrolne ravnine stikal in porabi strojnih virov za protokole, kot so usmerjanje, ARP (angl. Address Resolution Protocol), STP itd.

Zadnja slabost je vpeljava varnostne ali omrežne politike, ki temelji na skupinah VLAN in ne na posamezno končno napravo oziroma strežnik. Spreminjanje topologije omrežne infrastrukture vpliva na varnostno oziroma omrežno politiko.

2.3 Arhitektura sodobnih podatkovnih centrov

V zadnjih letih so arhitekture sodobnih podatkovnih centrov začele prevzemati vse večji delež na trgu v primerjavi s tradicionalnimi rešitvami. Tradicionalni podatkovni centri, ki so temeljili na hierarhični omrežni arhitekturi s tremi ravnmi, se vse bolj umikajo bolj elastičnim, razširljivim in zmogljivim rešitvam, ki temeljijo na principu CLOS.

Arhitektura CLOS je poimenovana po Charlesu Closu, ki jo je zasnoval v letih okoli 1950 in jo teoretično opisal za delovanje takratnih telefonskih omrežij.

Eden izmed glavnih razlogov za ta premik je hitro rastoča potreba po obvladovanju velikih količin podatkov in prometa v podatkovnih centrih, kar je posledica digitalne transformacije, oblačnih storitev in razvoja tehnologij, kot so internet stvari (angl. Internet of Things), umetna inteligenca in strojno učenje. Sodobne arhitekture, kot je CLOS oziroma arhitektura »Spine-Leaf«, omogočajo boljšo obravnavo vzhod-zahod prometa, ki prevladuje v današnjih podatkovnih centrih. Te arhitekture zagotavljajo nizko latenco, visoko pasovno širino in zmožnost preproste horizontalne in vertikalne razširitve, kar je ključnega pomena za sodobne aplikacije in storitve.

Poleg izboljšane zmogljivosti sodobne arhitekture omogočajo tudi večjo avtomatizacijo in lažje upravljanje. Tradicionalni podatkovni centri zahtevajo obsežno ročno konfiguracijo in vzdrževanje, kar povečuje operativne stroške in tveganje za napake. Nasprotno sodobne rešitve podpirajo avtomatizacijo omrežnih operacij, kar poenostavlja upravljanje, zmanjšuje stroške in povečuje zanesljivost.

Pri načrtovanju sodobnega podatkovnega centra je treba odgovoriti na vprašanja, ki predvsem naslavljajo opisane pomanjkljivosti tradicionalnih arhitektur, predstavljene v poglavju 2.2:

- Na kakšen način zagotoviti popolno izkoriščenost omrežnih povezav?
- Kako zagotoviti nizek konvergenčni čas ob izpadu posameznega gradnika topologije?
- Ali obstaja način, da prometni tokovi uporabljajo predvidljivo najkrajšo pot med izvorom in ponorom?
- Kako zagotoviti preprosto razširljivost v primeru potrebe po dodatnih strojnih virih?
- Na kakšen način ločiti odvisnost logične topologije in fizične lokacije gostovanja strežnikov?

- Zagotoviti je treba preprosto upravljanje in nadzor.

2.3.1 Arhitektura »Spine-Leaf«

Sodobni podatkovni center mora biti načrtovan kot zaključena celota, ki uporabnikom nudi gostovanje svojih aplikacij in storitev ter omogoča preprosto razširjanje in dodajanje strojnih virov glede na njihove potrebe. Podatkovnih centri, zgrajeni na arhitekturi »Spine-Leaf«, uporabljajo medsebojno povezane omrežne naprave, ki skupaj delujejo kot enotno, integrirano omrežje, ki ga lahko opišemo tudi kot veliko preklopno matriko (angl. Data Center Fabric Switching).

Opisani koncept prinaša več pomembnih lastnosti in koristi, vključno z visoko zmogljivostjo, razširljivostjo, nizko latenco in s preprostim upravljanjem.

V primerjavi s tradicionalno tri ravensko drevesno arhitekturo ima arhitektura »Spine-Leaf« praviloma dve ravni, in sicer:

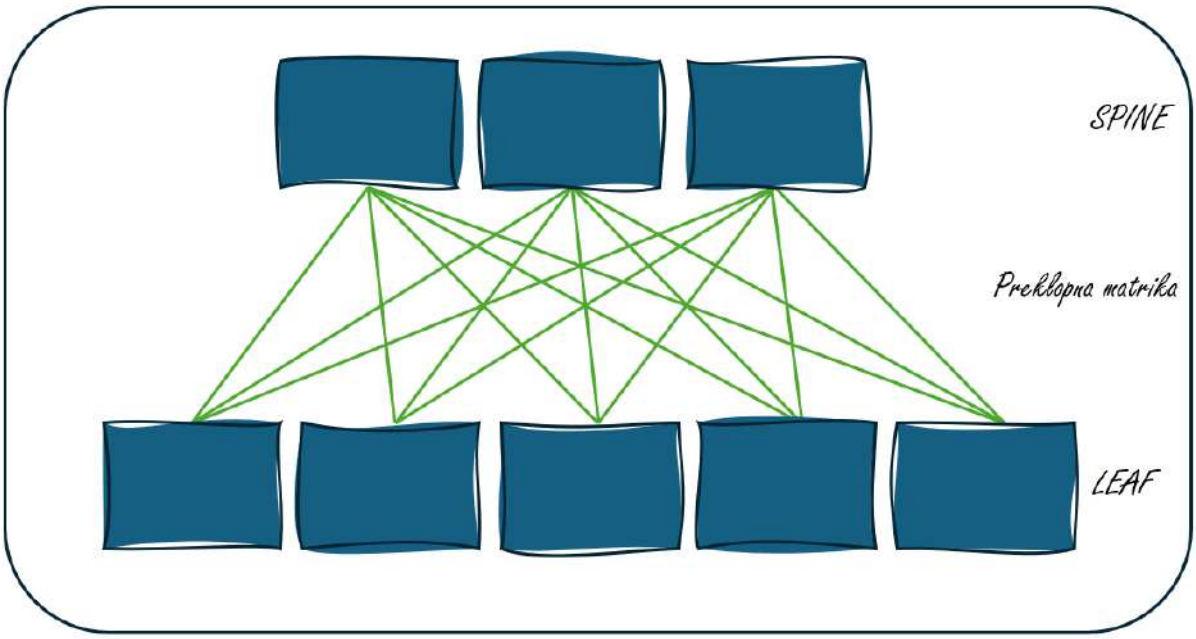
- Dostopno raven (angl. Leaf)

  Stikala dostopne ravni so neposredno povezana s strežniki in končnimi napravami v podatkovnem centru. Vsako stikalo »leaf« se povezuje z vsakim stikalom »spine«, kar omogoča preprosto in predvidljivo širitev omrežja. Iz tega izhaja, da ima vsako stikalo »leaf« enako število povezav do stikal »spine«. To zagotavlja enotno in predvidljivo zmogljivost za vse strežnike in naprave, ne glede na njihovo fizično lokacijo v podatkovnem centru. Stikala dostopne ravni se uporabljajo tudi za priklop servisnih naprav in povezljivost do ostalih logično zaključenih delov omrežja, npr. LAN/MAN/WAN (angl. Wide Area Network).

- Hrbtenična raven (angl. Spine)

  Stikala »spine« delujejo kot hrbtenica omrežja in povezujejo stikala »leaf« med seboj. Vsako hrbtenično stikalo je povezano z vsakim dostopovnim stikalom, kar ustvarja popolnoma povezano omrežje. Primer dobrih praks narekuje, da se na hrbtenična stikala ne povezujejo končne ali servisne naprave. Dopušča se možnost, da se stikala »spine« uporabljajo za povezavo drugih hrbteničnih stikal iz geografsko ločenih podatkovnih centrov.

Spodnja slika predstavlja arhitekturo »Spine-Leaf«.



Slika 3: Arhitektura »Spine-leaf«

Vir: (Lasten vir)

Število povezav med dostopnimi in hrbteničnimi stikali se izračuna po naslednji enačbi in je enako zmnožku števila stikal obeh ravni:

$$Število\ povezav = število\ dostopnih\ stikal \times število\ hrbteničnih\ stikal$$

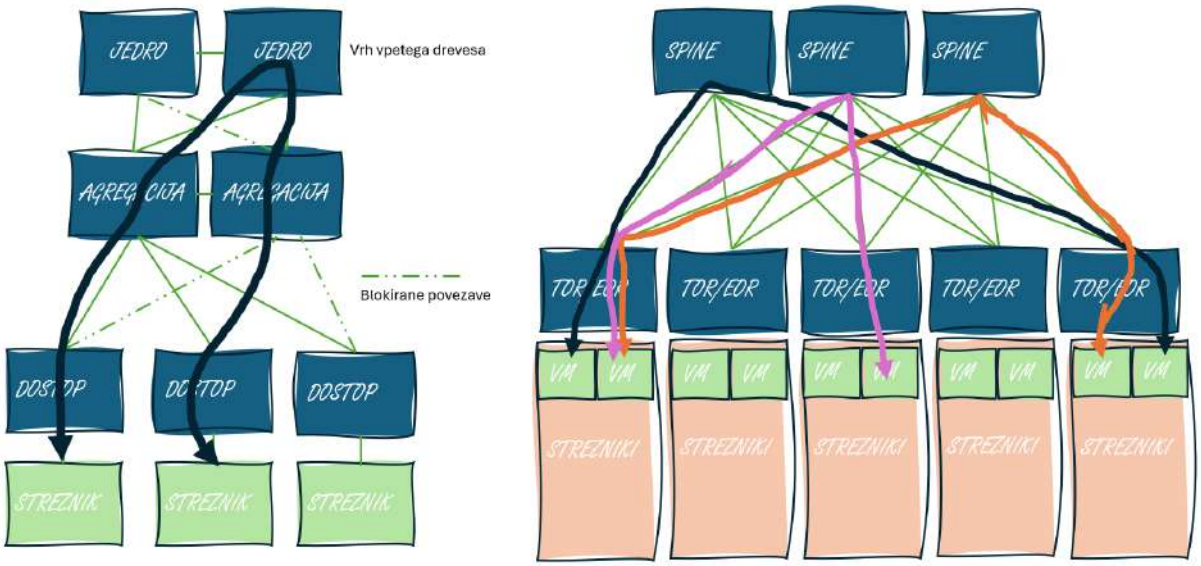
Geometrijska lastnost opisane topologije predpisuje pravilo, da ne glede na lokacijo priklopa končne naprave je med napravam vedno enaka in hkrati najkrajša dolžina poti. Iz tega izhaja, da so zakasnitve v omrežju nizke in predvidljive.

Tradicionalna arhitektura podatkovnih centrov temelji na protokolu vpetega drevesa in njegova narava delovanja postavi vse podvojene povezave v blokirano stanje. S tem izgubimo približno polovico povezav in pasovne širine. Soočamo se tudi z visokimi okrevalnimi časi v primeru ponovnega izračuna drevesa. V nasprotju s tem arhitektura »Spine-Leaf« v podložnem omrežju (angl. Underlay) uporablja povezave tipa L3 in s tem ni potrebe po protokolu STP. Mehanizem enakovrednega usmerjanja prometa (angl. ECMP) poskrbi, da so v prekrivnem omrežju (angl. Overlay) vse povezave enakomerno izkoriščene.

Spodnja slika predstavlja primerjavo med tradicionalno in sodobno arhitekturo omrežja podatkovnega centra in porazdelitev prometnih tokov glede na posamezno povezavo in vozlišče.

Leva stran slike predstavlja prometni tok, ki med dvema končnima napravama vedno poteka skozi vrh vpetega drevesa in zaradi narave delovanja protokola STP je približno polovica povezav neizkoriščenih. V primeru spreminjanja stanja povezav lahko pride do ponovnega izračuna topologije drevesa, kar ima lahko za posledico nepredvidljive zakasnitve in vpliv na prometne tokove.

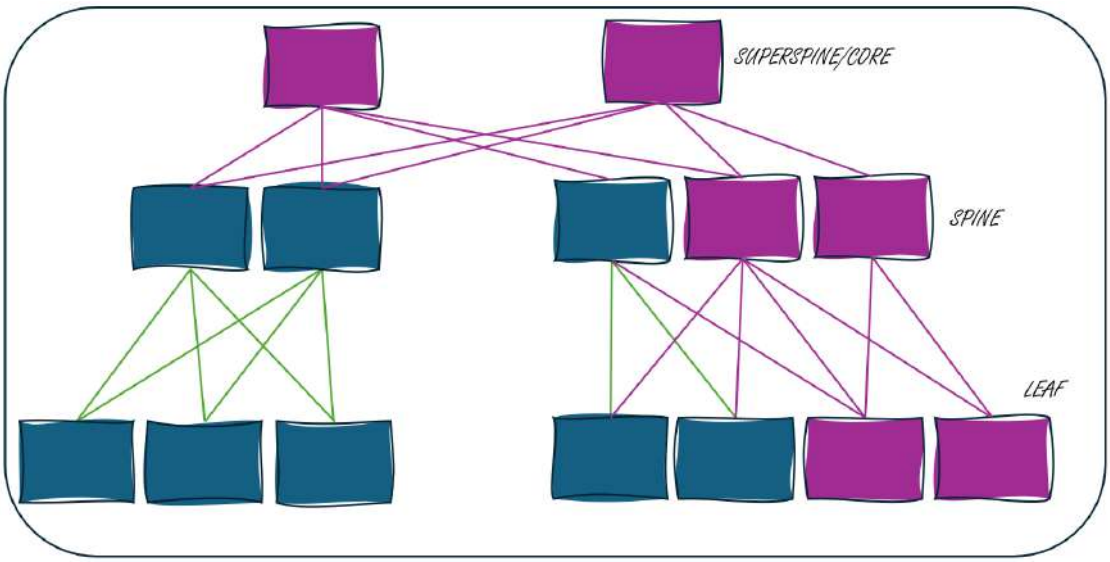
Desni del slike predstavlja prometne tokove med končnimi napravami ter izkoriščenost vseh povezav sočasno med stikali »leaf« in »spine«, kar je posledica uporabe usmerjevalnega protokola namesto protokola STP. Mehanizem porazdeljevanja bremena na podlagi enakih cen zagotavlja, da so vse povezave enakomerno obremenjene. Arhitektura omrežja, zasnovana na principu CLOS, v omrežje vnaša nižje, a predvsem predvidljive vrednosti zakasnitev zaradi svoje geometrijske oblike in sočasno aktivnih povezav.



Slika 4: Primerjava prometnih tokov med tradicionalno in sodobno arhitekturo

Vir: (Lasten vir)

Opisana arhitektura omogoča preprosto razširitev tako v horizontalni kot tudi vertikalni smeri v primeru potrebe dodajanja novih strojnih virov oziroma stikal v omrežje. Primer razširitve je prikazan na naslednji sliki (Slika 5), kjer je uporabljen faktor razširitve dva. Stikala »super spine« se v praksi uporabljajo za povezovanje več geografsko ločenih podatkovnih centrov, ki so zgrajeni na arhitekturi CLOS.



Slika 5: Primer razširitve arhitekture »Spine-Leaf«

Vir: (Lasten vir)

V sodobnih podatkovnih centrih je pojem POD (angl. Point of Delivery) uporabljen za opis modularne enote omrežne in računalniške infrastrukture, ki omogoča učinkovito razširjanje in upravljanje podatkovnega centra. POD je osnovna gradbena enota, ki omogoča preprosto širitev in prilagodljivost glede na potrebe podatkovnega centra.

Njegove glavne značilnosti in gradniki omogočajo izdelavo omrežja sodobnega podatkovnega centra, ki so opisane v nadaljevanju:

- Modularnost

  Zasnovan je kot samostojna enota, ki vključuje vse potrebne komponente za omrežno in računalniško infrastrukturo. Te komponente običajno vključujejo strežnike, omrežna stikala, usmerjevalnike, shranjevalne sisteme, napajalne enote (angl. Uninterruptible Power Supply – UPS), hlajenje in kabelsko infrastrukturo.

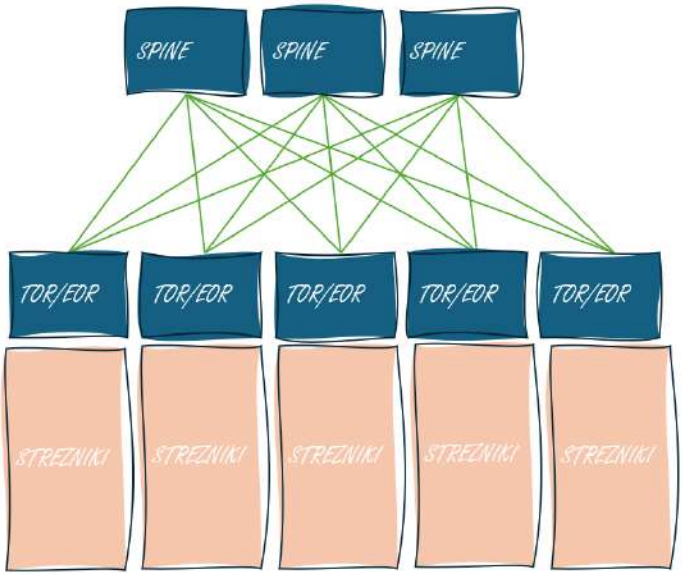
- Učinkovitost

  Optimizirani so za učinkovito delovanje in porabo energije. Standardizirane konfiguracije omogočajo preprosto načrtovanje in implementacijo, kar zmanjšuje čas in stroške namestitve.

- Razširljivost

  Omogočajo preprosto širitev podatkovnega centra. V primeru potrebe po večjih kapacitetah se preprosto dodajo novi POD-i brez potrebe po večjih spremembah obstoječe infrastrukture.

Spodnja slika predstavlja primer uporabe pojma POD v sodobnih podatkovnih omrežjih.



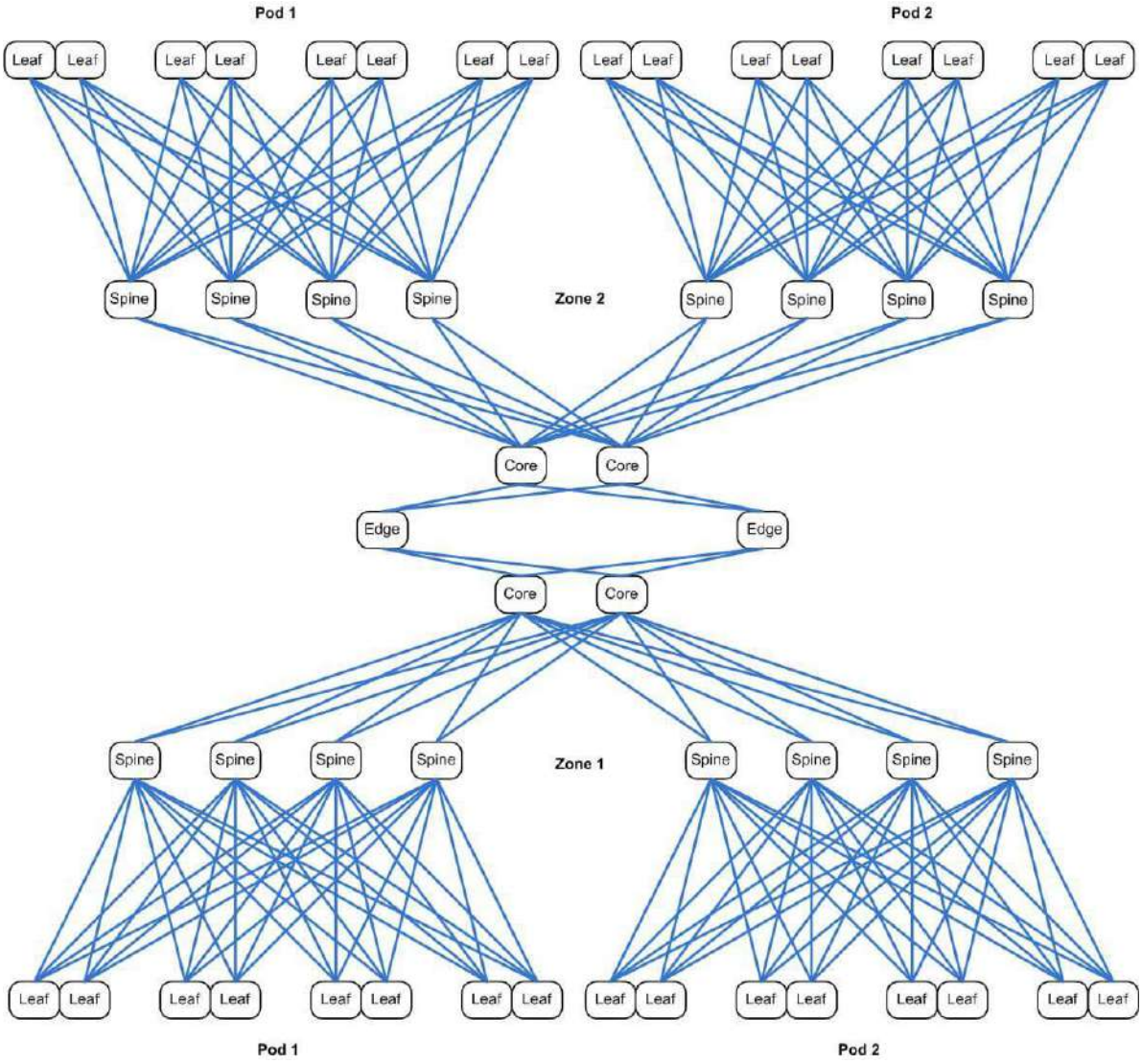
Slika 6: Primer uporabe koncepta POD

Vir: (Lasten vir)

Koncept POD v sodobnih podatkovnih centrih predstavlja modularni pristop k načrtovanju in implementaciji infrastrukture. Ta pristop omogoča preprosto širitev, prilagodljivost in učinkovito upravljanje podatkovnega centra, kar je ključno za podporo sodobnim aplikacijam in storitvam, ki zahtevajo visoko zmogljivost in zanesljivost. Ponudniki javnih oblačnih storitev, uporabljajo zgoraj opisane pristope, kajti le s takšnim arhitekturnim pristopom lahko izvajajo posodabljanje, odstranjevanje in dodajanje posameznih gradnikov. V nadaljevanju je predstavljena visoko ravenska topologija omrežja podatkovnega centra ponudnika DigitalOcean.

Nadgradnja podatkovnega centra ponudnika gostovanja DigitalOcean na lokaciji Frankfurt je poleg dodajanja boljših shranjevalnih polj obsegala tudi celostno prenovo omrežne infrastrukture v podatkovnem centru. Odločili so se za uporabo arhitekture »Spine-Leaf«, kjer dostopovno raven predstavljajo stikala »leaf« in povezujejo strežniške gostitelje v večdomni postavitvi. Vsak gostitelj je povezan na posamezno stikalo »leaf« v paru. Stikala »spine« medsebojno povezujejo vsa stikala dostopovne ravni. Omenjeni gradniki tvorijo zaključeno celoto POD.

Jedrna stikala medsebojno povezujejo več različnih POD-ov znotraj posamezne cone, ki v višjih ravneh abstrakcije ponudnika gostovanja predstavljajo domeno odpovedi. Naloga robnih usmerjevalnikov je povezovanje različnih con (Salvatore, 2015).



Slika 7: Primer arhitekture »Spine-Leaf« v omrežju ponudnika gostovanja DigitalOcean

Vir: (Salvatore, 2015)

3 UPORABLJENE TEHNOLOGIJE IN PROTOKOLI ZA IZGRADNJO SODOBNEGA OMREŽJA V PODATKOVNEM CENTRU

3.1 Tipi povezav

Opisana arhitektura »Spine-Leaf« je zasnovana za zagotavljanje visoke prepustnosti, nizke zakasnitve in razširljivosti v sodobnih podatkovnih centrih. Ena izmed ključnih komponent te arhitekture so povezave med stikali in njihove lastnosti. Za zagotavljanje visoke hitrosti tako na kratke kot tudi daljše razdalje je praviloma uporabljena tehnologija prenosa podatkov s pomočjo optičnih povezav različnih hitrosti. Danes so najpogosteje uporabljene hitrosti 10, 25 in 40 Gbs za priklop končnih naprav na dostopovna stikala ter hitrosti od 100Gbs dalje za medsebojno povezavo stikal in podatkovnih centrov.

Za izgradnjo povezav lahko uporabimo različne tipe vmesnikov SFP/QSFP, glede na razdaljo, hitrost, lastnosti optične povezave ipd. Najpogosteje se znotraj podatkovnih centrov uporablja tehnologija večrodovnega optičnega vlakna (angl. multi-mode fiber), saj so razdalje kratke. Prav v ta namen so proizvajalci omrežne opreme in kablov razvili poseben tip kabla, imenovan »DAC« (Direct Attach Cable) ali »twinax«. Gre za optični (lahko tudi bakren) kabel, ki ima na obeh koncih že tovarniško vgrajen priključni vmesnik.

Povezave med podatkovnimi centri so lahko zgrajene na več različnih načinov in njihova prepustnost je odvisna od količine prometa, ki se usmerja med lokacijami podatkovnih centrov. Uporabljene so lahko namenske najete optične povezave, transportni optični sistemi z zgoščenim valovnim ali grobim valovnim multipleksiranjem in L2 MPLS VPN-rešitvijo.

Osnovna velikost paketa se poveča zaradi ovijanja (enkapsulacije) v prekrivnem omrežju in je treba upoštevati višje vrednosti MTU na transportni poti.

3.2 Komunikacijske naprave

Za izgradnjo sodobnega podatkovnega centra z arhitekturo »Spine-Leaf« so ključna zmogljiva in fleksibilna stikala, ki podpirajo visoko gostoto priključkov, nizko zakasnitev in napredne funkcije za avtomatizacijo in upravljanje omrežja. Na tržišču obstaja več različnih proizvajalcev namenske opreme IKT, kot so Cisco Nexus 9000, Arista 7000, Juniper QFX ipd.

Stikala morajo zagotavljati podporo naslednjim protokolom in tehnologijam:

- VXLAN (Virtual Extensible LAN)

  VXLAN omogoča ustvarjanje navideznih L2-omrežij nad L3-infrastrukturo. Ovija okvirje Ethernet v UDP-pakete za prenos s pomočjo IP-omrežja.

- EVPN (Ethernet VPN)

  Tehnologija EVPN zagotavlja nadzorni protokol za VXLAN-omrežja, omogoča distribucijo naslovov MAC in informacij o VNI med omrežnimi napravami (Leaf).

- MP-BGP (Multiprotocol Border Gateway Protocol)

  Protokol MP-BGP predstavlja razširitev tradicionalnega BGP z dodatnimi atributi, ki omogočajo prenos informacij o L2- in L3-omrežjih in napravah. Uporablja se tudi za distribucijo EVPN-informacij med napravami.

- OSPF (Open Shortest Path First) ali IS-IS (Intermediate System to Intermediate System)

  Zagotavljata usmerjanje med omrežnimi napravami topologije »Spine-Leaf« in omogoča prenos VXLAN-paketov s pomočjo omrežja.

- BGP-EVPN (BGP Ethernet VPN)

  Implementacija BGP-EVPN je specifična implementacija EVPN, ki uporablja MP-BGP za distribucijo EVPN-informacij. Zagotavlja funkcionalnosti, kot so »anycast gateway«, »host mobility« in segmentacija omrežja.

3.3 Podložno in prekrivno omrežje

V današnjih sodobnih podatkovnih centrih sta učinkovito upravljanje in optimizacija omrežnih virov ključnega pomena za zagotavljanje visoke zmogljivosti, zanesljivosti in prilagodljivosti. V tem kontekstu se vse bolj uveljavljata koncepta podložnega omrežja (angl. underlay network) in prekrivnega omrežja (angl. overlay network). Ti dve plasti omrežne infrastrukture skupaj omogočata boljšo izkoriščenost navideznih virov in preprostejše upravljanje omrežja.

3.3.1 Podložno omrežje

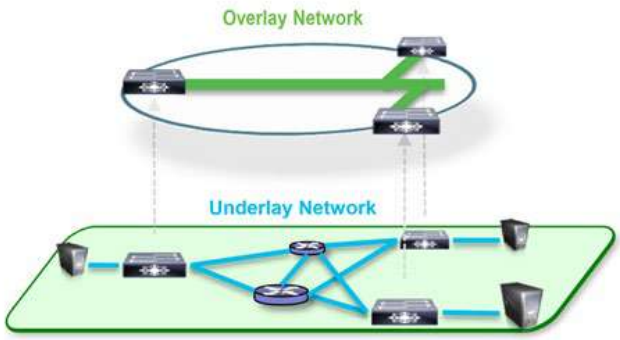
Predstavlja fizično infrastrukturo podatkovnega centra. Sestavljeno je iz stikal, usmerjevalnikov, kablov in drugih naprav, ki tvorijo osnovno mrežno strukturo. Podložno omrežje je odgovorno za prenos podatkov med različnimi napravami in lokacijami v podatkovnem centru ter zagotavlja stabilno in zanesljivo osnovo za delovanje prekrivnih omrežij. Njegova glavna naloga je zagotavljanje robustne, zanesljive in razširljive fizične povezljivosti, ki podpira vse omrežne operacije.

3.3.2 Prekrivno omrežje

Prekrivno omrežje na drugi strani deluje na vrhu podložnega omrežja in omogoča napredne funkcionalnosti, kot so navidezna omrežja, segmentacija prometa ter fleksibilno in dinamično upravljanje omrežnih virov. Sodobna prekrivna omrežja omogočajo različne protokole, kot so VXLAN, NVGRE in STT.

Med najbolj uveljavljenimi protokoli je protokol VXLAN, ki omogoča razširitev lokalnih omrežij s pomočjo fizičnih omrežja in zagotavlja virtualne povezave med različnimi deli omrežja, ne glede na njihovo fizično lokacijo.

Spodnja slika predstavlja zgoraj opisana koncepta obeh omrežij.



Slika 8: Podložno in prekrivno omrežje

Vir: (Zeni, 2024)

3.4 Preklopna matrika sodobnega podatkovnega centra

Preklopna matrika (angl. switch fabric) sodobnega podatkovnega centra predstavlja osrednji del omrežne infrastrukture, kjer se upravlja in usmerja promet med različnimi deli omrežja. Gre za visoko zmogljiv sistem, ki omogoča hitro in učinkovito preklapljanje podatkov med strežniki, shranjevalnimi polji in zunanjim omrežjem.

Zgradimo lahko preklopno matriko s preklapljanjem, ki deluje na ravni L2 oziroma z usmerjanjem na ravni L3. L2-preklapljanje omogoča hitro posredovanje podatkov na podlagi naslovov MAC, medtem ko L3-usmerjanje omogoča prenos na podlagi naslovov IP, kar je pomembno za povezovanje različnih segmentov omrežja.

3.4.1 Preklopna matrika s preklapljanjem

Skozi čas in razvoj različnih tehnologij za izdelavo omrežij podatkovnih centrov sta se pojavila dva protokola, ki temeljita na preklapljanju:

- TRILL in
- Shortest-Path Bridging – SPB.

3.4.1.1 Protokol Transparent Interconnection of Lots of Links – TRILL

TRILL je protokol, ki je bil razvit za izboljšanje delovanja tradicionalnih omrežij Ethernet, zlasti v velikih podatkovnih centrih. Protokol združuje prednosti tako L2- kot L3-omrežij, s čimer izboljšuje razširljivost, prilagodljivost in zanesljivost omrežja.

Njegove ključne značilnosti so:

- Uporaba usmerjevalnega protokola IS-IS

  TRILL uporablja omenjeni protokol za usmerjanje, kar omogoča učinkovito porazdelitev in upravljanje prometnih poti v omrežju.

- Zamenjava protokola STP

  TRILL zamenja protokol STP, kar omogoča uporabo vseh povezav v omrežju brez tveganja za zanke.

- Izboljšano usmerjanje

  Omogoča optimalno usmerjanje prometa med napravami na podlagi topologije omrežja.

3.4.1.2 Protokol Shortest-Path Bridging – SPB

Shortest-Path Bridging je standardiziran omrežni protokol, zasnovan za poenostavitev in izboljšanje zmogljivosti omrežij Ethernet, še posebej v velikih in kompleksnih okoljih, kot so podatkovni centri. SPB omogoča učinkovito usmerjanje prometa z uporabo najkrajših poti, kar povečuje izkoriščenost povezav in izboljšuje zmogljivost omrežja.

Njegove ključne značilnosti so:

- Uporaba najkrajše poti

  Protokol SPB uporablja algoritme za iskanje najkrajših poti za usmerjanje prometa, kar zmanjšuje zakasnitev in izboljšuje prepustnost omrežja.

- SPB temelji na usmerjevalnem protokolu IS-IS za izmenjavo informacij o topologiji omrežja in za izračun najkrajših poti.

- Ovijanje paketov MAC v MAC

  Protokol SPB uporablja tehnologijo MAC-in-MAC za ovijanje paketov, ki potujejo s pomočjo omrežja. Ta tehnika omogoča, da se promet znotraj posamezne skupine VLAN ohranja ločen in usmerjan s pomočjo najkrajših poti brez posredovanja vmesnih stikal.

3.4.2 Preklopna matrika z usmerjanjem

Skozi leta razvoja različnih načinov in tehnologij preklopnih matrik se je v svetu najbolj uveljavila preklopna matrika z usmerjanjem. V nasprotju s tradicionalnimi preklopnimi matrikami, ki se osredotočajo le na preklapljanje na osnovi naslovov MAC, preklopna matrika z usmerjanjem omogoča tudi usmerjanje prometa na podlagi naslovov IP.

Razlogi za uveljavitev preklopne matrike z usmerjanjem so dobro poznani in dokumentirani usmerjevalni protokoli, kot so BGP, OSPF in IS-IS, ter večina sistemskih skrbnikov že posreduje znanje o njih. Uporabljeni protokoli so nelastniški in zelo dobro podprti pri različnih proizvajalcih mrežne opreme.

Primeri dveh tehnologij, ki se uporabljata za izgradnjo preklopnih matrik z usmerjanjem, sta navedeni spodaj:

- VXLAN in
- NvGRE.

V sodobnih podatkovnih centrih se je kot »de-facto« standard najbolj uveljavila tehnologija izgradnje prekrivnih omrežij s pomočjo protokola VXLAN na podatkovni ravnini s kombinacijo protokolov MP-BGP EVPN za prenos informacij kontrolne ravnine. V naslednjem poglavju je podrobneje opisana rešitev.

3.5 Tehnologija VXLAN

VXLAN je tehnologija za navidezna omrežja, ki omogoča razširitev lokalnih omrežij s pomočjo fizičnih meja podatkovnega centra. VXLAN uporablja ovijanje paketov za prenašanje okvirjev Ethernet s pomočjo obstoječe IP-omrežne infrastrukture.

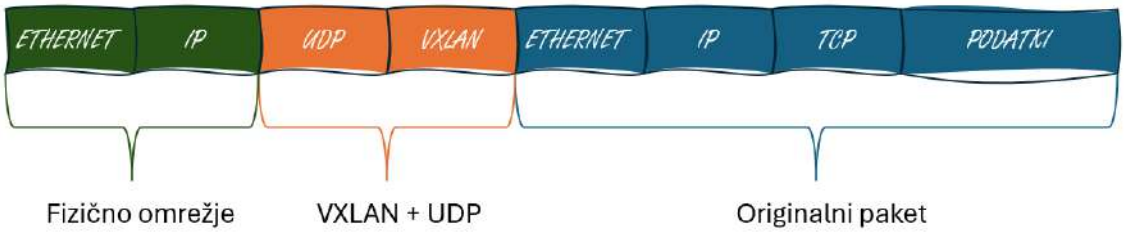
Njegove lastnosti in način delovanja zelo neposredno naslavljajo slabosti tradicionalnih arhitektur:

- Število navideznih omrežij je povečano iz 2^{12} na 2^{24} bitov, kar predstavlja 16 milijonov vrednosti,
- optimalnejša delitev prometnih tokov v podložnem omrežju zaradi uporabe naključno generiranih izvornih vrat,
- vidljivost naslovov MAC končnih naprav v komunikaciji je razvidna samo na dostopnih stikalih in je s tem kompleksnost prestavljena iz jedrnih stikal,
- podpora standarda pri vseh večjih proizvajalcih omrežne opreme.

3.5.1 Paket VXLAN

Protokol VXLAN omogoča razširitev segmentov Ethernet s pomočjo omrežja IP s pomočjo ovijanja okvirjev Ethernet v pakete protokola UDP. Končna točka, kot je npr. navidezni stroj, pošlje podatke in protokol VXLAN doda svojo glavo k protokolnim sporočilom, kjer se vse skupaj vstavi v paket protokola UDP. Glava vsebuje identifikator virtualnega omrežja (VNI) in tako omogoča ločevanje različnih omrežij.

Med dvema fizičnima točkama, imenovanima tudi VTEP, se v podložnem omrežju vzpostavi tunel, ki je namenjen prenosu podatkov. Originalni velikosti okvirja Ethernet se doda še zaglavje v velikosti 50 zlogov, ki vsebuje podatke o VXLAN, UDP in fizičnem omrežju.



Slika 9: Paket VXLAN

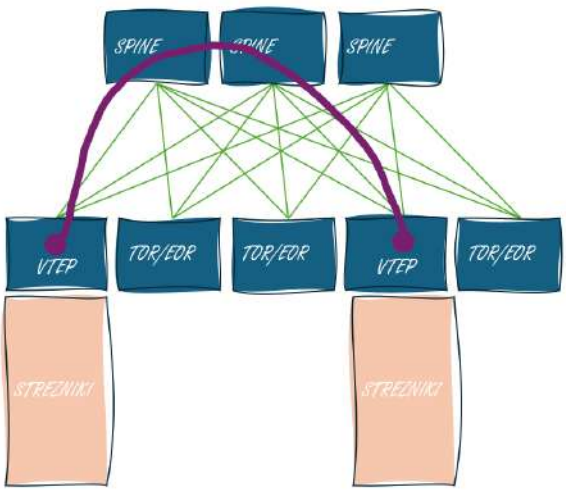
Vir: (Lasten vir)

3.5.2 Tuneli

Tuneli IP, opisani v predhodnem poglavju, ki so namenjeni prenosu paketov VXLAN med različnimi fizičnimi točkami v podložnem omrežju, se delijo na tri tipe:

- omrežne tunele,
- strežniške tunele in
- hibridne tunele.

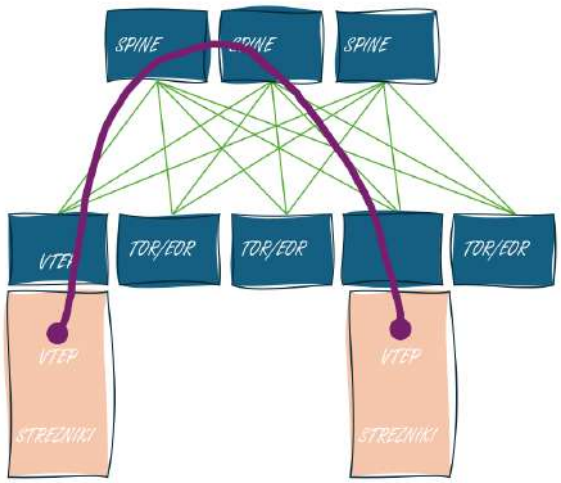
Glavni ključ delitve sta izvorna in ponorna točka VTEP-tunela, ki je odvisna od tega, kje se nahajata. Pri omrežnem načinu sta izvor in ponor VXLAN-tunela med omrežnima stikaloma »Leaf«, kot je prikazano na spodnji sliki. Naloga stikal je, da originalne okvirje na izvoru ovije v VXLAN in na ponorni strani poskrbi, da se ustrezno odstrani zaglavje VXLAN.



Slika 10: Tunel VXLAN – omrežni način

Vir: (Lasten vir)

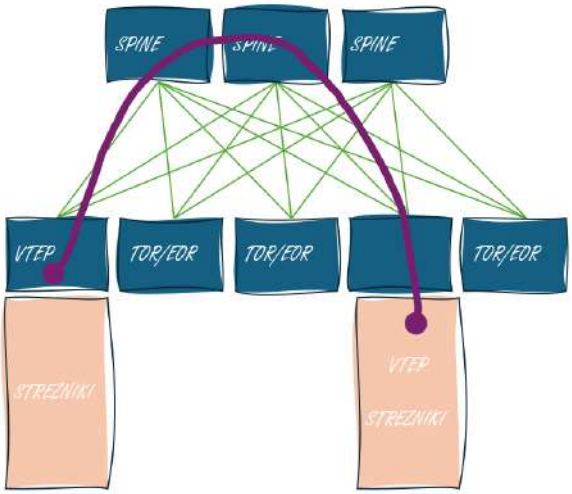
Strežniški način ustvarjanja tunelov VXLAN deluje na način, da sta točki VTEP na samem strežniku oziroma omrežnem stikalu gostitelja. Princip delovanja je predstavljen na spodnji sliki.



Slika 11: Tunel VXLAN – strežniški način

Vir: (Lasten vir)

Hibridni način deluje po principu, da je ena točka VTEP zaključena na dostopovnem stikalu »Leaf« in druga na strežniku oziroma gostitelju.



Slika 12: Tunel VXLAN – hibridni način

Vir: (Lasten vir)

3.5.3 Učenje naslovov končnih točk tunelov VTEP

V podatkovnih centrih, ki uporabljajo tehnologijo VXLAN, se naslovi končnih točk in tunelov VTEP učijo s pomočjo različnih metod. Dejstvo, da se dve končni napravi lahko nahajata v istem ali različnem omrežnem segmentu znotraj iste geografske lokacije podatkovnega centra ali na dveh ločenih, je skozi razvoj tehnologije prineslo različne načine in pristope, ki so opisani v naslednjih podpoglavjih:

- statičen način,
- učenje s poplavljanjem,
- učenje s protokolom MB-BGP EVPN.

3.5.4 Statično ustvarjeni tuneli

Najpreprostejši način vzpostavljanja tunelov VTEP je statično določanje izvorne in ponorne točke tunela. Sistemski skrbnik ročno nastavi naslove vseh VTEP-točk, kar omogoča neposredno komunikacijo med njimi. Takšna preprosta implementacija je primerna za manjša omrežja z manj spremembami. Hkrati je nepraktična in neučinkovita metoda za velika omrežja ali omrežja z dinamično spreminjajočo se topologijo.

3.5.5 Učenje s poplavljanjem

Način učenja s poplavljanjem (angl. flood and learn) je eden izmed tradicionalnih pristopov za učenje naslovov MAC v omrežjih z uporabo VXLAN. Ta metoda temelji na osnovnem principu poplavljanja prometa za odkrivanje končnih točk v podatkovni ravnini prekrivnega omrežja:

- v primeru, ko končna točka v omrežju VXLAN želi poslati podatke drugi končni točki, vendar njen MAC-naslov še ni vpisan v MAC-tabelo in pošiljatelj ne ve, kateri fizični gostitelj (VTEP) vsebuje naslov MAC;
- pošiljatelj sestavi podatkovni okvir z neznanim naslovom MAC-prejemnika. Ta okvir se ovije v paket VXLAN, ki vključuje zaglavje VXLAN in se nato s pomočjo protokolov UDP/IP dostavi do drugih VTEP-točk v omrežju. Okvir z neznanim naslovom MAC je poslan v obliki »multicast« ali »unicast« na vse druge točke VTEP v omrežju. To je proces, znan kot poplavljanje;

- ponorna točka VTEP, ki ima informacijo o ciljnem naslovu MAC, prejme sporočilo, namenjeno vsem, ustrezno odstrani zaglavje VXLAN in posreduje okvir končni napravi. Sočasno točka VTEP shrani (»se nauči«) izvorni naslov MAC v lastno tabelo naslovov MAC, skupaj s segmentom VNI in z naslovom IP izvorne točke VTEP;
- s tem ko je naslov MAC shranjen oziroma naučen v lokalnih tabelah točk VTEP, se vsa nadaljnja komunikacija izvaja neposredno, brez poplavljanja.

Prednost takšnega načina je preprosta implementacija, saj ni potrebe bo uvedbi dodatne nadzorne ravnine ali ostalih protokolov za razširjanje informacije o naslovih MAC.

Glavne slabosti so predvsem, da način temelji na protokolih tipa »multicast«, kar predstavlja dodatno obremenitev strojnih virov stikal in njihova uporaba ni vsakodnevna znotraj podatkovnih centrov. Ob uporabi učenja s poplavljanjem se dodatno poveča tudi količina prometa znotraj omrežij podatkovnih centrov.

3.5.6 Učenje s protokolom MB-BGP EVPN

Gre za uporabo protokola MP-BGP EVPN, ki je opisan v RFC 7432 in nudi rešitev za zagotavljanje informacij naslovov MAC in končnih točk VTEP. Omenjena rešitev je standardizirana in jo podpira večina proizvajalcev omrežne opreme ter je osnovana na protokolu MP-BGP VPN. Pri delovanju ne uporablja protokolov tipa »mutlicast« in s tem zmanjša nepotrebno količino prometa ter je del podatkovne ravnine omrežja VXLAN.

Točke VTEP oglašujejo naslove MAC in IP s pomočjo protokola BGP v omrežje podatkovnega centra.

Protokol EVPN pozna različne tipe usmerjevalnih poti, ki so uporabljene za oglaševanje različnih vrst informacij:

- Tip 2 MAC/IP služi za oglaševanje naslovov MAC.
- Tip 3 služi za oglaševanje informacij protokolov »multicast« in »broadcast«.
- Tip 5 je namenjen oglaševanju informacij o L3-omrežnih segmentih.

- V primeru, ko končna naprava želi poslati paket ciljni napravi, lokalna točka VTEP zabeleži naslov MAC in IP naprave ter jo objavi v omrežje s pomočjo MP-BGP EVPN.
- Ostale točke VTEP v omrežju prejmejo to informacijo.
- Promet tipa »unicast« se s pomočjo MP-BGP EVPN dostavi neposredno ciljni napravi. V primeru pošiljanja prometa »multicast« in »broadcast« se uporabi tip 3 usmerjevalne poti.

Glavne prednosti protokola so velika podpora ločevanju omrežnih segmentov na različne usmerjevalne instance ter podpora preklapljanju in usmerjanju. Obstajajo možnosti vpeljave večnajemništva, zmanjšana količina nepotrebnega prometa, povezovanje omrežnih naprav različnih omrežnih proizvajalcev in dobro poznavanje protokola BGP iz strani omrežnih skrbnikov.

3.6 Priklop končnih in servisnih naprav

V sodobnih podatkovnih centrih je priklop končnih naprav na stikala, kot so strežniki in shranjevalne naprave in ostale servisne naprave, ključnega pomena za zagotavljanje zanesljive povezljivosti in visoke prepustnosti. Stikala ponujajo možnost povezovanja naprav v načinu L2 (Layer 2) in L3 (Layer 3).

V L2-načinu obstajata dve možnosti, kako so končne naprave (strežniki, požarne pregrade itd.) priključene na omrežna stikala. Naprave so lahko priključne glede na funkcionalnost kot:

- »Access« – končna naprava pripada enemu segmentu VLAN, ki je določen na vmesniku stikala, na katerega je naprava priključena.
- »Trunk« – končna naprava pripada več segmentom VLAN. Tak vmesnik na stikalu je opredeljen kot vmesnik »trunk«. Na takšnem vmesniku so navadno specificirana omrežja VLAN, ki smejo potovati po tem vmesniku.

Glede na način priključitve so lahko naprave priključene:

- s pomočjo ene fizične povezave;
- s pomočjo več vzporednih fizičnih povezav, združenih v eno logično povezavo (LAG),
- s pomočjo več vzporednih fizičnih povezav, združenih v eno logično, vendar s pomočjo dveh sosednjih stikal (MC-LAG).

Na vmesnike z nastavitvijo »access« so priključene strežniške naprave, ki delujejo samostojno v okviru enega samega omrežja VLAN. V večini primerov so povezane neposredno na dostopovno stikalo.

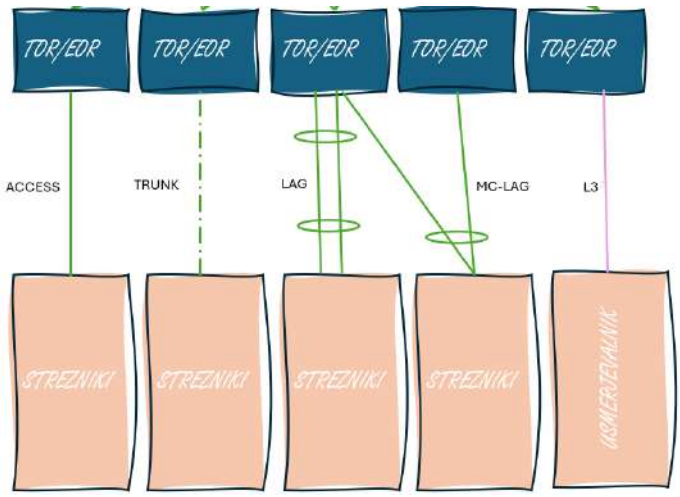
Na vmesnike tipa »trunk« so priključene naprave, ki omogočajo komuniciranje v več segmentih hkrati. Tipične naprave so lahko požarne pregrade, usmerjevalniki ali strežniške gruče. Običajno na vmesniku opredelimo, kateri segmenti omrežja VLAN so dovoljeni.

Zaradi zagotavljanja visoke razpoložljivosti in porazdeljevanja bremena pogostokrat strežnike povežemo na dostopovna stikala z več fizičnimi povezavami. Z uporabo funkcionalnosti »LAG« dosežemo, da več fizičnih povezav sestavlja eno združeno povezavo. Vsi fizični vmesniki v povezavi so istočasno aktivni in promet po njih se enakomerno razporeja glede na tip prometa in izbiro algoritma za deljenje bremena. Izpad ene povezave v združeni povezavi ne povzroči bistvenega vpliva na delovanje skupne povezave.

V primeru, da želimo dodatno izboljšati visoko razpoložljivost, lahko končne naprave povežemo na dve stikali. Z uporabo tehnologije »MC-LAG« si stikali izmenjata vse potrebne podatke, da lahko povezave na dveh ločenih stikalih delujejo, kot da so priključene na eno samo stikalo.

Ravno tako lahko končne naprave v L3-načinu priklopimo z eno ali več povezavami. Za oglaševanje usmerjevalnih poti in razdeljevanje prometa skrbi mehanizem, ki je vgrajen v usmerjevalnem protokolu.

Spodnja slika predstavlja zgoraj opisane načine priklopa.



Slika 13: Načini priklopa končnih naprav

Vir: (Lasten vir)

4 ZAGOTAVLJANJE VARNOSTI V OMREŽJIH SODOBNIH PODATKOVNIH CENTROV

Večnajemništvo (angl. multitenancy) je model, v katerem en sam podatkovni center gostuje več različnih uporabnikov ali organizacij, imenovanih najemniki. Vsak najemnik deluje v ločenem virtualnem okolju, ki mu omogoča varnost in zasebnost, hkrati deli fizične vire podatkovnega centra, kot so strežniki, omrežje in shranjevanje podatkov. Ta model prinaša številne prednosti, kot so optimizacija virov, nižji stroški in večja fleksibilnost, vendar tudi poseben izziv – zagotavljanje varnosti.

Pri zagotavljanju varnostnih mehanizmov je treba naslovit naslednje izzive:

- Izolacija najemnikov

  Zagotavljanje, da je vsak najemnik popolnoma izoliran od drugih najemnikov, da preprečimo nepooblaščen dostop ali uhajanje podatkov med najemniki.

- Nadzor dostopa

  Učinkovito upravljanje dostopa do virov podatkovnega centra, ki zagotavlja, da ima vsak najemnik dostop samo do svojih podatkov in aplikacij.

- Šifriranje podatkov

  Zagotavljanje varnosti podatkov v mirovanju in med prenosom z uporabo naprednih šifrirnih metod.

- Zaznavanja in odzivanje na kibernetske grožnje

  Sposobnost zaznavanja in odzivanja na varnostne grožnje v realnem času, da se zaščiti celotna infrastruktura podatkovnega centra.

- Skladnost z regulatornimi zahtevami in veljavnimi pravnimi predpisi

  Zagotavljanje, da je infrastruktura podatkovnega centra skladna z vsemi relevantnimi zakonodajnimi in regulatornimi zahtevami, kot so GDPR, HIPAA, ISO in drugi.

4.1 Varnostni mehanizmi

Varnost v sodobnih podatkovnih centrih je večplastna ter zahteva kombinacijo različnih varnostnih mehanizmov in dobrih praks. Segmentacija omrežja, nadzor dostopa, varnost protokolov, nadzor in zaznavanje vdorov ter zagotavljanje razpoložljivosti so ključni elementi varnostne strategije. Uporaba teh metod in orodij pomaga zaščititi omrežje pred različnimi grožnjami ter zagotavlja zanesljivo in varno delovanje podatkovnega centra. Spodaj je podrobneje predstavljenih nekaj posameznih mehanizmov.

- Segmentacija omrežja

  Delitev omrežja na podlagi skupine VNI omogoča logično ločevanje omrežnega prometa in izboljša varnost z omejevanjem dostopa do virov. Vsak VNI predstavlja ločeno omrežno domeno, kar preprečuje nepooblaščen dostop med različnimi deli omrežja.

  Uporaba navideznih usmerjevalnih instanc VRF omogoča ustvarjanje ločenih usmerjevalnih tabel za različne omrežne segmente znotraj iste fizične infrastrukture. To zagotavlja dodatno plast izolacije in varnosti.

- Šifriranje povezav

  Eden izmed načinov šifriranja povezav je mehanizem MACsec. Zagotavlja šifriranje na ravni dostopovne plasti, kar varuje podatke med prenosom s pomočjo Ethernet povezav. To je še posebej pomembno za povezave med stikali Ethernet, ki so geografsko na različnih lokacijah podatkovnih centrov.

- Overjanje in pooblaščanje

  To je mehanizem, ki omogoča preverjanje pristnosti uporabnikov in dodeljevanje dostopa, preden jim dovolimo dostop do omrežja. To je ključnega pomena za preprečevanje nepooblaščenega dostopa. Dostop do virov naj bo dodeljen po načinu minimalno potrebnega.

- Varnost protokolov z mehanizmi IPSec in SSL

  Varnostna mehanizma IPSec in SSL zagotavljata šifriranje in preverjanje pristnosti IP prometa, kar je ključnega pomena za zaščito podatkov med prenosom.

- Sistem IPS za zaznavanje in preprečevanje vdorov

  IDS/IPS-sistemi spremljajo omrežni promet ter onemogočijo prometne tokove, če prepoznajo sumljivo vsebino podatkov oziroma napadov.

- Sistem SIEM

  SIEM-sistemi zbirajo in analizirajo varnostne dogodke iz različnih virov v omrežju, kar omogoča boljše odkrivanje in odzivanje na varnostne incidente.

4.2 Segmentacija omrežja podatkovnega centra z novodobnimi pristopi

V sodobnih podatkovnih centrih je zagotavljanje varnosti, učinkovitosti in prilagodljivosti omrežja ključnega pomena. Tradicionalni načini segmentacije omrežij, ki temeljijo na fizičnih napravah in osnovnih omrežnih pravilih, so se izkazali za nezadostne pri obvladovanju naraščajočih potreb po varnosti in obvladovanju kompleksnosti. Zato se vse bolj uveljavljajo novodobni pristopi, ki omogočajo bolj dinamično, granularno in prilagodljivo segmentacijo omrežja.

To poglavje raziskuje različne metode in tehnologije, ki so na voljo za segmentacijo omrežij v podatkovnih centrih. Poseben poudarek je na rešitvah uporabe distribuiranih virtualnih požarnih pregrad, uporabi tradicionalnih fizičnih požarnih pregrad in omejevanju z listami dostopa. Ti pristopi omogočajo ustvarjanje ločenih varnostnih domen, izboljšano upravljanje prometa ter zagotavljanje visoke stopnje varnosti in skladnosti.

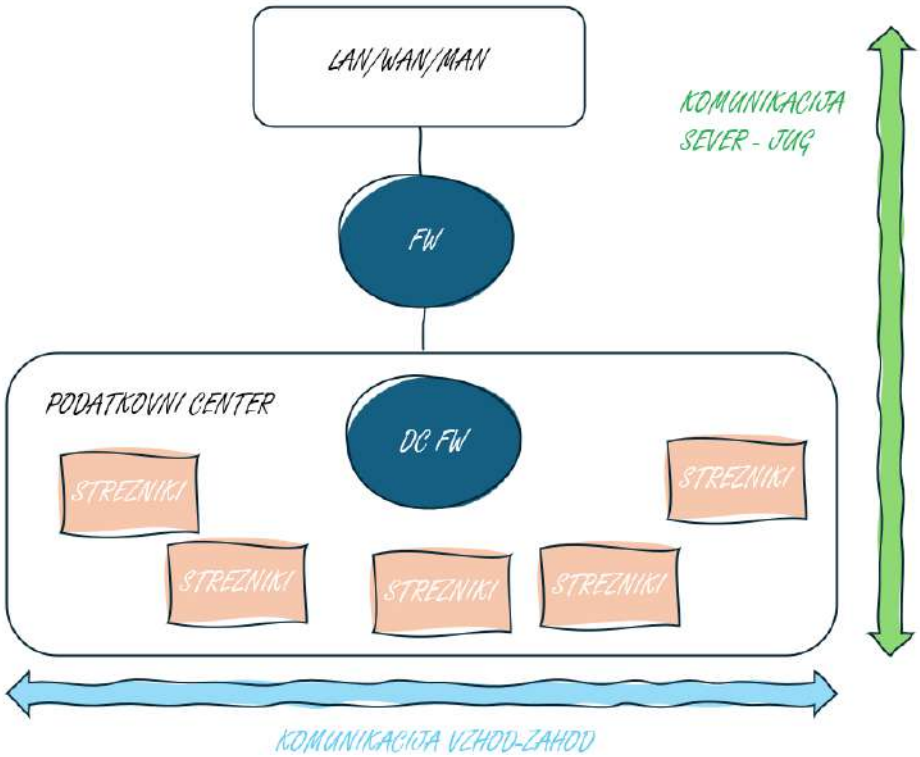
Novodobnimi pristopi se v omrežjih podatkovnih centrov prilagajajo dinamičnim poslovnim potrebam, omogočajo učinkovitejše upravljanje virov ter zagotavljajo boljšo zaščito podatkov in aplikacij. Poglavje bo podalo pregled teh sodobnih rešitev in primerjavo z bolj tradicionalnimi pristopi.

4.2.1 Uporaba list dostopa

Eden izmed tradicionalnih načinov omejevanja prometnih tokov v podatkovnem centru je z uporabo list dostopa, ki sovpadajo z omrežno topologijo. Takšen način se največkrat vzpostavi na omrežnih vmesnikih privzetih prehodov na stikalih. Večina sodobnih omrežnih stikal omogoča pisanje pravil z omejevanjem do ravni L4. Takšen način postaja kompleksnejši z dodajanjem novih gradnikov v omrežje podatkovnega centra, poveča se možnost napake in nudi manjšo fleksibilnost v primerjavi z namenskimi požarnimi pregradami.

4.2.2 Fizične požarne pregrade

Fizične požarne pregrade naslednje generacije so tradicionalne naprave, ki se uporabljajo za segmentacijo omrežij ter pregledovanje prometnih tokov in izvajanje varnostne politike. Postavijo se med različne varnostne domene. V primeru podatkovnih centrov sta tipična vzorca prometnih tokov v smeri sever-jug in vzhod-zahod. Z novodobnim razvojem ter s povečanjem števila aplikacij in količine prometa znotraj posameznega podatkovnega centra je treba zagotoviti dovolj zmogljivo požarno pregrado. Drug način umestitve požarne pregrade je na rob omrežja podatkovnega centra, kjer se izvaja varnostna politika pregledovanja prometnih tokov iz ostalih delov omrežja proti podatkovnemu centru. Spodnja slika predstavlja oba načina vzpostavitve.



Slika 14: Primer prometnih tokov

Vir: (Lasten vir)

Prednosti takšnega načina so centralno upravljanje in nadzor med omrežnimi segmenti, visoka zmogljivost namenskih naprav ter pogosto vključene napredne funkcionalnosti, kot so sistemi IDS/IPS. Ob veliki rasti količine prometa lahko takšne namenske naprave predstavljajo ozka grla, dodatno vzdrževanje in manjšo prilagodljivost, še posebej v okoljih, kjer so pogoste spremembe.

4.2.3 Distribuirane navidezne požarne pregrade

Programsko opredeljena omrežja so revolucionarno spremenila način upravljanja omrežij v podatkovnih centrih. S tem pristopom se fizična omrežna oprema loči od funkcionalnosti upravljanja, kar omogoča centraliziran nadzor in večjo prilagodljivost. To je ključno za obvladovanje kompleksnosti sodobnih podatkovnih centrov, ki se morajo hitro in učinkovito odzivati na spreminjajoče se poslovne potrebe in varnostne zahteve.

Glavni lastnosti uporabe distribuiranih požarnih pregrad sta:

- izgradnja dinamično izvedenih omrežnih topologij (angl. »on-demand network toplogy«),
- centralizirano upravljanje in nadzor tako izvedenih omrežnih topologij.

Ena izmed ključnih varnostnih rešitev v arhitekturah SDN (angl. Software Defined Network) je uporaba distribuiranih požarnih pregrad. Ta pristop omogoča postavitev varnostnih politik neposredno na raven navideznih omrežnih strojev in aplikacije. Distribuirane požarne pregrade omogočajo granularni nadzor prometnih tokov, neodvisno od fizične lokacije v omrežju, kar poenostavlja segmentacijo in izboljšuje zaščito znotraj podatkovnega centra.

Dva izmed vodilnih ponudnikov distribuiranih požarnih pregrad sta podjetji VMware NSX in Cisco s rešitvijo ACI.

4.2.3.1 VMware NSX

Produkt VMware NSX je rešitev za programsko opredeljena omrežja in varnost, ki omogoča popolno virtualizacijo omrežnih funkcij v podatkovnih centrih. NSX prinaša koncept distribuirane požarne pregrade, ki se izvaja neposredno na vsakem gostitelju. To pomeni, da se varnostne politike izvajajo na vsakem virtualnem omrežnem vmesniku, kar omogoča podrobno segmentacijo in zaščito med navideznimi stroji znotraj istega fizičnega strežnika.

Njegove glavne prednosti so:

- Omogoča uvedbo natančnih varnostnih politik na ravni posameznih navideznih strojev, kar zmanjšuje površino za izvedbo kibernetskega napada (angl. attack surface) in izboljšuje varnost omrežja.
- NSX omogoča mikrosegmentacijo, kjer so varnostne politike lahko aplicirane na osnovi aplikacijskih logik in uporabniških vlog ali drugih poslovnih meril. Zelo preprosto omogoča izgradnjo različnih okolij in s tem podpira gostovanje različnih uporabnikov.

- Varnostne politike se določajo centralno in se nato samodejno prenesejo in stopijo v veljavo po celotnem omrežju, kar poenostavi upravljanje in skladnost s predpisi.

4.2.3.2 Cisco Application Centric Infrastructure

Cisco Application Centric Infrastructure (ACI) je celovita rešitev za upravljanje omrežij in varnosti, ki temelji na politiki omrežnega ali aplikacijskega modela. ACI združuje strojno in programsko opremo za zagotavljanje avtomatizacije, centraliziranega upravljanja in nadzora nad omrežjem podatkovnega centra.

Njegove glavne prednosti so:

- Uporablja aplikacijske ali omrežne profile za določanje varnostnih politik, ki se uveljavijo glede na posamezno aplikacijo. To omogoča natančno določanje dovoljenih komunikacijskih poti med različnimi aplikacijskimi komponentami.
- Cisco ACI se lahko poveže z različnimi varnostnimi napravami in storitvami, vključno s požarnimi pregradami tretjih proizvajalcev, kar omogoča implementacijo varnostnih politik na več ravneh omrežja.
- Podobno kot NSX tudi ACI omogoča izvajanje varnostnih politik na vsakem omrežnem elementu, vendar z dodatno podporo za fizične naprave, kar omogoča obvladovanje varnostnih politik tako v fizičnih kot tudi navideznih okoljih.

5 UPRAVLJANJE OMREŽJA SODOBNEGA PODATKOVNEGA CENTRA

Upravljanje podatkovnih centrov je ključen vidik, ki vpliva na učinkovitost, varnost in zanesljivost celotne infrastrukture. Obstajajo različni načini upravljanja, ki segajo od ročnih metod do naprednih avtomatiziranih rešitev. Različni načini upravljanja podatkovnih centrov imajo svoje prednosti in slabosti, odvisno od potreb, velikosti in kompleksnosti infrastrukture. Medtem ko ročno upravljanje ponuja popoln nadzor, avtomatizirane rešitve z odprtokodnimi orodji in s CI/CD-koncepti omogočajo večjo učinkovitost, enotnost in razširljivost. Namenska programska oprema proizvajalcev omrežne opreme zagotavlja napredne funkcionalnosti in podporo, vendar s tem prinaša tudi višje stroške in odvisnost od enega proizvajalca.

5.1 Orodja in načini upravljanja

V nadaljevanju poglavja so predstavljeni štirje najpogostejši načini upravljanja IKT-gradnikov podatkovnih centrov s svojimi prednostmi in slabostmi.

5.1.1 Ročno upravljanje

Vse naloge, kot so konfiguracija omrežnih naprav, spremljanje delovanja, upravljanje strežnikov in izvajanje varnostnih politik, se izvajajo ročno s pomočjo grafičnega uporabniškega vmesnika ali ukazne vrstice. Pri takšnem načinu upravljanja je ključno vodenje dokumentacije o konfiguracijah, spremembah in postopkih za ohranjanje preglednosti, sploh ker lahko sočasno spremembe opravlja več skrbnikov.

- Prednosti

  Ni potrebe po dodatni programski opremi ali orodjih za avtomatizacijo postopkov.

  Skrbniki imajo popoln nadzor nad vsemi vidiki infrastrukture.

- Slabosti

  Ročne naloge so lahko zelo časovno zahtevne.

  Pogosteje se pojavijo napake, kar lahko vodi do izpadov ali varnostnih ranljivosti.

  Upravljanje velikih ali kompleksnih okolij postane neobvladljivo

5.1.2 Avtomatizirano upravljanje z odprtokodnimi orodji

Avtomatizirano upravljanje z odprtokodnimi orodji temelji na uporabi programske opreme, kot so Ansible, Puppet, Chef in Terraform, ki omogočajo avtomatizacijo različnih procesov v podatkovnih centrih. Ta orodja omogočajo uporabo skript in predlog za ponovljive in dosledne konfiguracije. Namesto ročnega izvajanja nalog lahko skrbniki ustvarijo avtomatizirane delovne tokove, ki pospešijo uvajanje in upravljanje infrastrukture. Avtomatizacija vključuje konfiguracijo omrežnih naprav, uvajanje strežnikov, namestitev aplikacij in spremljanje delovanja. Odprtokodna orodja imajo široko podporo skupnosti, kar omogoča stalne posodobitve in prilagoditve.

- Prednosti:
  - zmanjšanje ročnega dela in napak zaradi človeškega dejavnika,
  - lažje upravljanje velikih in kompleksnih okolij,
  - aktivne skupnosti za podporo in razvoj orodij.
- Slabosti:

  Potrebno je usposabljanje osebja za uporabo teh orodij in s tem nastanejo stroški uvajanja.

  Odprtokodna orodja morda ne ponujajo vseh funkcionalnosti, ki jih nudi namensko programsko orodje.

5.1.3 Upravljanje s koncepti DevOps in CI/CD

Koncepti CI/CD (angl. Continuous Integration/Continuous Delivery) in DevOps prinašajo avtomatizacijo in integracijo procesov razvoja, testiranja in uvajanja aplikacij v podatkovne centre. S pomočjo orodij, kot so Jenkins, GitLab CI in CircleCI, se izvorna koda nenehno integrira in preizkuša, kar omogoča hitro odkrivanje napak in stabilno dostavo programske opreme. Koncept infrastrukture kot kode (angl. IaC) je ključen v CI/CD, kjer se konfiguracije in nastavitve podatkovnih centrov upravljajo z uporabo kode, kar omogoča doslednost in ponovljivost. DevOps-prakse izboljšujejo sodelovanje med razvojno in operativno ekipo, kar vodi do hitrejšega uvajanja in zanesljivejše infrastrukture.

- Prednosti:
  - omogoča hitro in zanesljivo uvajanje sprememb v infrastrukturo in aplikacije,
  - boljša integracija med razvojnimi in operativnimi ekipami,uporaba kode zagotavlja doslednost pri uvajanju in upravljanju infrastrukture.
- Slabosti:
  - Implementacija CI/CD-procesov zahteva natančno načrtovanje in lahko poveča kompleksnost upravljanja;
  - potrebno je usposabljanje osebja za uporabo CI/CD-orodij in procesov.

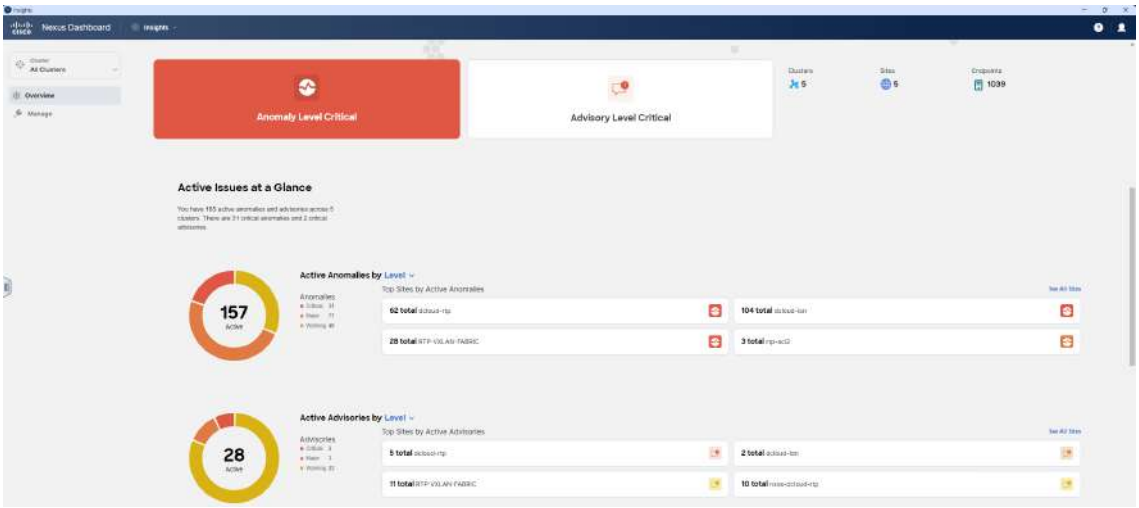
5.1.4 Namenska programska oprema proizvajalca omrežne opreme

Namenska programska oprema proizvajalca omrežne opreme je zasnovana za avtomatizacijo in upravljanje omrežij znotraj podatkovnih centrov. Proizvajalci, kot so Cisco, VMware, Juniper in Arista, ponujajo rešitve, kot so Cisco ACI, VMware NSX, Juniper Contrail in Arista CloudVision, ki so posebej prilagojene za njihovo strojno opremo. Te rešitve omogočajo celovito upravljanje omrežnih virov, avtomatizacijo konfiguracij, spremljanje delovanja in zagotavljanje varnosti. Integracija z obstoječo strojno opremo proizvajalca omogoča optimizirano zmogljivost in preprosto uvajanje novih storitev. Namenska programska oprema ponuja napredne funkcionalnosti, ki so ključne za sodobne podatkovne centre.

Marsikatera od njih za svoje delovanje uporablja mehanizme umetne inteligence in načela strojnega učenja, vendar podrobnosti delovanja niso poznane, saj gre za zaprtokodno lastniško programsko opremo. Omenjeni mehanizmi so največkrat uporabljeni za hitrejše odkrivanje anomalij in vzrokov napak, saj UI na podlagi naučenih modelov hitreje korelira podatke med seboj. S tem sistemskim skrbnikom olajša delo in uporabo poglobljenih metod odkrivanja napak.

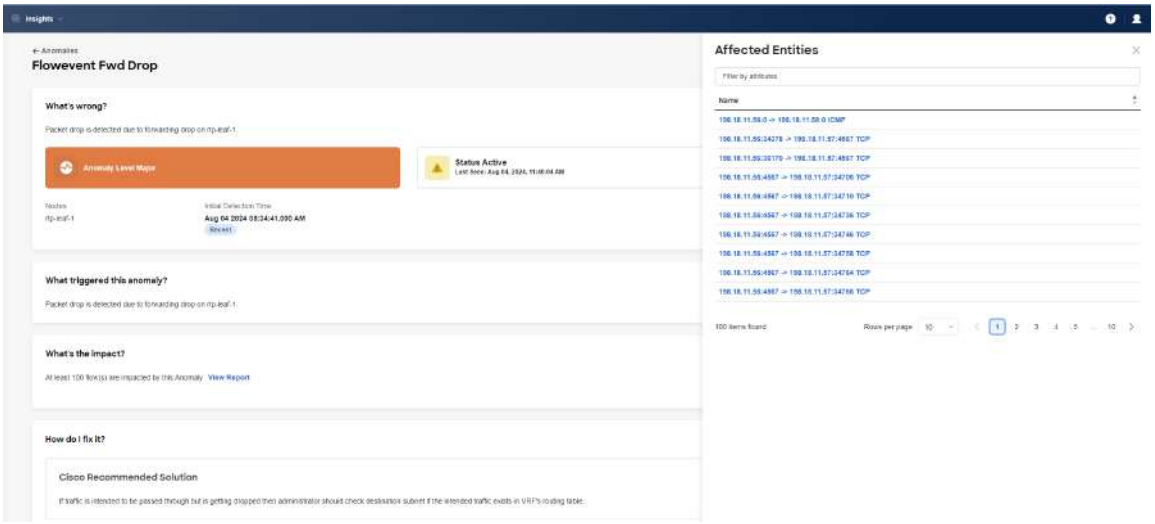
- Prednosti:
  - Popolna integracija z omrežno opremo proizvajalca omogoča optimizirano delovanje.
  - Zagotovljene so tehnična podpora in redne posodobitve iz strani proizvajalca.
  - Orodja ponujajo napredne funkcionalnosti, ki so posebej prilagojene za določene omrežne rešitve.

- Slabosti:
  - Licenčnine za lastniško programsko opremo so lahko zelo visoke.
  - Večja odvisnost od enega proizvajalca lahko omeji fleksibilnost pri izbiri rešitev.
  - Integracija s heterogenimi omrežji in z napravami drugih proizvajalcev je lahko otežena.



Slika 15: Primer lastniškega orodja Cisco Nexus Dashboards

Vir: (Lasten vir)



Slika 16: Primer uporabe UI pri upravljanju omrežne infrastrukture

Vir: (Lasten vir)

5.2 Uporaba metod umetne inteligence v sodobnih omrežjih podatkovnih centrov

Umetna inteligenca postaja vse bolj nepogrešljiv del vsakdana in posledično je povečana uporaba tudi v sodobnih omrežjih IKT. Z naraščajočo kompleksnostjo omrežij in eksponentno rastjo podatkov, ki jih ta omrežja obdelujejo, je tradicionalno upravljanje omrežij vse manj učinkovito in prinaša nove načine za optimizacijo delovanja, izboljšanje varnosti in zagotavljanje kakovosti storitev v sodobnih omrežjih.

5.2.1 Optimizacija omrežnih virov

UI omogoča avtomatizirano upravljanje omrežnih virov, kar vodi do boljše izrabe strojne in programske opreme. Algoritmi za strojno učenje lahko analizirajo prometne vzorce in optimizirajo razporeditev virov glede na trenutne potrebe. To vključuje dinamično prilagajanje pasovne širine, inteligentno usmerjanje prometa in optimizacijo latence, kar povečuje učinkovitost in zmanjšuje stroške.

5.2.2 Proaktivno zaznavanje in odpravljanje napak

Sodobna omrežja IKT so podvržena številnim potencialnim napakam in motnjam, ki lahko vplivajo na njihovo delovanje. UI omogoča proaktivno zaznavanje nepravilnosti z uporabo naprednih tehnik, kot so odkrivanje anomalij, predikcijska analitika in avtomatizirani odziv na incidente. S tem lahko omrežje samodejno odpravi napake, še preden te vplivajo na uporabnike, kar bistveno poveča zanesljivost in razpoložljivost omrežja.

5.2.3 Varnost v omrežjih

Varnost je eno izmed ključnih področij, kjer UI prinaša velike koristi. Algoritmi UI lahko v realnem času analizirajo velike količine podatkov, odkrivajo potencialne varnostne grožnje in avtomatizirajo odziv na napade. Uporaba UI za odkrivanje vdorov (IDS) in preprečevanje vdorov (IPS) omogoča boljše prilagajanje varnostnih ukrepov ter hitrejši in učinkovitejši odziv na varnostne incidente.

5.2.4 Samodejno upravljanje in orkestracija omrežij

Z naraščajočo priljubljenostjo omrežij, opredeljenih s programsko opremo (SDN) in z navideznimi omrežnimi funkcijami (NFV), postaja potreba po avtomatizaciji upravljanja omrežij vse večja. UI omogoča samodejno orkestracijo kompleksnih omrežnih operacij, kar vključuje konfiguracijo omrežnih naprav, upravljanje politik in optimizacijo delovanja omrežja v realnem času. To zmanjšuje potrebo po ročnih posegih in zmanjšuje možnost človeških napak.

5.2.5 Povečanje kakovosti storitev

S pomočjo UI lahko omrežja zagotavljajo višjo kakovost storitev (angl. Quality of Service) s prilagajanjem na specifične potrebe uporabnikov in aplikacij. Algoritmi strojnega učenja lahko napovedujejo potrebe po omrežnih virih in dinamično prilagajajo omrežje, da zagotavljajo optimalno uporabniško izkušnjo, tudi pri velikih obremenitvah.

Uporaba umetne inteligence v sodobnih omrežjih IKT prinaša številne prednosti, ki vključujejo optimizacijo virov, izboljšanje varnosti, avtomatizacijo upravljanja in izboljšanje kakovosti storitev. UI omogoča, da omrežja postanejo bolj prilagodljiva, zanesljiva in varna, kar je ključnega pomena za podporo vedno bolj povezanega in digitaliziranega sveta.

6 PRIMER OMREŽJA SODOBNEGA PODATKOVNEGA CENTRA

V nadaljevanju poglavja bomo predstavili poslovni primer (angl. business case) za vzpostavitev zasebnega oblaka in omrežja sodobnega podatkovnega centra, ki temelji na arhitekturi »Spine-Leaf« in tehnologijah, kot sta VXLAN in EVPN. Podjetje prihaja iz gospodarstva in se zaveda nenehne potrebe po razvoju in posodabljanju infrastrukture ter prilagajanju uporabniških storitev, ki jih ponuja svojim končnim uporabnikom in tudi zaposlenim, ter zagotavljanju prijetne uporabniške izkušnje. Odločitev za vzpostavitev zasebnega oblaka z omrežno arhitekturo, ki temelji na načelih CLOS, je bila sprejeta na podlagi zahtev zagotavljanja hitre prilagodljivosti, enostavne razširljivosti in zanesljivosti sistemov IKT. Prav tako sta bila dva ključna dejavnika visoka raven zagotavljanja varnosti podatkov in ohranjanje stroškovne učinkovitosti.

Podjetje uporablja novodobna načela razvoja programske opreme in aplikacij, ki so osnovani na tehnologiji vsebnikov (angl. containers) in postajajo vse pogostejši v njihovem produkcijskem okolju. Njihova lastnost elastičnosti in razširljivosti ob povečanih uporabniških obremenitvah je pogojena tudi z gostovanjem na fizičnih gostiteljih in posledično z lastnostmi omrežja podatkovnega centra, ki mora to omogočati.

Arhitektura omogoča model večnajmeništva in s tem lahko preprosto loči okolja, ki so namenjeni testiranju in razvoju programske opreme, od produkcijske uporabe.

V nadaljevanju je predstavljen primer omrežne arhitekture sodobnega podatkovnega centra iz prakse, ki temelji na stikalih proizvajalca Cisco Nexus 9300 ter uporablja najsodobnejše standarde, kot so VXLAN, EVPN in MP-BGP.

Multi-Site VXLAN EVPN-arhitektura je sodobna rešitev za izgradnjo razširljivih in zanesljivih omrežij podatkovnih centrov, ki omogočajo povezljivost med več lokacijami. Ta rešitev temelji na tehnologiji VXLAN za razširitev L2-omrežij s pomočjo L3-infrastrukture.

6.1 Opis uporabljenih gradnikov

Pričujoča podpoglavja natančneje opisujejo uporabljena stikala Ethernet in priključne kable z ostalimi IKT-gradniki omrežne infrastrukture podatkovnega centra.

6.1.1 Stikala Cisco Nexus 9300

Cisco Nexus 9336C-FX2 je visoko zmogljivo Ethernet stikalo, namenjeno za uporabo v podatkovnih centrih z visoko prepustnostjo in nizko latenco. Omogoča hitro in učinkovito povezljivost do ostalih stikal in drugih omrežnih naprav v podatkovnem centru. V našem primeru je uporabljeno kot hrbtenično stikalo.

Njegove lastnosti so:

- Vmesniki:
  - 36 x 100-Gigabit Ethernet QSFP28 vmesnikov,
  - vsak vmesnik100 G lahko deluje s hitrostjo 100 Gb/s, 40 Gb/s ali se razdeli na štiri 25 Gb/s ali 10 Gb/s vmesnike.
- Prepustnost:
  - skupna prepustnost: 7,2 Tbps,
  - skupna zmogljivost preklapljanja: 3,6 Bpps.

Slika 17: Hrbtenično stikalo Cisco Nexus 9336C-FX2

Vir: (Cisco Inc., 2024)

Cisco Nexus 93180YC-FX3 je stikalo s podporo protokolu Ethernet, zasnovano za zagotavljanje visoko zmogljivih povezav za strežnike in druge naprave v podatkovnih centrih. Stikalo podpira različne hitrosti povezav, kar omogoča raznovrstno povezavo z ostalimi napravami. V opisanem primeru je model stikala uporabljen v vlogi dostopovnih stikal.

Njegove lastnosti so:

- Vmesniki:
  - 48 x 1/10/25-Gigabit Ethernet SFP28 vmesnikov,
  - 6 x 40/100-Gigabit Ethernet QSFP28 vmesnikov.
- Prepustnost:
  - skupna prepustnost: 3,6 Tbps,
  - skupna zmogljivost preklapljanja: 2,6 Bpps.

Slika 18: Dostopovno stikalo Cisco Nexus 93180YC-FX3

Vir: (Cisco Inc. , 2024)

6.1.2 Priključni kabli in vmesniki

Optični »Direct Attach Cable« (DAC) kabli, ki jih ponuja proizvajalec Cisco, so zasnovani za visoko zmogljivost in nizko latenco, kar jih naredi idealne za povezovanje znotraj podatkovnih centrov. DAC-kabli so cenovno ugodna rešitev za kratke povezave med omrežnimi napravami, kot so stikala, usmerjevalniki in strežniki. Na tržišču obstajajo kabli različnih hitrosti vse od 10 Gbs, 25 Gbs, 40 Gbs do 100 Gbs. Slednji, s podporo hitrosti 100 Gbs, so v pričujočem primeru ključni element za povezljivost med stikali. Z različnimi dolžinami med 1 in 30 m ter s preprosto namestitvijo ponujajo prilagodljivo in zmogljivo rešitev za izgradnjo visoko zmogljivih omrežij.

Podatkovna centra sta medsebojno povezana s pomočjo dveh zakupljenih optičnih povezav in z uporabljenim vmesnikom tipa 100G-ERL-S proizvajalca Cisco nudita možnost povezave do razdalje 25 km ob ustreznih lastnostih optične trase (slabljenje, kromatska disperzija ipd.).

Slika 19: Primer priključnih kablov DAC- in QSFP-modula

Vir: (Cisco Inc. , 2024)

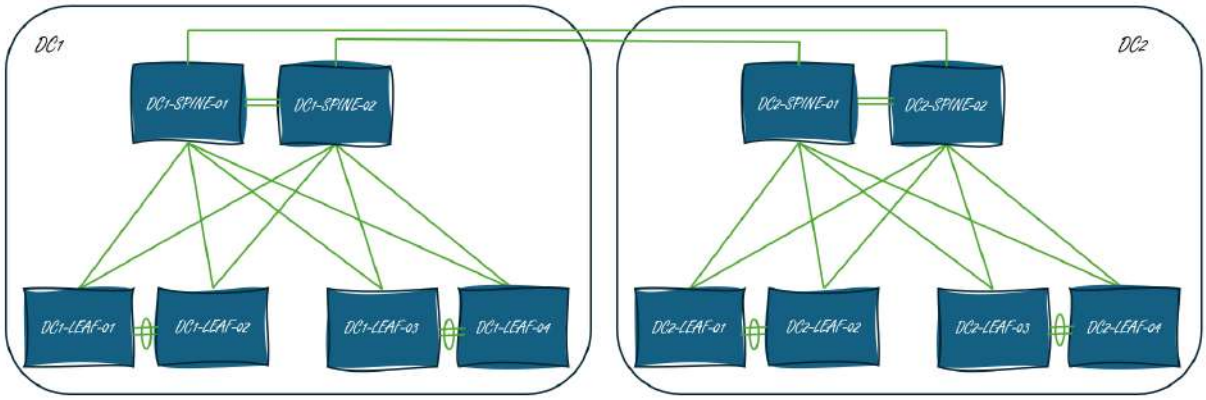
6.2 Fizična topologija omrežja

Fizična topologija omrežja je zgrajena na načelu dvostopenjske arhitekture »Spine-Leaf«. Prvo stopnjo predstavljajo štirje pari stikal »leaf«, po dva para v vsakem podatkovnem centru. Stikali znotraj para sta medsebojno povezani z dvema optičnima povezavama hitrosti 100 Gbps, z zagotavljanje podvojenosti v primeru izpada posameznega stikala v paru. Drugo raven predstavljajo stikala »spine«. Vsak podatkovni center ima en par takšnih stikal, ki sta medsebojno povezani z enako povezavo, kot prej omenjena stikala »leaf«. Vsako stikalo »leaf« ima povezavo s hitrostjo 100 Gbps do vsakega stikala »spine »znotraj podatkovnega centra. Podatkovna centra sta medsebojno povezana z dvema povezavama hitrosti 100 Gbps s pomočjo najetih optičnih povezav.

S takšnim povezovanjem stikal »leaf« in »spine« opisana topologija predstavlja visoko razpoložljivost na več načinov, in sicer:

- Vsako stikalo »leaf« je povezano na vsako stikalo »spine« znotraj lokacije podatkovnega centra in s tem zagotovimo podvojenost v primeru izpada posamezne povezave oziroma stikala »spine«.
- Fizični povezavi med stikaloma »leaf« v posameznem paru sta tisti, ki omogočata pravilno delovanje tehnologije vPC (angl. Virtual PortChannel), ki je podrobneje opisana v poglavju 6.3. Njen namen je predvsem zagotavljanje podvojenosti in visoke razpoložljivosti končnim napravam, ki so v omrežje priklopljene večdomno. S tem zagotovimo nemoteno delovanje končnih naprav v primeru izpada posameznega stikala znotraj para.
- Stikala »spine« na fizični ravni s svojimi povezavami tvorijo kvadrat, kar v primeru izpada posamezne povezave med njimi zagotavlja, da se t. i. »BUM« (angl. broadcast, unknown unicast, multicast) promet nemoteno posreduje dalje. Prav tako zagotavlja dodatno povezavo in stopnjo visoke razpoložljivosti v primeru izpada povezave med posameznima stikaloma »spine« med različnima podatkovnima centroma.

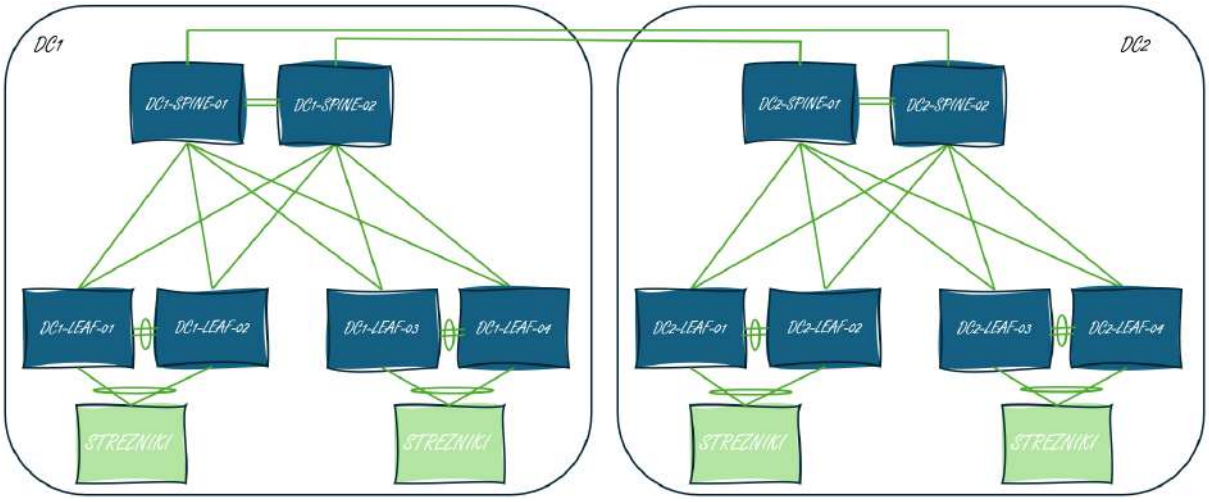
Spodnja slika predstavlja fizično topologijo omrežja.



Slika 20: Fizična topologija omrežja podatkovnega centra

Vir: (Lasten vir)

Strežniki so znotraj posameznega podatkovnega centra priključeni večdomno z vsaj eno povezavo na vsako stikalo »leaf« v paru. Hitrosti priklopov so različne in segajo od 1 Gbs do 25 Gbs. Način priklopa je razviden s spodnje slike.



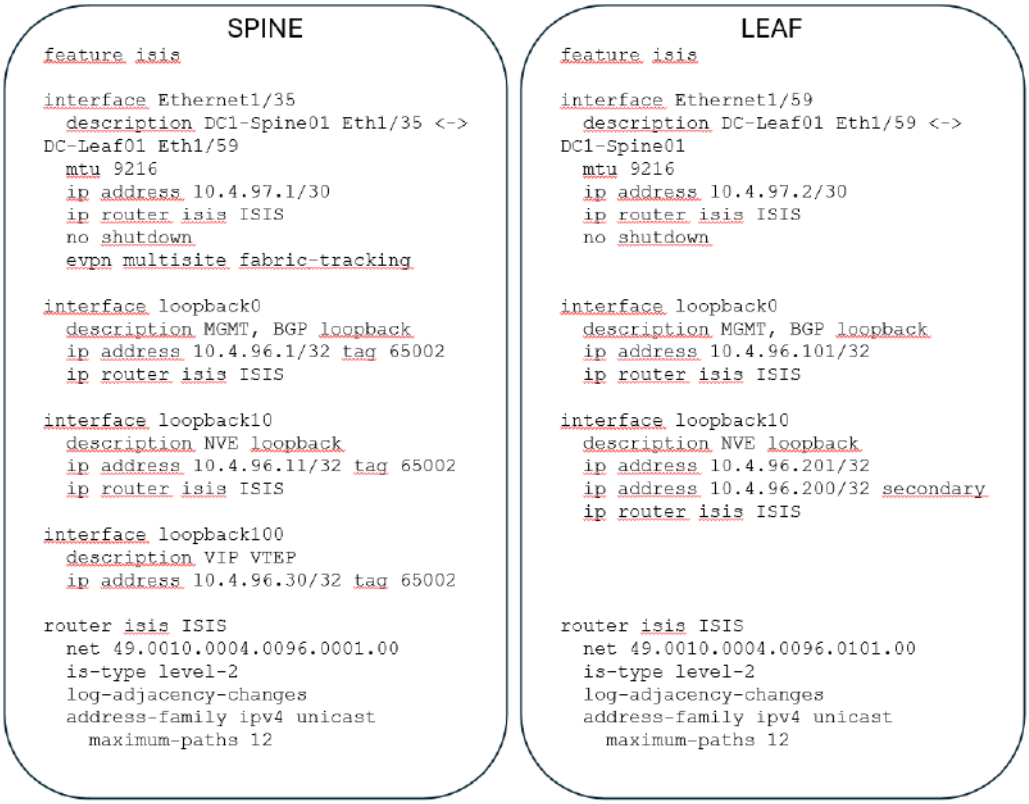
Slika 21: Primer priklopa strežnikov

Vir: (Lasten vir)

6.3 Podložno omrežje

Podložno omrežje v predstavljeni topologiji služi za zagotavljanje osnovne povezljivosti med stikali. Vse povezave med stikali »leaf« in »spine« so tipa L3 in imajo dodeljen omrežni naslov iz zasebnega naslovnega prostora. V praksi se praviloma povezavam tipa točka-točka dodeli omrežni naslov velikosti omrežne maske /30. Protokol IS-IS je učinkovit usmerjevalni protokol, ki se pogosto uporablja za upravljanje podložnih omrežij zaradi svoje zanesljivosti in zmogljivosti, predvsem hitrega konvergenčnega časa.

Protokol IS-IS skrbi za dosegljivost posameznih fizičnih povezav znotraj podatkovnega centra in logičnih vmesnikov tipa »Loopback«, ki so uporabljeni za izvor vmesnikov VTEP in vzpostavitve BGP-sosedstev. Implementacija rešitve s stikali Cisco Nexus predvideva uporabo istega naslova IP na vmesnikih Loopback med dvema stikaloma v vPC paru. Primeri konfiguracije podložnega omrežja, naslavljanja IP, usmerjevalnega protokola IS-IS in vmesnikov »Loopback« so prikazani na spodnji sliki.

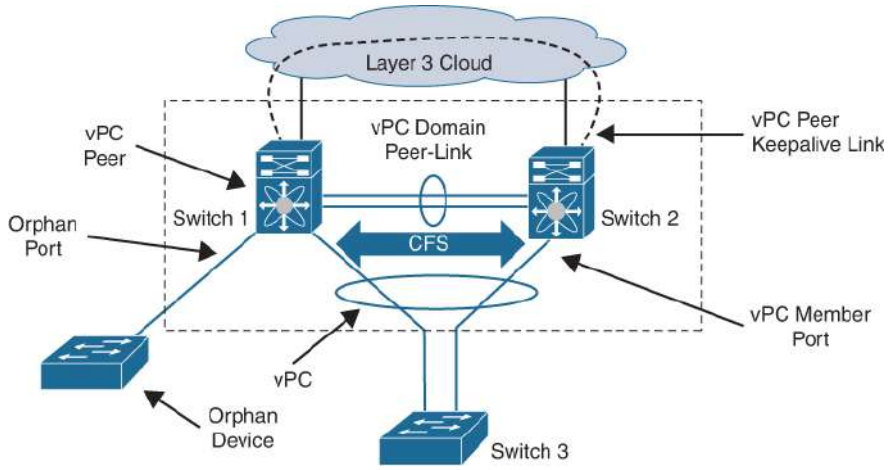


Slika 22: Primer konfiguracije podložnega omrežja

Vir: (Lasten vir)

Cisco Virtual Port-Channel (vPC) je napredna omrežna tehnologija, ki jo je razvil Cisco za izboljšanje zmogljivosti, podvojenosti in zanesljivosti omrežnih povezav. vPC omogoča povezavo ene naprave (npr. strežnika ali stikala) na dve fizično ločeni stikali, ki se obnašata kot ena logična naprava. Ta funkcionalnost povečuje omrežno prepustnost in razpoložljivost ter zmanjšuje čas izpada omrežja. Ključne komponente tehnologije vPC so:

- vPC Peer se uporablja za izmenjavo informacij o stanju povezav, usklajevanje MAC-naslovov, VLAN-informacij in drugih podatkov. Zagotavlja skladnost podatkov med obema stikaloma.
- vPC Peer Keepalive Link zagotavlja, da stikali v vPC-domeni nista v stanju razcepa (angl. split brain).
- vPC-vmesnik nudi povezave iz vsakega stikala v paru do končne naprave (npr. strežnika ali drugega stikala). Delujejo kot ena logična povezava, kar omogoča agregacijo prepustnosti.



Slika 23: Primer gradnikov tehnologije vPC

Vir: (Port Channels and vPCs, 2024)

Primer konfiguracije funkcionalnosti vPC je razviden s spodnje slike.

LEAF

```
feature vpc

vpc domain 10
  peer-switch
  role priority 100
  peer-keepalive destination 10.4.0.63
source 10.4.0.62
  peer-gateway
  layer3 peer-router
  auto-recovery
  ip arp synchronize

interface port-channel4096
  description vPC - DC1-Leaf01 < - >
DC1-Leaf02
  switchport
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link

interface Portchannel 10
 description to ESXi hosts
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 1-10
 vpc 10
```

LEAF

```
feature vpc

vpc domain 10
  peer-switch
  role priority 100
  peer-keepalive destination 10.4.0.62
source 10.4.0.63
  peer-gateway
  layer3 peer-router
  auto-recovery
  ip arp synchronize

interface port-channel4096
  description vPC - DC1-Leaf02 < - >
DC1-Leaf01
  switchport
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link

interface Portchannel 10
 description to ESXi hosts
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 1-10
 vpc 10
```

Slika 24: Primer konfiguracije mehanizma vPC

Vir: (Lasten vir)

6.4 *Prekrivno omrežje s kontrolno in podatkovno ravnino*

Prekrivno omrežje deluje z ovijanjem paketov v dodatne omrežne okvirje, ki se prenesejo s pomočjo obstoječe fizične infrastrukture (podložnega omrežja). To omogoča logično segmentacijo omrežja ne glede na fizično topologijo. VXLAN-tehnologija je bila uporabljena v danem omrežju. Uporabljen je tudi protokol MP-BGP EVPN za pravilno delovanje kontrolne ravnine in distribucijo informacij o naslovih MAC in IP med stikali »leaf«. Stikala »leaf« tvorijo BGP-sejo z vsakim stikalom »spine« znotraj posamezne lokacije podatkovnega centra. Stikala »spine« imajo vlogo reflektorja poti (angl. route refelector) v protokolu BGP. To nam omogoča, da ni treba vzpostaviti BGP-seje med vsemi stikali »leaf« in »spine«. Stikala »spine« so med različnimi geografskimi lokacijami podatkovnih centrov povezana s pomočjo sej BGP, ki so namenjene zagotavljanju povezljivosti. Iste seje se uporabljajo tudi za prenos informacij o končnih točkah.

SPINE

```
nv overlay evpn
feature bgp
feature vn-segment-vlan-based
feature nv overla

router bgp 65002
  router-id 10.4.96.1
  address-family ipv4 unicast
    redistribute direct route-map RMAP-
REDIST-DIRECT
    maximum-paths 4
  address-family l2vpn evpn
    retain route-target all
  template peer LEAF
    remote-as 65002
    description BGP to Leafs
    update-source loopback0
    address-family ipv4 unicast
      send-community
      send-community extended
      route-reflector-client
    address-family l2vpn evpn
      send-community
      send-community extended
      route-reflector-client
  template peer MULTISITE
    remote-as 65001
    description Multi-site BGP
    peer-type fabric-external
    address-family ipv4 unicast
    address-family l2vpn evpn
      send-community
      send-community extended
      rewrite-evpn-rt-asn
```

LEAF

```
nv overlay evpn
feature bgp
feature vn-segment-vlan-based
feature nv overla

router bgp 65002
  router-id 10.4.96.101
  address-family ipv4 unicast
    maximum-paths 4
  address-family l2vpn evpn
    advertise-pip
  template peer SPINE
    remote-as 65002
    description BGP to Spines
    update-source loopback0
    address-family ipv4 unicast
      send-community
      send-community extended
    address-family l2vpn evpn
      send-community
      send-community extended
  neighbor 10.4.96.1
    inherit peer SPINE
    description SPINE1
  neighbor 10.4.96.2
    inherit peer SPINE
    description SPINE2
  vrf DC-PROD
    address-family ipv4 unicast
      advertise l2vpn evpn
      maximum-paths 4
```

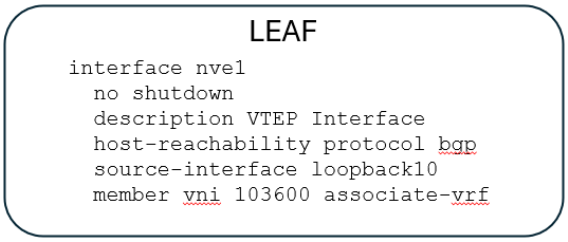
SPINE

```
neighbor 10.1.99.17
    inherit peer MULTISITE
    description SPINE1
  neighbor 10.1.99.21
    inherit peer MULTISITE
    description SPINE2
  neighbor 10.4.96.2
    remote-as 65002
    description BGP to Spine2
    update-source loopback0
    address-family ipv4 unicast
      send-community
      send-community extended
    address-family l2vpn evpn
      send-community
      send-community extended
  neighbor 10.4.96.101
    inherit peer LEAF
    description LEAF1
  neighbor 10.4.96.102
    inherit peer LEAF
    description LEAF2
  neighbor 10.4.96.103
    inherit peer LEAF
    description LEAF3
  neighbor 10.4.96.104
    inherit peer LEAF
    description LEAF4
  vrf DC-PROD
    address-family ipv4 unicast
      advertise l2vpn evpn
      maximum-paths 4
```

Slika 25: Primer konfiguracije MP-BGP z EVPN

Vir: (Lasten vir)

Za zagotavljanje ustreznega ovijanja originalnih okvirjev in vzpostavitve t. i. tunelov VTEP se uporabljajo namenski logični vmesniki, imenovani »nve«. Nastavitve pod njimi povedo, da je njihov izvorni vmesnik »Loopback« in za zagotavljanje dosegljivosti informacij kontrolne ravnine uporabljamo protokol BGP.



Slika 26: Primer konfiguracije vmesnika »VTEP«

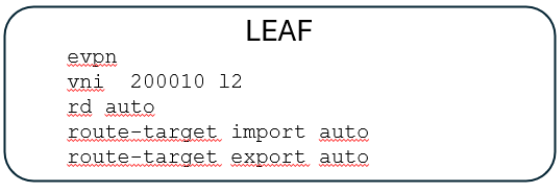
Vir: (Lasten vir)

Vsaki skupini VLAN se ročno doda vrednost atributa VNI, kar zagotavlja preslikavo VLAN – VXLAN in s tem omogočimo segmentacijo prometa na več navideznih omrežij znotraj posameznega stikala. Obenem s tem pridobimo možnost ponovne uporabe iste skupine VLAN na drugih stikalih za druge najemnike.

Slika 27: Primer preslikave VLAN – VXLAN

Vir: (Lasten vir)

Vzpostavitve mostovne domene (angl. bridge domain) je eden izmed ključnih konceptov, ki omogoča segmentacijo omrežnega prometa znotraj omrežja VXLAN. Poleg tega zagotovi razširitve L2-domene s pomočjo omrežja L3, služi za pravilno ovijanje in odvijanje okvirjev, učenje naslovov MAC in nudi podporo večnajemništva.



Slika 28: Primer nastavitve mostovne domene

Vir: (Lasten vir)

6.5 *Varnostni mehanizmi*

V nadaljevanju je predstavljenih nekaj uporabljenih varnostnih mehanizmov za zagotavljanje večje varnosti v omrežju podatkovnega centra. Večina uporabniških segmentov se zaključuje na namenski požarni pregradi naslednje generacije, kjer se tudi izvaja varnostna politika pregledovanja prometnih tokov. V nadaljevanju so podrobneje opisane rešitve, kot so:

- šifriranje povezav med podatkovnima centroma z mehanizmom MACSec,
- logična delitev prekrivnega omrežja in vpeljava večnajemnega modela,
- administrativni dostop do omrežnih naprav.

6.5.1 *Mehanizem MACSec*

MACSec je standard za varno komunikacijo na ravni podatkovne povezave, ki zagotavlja šifriranje podatkov in integriteto na omrežnih povezavah. Na stikalih Cisco Nexus 9300 MACsec omogoča šifriranje podatkovnega prometa med napravami na ravni L2, kar zagotavlja varnost pred prestrezanjem podatkov (angl. sniffing) in vrivanjem zlonamernih podatkov (angl. injection attacks).

Spodaj sta predstavljena primer konfiguracije mehanizma MACSec na stikalih »spine« in šifriranje povezav med podatkovnima centroma.

SPINE

```
feature macsec

key chain MACSEC-DCI-KEY macsec
  key 10
    key-octet-string 7 <GESLO>
     cryptographic-algorithm AES_256_CMAC

macsec policy MACSEC-DCI-POLICY
  cipher-suite GCM-AES-256

interface Ethernet1/2
macsec keychain MACSEC-DCI-KEY policy
   MACSEC-DCI-POLICY
```

Slika 29: Primer konfiguracije MACsec

Vir: (Lasten vir)

6.5.2 Vpeljava večnajmenega modela

Z uporabo različnih navideznih usmerjevalnih instanc VRF je omogočeno ločevanje omrežnih poti na istem podložnem omrežju podatkovnega centra, s čimer lahko vpeljemo model večnajmeništva med različnimi uporabniškimi skupinami, naročniki, okolji.

Vsaka instanca VRF omogoča segmentacijo omrežja znotraj ene fizične infrastrukture in deluje kot ločen usmerjevalni sistem z lastno tabelo usmerjanja, kar pomeni, da lahko dve različni instanci uporabljata isti naslovni prostor brez medsebojnega oviranja in morebitnih težav.

Posamezna navidezna usmerjevalna instanca VRF preprečuje, da promet iz posamezne instance vpliva na promet v drugi instanci in s tem je omogočena uporaba različnih politik usmerjanja.

Spodaj je primer segmentacije omrežja glede na tip okolja, kot so »PROD«, »STAGE«, »DEVELOP« in »GUEST«.

SPINE IN LEAF

```
vrf context DC-PROD
  vni 100100
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context DC-STAGE
  vni 100200
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context DC-DEVELOP
  vni 100200
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context DC-GUEST
  vni 100300
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
```

SPINE IN LEAF

```
interface Vlan3600
  description L3 VNI VXLAN usmerjanje
za DC-PROD
  no shutdown
  mtu 9216
  vrf member DC-PROD

interface Vlan3100
  description L3 VNI VXLAN usmerjanje
za DC-STAGE
  no shutdown
  mtu 9216
  vrf member DC-STAGE

interface Vlan3620
  description L3 VNI VXLAN usmerjanje
za DC-DEVELOP
  no shutdown
  mtu 9216
  vrf member DC-DEVELOP


interface Vlan3630
  description L3 VNI VXLAN usmerjanje
za DC-GUEST
  no shutdown
  mtu 9216
  vrf member DC-GUEST
  no ip redirects
  ip forward
  no ipv6 redirects
```

Slika 30: Primer segmentacije prekrivnega omrežja

Vir: (Lasten vir)

6.5.3 Administrativni dostop do omrežnih naprav

Na stikalih v podatkovnih centrih je pogosto uporabljena ločena instanca VRF, namenjena za upravljanje (angl. management), kar omogoča izolacijo administrativnega prometa od produkcijskega. Instanca VRF za upravljanje se uporablja za ločevanje administrativnih povezav in protokolov, kot so SSH, TACACS+, NTP, SNMP, SYSLOG itd., od ostalega omrežnega prometa. Naslednja slika prikazuje konfiguracijo uporabljenih protokolov za upravljanje na stikalih v podatkovnem centru.

SPINE IN LEAF

```
feature tacacs+

username admin password 5 <GESLO> role network-admin

ip domain-lookup
ip domain-name domena.local
ip name-server 10.1.10.100 use-vrf management

tacacs-server host 10.1.11.3 key 7 „GESLO"
tacacs-server host 10.1.12.3 key 7 „GESLO"

aaa group server tacacs+ ISE
    server 10.1.11.3
    server 10.1.12.3
    use-vrf management
    source-interface mgmt0

aaa authentication login default group ISE local
aaa authorization commands default group ISE local
aaa accounting default group ISE local

snmp-server contact DC1
snmp-server user snmpuser network-admin auth md5 <HASH> priv des <HASH>
localizedkey

ip access-list SNMP
  15 permit ip 10.3.100.0/28 any
  20 deny ip any any log

ntp server 10.1.14.15 use-vrf management
ntp source-interface mgmt0

logging server 10.1.15.10 4 use-vrf management
```

Slika 31: Primer upravljavskih protokolov

Vir: (Lasten vir)

7 ZAKLJUČEK

V diplomskem delu sem raziskal in analiziral ključno vlogo, ki jo sodobna omrežna arhitektura ima pri zagotavljanju visoke zmogljivosti, zanesljivosti in prilagodljivosti podatkovnih centrov. Na podlagi teoretičnih izhodišč in praktičnih primerov sem predstavil arhitekturo CLOS, ki temelji na topologiji »Spine-Leaf«, kot eni izmed najbolj optimalnih rešitev za sodobne podatkovne centre.

Hipoteza 1: Arhitektura »Spine-Leaf« omogoča boljšo razširljivost podatkovnih centrov v primerjavi s tradicionalnimi topologijami.

Hipoteza je potrjena. Arhitektura zagotavlja preprosto razširljivost, saj omogoča dodajanje novih stikal »leaf« in »spine« brez prekinitev obstoječih storitev. Omogoča enotno in predvidljivo latenco med končnimi točkami, kar je ključno za podporo sodobnim aplikacijam in storitvam, ki zahtevajo nizko zakasnitev. Poleg tega je arhitektura »Spine-Leaf« zasnovana z mislijo na podporo za sodobne protokole in tehnologije, kot sta VXLAN in EVPN, ki omogočajo prilagodljivo in varno segmentacijo omrežja.

Hipoteza 2: Podatkovni centri, zgrajeni na topologiji »Spine-Leaf«, dosegajo nižjo omrežno latenco in so zanesljivejši v primerjavi s podatkovnimi centri, ki uporabljajo tradicionalne topologije.

Hipoteza je potrjena. Topologija »Spine-Leaf« je zasnovana z namenom optimizacije omrežnega prometa in zmanjšanja latence. V tej topologiji sta prisotna dva sloja stikal, in sicer hrbtenična in dostopovna. Takšna struktura omogoča, da vsak prometni tok prehaja le skozi eno stopnjo, kar zmanjšuje število prehodov in s tem tudi latenco. V tradicionalnih topologijah se lahko promet preusmerja skozi več stopenj stikal (npr. dostopna stikala, agregacijska stikala in jedrna stikala), kar povečuje število prehodov in s tem latenco.

Topologija »Spine-Leaf« prav tako izboljšuje zanesljivost omrežja. V tej zasnovi se vsako stikalo »leaf« povezuje z vsemi stikali »spine«, kar zagotavlja podvojene poti za vsak prometni tok. To pomeni, da v primeru okvare enega ali več stikal »spine« promet še vedno lahko teče s pomočjo drugih, brez večjih motenj v delovanju omrežja.

Hipoteza 3: Arhitektura »Spine-Leaf« omogoča večjo prilagodljivost pri upravljanju omrežja, kar vodi k hitrejšemu prilagajanju spreminjajočim se potrebam podatkovnega centra.

Hipoteza je potrjena. Arhitektura »Spine-Leaf« omogoča hitro in preprosto dodajanje ali odstranjevanje naprav v omrežju brez potrebe po obsežnih konfiguracijskih spremembah. V tej topologiji so vsa stikala »leaf« povezana z vsemi stikali »spine«, kar pomeni, da dodajanje novih stikal »leaf« ali strežnikov ne vpliva na obstoječe povezave in omogoča, da se nove naprave preprosto povežejo v omrežje. Takšna prilagodljivost zmanjšuje potrebo po načrtovanju in zmanjšuje motnje v delovanju obstoječega omrežja. Opisana arhitektura je zasnovana tako, da podpira napredne tehnologije in inovacije. Zasnova omrežja omogoča preprosto integracijo novih tehnologij in rešitev, kar pomeni, da podatkovni centri lahko hitro sprejmejo novosti, kot so višje hitrosti prenosa podatkov ali novi standardi omrežnih protokolov, brez potrebe po obsežnih prenovah omrežja.

Hipoteza 4: Arhitektura »Spine-Leaf« omogoča preprostejše upravljanje in s tem bolj optimalne stroške za delovanje omrežja podatkovnih centrov.

Hipoteza je potrjena. Arhitektura »Spine-Leaf« ponuja poenostavljeno strukturo omrežja z dvema ravnima stikal, kar zmanjša kompleksnost omrežne topologije v primerjavi z bolj zapletenimi tradicionalnimi arhitekturami. Zaradi preproste topologije in standardizacije gradnikov arhitektura »Spine-Leaf« omogoča preprostejše upravljanje in vzdrževanje omrežja. Zmanjšana kompleksnost pomeni manj napak pri konfiguraciji in potrebo po manjšem številu tehničnih virov za podporo omrežja. Manjše tveganje za napake in hitrejše reševanje težav zmanjšujeta stroške operacij in vzdrževanja, kar prispeva k bolj optimalnim skupnim stroškom delovanja.

Omogoča preprostejšo integracijo z naprednimi nadzornimi orodji, ki lahko samodejno spremljajo in optimizirajo delovanje omrežja. Te orodja lahko hitro identificirajo in rešujejo težave ter omogočajo boljše načrtovanje zmogljivosti. Preprostejši nadzor pripomore k zmanjšanju stroškov dela in izboljša učinkovitost upravljanja omrežja.

Hipoteza 5: Zaradi preproste arhitekture omrežij »Spine-Leaf« je uvajanje v UI preprostejše ter tako natančnejše in hitrejše odkrivanje nepravilnosti tako v konfiguracijah kot tudi v delovanju omrežja.

Hipoteza je potrjena. Arhitektura »Spine-Leaf« se dobro povezuje z naprednimi nadzornimi orodji in s sistemi za upravljanje omrežja. Ta orodja lahko preprosto analizirajo in vizualizirajo stanje omrežja ter hitro identificirajo težave, saj so povezave in poti v omrežju jasne in preprosto sledljive. To omogoča boljšo analizo podatkov in natančnejše napovedovanje težav, kar povečuje hitrost in natančnost pri odkrivanju nepravilnosti. V uporabljeni tehnični rešitvi metod in algoritmov UI nisem mogel potrditi, vendar so v poglavju 5.2 predstavljeni teoretični vidiki potencialne uporabe.

Zaključujem, da je arhitektura CLOS pomemben korak naprej v razvoju podatkovnih centrov, saj omogoča izpolnjevanje zahtev sodobnega poslovanja in tehnoloških inovacij. Njena uvedba lahko organizacijam prinese konkurenčno prednost z izboljšanjem učinkovitosti, znižanjem operativnih stroškov in s povečano odpornostjo proti morebitnim motnjam v delovanju. V prihodnosti bo njena vloga v IT-infrastrukturi še naprej rasla, saj postaja ključna komponenta za podporo digitalne preobrazbe in inovacij.

S pospešenim razvojem in z uporabo UI bo upravljanje sodobnih omrežij IKT postajalo preprostejše. Njena vloga bo predvsem samodejno reševanje in prepoznavanje anomalij v prometnih tokovih, kar bo znatno olajšalo delo sistemskim skrbnikom.

S praktičnim primerom sem potrdil teoretična izhodišča in uporabo opisane arhitekture v produkcijskem okolju, ki podpira poslovne potrebe podjetja pri poslovanju.

8 VIRI IN LITERATURA

Al-shawi, M., & Andre, L. (2016). *Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide: CCDP ARCH 300-320, 4th Edition.* Cisco Press.

Chandrasekaran, K. (2014). *Essentials of Cloud Computing 1st Edition.* Chapman and Hall/CRC.

Cisco Inc. . (9. april 2024). *Cisco 100GBASE QSFP-100G Modules Data Sheet*. Pridobljeno iz https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html.

Cisco Inc. . (7. junij 2024). *Cisco Nexus 9300-FX3 Series Switches Data Sheet*. Pridobljeno iz https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-744052.html.

Cisco Inc. (2024). *Cisco Nexus 9336C-FX2 Switch*. Pridobljeno iz https://www.cisco.com/c/en/us/products/switches/nexus-9336c-fx2-switch/index.html.

Cloud Appliances. (brez datuma). *QSFP Transceiver*. Pridobljeno iz https://www.cloudappliances.co.uk/product/cisco-qsfp-100g-erl-s-spare/.

Gartner. (20. maj 2024). *Gartner Forecasts Worldwide Public Cloud End-User Spending to Surpass $675 Billion in 2024*. Pridobljeno iz Press Release: https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024.

Modrijan, G. (2016). Storitve sodobnih dostopovnih in jedrnih telekomunikacijskih omrežij.

Pasanen, T. (2019). *Virtual Extensible LAN (VXLAN): A Practical guide to VXLAN solution.* Samozaložba.

Pasanen, T. (2020). *VXLAN Fabric with BGP EVPN Control-Plane: Design Considerations.* Samozaložba.

Port Channels and vPCs. (2024). Pridobljeno iz https://www.ciscopress.com/articles/article.asp?p=3150966&seqNum=2.

Salvatore, L. (25. 8 2015). *Building the Next Generation of DigitalOcean Networking*. Pridobljeno iz Digital Ocean: https://www.digitalocean.com/blog/building-the-next-generation-of-digitalocean-networking.

Zeni, D. (2024). *Cisco SD-Access*. Pridobljeno iz https://www.lookingpoint.com/blog/sd-access.

Zsiga, Z. (2023). *Cisco Certified Design Expert (CCDE 400-007) Official Cert Guide.* Cisco Press.