Tehnologija EVPN i njena primjena u računalnim mrežama

Volarević, Ante

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1325

TEHNOLOGIJA EVPN I NJENA PRIMJENA U RAČUNALNIM MREŽAMA

Ante Volarević

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1325

TEHNOLOGIJA EVPN I NJENA PRIMJENA U RAČUNALNIM MREŽAMA

Ante Volarević

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 4. ožujka 2024.

ZAVRŠNI ZADATAK br. 1325

Pristupnik:	**Ante Volarević (0036541973)**
Studij:	Elektrotehnika i informacijska tehnologija i Računarstvo
Modul:	Računarstvo
Mentor:	prof. dr. sc. Željko Ilić

Zadatak: **Tehnologija EVPN i njena primjena u računalnim mrežama**

Opis zadatka:

Tehnologija EVPN (engl. Ethernet Virtual Private Network) osigurava prijenos okvira te proširuje povezivost virtualnih privatnih mreža na sloju podatkovne poveznice. Vaš je zadatak istražiti sve značajke tehnologije EVPN kao i njenu primjenu u računalnim mrežama. Svu potrebnu literaturu i uvjete za rad osigurat će Vam Zavod za telekomunikacije.

Rok za predaju rada: 14. lipnja 2024.

Mentor: prof. dr. sc. Željko Ilić

Voditelj rada: prof. dr. sc. Željko Ilić

Sadržaj

1. Uvod

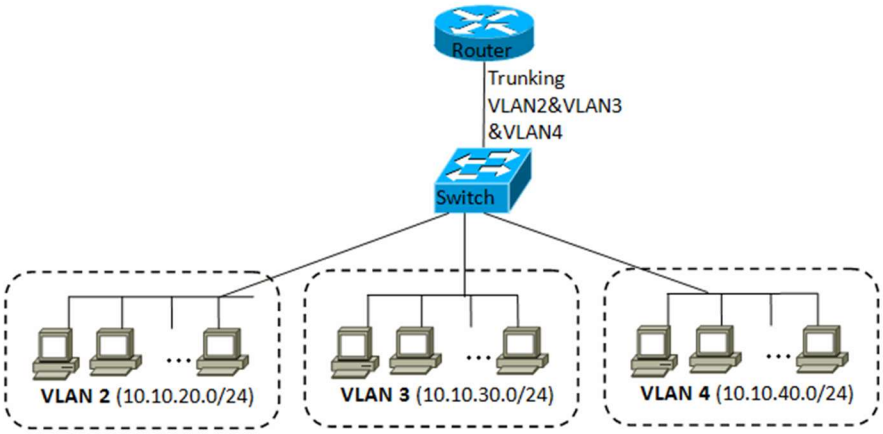
Virtualna privatna mreža drugog sloja (*engl. Ethernet Virtual Private Network*, skraćeno EVPN) tehnologija je koja se primarno koristi za povezivanje dijelova mreže koristeći istu infrastrukturu (*engl. Ethernet infrastructure*). Ovaj tip arhitekture, uz korištenje određenih protokola, pruža značajna poboljšanja u vidu skalabilnosti, efikasnosti i sigurnosti mrežnog upravljanja.

U ovom radu će se temeljito analizirati terminologija koja je povezana s EVPN tehnologijom, kao i njezine glavne prednosti. Nakon uvodnog dijela, u drugom paragrafu detajno će se opisati i analizirati strukture podatkovnih okvira te karakteristike virtualnih i virtualnih proširivih lokalnih mreža koje se mogu koristiti u kombinaciji s EVPN-om.

U trećem poglavlju razmatra se sama tehnologija EVPN, uključujući njenu terminologiju, arhitekturu, i tehnologiju EVPN-VXLAN. Također će biti predstavljene različite vrste EVPN ruta koje omogućavaju efikasnije usmjeravanje i prijenos podataka unutar mreže. Nadalje, opisati će se primjena tehnologije EVPN u računalnim mrežama te će se objasniti mehanizam djelovanja i prednosti ove tehnologije u praktičnoj primjeni.

2. Virtualne lokalne mreže

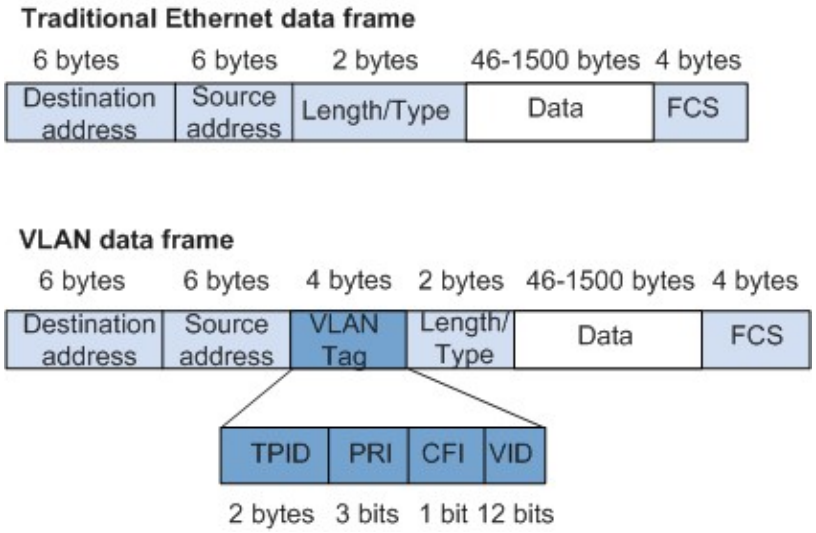
Lokalna mreža (*engl. Local Area Network*, skraćeno LAN) predstavlja računalnu mrežu čiji se doseg najčešće odnosi na područje unutar jedne ili skupine zgrada. Budući da se na njih može spojiti ograničen broj korisnika, bitno je dobro organizirati arhitekturu jedne takve mreže. Jedna od tehnologija koja pružaja rješenje za navedeni problem jesu virtualne lokalne mreže (*engl. Virtual Local Area Network*, skraćeno VLAN). Njihovom se primjenom jedna lokalna mreža dijeli u više logičkih podmreža. Koristeći ovu tehnologiju mreža trećeg sloja (*engl. Layer 3 network*) se prevodi na infrastrukturu mreže drugog sloja (*engl. Layer 2 network*). Ova funkcionalnost omogućuje komutatorima (*engl. switch*) mogućnost upravljanja i usmjeravanja prometa između različitih logičkih segmenata unutar iste fizičke mreže. Navedena podjela na logičke podmreže provodi se na način da se grupiraju korisnici koji imaju slične zahtjeve i potrebe za resursima. Primjer jedne virtualne lokale mreže prikazan je na slici (Slika 1Slika 1).



Slika 1 Virtualna lokalna mreža [12]

2.1. Struktura podatkovnog okvira virtualnih lokalnih mreža

Podatkovni okvir vrlo je sličan običnom LAN-ovom podatkovnom okviru, uz iznimku dodavanja oznake virtualne lokalne mreže (*engl. Virtual Local Area Network tag*, skraćeno VLAN tag). Ta četiri okteta neophodna su kako bi komutator mogao identificirati kojoj virtualnoj podmreži pripada pojedini okvir. Navedena usporedba prikazana je na slici (Slika 2).



Slika 2 Usporedba tradicionalnog Ethernet okvira i VLAN-ovog okvira [13]

Oznaka virtualne lokalne mreže sastavljena je od četiri polja. Identifikator protokola oznake (*engl. Tag Protocol Identifier*, skraćeno TPID) zajednički je za sve VLAN-ove i omogućuje uređajima u mreži da prepoznaju VLAN okvire. Prema IEEE 802.1Q standardu, njegova uobičajena vrijednost je *0x81-00.* Preostala dva okteta odnose se na kontrolnu informaciju za označavanje okvira. Kanonski indikator formata (*engl. Canonical Format Indicator*, skraćeno CFI) je jednobitna oznaka koja označava jesu li MAC adrese enkapsulirane u standardnom obliku (vrijednost 0) ili nisu. U slučaju virtualnih lokalnih mreža, vrijednost tog polja uvijek iznosi 0. Kod točke prioriteta (*engl. Priority Code Point*, skraćeno PRI) zauzima tri bita i predstavlja oznaku prioriteta čije su vrijednosti prikazane u tablici (Tablica 1).

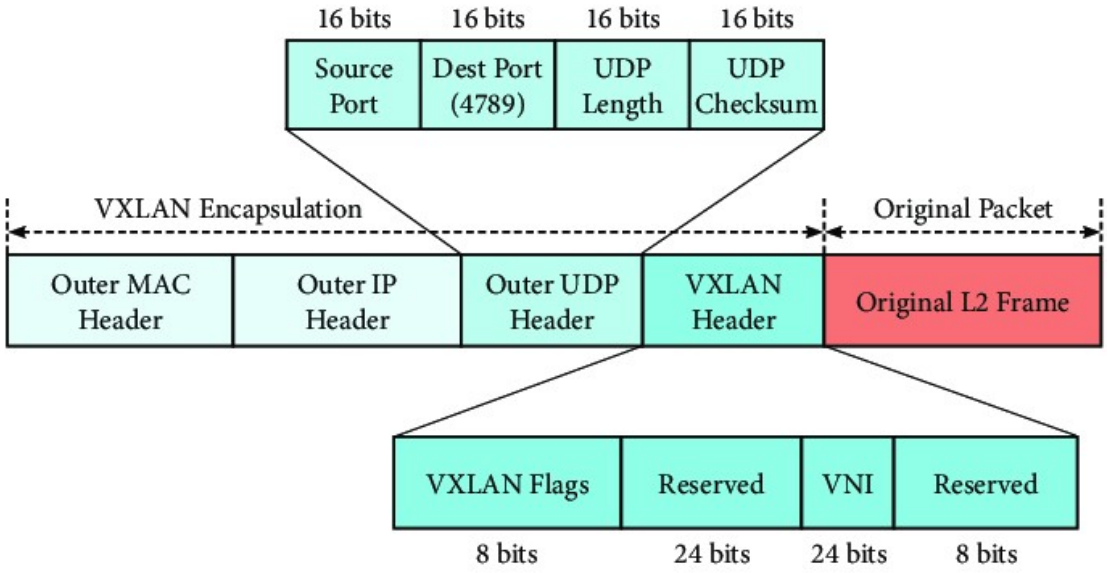
Tablica 1 Prikaz prioriteta VLAN okvira

PRI Vrijednost	Prioritet
7	Upravljanje mrežom (npr. ICMP poruka)
6	Govorni promet (kašnjenje < 10 ms)
5	Video (kašnjenje < 100 ms)
4	Kontrolirano opterećenje (kritični podaci)
3	Excellent Effort (najvažniji dio Best-Effort)
2	Best Effort (npr. transfer datoteka)
1	Rezerva
0	Pozadinski promet (npr. backup)

Najbitniji dio spomenutog tag-a je identifikator virtualne lokalne mreže (*engl. Virtual local area network Identifier*, skraćeno VID) koji predstavlja jedinstvenu oznaku za pojedinu podmrežu. Kod standardnog VLAN-a, za pohranu identifikatora koristi se 12 bitova, što omogućava maksimalno 4096 različitih logičkih podmreža (2^12 = 4096) [2]. Međutim, isto može predstavljati problem jer za velike organizacije i podatkovne centre (*engl. Data centers*) to može biti nedovoljno. Oni zahtijevaju više od 4096 različitih logičkih mreža za učinkovitu segmentaciju i upravljanje mrežnim resursima. Jedno od rješenja za taj problem predstavljaju virtualne proširive lokalne mreže.

2.2. Virtualne proširive lokalne mreže

Virtualne proširive lokalne mreže (*engl. Virtual Extensible Local Area Network*, skraćeno VXLAN) predstavljaju značajnu nadogradnju tehnologije tradicionalnih logičkih podmreža. Ključna razlika leži u proširenom prostoru za identifikaciju virtualnih mreža. Umjesto ograničenih 12 bitova za tradicionalne VLAN identifikatore, virtualne proširive lokalne mreže rezerviraju 24 bita za Virtual Identificator (VID). Ovo značajno povećanje omogućuje VXLAN-u da podrži oko 17 milijuna različitih vrijednosti identifikatora za virtualne podmreže (2^24 = 16,777,216 kombinacija). Prilikom prijenosa podataka koristeći ovu tehnologiju, podaci se direktno enkapsuliraju u UDP (*engl. User Data Protocol*) pakete, što je prednost jer nema potrebe za korištenje dodatnih uređaja.



Slika 3 Prikaz VXLAN-ovog podatkovnog okvira i zaglavlja [14]

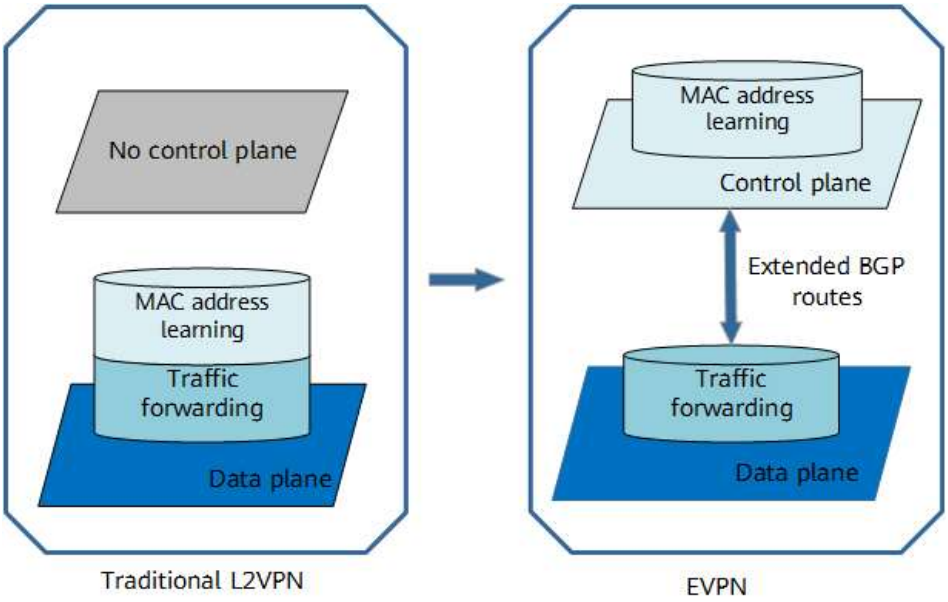
Slika 3 prikazuje izgled jednog okvira virtualne proširive lokalne mreže. Na osnovne podatke s drugog sloja, redom se dodaju VXLAN, UDP te IP (*engl. Internet protocol*) zaglavlja koja su neophodna za ispravan rad [3]. Ova tehnologija često se koristi u kombinaciji s Ethernet virtualnom privatnom mrežom (*engl. Ethernet Virtual Private Network*, skraćeno EVPN) kako bi se postiglo efikasnije upravljanje mrežom, što će se kasnije detaljno opisati u radu.

3. Ethernet virtualne privatne mreže

Široka prihvaćenost usluga Ethernet VPN i pojava novih aplikacija za tu tehnologiju, kao što je povezivanje podatkovnih centara, rezultirali su novim skupom zahtjeva koji se ne mogu lako riješiti u dosad spomenutim tehnologijama. Konkretno, multihoming s aktivnim prosljeđivanjem svih veza nije podržan, a ne postoji ni rješenje koje bi iskoristilo Multipoint-to-Multipoint (skraćeno MP2MP) Label Switched Paths (skraćeno LSPs) za optimizaciju dostave višeciljnih okvira [1]. Rješenje za prethodno navedene probleme predstavlja tehnologija Ethernet virtualnih privatnih mreža.

3.1. Terminologija EVPN-a

Ethernet virtualna privatna mreža je tehnologija koja ostvaruje efikasnu distribuciju Ethernet okvira između različitih domena slojeva druge i treće razine. Njezin glavni cilj je jednostavno proširivanje lokalnih mreža između različitih lokacija, a da i dalje osiguramo visoku razinu sigurnosti i efikasnosti.



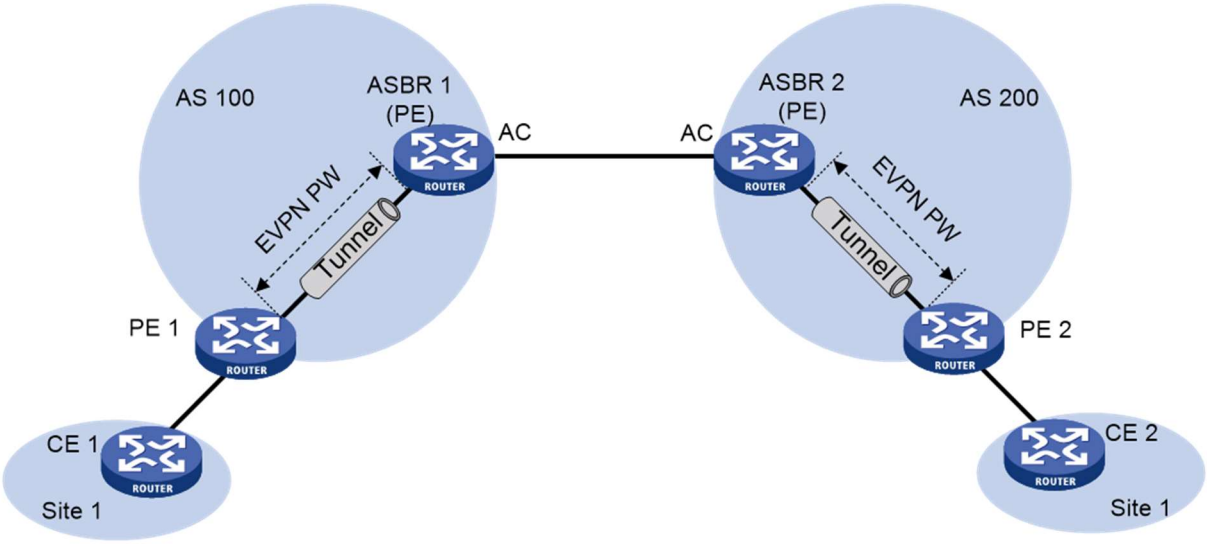
Slika 4 Usporedba tradicionalnog i rješenja nove generacije [16]

Slika 4 prikazuje prednosti ove tehnologije u odnosu na dosadašnju varijantu. Ethernet VPN obavlja funkcije upravljačke razine (*engl. control plane*), to jest odgovoran je za donošenje odluka o prijenosu i kontroli prometa unutar mreže. Temeljen je na protokolu BGP

(*engl. Border Gateway Protocol*), koji je standard za razmjenu mrežnih informacija između autonomnih sustava na internetu. Protokol BGP omogućuje Ethernet virtualnim privatnim mrežama da dinamički uče i razmjenjuju informacije o adresama medijskog pristupa (*engl. Media Access Control*, skraćeno MAC) i IP adresama između mrežnih uređaja, što olakšava upravljanje i slanje podataka na mreži [5]. Za razliku od tradicionalnih servisa drugog sloja, koji adrese medijskog pristupa drže u podatkovnoj razini, ova tehnologija učenje MAC adresa provodi u upravljačkoj razini.

3.2. Arhitektura EVPN-a

Koncept Ethernet VPN-a temelji se na upotrebi korisničkih uređaja (*engl. Customer Equipment*, skraćeno CE) koji su povezani s rubnim uređajima pružatelja usluga (*engl. Provider Edge*, skraćeno PE). CE uređaj može biti host, usmjerivač ili komutator. PE uređaj pruža virtualnu mostnu povezanost između CE uređaja [16]. U pojedinoj mreži može postojati više EVPN-ova. Učenje između PE usmjerivača odvija se u upravljačkoj razini (*engl. control plane*) koristeći protokol BGP, za razliku od tradicionalnog mosta gdje se učenje odvija u podatkovnoj razini (*engl. data plane*). Slika 5 prikazuje primjer jednog sustava koji koristi EVPN tehnologiju.



Slika 5 Prikaz arhitekture EVPN-a [16]

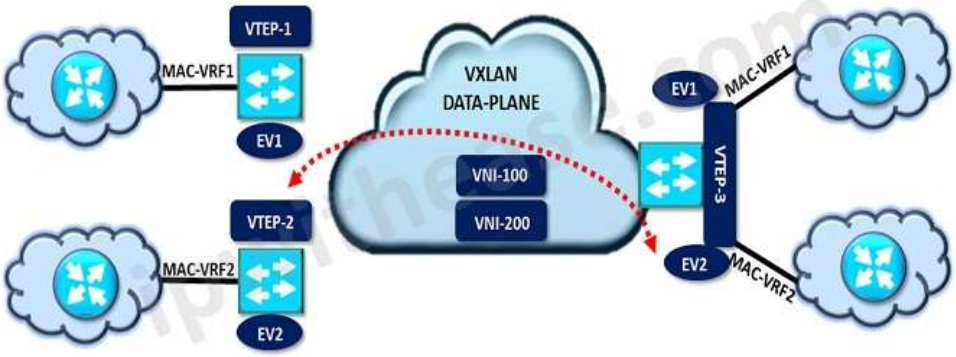
3.3. Tehnologija EVPN-VXLAN

Korištenje drugih tehnologija može rezultirati preplavljivanjem mreže (*engl. flooding*), što nije poželjno zbog smanjenja propusnosti i mogućeg gubitka resursa. Za razliku od toga, Ethernet virtualne privatne mreže ne koriste preplavljivanje, već primjenjuju druge mehanizme, poput protokola BGP, s ciljem informiranja drugih dijelova mreže o resursima koje posjeduju [7].

Tehnologija EVPN se u praksi često koristi s virtualnim proširenim lokalnim mrežama (skraćeno VXLAN). U takvoj kombinaciji, VXLAN-ovi imaju ulogu podatkovne razine (*engl. data plane*), dok EVPN signalizira VXLAN-u put koji treba koristiti za dostavu podataka. Tako VXLAN je odgovoran za učinkovit prijenos enkapsuliranih okvira do odredišta, dok ga EVPN navodi i rješava pitanja usmjeravanja u mreži.

Tehnologija VXLAN definira tuneliranje (*engl. tunneling*) koje prekriva sloj druge razine na treći sloj. Omogućava optimalno usmjeravanje Ethernet okvira uz podršku za višesmjerno usmjeravanje unicast i multicast prometa koristeći UDP/IP enkapsulaciju.

S druge strane, karakteristika EVPN-a je da se učenje MAC adresa između pružatelja usluga (*engl. Provider Edge*, skraćeno PE) odvija u kontrolnoj razini. Nova MAC adresa otkrivena od strane korisničkih uređaja (*engl. Customer Equipment*, skraćeno CE) oglašava se putem lokalnog PE-a svim udaljenim PE uređajima, koristeći već spomenuti protokol BGP. Ova metoda se razlikuje od postojećih tradicionalnih rješenja poput VPLS-a *(engl. Virtual Private LAN Service*), koje uče preplavljivanjem nepoznatih višeodredišnih (*engl. unicast*) paketa u podatkovnoj razini.



Slika 6 Mehanizmi djelovanja EVPN-VXLAN tehnologije [4]

Ova kombinacija tehnologija omogućuje veću razinu fleksibilnosti, skalabilnosti i sigurnosti mreže te olakšava upravljanje više podmreža i virtualnih mreža unutar iste fizičke infrastrukture, pružajući efikasno rješenje za različite zahtjeve aplikacija i korisnika [4][8].

3.4. Vrste EVPN ruta

Ovisno o funkcionalnosti koju želimo ostvariti korištenjem EVPN-a, prema [10] razlikujemo pet vrsta takvih ruta. Ova podjela prikazana je u tablici (Tablica 2).

Tablica 2 Podjela EVPN ruta [10]

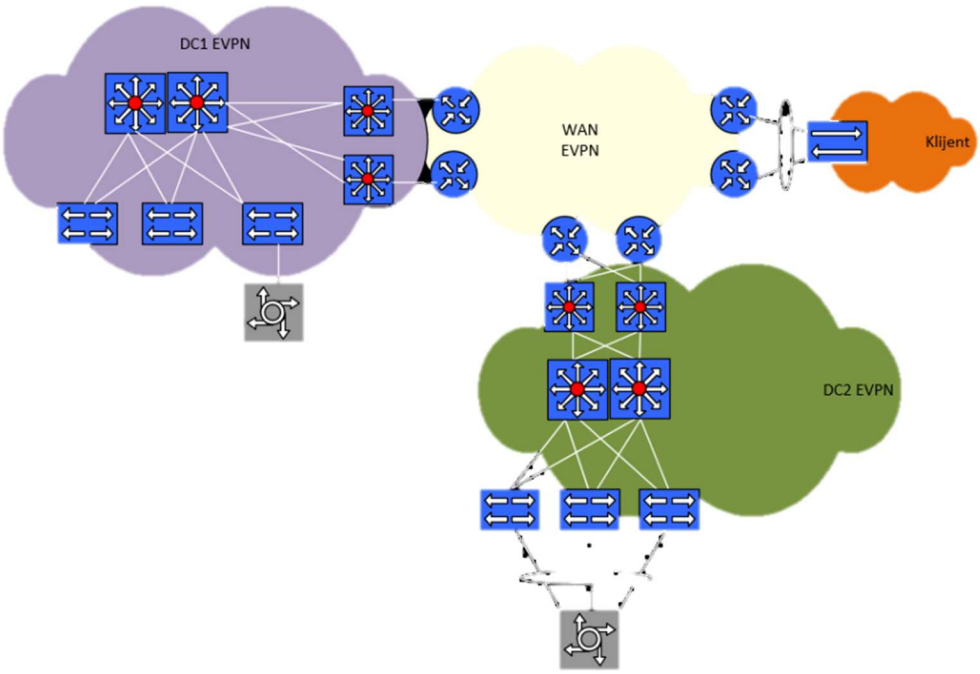
Route type	Naziv	Primjena
Type-1	Ethernet Auto-Discovery (AD) Route	Po ES-u šalje nekoliko ruta sa informacijom o listi EVI-u unutar jednog ES-a
Type-2	MAC/IP Advertismend Route	NLRI koji sadrži sami zapis za MAC adresom ili MAC-IP vezom za krajnju točku
Type-3	Inclusive Multicast Ethernet Tag Route	Multicast Tunnel End point discovery
Type-4	Ethernet Segment Route	Redundancy group discovery, Designated Forwarded election
Type-5	IP prefix route	Oglašavanje L3 IP prefix-a za L3VPN servise

3.5. Primjene tehnologije EVPN u računalnim mrežama

Ethernet virtualna privatna mreža pruža efikasnu i sigurnu opciju. Upravo iz tih razloga primjenjuje se u različitim područjima, a neka od njih su povezivanje podatkovnih centara, proširenje domena drugog sloja (*engl. Layer 2*, skraćeno L2) te pružanje servisa trećem sloju (*engl. Layer 3*, skraćeno L3).

Podatkovni centri (*engl. data centers*) su fizički ili virtualni prostori koji se koriste za pohranu, obradu i distribuciju podataka i aplikacija. Radi visoke razine sigurnosti koju zahtijevaju kombinacija tehnologija EVPN-VXLAN predstavlja idealno rješenje za integraciju tako složenih zahtjeva. Ako postoji potreba za izolacijom prometa pojedinog korisnika, EVPN može izolirati njihov promet kroz vlastite virtualne mreže. Sposobnost EVPN-ovog pronalaženja alternativnih puteva je također bitna značajka, jer ako dođe do kvara nekog uređaja ili preopterećenja nekog dijela mreže, ova tehnologija može preusmjeriti promet po punim

brzinama na druge dostupne pravce i ne izazvati velike gubitke u performancama [9]. Primjer jednog povezivanja podatkovnih centara prikazan je na slici (Slika 7).



Slika 7 Povezivanje podatkovnih centara tehnologijom EVPN [10]

Primjenom EVPN-a za proširenje Layer 2 domena postiže se jednostavno proširenje lokalnih mreža između udaljenih lokacija bez potrebe za korištenje složenijih konfiguracija ili dodatne opreme. S druge strane, EVPN se također primjenjuje za pružanje Layer 3 usluga omogućavajući organizacijama da koriste istu infrastrukturu za L2 i L3 usluge, smanjujući složenost mreže i troškove održavanja, dok istovremeno pruža napredne mrežne funkcionalnosti i visoku razinu sigurnosti.

Sažetak

Tehnologija Ethernet Virtual Private Network (EVPN) omogućuje efikasno povezivanje dijelova mreže koristeći zajedničku Ethernet infrastrukturu. Time se postižu značajna poboljšanja u vidu skalabilnosti, efikasnosti i sigurnosti mrežnog upravljanja. Kroz ovaj rad, detaljno su opisani ključni pojmovi i prednosti EVPN-a u odnosu na postojeće tehnologije, kao i vrste virtualnih lokalnih mreža koje se koriste u kombinaciji s EVPN-om. Objašnjene su različite vrste EVPN ruta i njihove funkcionalnost, kao i praktične primjene tehnologije u povezivanju podatkovnih centara, proširenju domena drugog sloja i pružanju usluga trećeg sloja. Osim sveobuhvatnog pregleda tehnologije EVPN, rad posebno naglašava njenu važnost i budući potencijal za razvoj mrežnih rješenja.

Summary

Ethernet Virtual Private Network (EVPN) technology enables efficient network segment interconnection using a common Ethernet infrastructure, offering significant improvements in scalability, efficiency, and security of network management. This paper thoroughly explores the key concepts and advantages of EVPN over existing technologies, as well as Virtual Local Area Networks (VLANs) and Virtual Extensible Local Area Networks (VXLANs) that are used in combination with EVPN. The various types of EVPN routes and their functionalities are explained, along with practical applications of the technology in connecting data centers, extending Layer 2 domains, and providing Layer 3 services. This paper not only provides a detailed overview of EVPN technology but also highlights its importance and future potential for the development of network solutions.

Zaključak

Ethernet virtualne privatne mreže predstavljaju značajan napredak naspram tradicionalnih rješenja, u vidu upravljanja i povezivanja mreža, posebno u složenim okruženjima kao što su podatkovni centri. Korištenjem EVPN-a u kombinaciji s virtualnim proširenim lokalnim mrežama, omogućava se visoka skalabilnost, efikasnost i sigurnost mrežnog prometa. Primjenom protokola BGP za učenje i razmjenu MAC i IP adresa, EVPN poboljšava upravljanje mrežom i smanjuje rizik od preopterećenja i gubitka podataka. Zbog navedenih osobina, ova tehnologija često se primjenjuje za povezivanje velikih podatkovnih centara. Konačno, Ethernet virtualne privatne mreže pružaju pouzdano i efikasno rješenje za suvremene mrežne potrebe, osiguravajući stabilnost i visoke performanse mrežnih infrastruktura.

Literatura

[1] IETF RFC 7209: *Requirements for Ethernet VPN (EVPN)* May 2014 (available at: https://datatracker.ietf.org/doc/html/rfc7209)

[2] TechHub.hpe: *VLAN frame encapsulation* (available at: https://techhub.hpe.com/eginfolib/networking/docs/switches/5510hi/5200-0075b_l2-lan_cg/content/496798293.htm)

[3] Jupter Networks: *What is VXLAN* (available at: https://www.juniper.net/us/en/research-topics/what-is-vxlan.html)

[4] IPWithEase: *An Overview of EVPN* (Ethernet VPN) (available at: https://ipwithease.com/evpn-basics/)

[5] CloudFlare: *What is BGP?* (available at: https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-bgp/)

[6] https://www.linkedin.com/pulse/bgp-evpn-vxlan-datacenter-satish-patel/

[7] NETWORKING WITH H: *EVPN explained in simple terms* (available at: https://www.youtube.com/watch?v=UZR0K6N1lAE)

[8] ArubaNetworks: *What is EVPN-VXLAN?* (available at: https://www.arubanetworks.com/faq/what-is-evpn-vxlan/)

[9] Jupter Networks: *VXLAN Data Center Interconnect Using EVPN Overview* (available at: https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/concept /vxlan-evpn-integration-overview.html)

[10] Karlo Crnjak: *Ethernet VPN (EVPN) pregled, April 2023* (available at: https://nog.hr/files/meetup2/2023-04-20-Meetup02_05_Karlo_Crnjak-CS_Computer_Systems-Ethernet_VPN-EVPN.pdf)

[11] Jupter Networks: *EVPN Multihoming Overview* (available at: https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/concept/evpn-bgp-multihoming-overview.html)

[12] Medium: *VLANs: "Segmenting Networks for Better Performance and Security.", February 2023* (available at: https://yoursmaddy.medium.com/vlans-segmenting-networks-for-better-performance-and-security-306d5d6b47a)

[13] NetworkCorner: *Understanding 802.1Q VLAN Tagging* (available at: https://www.networkcorner.co.uk/understanding-802-1q/)

[14] ResearchGate: *VXLAN-Packet-Encapsulation* (available at: https://www.researchgate.net/publication/354232739/figure/fig1/AS:1062674947395584@1630372859266/VXLAN-Packet-Encapsulation.png)

[15] ResearchGate: *VPN Tunneling structure* (available at: https://www.researchgate.net/figure/VPN-Tunneling-structure_fig1_320536838)

[16] H3C: *18-EVPN Configuration Guide* (available at: https://www.h3c.com/en/d_202212/1732407_294551_0.htm)

Skraćenice

VPN	Virtual Private Network
EVPN	Ethernet Virtual Private Network
LAN	Local Area Network
VLAN	Virtual Local Area Network
VXLAN	Virtual Extensible Local Area Network
EVPN	Ethernet Virtual Private Network
L2	Layer 2
L3	Layer 3
UDP	User Data Protocol
IP	Internet Protocol
PE	Provider edge
CE	Customer edge
TPID	Tag Protocol Identifier
CFI	Canonical Format Indicator
PRI	Priority Code Point
MAC	Medium Access Control
VID	Virtual local area network Identifier
MP2MP	Multipoint-to-Multipoint
LPS	Label Switched Paths
VPLS	Virtual Private LAN Service