Primjena standarda VXLAN u lokalnim mrežama

Žaja, Luka

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1326

PRIMJENA STANDARDA VXLAN U LOKALNIM MREŽAMA

Luka Žaja

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1326

PRIMJENA STANDARDA VXLAN U LOKALNIM MREŽAMA

Luka Žaja

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 4. ožujka 2024.

ZAVRŠNI ZADATAK br. 1326

Pristupnik:	**Luka Žaja (0036542512)**
Studij:	Elektrotehnika i informacijska tehnologija i Računarstvo
Modul:	Računarstvo
Mentor:	prof. dr. sc. Željko Ilić

Zadatak: **Primjena standarda VXLAN u lokalnim mrežama**

Opis zadatka:

Koncept virtualna lokalna mreža (engl. Virtual LAN) je podjela lokalne mreže na logičke domene neovisno o fizičkoj povezanosti mrežnih uređaja. Također, ograničenje u broju VLAN-ova koji se mogu adresirati na sloju podatkovne poveznice dovelo je do pojave standarada VXLAN (engl. Vrtual eXtensible LAN). Vaš je zadatak istražiti standard VXLAN-a te njegovu primjenu u lokalnim mrežama. Svu potrebnu literaturu i uvjete za rad osigurat će Vam Zavod za telekomunikacije.

Rok za predaju rada: 14. lipnja 2024.

Sadržaj

1. Uvod

Virtualna proširena lokalna mreža (*eng.* Virtual extensible local area network, *skr.* VXLAN) predstavlja jednu od ključnih tehnologija u modernim mrežnim arhitekturama koje omogućuju proširivanje podatkovnih centara i poboljšanje skalabilnosti mreža. VXLAN je osmišljen kako bi prevladao ograničenja tradicionalnih virtualnih lokalnih mreža (*eng.* Virtual local area network, *skr.* VLAN) omogućavajući veću fleksibilnost i skalabilnost. U kontekstu današnjeg brzog rasta usluga računarstva u oblaku i potrebe za učinkovitijim mrežnim rješenjima, razumijevanje i implementacija VXLAN tehnologije postali su iznimno relevantni.

Ovaj završni rad istražuje temeljne aspekte VXLAN tehnologije, objašnjavajući njezine ključne komponente, prednosti i praktične primjene. Rad je strukturiran tako da čitatelju pruži detaljno razumijevanje različitih aspekata VXLAN-a.

Prvi segment bit će posvećen uvodu u VLAN. Ovaj dio rada pružit će osnovne informacije o toj tehnologiji, objašnjavajući njezinu ulogu i važnost u mrežnim arhitekturama. Detaljno će biti objašnjeno kako VLAN-ovi omogućuju segmentaciju mreže, poboljšanje sigurnosti i optimizaciju mrežnih resursa, a taj segment je ključan jer postavlja temelj za bolje razumijevanje VXLAN tehnologije pošto ona proširuje osnovne koncepte VLAN-a za veće i složenije mrežne okoline.

U drugom segmentu rada fokusirat ćemo se na različite tipove komunikacija između dva ili više virtualna stroja unutar VXLAN mreže. Detaljno ćemo opisati kako VXLAN omogućuje komunikaciju između VM-ova smještenih na različitim fizičkim lokacijama unutar podatkovnog centra ili čak između različitih podatkovnih centara. Analizirat ćemo postupak enkapsulacije i dekapsulacije paketa te kako VXLAN header pomaže u usmjeravanju paketa prema odgovarajućem odredištu. Ovaj će dio također uključivati primjere i dijagrame za bolju vizualizaciju procesa.

U trećem segmentu analizirat ćemo VXLAN format okvira. Proučit ćemo strukturu VXLAN header-a, uključujući polja kao što su VXLAN identifikator mreže(VNI), zastavice i ostale bitne komponente. Objasnit ćemo svrhu svakog polja te kako zajedno doprinose funkcionalnosti VXLAN-a. Ovaj dio rada bit će tehnički detaljan, s primjerima okvira koji ilustriraju kako izgleda paket unutar VXLAN mreže.

Četvrti segment bavit će se različitim scenarijima implementacije VXLAN-a. Ovdje ćemo istražiti kako se VXLAN može integrirati u postojeće mrežne infrastrukture, uključujući podatkovne centre. Razmotrit ćemo različite topologije te pružiti smjernice za implementaciju u stvarnim mrežnim okruženjima.

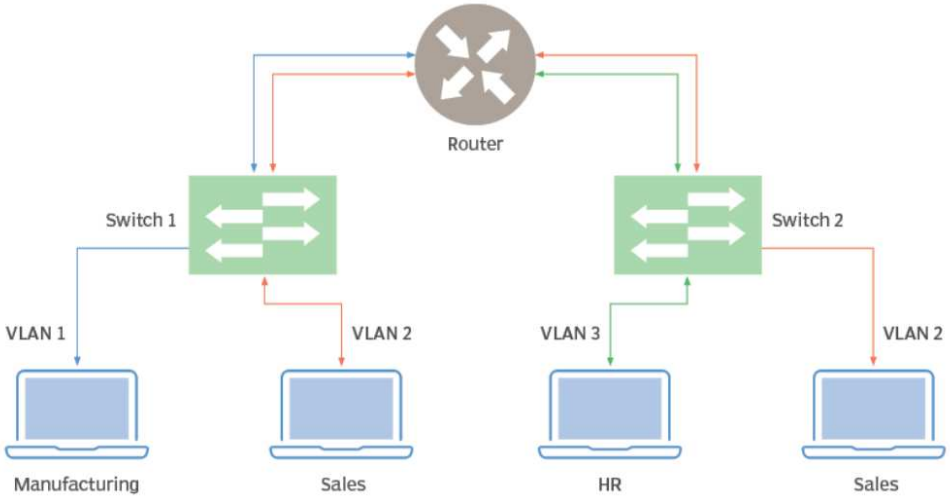
Konačni segment rada posvećen je sigurnosnim aspektima VXLAN-a. Rad će analizirati potencijalne sigurnosne prijetnje i ranjivosti koje mogu nastati prilikom korištenja VXLAN tehnologije te kako ih mitigirati. Također će se razmotriti sigurnosni protokoli i najbolje prakse koje se preporučuju za zaštitu mrežnih okruženja koja koriste VXLAN.

2. VXLAN

Kako bismo mogli objasniti pojam VXLAN-a, bitno je imati osnovno poznavanje VLAN-a.

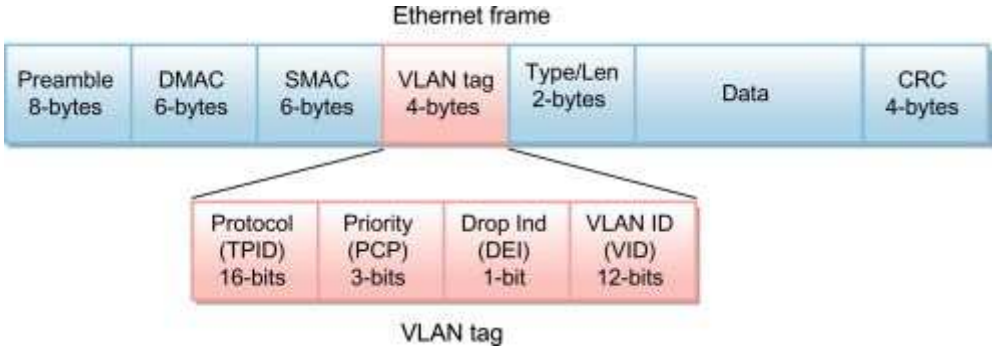
2.1. Osnovno o VLAN-u i uvod u VXLAN

Virtualna lokalna mreža je logički nadređena mreža koja grupira neki podskup uređaja ili korisnika na određenom LAN-u. Glavna svrha VLAN-a je izoliranje prometa za svaku grupu uređaja. Ta karakteristika značajno poboljšava performanse mreže, povećava sigurnost te olakšava administraciju. Neki VLAN-ovi imaju jednostavne uloge poput odvajanja koja računala mogu koristiti printere na nekoj mreži, dok neki obavljaju puno kompleksnije zadaće. Na donjoj slici (**Error! Reference source not found.**) možemo vidjeti primjer jednog VLAN-a [2].



Slika 1. – Primjer VLAN-a [2]

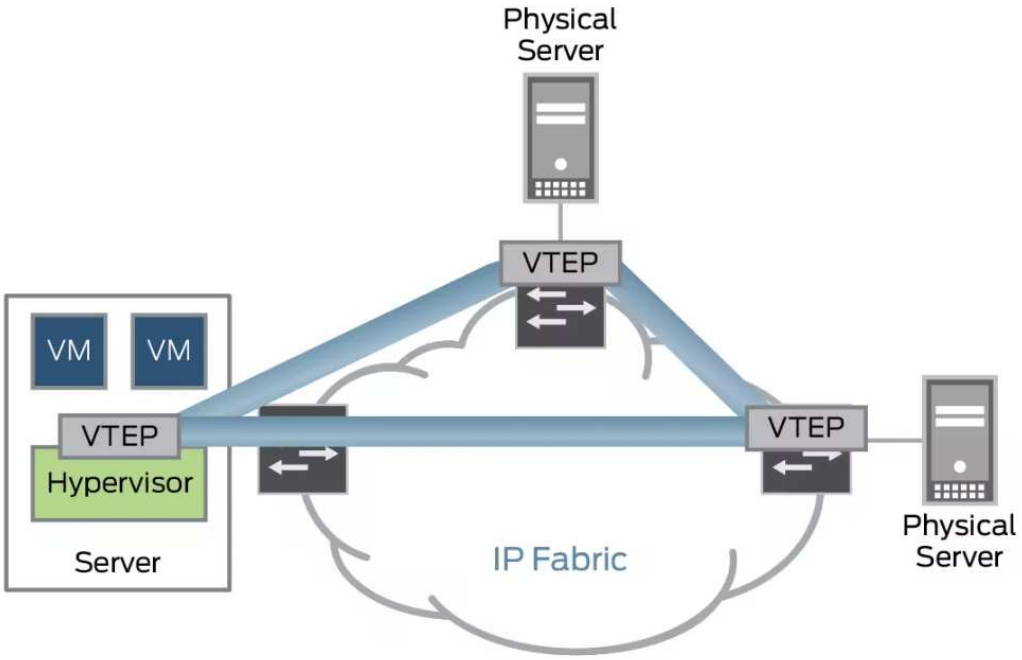
Na mrežnim komutatorima VLAN se identificira s pomoću VLAN ID-a. On se prevodi u VLAN oznaku, 12-bitno polje u zaglavlju svakog ethernet okvira poslanog na neku VLAN mrežu (Slika 2. – Ethernet okvir). Tu oznaku dodjeljuje komutator te prosljeđuje okvir prema odredišnoj MAC adresi i to samo na priključke s kojima je VLAN povezan. Kada okvir dosegne odredišni priključak komutatora, VLAN oznaka se uklanja prije nego što se okvir prenese na odredišni uređaj [2].



Slika 2. – Ethernet okvir [5]

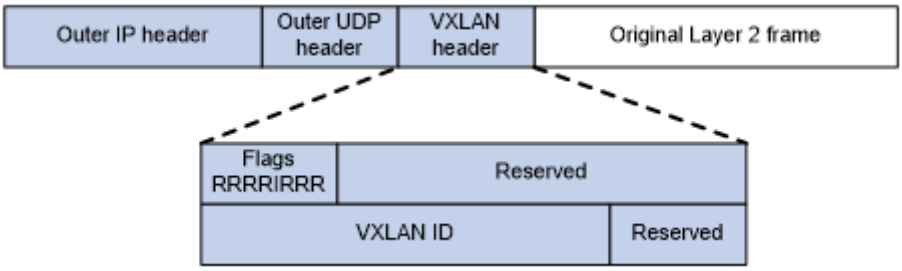
Virtualizacija servera postavila je sve veće zahtjeve na fizičku mrežnu infrastrukturu. Poslužitelj sada ima više virtualnih strojeva (*eng.* Virtual machine), svaki s vlastitom MAC adresom. U slučaju kada se virtualni strojevi u podatkovnom centru grupiraju prema njihovom VLAN-u, moglo bi biti potrebno na tisuće VLAN-ova kako bi se mrežni promet podijelio na odgovarajuće particije kojoj VM može pripadati. Trenutni limit od 4094 VLAN-ova, koji nastaje zbog prethodno spomenutog 12-bitnog adresiranja, nije dovoljan u takvim situacijama. Također, čim paket koji sadrži VLAN oznaku stigne do usmjerivača, sva ta VLAN informacija se uklanja. To znači da VLAN paketi putuju samo do kuda osnovna mreža drugog sloja može doseći. Ova činjenica sprječava skaliranje drugog sloja mreže preko različitih lokacija podatkovnog centra što onemogućuje učinkovitu alokaciju računalnih, mrežnih te pohranjivačkih resursa [3].

Rješenje za opisane probleme u potpoglavlju 2.1 ponudio je VXLAN. Virtualna proširena lokalna mreža jedan je od standarda za virtualizaciju mreže koji je nastao od organizacije IETF 2014. godine. Omogućuje jednoj fizičkoj mreži da se dijeli među više različitih organizacija ili zakupnika, bez da bilo koji zakupnik može vidjeti promet mreže bilo kojeg drugog. Za razliku od VLAN-a koji ima limit segmentacije od 4094, VXLAN s pomoću svojeg VNI-a koji koristi 24 bita može adresirati približno 16 milijuna unikatnih VXLAN segmenata. Bitan pojam koji treba uvesti kada pričamo o VXLAN-ovima je VTEP, odnosno Virtual Tunnel Endpoint. On služi za preusmjeravanje podataka između podmreža ili same mreže. Dvije najčešće njegove izvedbe su kao neovisni mrežni uređaj, poput fizičkog usmjerivača ili komutatora, ili kao virtualnog komutatora implementiranog na serveru. Na slici (Slika 3) je prikazan jedan sustav koji koristi VXLAN [4].



Slika 3. – Primjer VXLAN okruženja [4]

Međutim, VTEP ima i drugu uloga koja obavlja enkapsulaciju i dekapsulaciju originalnog paketa u UDP paket. Zaglavlje tog paketa sadrži IP adresu destinacije te 8 bajtno VXLAN zaglavlje. To zaglavlje se sastoji od: 24 bitnog VNI-a, 8 bitne zastavice kojoj je jedan bit u jedinici te dva polja koja su zajedno veličinom 32 bita i rezervirana za buduće potrebe. Na donjoj slici (Slika 4) prikazan je izgled ovog zaglavlja [4].



Slika 4. – VXLAN zaglavlje [6]

Budući da su VXLAN-ovi enkapsulirani unutar UDP paketa, mogu se izvoditi na bilo kojoj mreži koja može prenositi UDP pakete. Fizički raspored i geografska udaljenost između čvorova osnovne mreže nisu bitni, sve dok se UDP datagrami prosljeđuju od enkapsulirajućeg VTEP-a do dekapsulirajućeg VTEP-a. U idućim cjelinama, cijeli taj proces bit će detaljno razrađen.**Error! Reference source not found.**

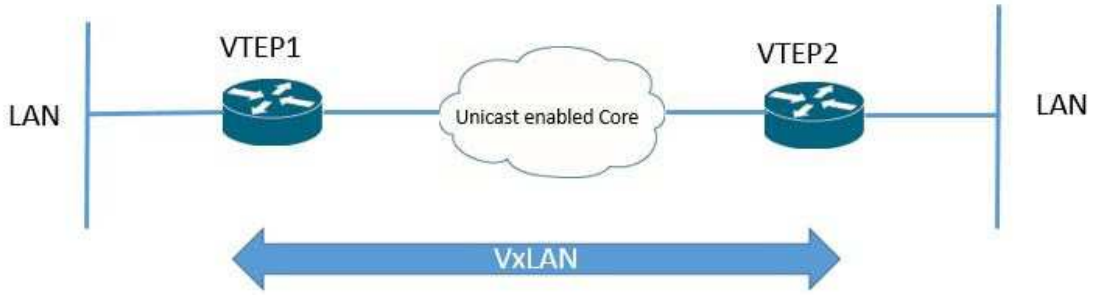
U sljedećim poglavljima raspravlja se o tipičnim scenarijima prijenosa prometa u VXLAN okruženju koristeći jedan tip kontrolne sheme - učenje putem podatkovne ravnine. To je proces u kojem mrežna oprema, poput komutatora ili usmjerivača, automatski uči o povezanostima između adresa na mreži. U kontekstu VXLAN-a, to znači da komutatori i usmjerivači uče o tome koji VM-ovi koriste koje MAC adrese i na kojim VTEP IP adresama se ti VM-ovi nalaze. Ovo učenje se događa na samoj mrežnoj opremi što omogućava efikasno preusmjeravanje prometa između VM-ova unutar VXLAN mreže.

2.2. Jednoodredišna VM-VM komunikacija

Razmotrimo VM koji se nalazi unutar VXLAN podmreže, te nije svjestan da se u njoj nalazi. Kako bi taj VM mogao komunicirati s nekim drugim VM-om koji se nalazi na drugom poslužitelju, on šalje MAC okvir namijenjen cilju odnosno tom drugom VM-u. Nakon toga, VTEP koji se nalazi na fizičkom poslužitelju pretražuje VNI-ove s kojim je taj VM povezan, te određuje je li odredišna MAC adresa na istom segmentu i postoji li mapa te adrese na nekom udaljenom VTEP-u.

Ako je neki od uvjeta ispunjen, na originalni okvir se dodaje vanjsko zaglavlje (Slika 4) koje se sastoji od IP zaglavlja, UDP zaglavlja te VXLAN zaglavlja. Tako enkapsulirani paket prosljeđuje se prema udaljenom VTEP-u. Prilikom primanja tog paketa, udaljeni VTEP provjerava valjanost VNI-a te postoji li VM na toj mreži koji koristi taj VNI koji je asociran s MAC adresom koja odgovara unutrašnjoj MAC adresi pristiglog paketa. Ako takav VM postoji, sva zaglavlja koja su enkapsulirala početni okvir se uklanjaju te se on prosljeđuje odgovarajućem odredištu. To znači da VM koji je primio paket ne saznaje o VNI-u ili da je okvir prenesen s pomoću VXLAN-a.

Osim što prosljeđuje paket odredišnom VM-u, udaljeni VTEP mapira unutarnju izvornu MAC adresu na vanjsku izvornu IP adresu. Ta informacija se pohranjuje u tablicu tako da kada odredišni VM pošalje svoj odgovor, nema potrebe za poplavljivanjem [1].



Slika 5. – Jednoodredišna komunikacija [7]

2.3. Komunikacija razašiljanjem

Razmotrimo VM koji pokušava komunicirati s drugim VM-om. Ako pretpostavimo da se nalaze na istoj podmreži, znamo da će izvorišni VM razašiljati ARP okvir. U okruženju bez VXLAN-a, taj okvir bi se razašiljao s pomoću MAC adresa preko svih komutatora.

S VXLAN-om, zaglavlje koje sadrži VNI se dodaje na početak tog paketa zajedno sa IP zaglavljem i UDP zaglavljem. Međutim, taj paket se šalje jedino IP grupi na kojoj je ta VXLAN podmreža realizirana.

Kako bi to bilo omogućeno, moramo imati poveznicu između VNI-a i IP grupe kojoj šaljemo taj paket. To mapiranje se izvodi na upravljačkom sloju i ono je dostupno svakom VTEP-u kroz upravljački kanal. S pomoću njega svaki VTEP može pružiti IGMP izvještaje o članstvu prema uzvodnom komutatoru ili usmjerivaču kako bi se pridružio ili napustio IP grupu povezanu s nekim VXLAN-om. Nadalje, korištenjem protokola usmjeravanja može se dodatno povećati učinkovitost stabla razašiljanja.

Odredišni VM šalje standardni ARP odgovor s pomoću jednoodredišne komunikacije. Taj okvir bit će enkapsuliran i vraćen izvornom VTEP-u [1].

2.4. Zahtjevi fizičke infrastrukture

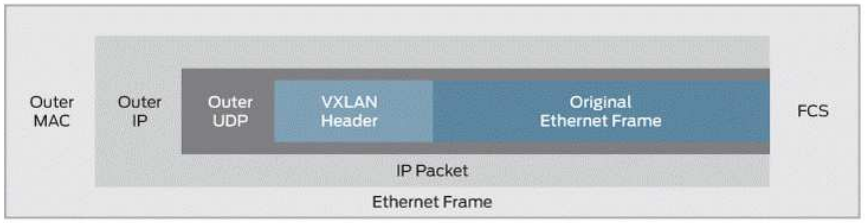
Kada se unutar mrežne infrastrukture koristi IP razašiljanje, onda komutatori i usmjerivači unutar mreže koriste protokol za usmjerivanje poput PIM-a. To omogućuje efikasnu izgradnju stabla razašiljanja kako bi poslani okviri stigli do svog odredišta.

Isto tako, nema potrebe da mreža koja spaja izvorišni i odredišni VM bude L3. VXLAN može raditi i na L2 mrežama. U svakom slučaju, učinkovita replikacija unutar L2 mreže može se postići korištenjem IGMP-a [1].

VTEP-ovi ne smiju fragmentirati VXLAN pakete, ali posrednički usmjerivači ponekad mogu fragmentirati enkapsulirane VXLAN pakete zbog većeg okvira. U tom slučaju odredišni VTEP će odbaciti takve pakete. Kako bi se osigurao prijenos paketa bez fragmentacije, preporučeno je da se MTU (Maximum Transmission Units) preko cijele mrežne infrastrukture postavi na vrijednost koja može podnijeti povećanu veličinu okvira koja je uzrokovana enkapsulacijom.

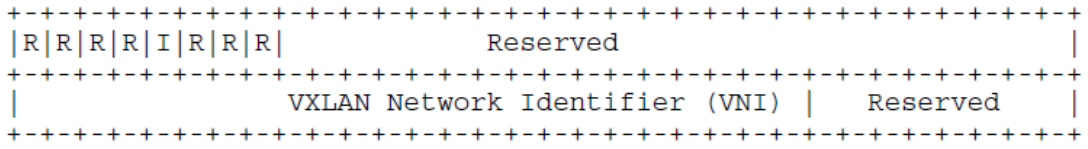
2.5. VXLAN format okvira

Format okvira VXLAN-a bit će prikazan u nastavku. Njegovo razlaganje počinje s dna gdje se nalazi unutarnji MAC okvir sa svojim ethernet zaglavljem koje sadrži izvorne i odredišne MAC adrese, zajedno s poljem koje označava tip. Taj MAC okvir je redom enkapsuliran s VXLAN zaglavljem, vanjskim UDP zaglavljem, vanjskim IP zaglavljem te vanjskim ethernet zaglavljem.



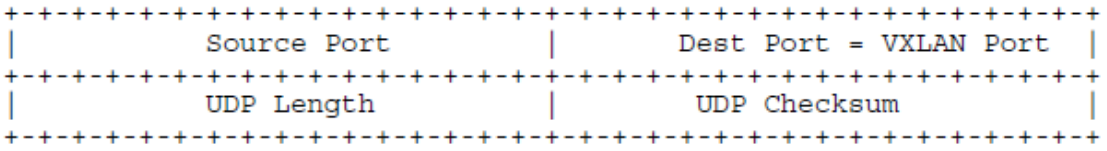
Slika 6. – VXLAN format okvira [8]

VXLAN zaglavlje je polje od 8 bajtova, a ono nam pruža sljedeće informacije. U njemu se prvo nalazi zastavica od 8 bitova gdje I zastavica mora biti postavljena na 1 za valjanu VXLAN mrežnu identifikaciju (VNI). Ostalih 7 bitova označenih kao R su rezervirana polja i moraju biti postavljena na 0 prilikom prijenosa te se ignoriraju prilikom primanja okvira. Nakon zastavice slijedi identifikator VXLAN segmenta (VNI). To je vrijednost od 24 bita koja se koristi za označavanje pojedinačne VXLAN podmreže na kojoj VM-ovi komuniciraju. VM-ovi koji se nalaze na različitim VXLAN podmrežama ne mogu međusobno komunicirati. Zatim slijede dva rezervirana polja, jedno od 24 bita, a drugo od 8 bitova, koja također moraju biti postavljena na 0 tijekom prijenosa te ignorirana tijekom primanja [1].



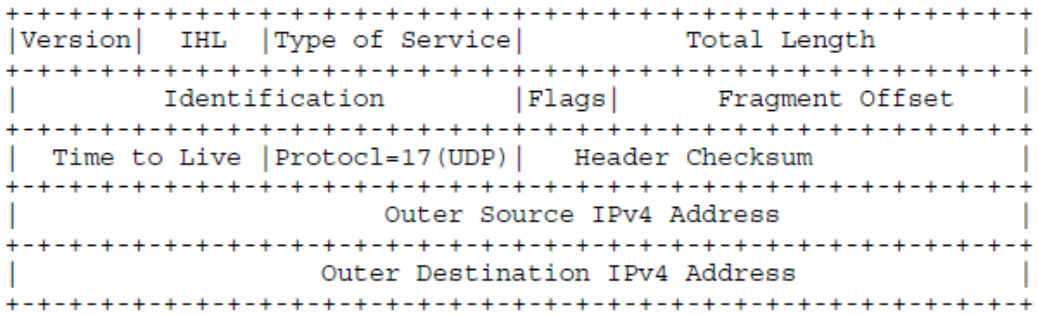
Slika 7. – VXLAN zaglavlje [1]

Sljedeće na redu je vanjsko UDP zaglavlje. Ono se sastoji od izvorišnog porta, odredišnog porta, UDP kontrolne sume te polja koje označava duljinu UDP-a. Izvorišni port je dobavljen od strane VTEP-a, a odredišni port je poznati UDP port. Odredišnom portu je IANA dodijelila vrijednost 4789 za VXLAN UDP priključak te se ta vrijednost koristi kao zadana vrijednost. Neke ranije implementacije VXLAN-a koristile su druge vrijednosti za odredišni priključak. Kako bi se omogućila interoperabilnost s tim implementacijama, odredišni port bi se trebao konfigurirati. Kod vrijednosti izvorišnog porta malo je drukčija situacija. Za njeno računanje preporučuje se korištenje neke hash funkcije na temelju podataka iz unutarnjeg paketa npr. unutarnjeg zaglavlja ethernet okvira. Ovo je kako bi se omogućila razina entropije koja služi za balansiranje opterećenja prometa unutar VXLAN podmreže. Preporučeno je da njena vrijednost bude u rasponu 49152-65535. Zadnje polje kod UDP zaglavlja je UDP kontrolna suma. Kada se paket primi s UDP kontrolnom sumom 0, on mora biti prihvaćen za dekapsulaciju. Ako paket uključuje UDP kontrolnu sumu različitu od nule, ona mora biti ispravno izračunata na temelju IP zaglavlja, UDP zaglavlja, VXLAN zaglavlja te enkapsuliranog MAC okvira. Kada krajnja točka dekapsulacije primi paket s kontrolnom sumom različitom od 0, ona provjerava vrijednost kontrolne sume. Ako provjera ne uspije, paket će biti odbačen. Svi paketi kojima je kontrolna suma jednaka 0 se automatski prihvaćaju [1].



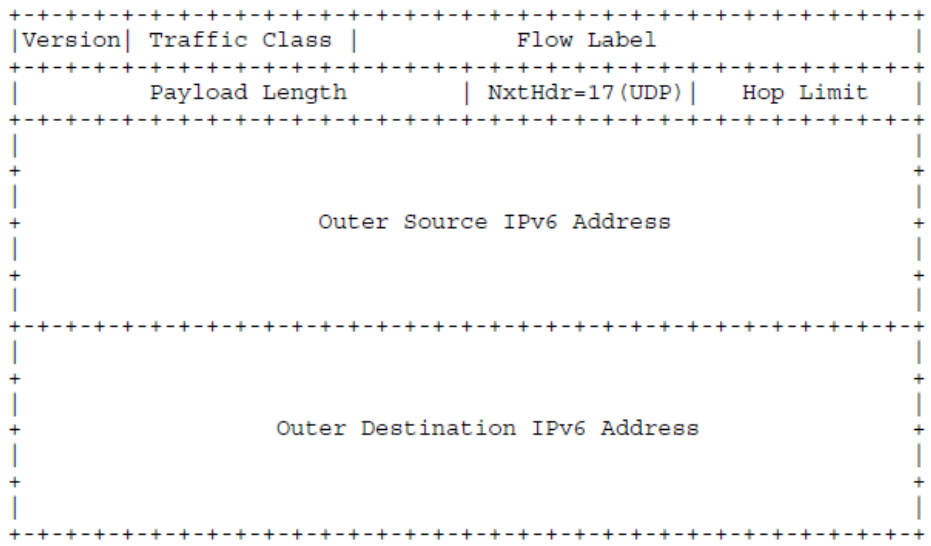
Slika 8. – Vanjsko UDP zaglavlje [1]

Vanjsko IP zaglavlje sastoji se od ukupno 12 polja. Izvorišna IP adresa predstavlja IP adresu VTEP-a preko kojega neki VM komunicira. Odredišna adresa može biti jednoodredišna ili višeodredišna. Kada je odredišna adresa jednoodredišna ona predstavlja IP adresu VTEP-a na koje se spaja VM s kojim naš izvor pokušava komunicirati. Na donjoj slici (Slika 9) prikazan je detaljan izgled vanjskog IP zaglavlja.



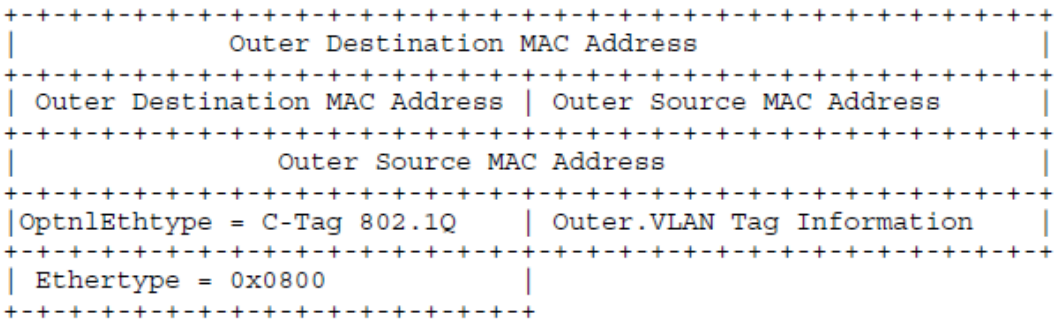
Slika 9. – Vanjsko IPv4 zaglavlje [1]

Kada se umjesto IPv4 koristi IPv6 onda je izgled tog zaglavlja malo drugačiji. Ostala zaglavlja ostaju ista neovisno koja verzija se koristi.



Slika 10. – Vanjsko IPv6 zaglavlje [1]

Kod vanjskog ethernet zaglavlja odredišna MAC adresa može predstavljati adresu ciljanog VTEP-a ili posrednog usmjerivača trećeg sloja. Vanjska VLAN oznaka je opcionalna. Ako je prisutna može se koristiti za razgraničavanje VXLAN prometa na LAN-u [1].

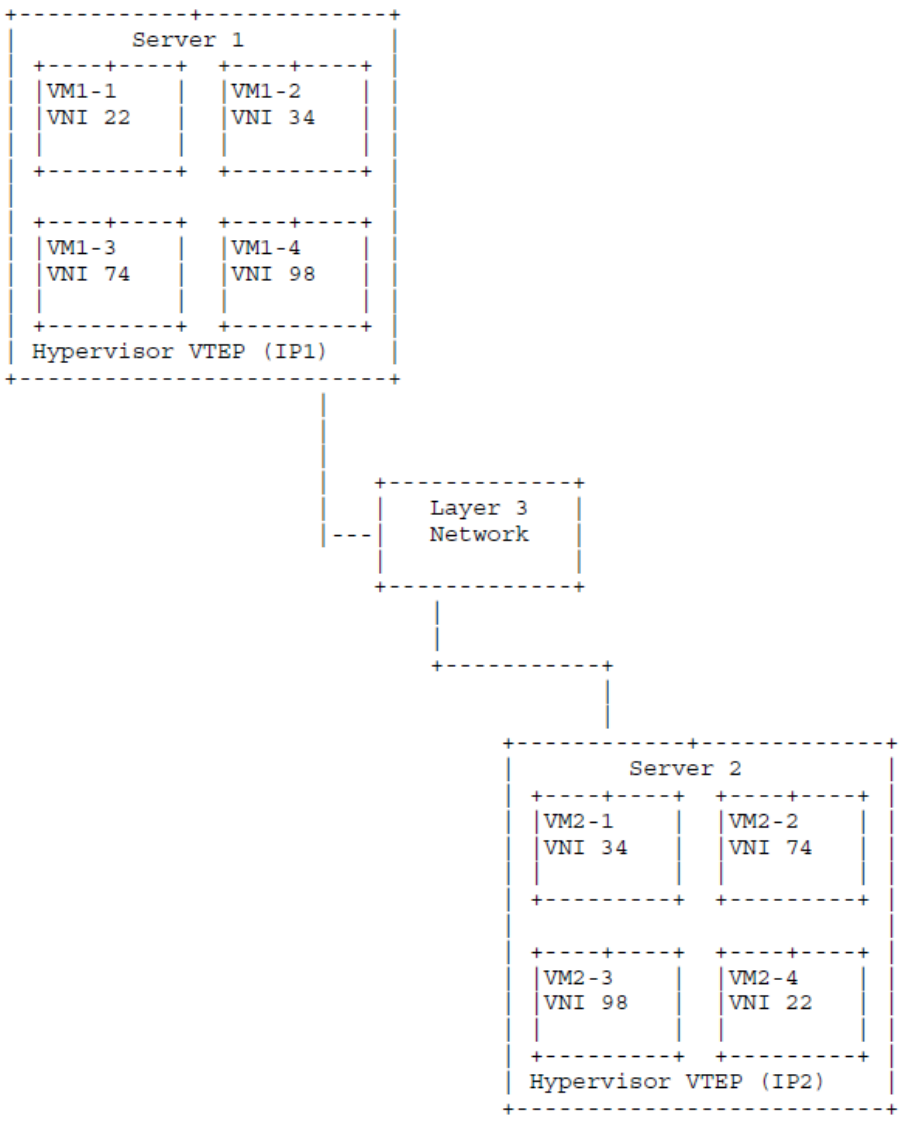


Slika 11. – Vanjsko ethernet zaglavlje [1]

2.6. Scenariji implementacije VXLAN-a

VXLAN se obično implementira u podatkovnim centrima na virtualiziranim poslužiteljima koji mogu biti raspoređeni preko više serverskih ormara. Individualni serverski ormari mogu biti dijelovi različitih L3 mreža ili mogu biti u jednoj L2 mreži. VXLAN mreže preklapaju se preko ovih L2 ili L3 mreža.

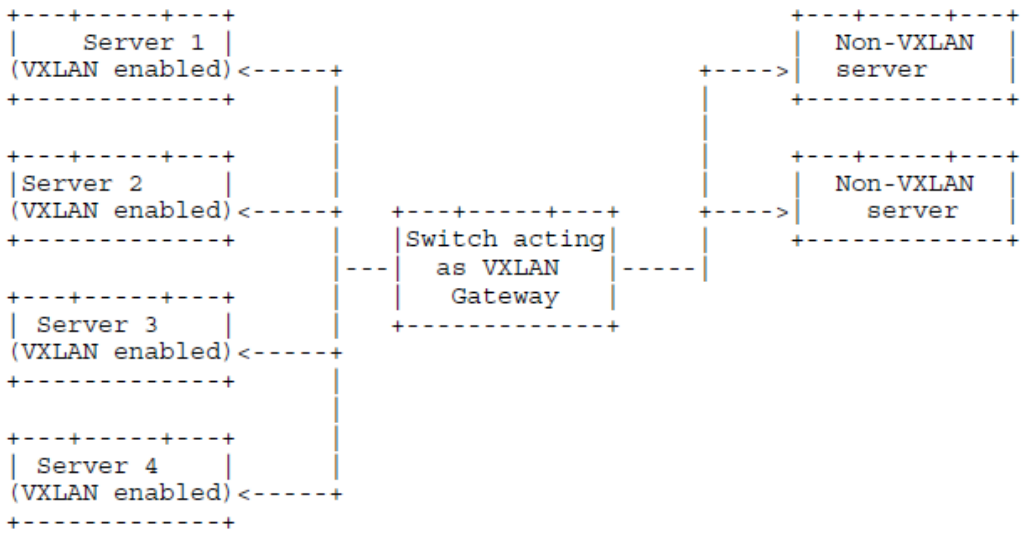
Razmotrimo donju sliku (Slika 12) koja prikazuje dva virtualizirana poslužitelja povezana s L3 infrastrukturom. Poslužitelji mogu biti u istom serverskom ormaru, na različitim serverskim ormarima ili potencijalno u različitim podatkovnim centrima unutar iste administrativne domene. Postoje četiri VXLAN podmreže identificirane VNI-ovima 22, 34, 74 i 98. Razmotrimo slučaj VM1-1 na poslužitelju 1 i VM2-4 na poslužitelju 2, koji su u istoj VXLAN podmreži identificiranoj s VNI-em 22. VM-ovi ne znaju o podmreži i načinu prijenosa budući da se enkapsulacija i dekapsulacija događaju transparentno na VTEP-ovima na poslužiteljima 1 i 2. Ostale podmreže i odgovarajući VM-ovi su: VM1-2 na poslužitelju 1 i VM2-1 na poslužitelju 2 s VNI-em 34, VM1-3 na poslužitelju 1 i VM2-2 na poslužitelju 2 s VNI-em 74 i naposljetku VM1-4 na poslužitelju 1 i VM2-3 na poslužitelju 2 s VNI-em 98 [1].



Slika 12. – VTEP-ovi preko L3 mreže [1]

Alternativni scenarij je kada čvorovi na VXLAN podmreži trebaju komunicirati s čvorovima na mrežama koje mogu biti temeljene na VLAN-u. Ti čvorovi mogu biti fizički čvorovi ili virtualni strojevi. Da bi se omogućila ta komunikacija, mreža može sadržavati VXLAN pristupnik koji prosljeđuju promet između VXLAN i ne-VXLAN okruženja.

Razmotrimo donju sliku za sljedeću raspravu. Za dolazne okvire na VXLAN povezanom sučelju, pristupnik uklanja VXLAN zaglavlje i prosljeđuje ga na fizički priključak na temelju odredišne MAC adrese unutarnjeg ethernet okvira. Dekapsulirani okviri s unutarnjim VLAN ID-om trebali li biti odbačeni osim ako nije eksplicitno konfigurirano da se prosljeđuju na ne-VXLAN sučelje. U suprotnom smjeru, dolazni okviri s ne-VXLAN sučelja mapiraju se na određenu VXLAN podmrežu na temelju VLAN ID-a u okviru. Osim ako nije eksplicitno konfigurirano, ovaj VLAN ID se uklanja prije nego što se okvir enkapsulira za VXLAN [1].



Slika 13. – Komunikacija VXLAN – VLAN [1]

2.7. Sigurnosni aspekti

Tradicionalno, L2 mreže mogu biti napadnute samo "iznutra" putem zlonamjernih krajnjih točaka. Neki od najčešćih načina su putem neovlaštenog pristupa LAN-u i prisluškivanjem prometa, ubacivanjem krivotvorenih paketa radi "preuzimanja" druge MAC adrese ili putem poplavljivanja i uzrokovanja uskraćivanja usluge. Ti napadi mogu se ublažiti ograničavanjem upravljačkog i administrativnog opsega tko implementira i upravlja VM-ovima te VXLAN pristupnicima u VXLAN okruženju.

Promet tuneliran preko IP mreže može se osigurati tradicionalnim sigurnosnim mehanizmima poput IPsec-a koji autenticiraju i po potrebi šifriraju VXLAN promet. Naravno, ovo će zahtijevati povezivanje s infrastrukturom za autentifikaciju kako bi ovlaštene krajnje točke dobile i distribuirale vjerodajnice.

VXLAN podmreže označavaju se i operiraju preko postojeće LAN infrastrukture. Kako bi se osiguralo da su VXLAN krajnje točke i njihovi VTEP-ovi ovlašteni na LAN-u, preporučuje se da se odredi VLAN za VXLAN promet te da poslužitelji i VTEP-ovi šalju VXLAN promet preko tog VLAN-a kako bi pružili dodatnu mjeru sigurnosti [1].

Sažetak

Virtualna proširena lokalna mreža (*eng.* Virtual Extensible Local Area Network, *skr.* VXLAN) je tehnologija koja značajno poboljšava skalabilnost i fleksibilnost mreža, posebno u kontekstu modernih podatkovnih centara. Dizajnirana je kako bi prevladala ograničenja tradicionalnih VLAN-ova, omogućujući proširenje mreže izvan granica fizičkih infrastruktura.

VXLAN je standardiziran od strane organizacije IETF 2014. godine te omogućuje kreiranje do 16 milijuna jedinstvenih segmenata zahvaljujući 24-bitnom VXLAN mrežnom identifikatoru (VNI). Ključna komponenta VXLAN-a je krajnja točka virtualnog tunela (VTEP), koji preusmjerava podatke između podmreža i obavlja enkapsulaciju i dekapsulaciju paketa unutar UDP paketa. Ovo omogućava VXLAN-u da radi preko bilo koje mreže koja podržava prijenos UDP paketa, bez obzira na fizički raspored čvorova.

Unutar VXLAN mreže, komunikacija između VM-ova može biti jednoodredišna ili razašiljanje. U jednoodredišnoj komunikaciji, VTEP enkapsulira originalni paket i prosljeđuje ga odgovarajućem udaljenom VTEP-u, koji zatim dekapsulira paket i prosljeđuje ga ciljanom VM-u. Kod komunikacije razašiljanjem, paket se šalje IP grupi povezanoj s VXLAN podmrežom, a VTEP-ovi koriste IGMP izvještaje za pridruživanje ili napuštanje te IP grupe.

VXLAN može raditi na L2 i L3 mrežama. VTEP-ovi ne smiju fragmentirati VXLAN pakete, ali usmjerivači mogu fragmentirati enkapsulirane pakete zbog povećane veličine okvira. Iz tog razloga preporučeno je postaviti MTU (*eng.* Maximum transmission unit) na cijeloj mrežnoj infrastrukturi na vrijednost koja može podnijeti povećanu veličinu okvira.

Format VXLAN okvira uključuje unutarnji MAC okvir, VXLAN zaglavlje, vanjsko UDP zaglavlje, vanjsko IP zaglavlje i vanjsko ethernet zaglavlje. VXLAN zaglavlje sadrži informacije o VNI-u i zastavici, dok vanjsko UDP zaglavlje koristi odredišni port 4789. Vanjsko IP zaglavlje može biti IPv4 ili IPv6, a vanjsko Ethernet zaglavlje može uključivati opcionalnu VLAN oznaku.

VXLAN se često implementira u virtualiziranim podatkovnim centrima koji se prostiru preko više serverskih ormara i mrežnih segmenata. Alternativno, VXLAN se može integrirati s VLAN okruženjima s pomoću VXLAN pristupnika, koji omogućuju komunikaciju između VXLAN i ne-VXLAN mreža.

Sigurnost u VXLAN okruženju može se poboljšati korištenjem IPsec-a za autentifikaciju i šifriranje prometa. VXLAN promet se može odvojiti na poseban VLAN za dodatnu sigurnost. Također, kontrola pristupa i administracije VM-ova i VTEP-ova ključna je za zaštitu od zlonamjernih aktivnosti unutar mreže.

Summary

Virtual extensible local area network (VXLAN) is a technology that significantly improves the scalability and flexibility of networks, especially in the context of modern data centers. It is designed to overcome the limitations of traditional VLANs, enabling network expansion beyond the boundaries of physical infrastructures.

VXLAN was standardized by the IETF organization in 2014 and allows the creation of up to 16 million unique segments thanks to the 24-bit VXLAN network identifier (VNI). A key component of VXLAN is the virtual tunnel endpoint (VTEP), which routes data between subnets and performs packet encapsulation and decapsulation within UDP packets. This allows VXLAN to work over any network that supports UDP packet transmission, regardless of the physical layout of the nodes.

Within a VXLAN network, communication between VMs can be unicast or broadcast. In unicast communication, the VTEP encapsulates the original packet and forwards it to the corresponding remote VTEP, which then decapsulates the packet and forwards it to the target VM. In broadcast communication, a packet is sent to an IP group associated with a VXLAN subnet, and VTEPs use IGMP reports to join or leave that IP group.

VXLAN can work on L2 and L3 networks. VTEPs must not fragment VXLAN packets, but routers can fragment encapsulated packets due to the increased frame size. For this reason, it is recommended to set the MTU (Maximum transmission unit) on the entire network infrastructure to a value that can handle the increased frame size.

The VXLAN frame format includes an inner MAC frame, a VXLAN header, an outer UDP header, an outer IP header, and an outer ethernet header. The VXLAN header contains VNI and flag information, while the outer UDP header uses destination port 4789. The outer IP header can be IPv4 or IPv6, and the outer Ethernet header can include an optional VLAN tag.

VXLAN is often implemented in virtualized data centers that span multiple server racks and network segments. Alternatively, VXLAN can be integrated with VLAN environments using VXLAN gateways, which allow communication between VXLAN and non-VXLAN networks.

Security in a VXLAN environment can be improved by using IPsec to authenticate and encrypt traffic. VXLAN traffic can be separated on a separate VLAN for added security. Also, controlling access and administration of VMs and VTEPs is essential to protect against malicious activity within the network.

Zaključak

Virtualna proširena lokalna mreža (VXLAN) predstavlja revolucionarni korak naprijed u modernim mrežnim arhitekturama, posebno u kontekstu proširivanja podatkovnih centara i unaprjeđenja skalabilnosti mreža. VXLAN je razvijen kako bi prevladao ograničenja tradicionalnih virtualnih lokalnih mreža (VLAN) i omogućio veću fleksibilnost te skalabilnost. VLAN-ovi omogućuju segmentaciju mreže, što poboljšava sigurnost i optimizira mrežne resurse, no njihov limit od 4094 VLAN-ova predstavlja značajno ograničenje u današnjim velikim podatkovnim centrima. VXLAN proširuje taj limit koristeći 24-bitni identifikator VXLAN mreže (VNI), što omogućuje adresiranje do 16 milijuna unikatnih VXLAN segmenata, čime se učinkovito rješava problem skalabilnosti. Jedan od ključnih elemenata VXLAN-a je Virtual Tunnel Endpoint (VTEP), koji služi za enkapsulaciju i dekapsulaciju originalnih paketa unutar UDP paketa. VTEP-ovi omogućuju preusmjeravanje podataka između podmreža ili različitih mreža, bez obzira na njihovu fizičku lokaciju. Ova funkcionalnost omogućuje VM-ovima da komuniciraju kao da su na istoj fizičkoj mreži, što je od iznimne važnosti za moderne podatkovne centre. Tehnički detalji VXLAN formata okvira pružaju duboko razumijevanje načina na koji se podaci enkapsuliraju i dekapsuliraju. VXLAN zaglavlje sadrži ključne informacije kao što su VNI, zastavice i rezervirana polja, dok vanjska zaglavlja (UDP, IP, Ethernet) omogućuju prijenos podataka kroz različite mrežne infrastrukture. Implementacijski scenariji VXLAN-a demonstriraju kako se ova tehnologija može integrirati u postojeće mrežne infrastrukture, uključujući podatkovne centre. Primjeri uključuju komunikaciju između VM-ova smještenih na različitim poslužiteljima i podatkovnim centrima, kao i integraciju VXLAN-a s tradicionalnim VLAN-ovima putem VXLAN pristupnika. Ovi scenariji pokazuju fleksibilnost i prilagodljivost VXLAN-a u različitim mrežnim okruženjima. Sigurnosni aspekti VXLAN-a ističu važnost zaštite mrežnog prometa i sprječavanja potencijalnih sigurnosnih prijetnji. VXLAN omogućuje korištenje tradicionalnih sigurnosnih mehanizama poput IPsec-a za autentifikaciju i enkripciju prometa. Također, preporučuje se segmentacija VXLAN prometa putem VLAN-ova kako bi se dodatno osigurala mrežna infrastruktura. Zaključno, VXLAN predstavlja ključnu tehnologiju za modernizaciju i skalabilnost mrežnih arhitektura u podatkovnim centrima. Njegova sposobnost da prevlada ograničenja VLAN-a i omogući fleksibilno i skalabilno mrežno okruženje čini ga neophodnim alatom u kontekstu računarstva u oblaku i drugih modernih mrežnih usluga. Razumijevanje i implementacija VXLAN-a omogućuje mrežnim inženjerima da efikasno upravljaju rastućim zahtjevima za mrežnim resursima, osiguravajući pritom visoku razinu sigurnosti i performansi.

Literatura

[1] IETF RFC 7348 – Virtual eXtensible Local Area Network (VXLAN), 2014 (available at: https://datatracker.ietf.org/doc/html/rfc7348)

[2] TechTarget – VLAN (virtual LAN), 2022 (available at: https://www.techtarget.com/searchnetworking/definition/virtual-LAN)

[3] TechTarget - VXLAN vs. VLAN: What's the difference?, 2022 (available at: https://www.techtarget.com/searchnetworking/tip/VXLAN-vs-VLAN-Whats-the-difference)

[4] Juniper Networks – What is VXLAN?, 2023 (available at: https://www.juniper.net/us/en/research-topics/what-is-vxlan.html)

[5] ScienceDirect – Virtual Local Area Network Tag, 2014 (available at: https://www.sciencedirect.com/topics/computer-science/virtual-local-area-network-tag)

[6] TechHub - VXLAN packet format, 2018 (available at: https://techhub.hpe.com/eginfolib/networking/docs/switches/5710/5200-5004_vxlan_cg/content/517705090.htm)

[7] Protocoholic - VxLAN Unicast mode Configuration and Verification, 2018 (available at: https://protocoholic.com/2018/05/06/asr1000-vxlan-unicast-mode-configuration-and-verification)

[8] Juniper Networks – Understanding VXLANs, 2023 (available at: https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/topic-map/sdn-vxlan.html)

Skraćenice

VLAN	Virtual Local Area Network
VXLAN	Virtual eXtensible Local Area Network
STP	Spanning Tree Protocol
VTEP	VXLAN Tunnel End Point
VNI	VXLAN Network Identifier
VM	Virtual Machine
ARP	Address Resolution Protocol
UDP	User Datagram Protocol
IP	Internet Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
PIM	Protocol Independent Multicast
L2	Layer 2
L3	Layer 3
IANA	Internet Assigned Numbers Authority