HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Virtualne lokalne računalne mreže (VLAN)

CCERT-PUBDOC-2006-03-153

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. UVOD 4

2. VLAN TEHNOLOGIJA 5

2.1. IEEE 802.1Q PROTOKOL 6
2.2. VRSTE VLAN-OVA 8
2.2.1. VLAN-ovi bazirani na priključcima preklopnika 8
2.2.2. VLAN-ovi bazirani na tipu protokola 9
2.2.3. VLAN-ovi bazirani na MAC adresama 9
2.2.4. Korisnički definirano povezivanje 10
2.2.5. VLAN-ovi bazirani na definiranim pravilima 10
2.3. SPREGA IEEE 802.1Q PROTOKOLA S IEEE 802.1P PROTOKOLOM 10

3. PREDNOSTI I NEDOSTACI VLAN MREŽA 10

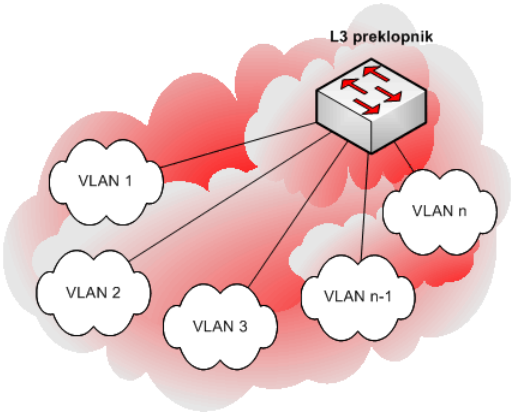
3.1. GLAVNE PREDNOSTI UPOTREBE VLAN-OVA 10
3.1.1. Povećanje performansi mreže 10
3.1.2. Olakšana administracija mreža 11
3.1.3. Neovisnost o fizičkoj topologiji mreža 11
3.1.4. Ograničenje razašiljanja prometa na VLAN-u 11
3.1.5. Zaštita od malicioznih korisnika 11
3.1.6. Povećana sigurnost mreže 11
3.1.7. Prioritiziranje mrežnog prometa 11
3.2. GLAVI NEDOSTACI UPOTREBE VLAN-OVA 12
3.2.1. Komunikacija između VLAN-ova 12
3.2.2. Kompleksnost VLAN-ova 12
3.2.3. Noseći kapacitet usmjerivača 12
3.2.4. Neovlašteno uključivanje u pojedini VLAN 12

4. ZAKLJUČAK 13

5. REFERENCE 13

1. Uvod

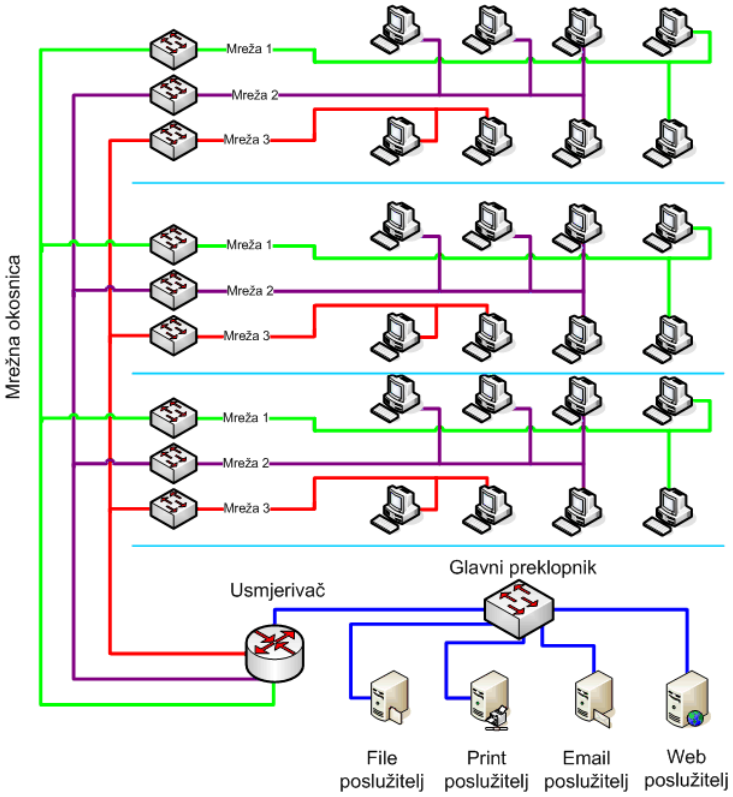
Virtualne lokalne računalne mreže (eng. *Virtual Local Area Networks* -VLANs) su način logičke segmentacije mreže koja se može dinamički mijenjati i nije ovisna o fizičkoj topologiji. Kod segmentiranje mreže na tradicionalni način računala zaposlenika fizički se grupiraju prema opisu radnog mjesta zaposlenika. Grupe računala se međusobno povezuju uz pomoć preklopnika ili koncentratora, a koncentratori i preklopnici se povezuju međusobno uz pomoć usmjerivača. Nasuprot tome, VLAN predstavlja grupu računala koji mogu biti na jednoj ili više odvojenih računalnih mreža, a koje su konfigurirane na takav način koji im omogućava međusobnu komunikaciju kao da se nalaze u istoj fizičkoj mreži iako se zapravo nalaze u više odvojenih računalnih mreža. Povezivanje tih udaljenih računala obavlja se korištenjem posebno konfiguriranih preklopnika.
Ovaj dokument opisuje osnovne principe VLAN tehnologije, IEEE 802.1Q protokol, glavne vrste VLAN-ova, vezu s IEEE 802.1P protokolom te glavne prednosti i nedostatke korištenja VLAN-ova.



Slika 1: VLAN koncepcija

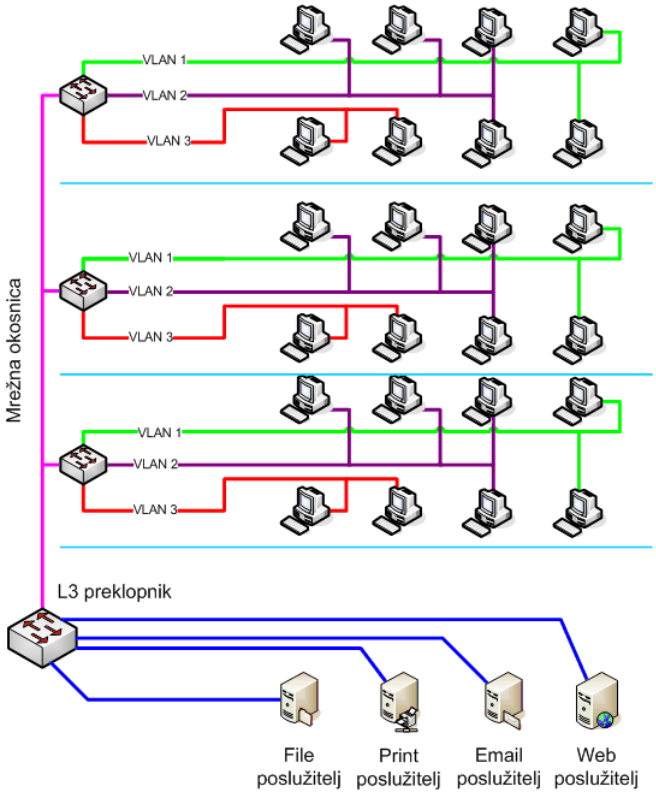
2. VLAN tehnologija

Lokale računalne mreže (eng. *Local Area Networks* – LANs) su prvotno organizirane kao mreže računala locirane fizički na istoj poziciji. Današnji LAN-ovi su definirani kao jedna logička domena razašiljanja (eng. *single broadcast domain*). To znači da ukoliko korisnik razašilje informacije na svom LAN-u, informacije će biti poslane svim računalima na tom LAN-u. Paketi koji su poslani svim računalima u LAN-u neće se proširiti na ostale LAN-ove zahvaljujući preklopnicima (eng. *switch*) koji odvajaju LAN-ove.



Slika 2: Izvedba mrežne arhitekture bez primjene VLAN-ova

Da bi se otklonili negativni učinci razašiljanja velikih količina paketa unutar LAN-ova, u upotrebu je uveden koncept virtualnih LAN-ova. Virtualni LAN-ovi nude metodu segmentiranja fizičke mreže na višestruke domene razašiljanja. VLAN-ovi predstavljaju logičku segmentaciju fizičkih mreža koja se može dinamički mijenjati i nije ovisna o fizičkoj topologiji. Sastoje se od čvorova i računala koji su spojeni u jednu LAN domenu razašiljanja grupiranu po funkciji (npr. računovodstvo, uprava, projekti, gosti, …), koji međusobno komuniciraju bez obzira na fizičku lokaciju korisnika.
Podloga za ostvarivanje VLAN mreža je preklapanje veza i tzv. ravna (eng. *flat*) mrežna arhitektura, u kojoj ne postoji fizička segmentacija mreže već se sve podjele provode logički te se stoga lako mijenjaju prema potrebi.

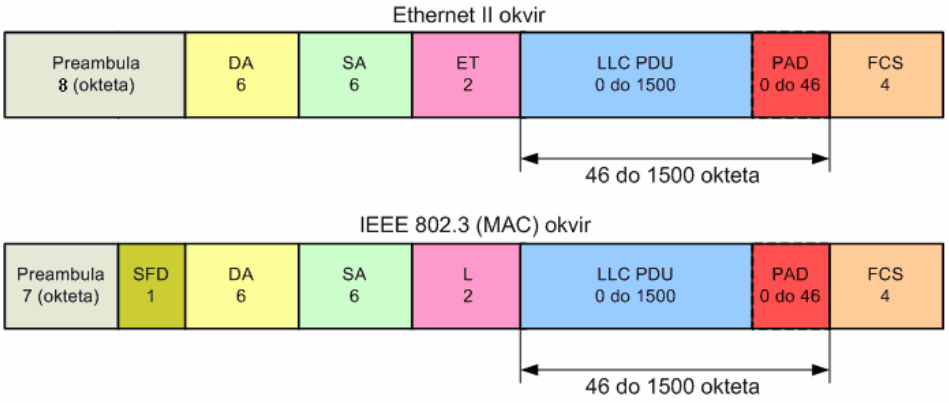


Slika 3: Izvedba mrežne arhitekture primjenom VLAN-ova

2.1. IEEE 802.1Q protokol

Skupina proizvođača mrežne opreme koji su na projektu lokalne mreže bili ujedinjeni pod nazivom DIX (*Digital, Intel and Xerox*) prva je definirala standard *Ethernet*. *Ethernet* je specifikacija lokalne mreže koja koristi pristupnu metodu CSMA/CD (eng. *Carrier Sense Multiple Access with Collision Detection*). DIX je objavio dva standarda, poznata pod nazivom *Ethernet I* i *Ethernet II*, a odbor IEEE 802.3 je nastavio rad koji je DIX započeo. Iako standardi *Ethernet* i IEEE 802.3 nisu identični, danas se u svijetu za obje vrste lokalnih mreža koristi uvriježeni naziv *Ethernet*.

VLAN predstavlja nadogradnju na *Ethernet* i IEEE 802.3 standarde. Temelj za primjenu VLAN-ova predstavlja preporuka IEEE 802.1Q "*Virtual Bridged Local Area Networks*". Unutar preporuke opisano je označavanje okvira (eng. *frame tagging*). Svakom VLAN-u unutar mreže pridodan jedinstveni broj koji ga jednoznačno određuje. Prije slanja na okosnicu preklopnik u zaglavlju paketa postavlja jedinstveni identifikator veličine 4 okteta koji označava VLAN kojemu taj paket pripada. Po primitku paketa, a prije slanja krajnjim uređajima okvir se modificira - dodani identifikator se briše.

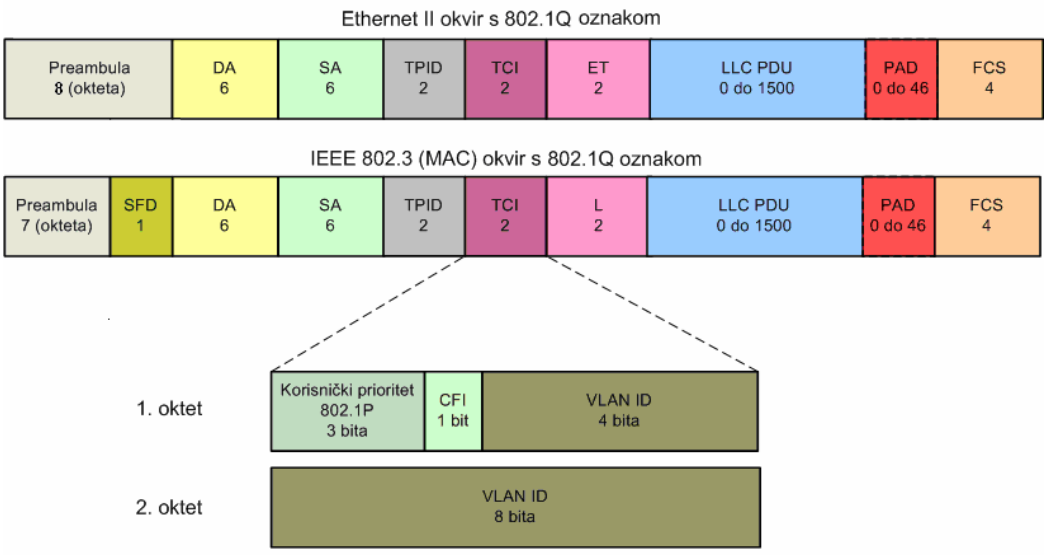


Slika 4: Struktura *Ethernet II* i IEEE 802.3 okvira

Na prethodnoj slici vidljiva je struktura *Ethernet II* i IEEE 802.3 okvira koja se sastoji od sljedećih elemenata:

- Preambula (eng. *preambule*) – sastoji se od sedam okteta kod IEEE 802.3 okvira, tj od osam okteta kod *Ethernet II* okvira. Svaki oktet sadrži isti slijed bita: 10101010. Jedino osmi oktet kod *Ethernet II* okvira sadrži zadnji bit postavljen na 1 – 10101011 kako bi označio kraj sinkronizacijskog dijela. Preambula je namijenjena sinkronizaciji na razini bita. Prijemnik koristi ovaj slijed jedinica i nula kako bi detektirao novi poslani okvir. Na taj se način postiže usklađenost takta između predajnika i prijemnika. Preambula ima značenje samo na fizičkom sloju (pri slanju okvira se kreira na fizičkom sloju, a kod prijema fizički sloj ju ukida).
- Oznaka početka okvira (eng. *Start Frame Delimiter* – SFD) – definiran unutar IEEE 802.3 standarda, a sastoji se od jednog okteta i koristi se samo za određivanje početka okvira (sinkronizacija na razini okvira). Taj oktet jednak je osmom oktetu preambule *Ethernet II* okvira (10101011) te stoga *Ethernet II* i IEEE 802.3 imaju različite nazive, ali isti zapis za prvih osam okteta.
- Polje odredišne adrese (eng. *Destination Address* – DA) - sastoji se od šest okteta i određuje MAC adresu krajnjeg uređaja kojem se dotični okvir šalje.
- Polje izvorišne adrese (eng. *Source Address* – SA) - sastoji se od šest okteta i određuje MAC (*Medium Access Control*) adresu krajnjeg uređaja koji šalje taj okvir.
- Polje IEEE 802.3 standarda L (eng. *Length*) određuje duljinu korisničkog polja (na slici označeno kao LLC PDU). Maksimalna dozvoljena duljina korisničkog polja iznosi 1500 okteta.
- Za razliku od IEEE 802.3 okvira, na mjestu polja L u *Ethernet* II okvirima nalazi se polje ET (eng. *EtherType*). To polje određuje protokol mrežnog sloja čiji se podaci pakiraju u korisničko polje *Ethernet* okvira (npr. prilikom slanja IP datagrama *Ethernet*-om, sadržaj polja ET je x'0800). S obzirom da je osnovna ideja bila da se istim fizičkim LAN-om zajedno mogu prenositi *Ethernet II* i IEEE 802.3 okviri, sadržaj polja ET poprima iznose koji su veći od najveće dozvoljene duljine korisničkog polja. Istovremeno, zbog toga što je trajanje fiksnog vremenskog odsječka jednako trajanju 512 bita, najmanja dozvoljena duljina *Ethernet* paketa iznosi 64 okteta.
- Ako nema dovoljno korisničkih okteta za popunjavanje korisničkog polja, koristi se polje za popunjavanje (eng. *Padding* – PAD). Duljina polja PAD kreće se u rasponu od 0 do 46 okteta.
- Na kraju okvira nalazi se polje nazvano slijed za provjeru ispravnosti okvira (eng. *Frame Check Sequence* – FCS). Sadržaj tog polja kreira se u predajniku pomoću metode cikličkog kodiranja (eng. *Cyclic Redundancy Check* – CRC). U prijemu se istom metodom na MAC podsloju, namijenjenog upravljanju pristupa prijenosnom mediju, na temelju primljenog okvira proračunava slijed od četiri okteta koji se zatim uspoređuje s primljenim FCS-om. Ako je podudarnost potpuna, to je znak da je primljeni okvir ispravan (iako to ne mora biti potpuno točno jer postoji mogućnost da CRC ne otkrije neke višestruke pogreške). Ako otkrije da je neki okvir neispravan, MAC podsloj ga odbacuje. U LAN-ovima se ponovno slanje (retransmisija) okvira primljenih s pogreškom implementira najčešće na višim protokolnim slojevima (npr. na transportnom sloju), a rjeđe na podsloju upravljanja logičkim linkom (eng. *Logical Link Control* – LLC), i to je opcija koju po potrebi odabire korisnik. Dakle, ako transportni sloj ili podsloj LLC u prijemnom entitetu krajnjeg uređaja otkrije da neki okvir nedostaje, tada ravnopravnom protokolnom sloju, odnosno podsloju u predajniku na drugom kraju linka šalje zahtjev za retransmisijom okvira.

IEEE 802.1Q preporuka donosi standardnu metodu označavanja MAC i *Ethernet* okvira s VLAN pripadajućom informacijom o članstvu. U standardni okvir, između SA i L/ET polja, dodaju se 4 okteta kao što je vidljivo na sljedećoj slici.



Slika 5: Struktura *Ethernet II* i IEEE 802.3 okvira s VLAN oznakom

Oznaku VLAN-a čine četiri okteta ugrađena u tradicionalni okvir koji povećavaju maksimalnu duljinu okvira s 1518 na 1522 okteta: polje TPID (eng. *Tag Protocol* ID) i upravljačko polje (eng. *Tag Control Information*), svako duljine dva okteta. U polje TPID upisuje se heksadekadski broj vrijednosti 8100 koji označava da se radio o IEE 802.1Q paketu.. Prva tri bita upravljačkog polja namijenjena su dodjeli prioriteta prometnim tokovima u LAN-u, definiranoj preporukom IEEE 802.1P. Nadalje, ako je bit CFI (eng. *Canonical Format Indicator*) jednak jedinici, moguće je dodatno povećanje duljine MAC okvira za 2 okteta koji slijede odmah iza polja L/ET. Ta dva okteta čine polje E-RIF (eng. *Extra Embeded Routing Information*), koje pokazuje da je okvir promijenjen iz *Token Ring*/FDDI formata u *Ethernet* format. Sama oznaka VLAN-a, duljine 12 bita, omogućuje jednoznačno označavanje virtualnih LAN-ova.
Od 4096 raspoloživih VLAN ID-a (od 0 do 4095), neki su identifikatori rezervirani. ID koji je jednak nuli (tzv. *null* VLAN ID) u označenom okviru signalizira da niti jedan VLAN ID nije pridijeljen nekom VLAN-u. VLAN ID koji je jednak 4095 također je rezerviran za posebne namjene. Dakle, VLAN-ovima je moguće dodijeliti VLAN ID u rasponu od 1 do 4094.
Označavanje okvira ne mijenja sadržaj polja ET, odnosno polja duljine LLC PDU-a. Prilikom svakog dodavanja ili skidanja oznake potrebno je ponovno proračunati vrijednost polja FCS.

2.2. Vrste VLAN-ova

Pridjeljivanje računala odnosno korisnika VLAN-ovima može se izvesti na nekoliko načina koji su opisani u nastavku ovog poglavlja.

2.2.1. VLAN-ovi bazirani na priključcima preklopnika

VLAN-ovi bazirani na priključcima preklopnika (eng. *port based*), tzv. statički ili *Layer* 1 VLAN-ovi, obično se koriste u organizacijama kako bi omogućili smanjivanje prometa razašiljanja te za povećanje sigurnost računalne mreže. Pripadnost pojedinog računala određenom VLAN-u određena je dodjelom priključka preklopnika, na koji je to računalo spojeno, tom definiranom VLAN-u. Time, uređaj postaje član određenog VLAN-a na osnovu pripadnosti priključka na preklopniku tom definiranom VLAN-u.
Implementacija VLAN-ova baziranih na priključcima preklopnika je relativno jednostavna pošto nije potrebna implementacija nikakvog protokola da bi se krajnji uređaj smjestio u odgovarajući VLAN. Tijekom svog rada, krajnji uređaji ne znaju za postojanje VLAN-a, a grupa mrežnih korisnika dodijeljena jednom VLAN-u formira zasebnu domenu razašiljanja koja je odvojena od ostalih VLAN-ova konfiguriranih na mreži. Paketi se prosljeđuju samo između priključaka preklopnika koji prenose promet za konkretni VLAN. Promet razašiljanja između pojedinih VLAN-ova je eliminiran na preklopnicima (osim ako se ne intervenira korištenjem *Layer* 3 uređaja) i širina propusnog sloja je sačuvana tako što se dopušta preplavljivanje paketa na samo određene priključke preklopnika.

Priključci na preklopniku se u odgovarajući VLAN smještaju statički i administrator mora za svaki priključak odrediti pripadnost određenom VLAN-u. Na osnovu pripadnosti pojedinom VLAN-u, priključci dobivaju *Port* VLAN ID (PVID) koji pokazuje njihovu pripadnost odgovarajućem VLAN-u. Time je omogućena brza i jednostavna dodjela VLAN-a krajnjem uređaju i ukoliko se korisnik preseli na drugi priključak, a želi imati isti VLAN kao i prije, tada se mora obaviti pridjeljivanje priključka u odgovarajući VLAN, tzv. *port-to-VLAN* dodjeljivanje.

Priključak na preklopniku	VLAN ID
1	1
2	1
3	2
4	3
5	4
6	3
7	4
8	1

Tablica 1: Primjer pripadnosti priključaka preklopnika pojedinim VLAN-ovima

2.2.2. VLAN-ovi bazirani na tipu protokola

Mrežni promet se može razdvajati u pojedine VLAN-ove na temelju protokola koji se koriste. Time pojedini protokoli bivaju smješteni u definirani VLAN. Preklopnici pri tome koriste liste tipova protokola kako bi dodjeljivali korisnike u definirane VLAN-ove.
Ovo je jedan vrlo fleksibilan način povezivanja koji se bazira na programskoj konfiguraciji računala. Promjenom konfiguracije i korištenih protokola korisnik sam mijenja pripadnost VLAN mreži. U nekim je okolnostima ova osobina poželjna zbog svoje jednostavnosti, ali negdje može biti i nepoželjna zbog sigurnosnih razloga.

Protokol	VLAN ID
IP	1
PBX	2
VoIP	3

Tablica 2: Primjer pripadnosti protokola pojedinim VLAN-ovima

2.2.3. VLAN-ovi bazirani na MAC adresama

Kod VLAN-ova baziranih na MAC adresama mrežnih kartica, tzv. dinamički ili *Layer* 2 VLAN-ovi, preklopnici se konfiguriraju s pristupnim listama (eng. *access lists*) koje povezuju individualne MAC adrese krajnjih uređaja s definiranim VLAN-ovima. Time je pripadnost određenom VLAN-u određena MAC adresom krajnjeg uređaja. Kada se krajnji uređaj spoji na preklopnik, preklopnik mora pregledati bazu kako bi krajnji uređaj smjestio u odgovarajući VLAN. Administrator mora u tu bazu unijeti MAC adrese i VLAN-ove u koje te MAC adrese treba smjestiti. Budući da su MAC adrese dio mrežne kartice, kada se uređaj premjesti na neku drugu lokaciju nije potrebna nikakva nova konfiguracija da bi korisnik ostao na istom VLAN-u. Ovakav način daje veću fleksibilnost.

MAC adresa	VLAN ID
080007A92BFC	1
090007A9B2EB	4
09104AB9E2A4	4
006008C499AA	2
08000935C99D	4
009027A79DDA	3

Tablica 3: Primjer pripadnosti MAC adresa pojedinim VLAN-ovima

2.2.4. Korisnički definirano povezivanje

Najfleksibilniji način povezivanja, ali ga podržava mali broj opreme. Pripadnost VLAN mreži je definirana kroz identifikaciju korisnika, aplikacije koje korisnik trenutno upotrebljava i sl. Potrebno je izgraditi centraliziranu bazu podataka o korisnicima i njihovim pravima pristupa, što je znatan posao pri izgradnji mreže, ali znatno olakšava kasnije održavanje i nadzor.

2.2.5. VLAN-ovi bazirani na definiranim pravilima

Određeni proizvođači omogućili su u svojim uređajima korištenje VLAN-ova baziranih na definiranim pravilima (eng. *rule based*) koji omogućavaju administratorima kreiranje takvih VLAN-ova gdje se pripadnost određenom VLAN-u određuje na informacijama koje se nalaze u mrežnom paketu koji se prosljeđuje preko preklopnika. Iako ova metoda pruža veliku fleksibilnost, postavljanje i održavanje ovakve mreže može biti kompleksno. Primjer definiranog pravila za pripadnost jednom VLAN-u:

```
Svi uređaji s IP adresama 100.100.10.x
   Osim uređaja s IP adresama 100.100.10.10 i 100.100.10.11
   Osim uređaja s MAC adresom 06-1A-0A-05-3C-02-04
```

2.3. Sprega IEEE 802.1Q protokola s IEEE 802.1P protokolom

IEEE 802.1P protokol omogućava *Layer* 2 preklopnicima da prioritiziraju mrežni promet pri čemu se izvodi dinamičko filtriranje prometa prema važnosti. Sama prioritizacija se obavlja na MAC sloju. Drugi naziv za prioritiziranje prometa je CoS (eng. *Class of Service*) jer se promet dijeli u klase prioriteta zavisno o protokolima koji se koriste. Pri tome se e-mail i http prometu često pridjeljuju najniži prioriteti. CoS predstavlja samo dio QoS-a (eng. *Quality of Service*) standarda očuvanja kvalitete usluge.

IEEE 802.1P protokol predstavlja nadopunu na IEEE 802.1Q protokol i oni rade u tandemu. IEEE-ovo 802.1Q zaglavlje u mrežnom paketu uključuje 802.1P polje koje se sastoji od 3 bita što omogućava grupiranje mrežnih paketa u 8 različitih klasa prioriteta. Iako mrežni administratori mogu definirati željeni poredak prioriteta, IEEE je preporučio da se u najviši prioritet 7 stavlja mrežni promet visokog prioriteta kao što su RIP (eng. *Routing Information Protocol*) i OSPF (eng. *Open Shortest Path First*) protokoli za definiranje usmjeravanja mrežnog prometa. Vrijednosti 6 i 5 imaju niži prioritet i preporuča se njihovo korištenje za mrežne pakete koji nose promet koji bi trebao biti isporučen u stvarnom vremenu – npr. interaktivni video prikaz ili glas. Vrijednosti od 4 do 1 preporuča se koristiti za aplikacije koje posjeduju poslovnu važnost kao što su npr. razmjene poslovnih podataka pa sve do prometa koji se može i izgubiti. Razina 0 je predefinirana vrijednost koja će biti automatski postavljena ukoliko se ne definira niti jedna druga vrijednost.

Određivanje razina za pojedini promet obavlja se na preklopnicima te ukoliko određeni preklopnik postane zagušen mrežnim paketima, preklopnik počinje odbacivati mrežne pakete počevši s onima koji su najnižeg prioriteta.

3. Prednosti i nedostaci VLAN mreža

3.1. Glavne prednosti upotrebe VLAN-ova

U nastavku ovog poglavlja navedene su neke od glavnih prednosti upotrebe VLAN-ova u računalnim mrežama.

3.1.1. Povećanje performansi mreže

U preklapanim mrežama grupiranje korisnika u VLAN-ove rezultira povećanjem performansi mreže limitiranjem prometa na korisnike koji provode slične funkcije ili se nalaze unutar individualnih grupa. Isto tako budući da se kreira manje prometa, to znači da se i manje prometa usmjerava prema drugim mrežama što rezultira s manjenom latencijom koju uzrokuju usmjerivači.

3.1.2. Olakšana administracija mreža

Uporabom virtualnih LAN-ova mreža s preklapanjem se logički segmentira (dijeli) prema nekoj funkciji: organizacijskoj strukturi, radu na projektu ili prema tome koju aplikaciju neki korisnik rabi, a ne prema fizičkoj odnosno zemljopisnoj lokaciji. Tako VLAN-ovi pružaju jednostavniji, fleksibilniji i jeftiniji način administriranja mreža u okolinama koje se konstantno i učestalo mijenjaju. Također, VLAN-ovi kod administriranja i održavanja velikih mreža dopuštaju centraliziranu konfiguraciju krajnjih uređaja koji su fizički dislocirani jedni od drugih.

3.1.3. Neovisnost o fizičkoj topologiji mreža

VLAN-ovi omogućavaju neovisnost o fizičkoj topologiji mreže dopuštajući grupiranje korisnika na različitim lokacijama, pri čemu su oni logički spojeni u iste domene razašiljanja. Ujedno ako se mijenja lokacija korisnika i krajnjih uređaja, jednostavnim dodjeljivanjem priključaka na preklopniku pojedinom VLAN-u korisnik ostaje u svom VLAN-u.

3.1.4. Ograničenje razašiljanja prometa na VLAN-u

VLAN-ovi promet razašiljanja (eng. *broadcast*) zadržavaju samo unutar sebe. Iako na jedan preklopnik može biti spojeno više krajnjih uređaja, ako oni ne pripadaju istom VLAN-u, pakete koje jedno od računala pošalje neće dobiti sva ostala računala spojena na isti preklopnik, već samo ona koja se nalaze u istom VLAN-u.
Računala koja su spojena na jedan preklopnik, a pripadaju različitim VLAN-ovima međusobno ne mogu komunicirati, osim ako je to dozvoljeno. Da bi paketi mogli prolaziti između različitih VLAN-ova potrebno je imati L3 preklopnik ili usmjerivač koji će znati usmjeravati pakete s jedne mreže na drugu.

3.1.5. Zaštita od malicioznih korisnika

Pošto su u VLAN-ovima svi korisnici na jednoj podmreži, ako se jedan od njih zarazi virusom ili nekim drugim malicioznim programom postoji velika mogućnost da se i ostali korisnici tog VLAN-a isto zaraze. Ali u mrežama gdje nisu implementirani VLAN-ovi svi korisnici na mreži mogu biti zaraženi malicioznim kodom, dok je kod mreža izvedenih pomoću VLAN-ova prijetnja ograničena samo na dotični VLAN.

3.1.6. Povećana sigurnost mreže

Na usmjerivačima ili L3 preklopnicima se može implementirati kontrola prometa između VLAN-ova. Na taj način je moguće već na mrežnom nivou zaštititi određene dijelove mreže (npr. računovodstvo, dekanat,…). Primjer takve povećane sigurnosti je *Blaster* crv koji tokom svog rada generira ogromnu količinu *broadcast*-a, koja je u ovom slučaju ograničena samo na pripadajući VLAN. Računala koja su spojena na jedan preklopnik, a pripadaju različitim VLAN-ovima međusobno ne mogu komunicirati. Da bi paketi mogli prolaziti između VLAN-ova potrebno je imati usmjerivač koji će znati usmjeravati pakete s jedne mreže na drugu.
Ukoliko postoji nekoliko međusobno spojenih preklopnika te na njima definirano nekoliko istih VLAN-ova potrebno je omogućiti promet između dva računala koja se nalaze u istom VLAN-u, ali su spojena na različite preklopnike. Za to je potrebno koristiti *VLAN Trunking Protocol* (VTP). Ovaj protokol omogućava da se preko jednog sučelja prenosi promet svih VLAN-ova. Na Cisco uređajima u istu svrhu se može koristiti i ISL (eng. *Inter- Switch Link Protocol*).

3.1.7. Prioritiziranje mrežnog prometa

IEEE 802.1Q posjeduje mogućnost rada u tandemu s IEEE 802.1P standardom koji omogućava prioritiziranje mrežnog prometa. Time je moguće povećati kvalitetu usluge prijenosa mrežnog prometa. Svaki put kad se unutar preklopnika spremnici koji čuvaju primljene mrežne pakete prepune, preklopnik može na temelju prioriteta koji su dodijeljeni pojedinim mrežnim paketima, odrediti koje pakete treba početi prvo uklanjati. Takvim načinom rada mrežni promet višeg prioriteta ima veću mogućnost dolaska na cilj.

3.2. Glavi nedostaci upotrebe VLAN-ova

Iako se o VLAN-ovima prvenstveno razmišlja kao o unaprjeđenju postojećih mreža, VLAN-ovi ipak imaju i svoje nedostatke od kojih su glavni razloženi u nastavku ovog poglavlja.

3.2.1. Komunikacija između VLAN-ova

Računala koja se nalaze u kreiranim VLAN-ovima međusobno nisu vidljiva te ukoliko se želi omogućiti međusobna komunikacija, potrebno je koristiti usmjerivač. Ukoliko je potrebno da usmjerivač preusmjerava pakete iz jednog VLAN-a u drugi, mrežno sučelje usmjerivača treba podijeliti na onoliko podsučelja koliko postoji VLAN-ova. Svakom od tih virtualnih sučelja se dodjeljuje IP adresa iz raspona pojedinog VLAN-a i tu je ujedno adresa predefiniranog izlaza (eng. *default gateway*) za taj VLAN. Osim adrese, na podsučelju je potrebno definirati kojem VLAN-u pripada te koji *trunking* protokol podržava.

3.2.2. Kompleksnost VLAN-ova

S povećavanjem računalne mreže bazirane na VLAN-ovima povećava se proporcionalno i broj VLAN-ova te broj pripadnika pojedinih VLAN-ova. Također potrebno je definirati i nove politike propuštanja prometa između VLAN-ova te modificirati postojeće. Svime time raste ukupna kompleksnost konfiguracije i implementacije VLAN-ova.

3.2.3. Noseći kapacitet usmjerivača

Ukoliko se usmjerivači koriste za usmjeravanje prometa između različitih VLAN-ova tada se može pojaviti problem propusnosti usmjerivača. Kod velikih mreža koje imaju mnogo VLAN-ova nije dobro da se za usmjeravanje koristi jedan usmjerivač zbog nemogućnosti obrade velikih količina paketa.

3.2.4. Neovlašteno uključivanje u pojedini VLAN

Ukoliko lokalni korisnici imaju mogućnost pristupa preklopniku koji određuje pripadnost pojedinim VLAN-ovima, tada su oni u mogućnosti neovlašteno se uključiti u VLAN u koji ne pripadaju. Ovaj slučaj moguć je kod VLAN-ova baziranih na priključcima preklopnika koji su ujedno i najčešći oblik, a rješenje za to je korištenje nekog drugog sustava VLAN-ova kao što je npr. sustav VLAN-ova baziranih na MAC adresama.

4. Zaključak

Korištenje VLAN-ova u računalnim mrežama posjeduje brojne prednosti koje se očituju u prvom redu u mogućnosti kontrole i smanjena negativnih utjecaja razašiljanja. Razdvajanjem mreže na manje dijelove, VLAN-ove, povećava se količina raspoloživog propusnog linka (eng. *bandwith*). Administratori korištenjem VLAN-ova mogu na jednostavan način grupirati uređaje u logičke grupe, a da pri tome pojedina računala koja spadaju u istu grupu ne moraju biti na istoj fizičkoj lokaciji.
Grupiranje uređaja u VLAN-ova ne mora se nužno obavljati na temelju pripadnosti priključaka preklopnika pojedinim VLAN-ovima što je ujedno i najčešći slučaj. Administratori mogu VLAN-ove formirati i na drugim principima (IP adrese, MAC adrese, protokoli,…). Ipak, za implementaciju svih oblika VLAN-ova potrebno je posjedovati opremu koja će to podržavati.
Iako se korištenjem VLAN-ova smanjuju troškovi na opremu koja bi se trebala koristiti kako bi se mreža segmentirala u željene podmreže, za povezivanje različitih VLAN-ova potrebno je koristiti *Layer* 3 uređaje što povećava troškove i promet preko tih uređaja.

5. Reference

[1] Specifikacija IEEE 802.1P "Standard for Local and Metropolitan Area Networks - Supplement to Media Access Control (MAC) Bridges: Traffic Class Expediting and Dynamic Multicast Filtering"
[2] Specifikacija IEEE 802.1Q "Standard for Virtual Bridged Local Area Networks",
http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf : IEEE 802.1Q Standard
[3] VLAN: Virtual Local Area Network and IEEE 802.1Q,
http://www.javvin.com/protocolVLAN.html
[4] Prioritization of Network Traffic, http://www.linktionary.com/p/prioritization.html
[5] 802.1Q VLANs for better bandwidth,
http://www.networkworld.com/news/tech/2001/0305tech.html