Menadžment procesa segmentacije LAN

STEFAN S. ČELANOVIĆ, Fakultet za saobraćaj, komunikacije i logistiku, Budva, Crna Gora
MARKO S. ASANOVIĆ, Fakultet za saobraćaj, komunikacije i logistiku, Budva, Crna Gora
NATAŠA M. GOSPIĆ, Fakultet za saobraćaj, komunikacije i logistiku, Budva, Crna Gora

Prethodno saopštenje
UDC: 004.732:004.451.353
DOI: 10.5937/tehnika1803417C

U ovom radu obrađuju se procesi segmentacije lokalne računarske mreže multisektorskog preduzeća. Srž rada je fokusirana na problematiku praktičnog kreiranja i konfigurisanja segmentisane računarske mreže pomoću „Cisco IOS" interfejsa komandnih linija. Navedeni procesi i njihova interakcija sa realnim okruženjem su simulirani i grafički predstavljeni virtuelizacionim softverom. Komandne linije kao upravljački procesi predstavljeni su i simulirani u cilju testiranja funkcionalnosti ostvarene topologije segmentisane mreže. Prikazana je struktura protokola koji uobličavaju segmentaciju računarske mreže na virtuelne lokalne računarske mreže kao najefikasnije metode segmentacije. Objašnjeni su benefiti koje donosi segmentacija lokalne računarske mreže. Najveća pažnja pridata je upotrebi komandi „Cisco IOS" jezičke sintakse kao najčešćeg programskog jezika među mrežnim uređajima.

Ključne riječi: *Frejm, dot1q, enkapsulacija, segment, Eternet, kolizioni domen*

1. UVOD

Poslovno okruženje svakog preduzeća zahtjeva da bude informaciono opremljeno i da u tom domenu prati najnovije standarde, protokole i preporuke, budući da korišćenje računara kao alata pri poslovanju predstavlja konkurentnu prednost. Uvođenje računarskih tehnologija u poslovanje preduzeća omogućava mnogostruke prednosti od povećanja efektivnosti i ekonomičnosti poslovanja, proizvodnih mogućnosti, pouzdanosti, osiguravanja povjerljivih dokumenata do ekološke svjesnosti. Kreiranje interne računarske mreže unutar preduzeća predstavlja korak koji omogućava međusektorsku komunikaciju i brže djelovanje na zahtjeve tržišta. Povećanjem subjekata u okviru jedne kompletne računarske mreže može doći do pojave određenih problema koji sputavaju prirodni tok komunikacije računara u okviru te mreže. Radi toga kao i razloga lakšeg upravljanja mrežom javila se potreba za korišćenjem virtuelnih lokalnih računarskih mreža – VLAN (eng. Virtual Local Area Network).

U ovom radu dat je prikaz modela dizajniranja i segmentacije jedne lokalne računarske mreže za preduzeće čija organizacija obuhvata više sektora. Mreža je konstruisana kao virtuelna, korišćenjem virtuelizacionog softvera - „Cisco Packet Tracer". Osnovni cilj rada je prikaz prednosti koje se dobijaju kreiranjem virtuelnih lokalnih računarskih mreža (eng. Virtual Local Area Network- VLAN).

2. RAZLOZI UVOĐENJA VLAN SEGMENATA

Razlozi zbog kojih se uvodi raščlanjivanje računarske mreže na više segmenata su:

- Smanjivanje zagušenosti mreže – Povećanje performansi, budući da dolazi do smanjenja broja hostova po segmentu mreže, smanjujući lokalni saobraćaj;
- Poboljšanje sigurnosti mreže – Broadcast paketi se zadržavaju u okviru lokalne mreže. Time se omogućava da unutrašnja struktura mreže nije vidljiva subjektima koji se nalaze izvan lokalne mreže. Ukoliko dođe do bezbjednosnog kompromitovanja jednog uređaja u mreži, smanjuje se mogućnost prelivanja malicioznih sadržaja na druge uređaje u mreži, ograničavajući domet napadača samo na okvire te virtuelne lokalne mreže. Stoga je redovna praksa mrežnih inženjera da mrežu podijele na segmente gdje se serveri, baze

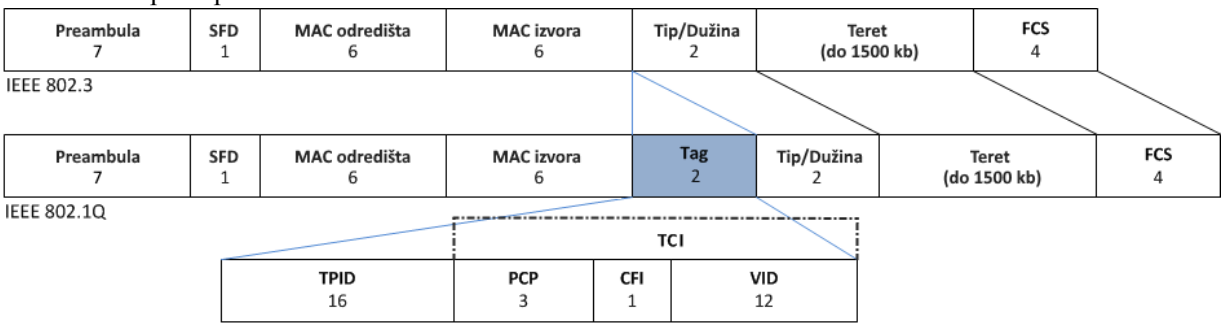
Adresa autora: Stefan Čelanović, Fakultet za saobraćaj, komunikacije i logistiku, Budva, Žrtava fašizma bb, Crna Gora
E-mail: celanovic.stefan69@gmail.com
Rad primljen: 01.06.2018.
Rad prihvaćen: 07.06.2018.

podataka i korisnički terminali nalaze svaka na svojim izolovanim virtuelnim segmentima lokalne mreže;

- Ograničavanje mrežnih problema – Ograničavanje negativnih efekata problema lokalnih mrežnih uređaja, na taj način da ukoliko dođe do zakazivanja jednog mrežnog uređaja, ne dođe do zakazivanja čitave mreže;
- Kontrolisanje nivoa pristupa posjetiocima – Stvaranjem izolovanog segmenta namijenjenog gostima u mreži ograničava se njihov pristup informacijama. Gosti na taj način neće biti u mogućnosti da pristupom na mrežu dođu do internih baza podataka, servera i povjerljivih servisa za preduzeće.

Potrebno je razumjeti da virtuelna lokalna mreža procese segmentacije vrši na drugom sloju, te s toga nije u mogućnosti da razlikuje aplikacije, korisnike i sadržaj transmitovanih poruka.

S toga, sa pogleda nivoa bezbjednosti, ovaj vid komunikacije ne pruža zaštitu uređaja od malicioznih napada poput malicioznih softvera, eksploatacije mana operativnih sistema i slično, već isključivo pruža osnovno povećanje stepena bezbjednosti uključivanjem enkapsulacije frejmova u saobraćaj podataka.



Slika 1 - Poređenje struktura frejmova IEEE 802.3 i IEEE 802.1Q

3. VLAN PROTOKOLI

Prije pojave VLAN segmentacije mreže su obično bile segmentisane zasebnim mrežnim uređajem. Ovakve akcije su bile posebno korisne u slučajevima topologija magistrale, sada prevaziđenog rješenja za lokalnu računarsku mrežu. Masovnijom pojavom svičeva pojavilo se prvo značajnije rješenje problema segmentacije. Svičevi su dijelili cjelokupnu lokalnu računarsku mrežu na setove kolizionih domena.

Kolizija paketa jeste pojava do koje dolazi transmitovanjem saobraćaja od strane više uređaja istovremeno, koristeći se zajedničkim medijumom. Pri koliziji paketa dolazi do uništenja svih uključenih paketa što dalje vodi do potrebe za njihovim ponovnim transmitovanjem.

Kolizioni domen predstavlja cjelokupni mrežni prostor u okviru kojeg postoji mogućnost događanja kolizije.

Broadcast domen sa druge strane predstavlja logički prostor svih uređaja do kojih broadcast poruke drugog sloja mogu dospjeti. [1]

Budući da kroz jedinstven broadcast domen putuju sve broadcast poruke, čak i u slučajevima lančanog povezivanja više svičeva.

U ovoj situaciji, broadcast poruka koja dolazi do sviča će biti proslijeđena kroz sve portove, uključujući i port na koji je lančano povezan sledeći svič koji će ih takođe proslijediti i kroz sve svoje portove.

Povećanjem LAN-ova došlo je i do povećanja brzina transmitovanja, povećanja brojnosti i dinamičnosti krajnjih korisničkih terminala. Ova činjenica je dovela izuzetnih komplikacija pri organizovanju i održavanju mreže. Eventualna promjena pozicije jednog zaposlenog u preduzeću je počela da dovodi do sve većih problema koji su se ogledali u potrebnoj prostornoj reorganizaciji mrežnih uređaja i medijuma i ponovne konfiguracije dodijeljenih portova.

Pod VLAN se podrazumijeva broadcast domen koji je izolovan od lokalne računarske mreže na drugom sloju OSI modela – sloju veze podataka. VLAN funkcionišu na principu dodavanja određenih znakova paketima podataka koji raspoređuju pakete po naznačenim segmentima segmentisane mreže. Po ovom principu, segmentisane mreže mogu da se ponašaju kao odvojeni samostalni entiteti bez potrebe za uvođenjem dodatnih mrežnih uređaja, povlačenjem dodatnih kablova i generalnim širenjem mrežne arhitekture. Segmentacija računarskih mreža predstavlja čin ili praksu raščlanjivanja računarske mreže u podmreže, od kojih svaka predstavlja samostalni segment mreže. [2]

A. 802.3 Eternet frejm

IEEE 802.3 predstavlja porodicu standarda kojom se definišu protokoli fizičkog sloja i sloja veze podataka Eternet tehnologije. Na osnovu ovih standarda dolazi do uniformne strukture Eternet frejmova podataka koji grupišući se u pakete podataka čine osnovnu funkcionalnu cjelinu Internet saobraćaja.

Eternet frejmovi uređuju strukturu u okviru koje se nalaze informacije o fizičkoj (MAC) adresi destinacije i izvora frejma, kao i sam „korisni prtljag“ – transportovane podatke radi kojih je uopšte i došlo do formiranja konkretnog prtljaga.

Osnovni strukturni činioci Eternet frejma 802.3 grupe standarda su:

- Preambula – 7 okteta naizmjeničnih bitskih jedinica i nula kojima se označava početak frejma i pomoću kojih dolazi do sinhronizacije internih satova;
- SFD – oktet kojim se završava preambula i označava početak MAC destinacione adrese (eng. Start of Frame Delimiter);
- MAC adresa – 12 okteta kojima se označavaju odredišna i početna MAC adresa;
- Tip i dužina Eternet frejma – 2 okteta pomoću kojih se označavaju tip i dužina Eternet frejma;
- Korisni teret – konkretnog materijala u čiju svrhu dolazi do formiranja Eternet frejmova (eng. Payload);
- Sekvenca provjere frejma – 4 okteta u okviru kojih se nalazi suma bitova frejma na osnovu koje se provjerava integritet frejma (eng. Frame Check Sequence.) [3]

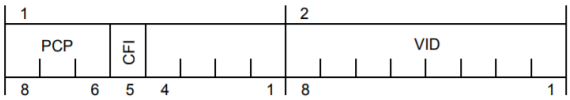
B. 802.1Q Eternet frejm

IEEE 802.1Q, često nazivan i „Dot1q“ standard predstavlja standard Eternet frejmova sa podrškom VLAN segmentacije računarske mreže. Na osnovu ovog standarda uređuju se akcije VLAN označavanja Eternet frejmova. Akcije VLAN označavanja Eternet frejmova se obavljaju u svim računarskim mrežama osposobljenim za VLAN segmentaciju, pri čemu se frejmovima nakon izvorišne MAC adrese dodaje četvorobajtna oznaka koja predstavlja 802.1Q zaglavlje. [4] Pomoću podataka u okviru zaglavlja dobija se jedinstveni VLAN identifikator Eternet frejma.

Struktura IEEE 802.1Q oznake sadrži sledeće podatke: [5]

- TPID – identifikator IEEE 802.1Q protokola (eng. Tag Protocol Identifier), 2 okteta vrijednosti 0x8100. Na osnovu ovih podataka mrežni uređaj dobija informaciju da se radi o VLAN označenom frejmu podataka;
- TCI – upravljačke informacije o oznaci (eng. Tag Control Information), 2-oktetno polje, pri čemu prva 4 bita označavaju trobitno polje tačke prioriteta koda (eng. Priority Code Point) pomoću koje se ostvaruje prioritetnost frejmova i jednobitnog indikatora kanonskog formata (eng. Canonical Format Indicator) na osnovu čije vrijednosti se utvrđuje format informacija o MAC adresama. Sledećih 12 bitova nose informacije o VLAN identifikatoru. VLAN identifikator se kodira u vidu heksadecimalnog dvanaestobitnog broja pri čemu vrijednost 0 označava da zaglavlje oznake nosi samo podatke o prioritetu frejma.

  Na slici 2 prikazan je format TCI polja.



Slika 2 - TCI polje 802.1Q oznake

4. PRIMJER SEGMENTISANJA LAN NA VIRTUELNE SEGMENTE

U daljem tekstu dat je prikaz uspostavljanja i konfiguracije VLAN u okviru lokalne računarske mreže korištenjem emulacionog programa „GNS3 – Graphical Network Simulator“. Ovaj program može da izvrši emulaciju operativnog sistema na virtuelnoj mašini u okviru sistema domaćina. Za potrebe prikazivanja uspostavljanja VLAN, programom „VMware Workstation Pro“ pokrenut je program GNS3 – grafički simulator mreže (eng. Grafic Network Simulator). Ovim softverom je omogućeno upravljanje konzolom virtuelnih mrežnih uređaja.

Mrežni uređaji korišteni u ovom primjeru su:

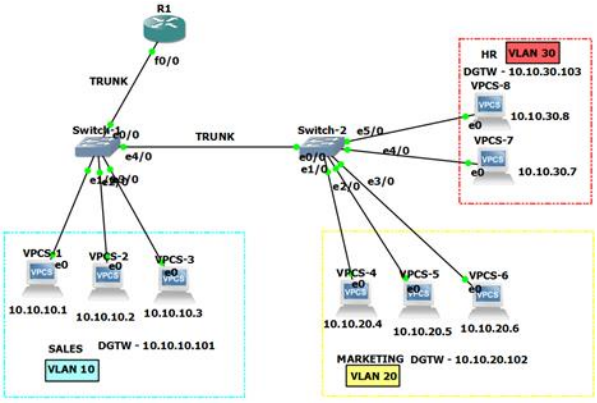
- 1 ruter – Cisco 7200, verzija 12.4(24)T8. Ruteru je dodijeljeno 512 MB RAM memorije, 512 KB NVRAM i jedan C7200-IO-FE adapter u slotu 0 radi konektivnosti sa drugim mrežnim uređajima;
- 2 sviča – Cisco vIOS-L2. Svičevima je dodijeljeno po 1024 MB RAM memorije, po 2 virtuelna jezgra dvojezgranog procesora i po 5 mrežnih adaptera tipa Intel Gigabit Ethernet (e1000).
- 8 krajnjih uređaja – Virtuelni računari dobiveni u sklopu grafičkog simulatora mreže – GNS3.

Mrežna topologija je povezana eternet kablovima, pri čemu su portovi između rutera i sviča i između dva sviča konfigurisani pod „trunk“ modom, dok su portovi između svičeva i virtuelnih računara konfigurisani pod „access“ modom.

Virtuelnim računarima su dodijeljene IP adrese u 10.10.x.x domenu sa 255.255.255.0 subnet maskom. Default gateway se razlikuje za svaki VLAN što će dalje biti objašnjeno u primjeru.

Elementi kojima se može manipulisati u okviru GNS3 softvera ogledaju se u vidu mrežnih uređaja sa pripadajućim operativnim sistemima, kao i virtuelnih krajnjih uređaja sa klijentskim softverima u vidu pretraživača i korisničkih operativnih sistema poput pretraživača otvorenog koda „Mozilla Firefox“ i OS „Linux“ koji se mogu dobaviti softverom GNS3 pri čemu simulacioni softver ostvaruje konekciju sa serverima na kojima se nalaze željeni elementi. Na sl. 3. prikazan je krajnji proizvod koji želimo postići da bi

na lakši način stekli sliku o željenoj topologiji jer će nam ta slika biti potrebna pri daljem radu na konfigurisanju VLAN segmenata. Recimo da u preduzeću postoje departmani prodaje, marketinga i upravljanja ljudskim resursima. Svaki od ovih departmana ima potrebu da pristupi zajedničkoj mreži, ali pri tome svaki deptarman iz sigurnosnih razloga želi da njihov dio mreže bude samostalan i da entiteti iz drugih segmenata nemaju pristup njihovim podacima. Ovakav proizvod je moguće postići segmentacijom na tri virtuelne lokalne mreže od kojih svaka nosi drugačije ime, u primjeru konkretno 10, 20 i 30.



Slika 3 - Prikaz segmentisane LAN topologije

Da bi mrežni uređaj bio u stanju da ostvari konekciju sa drugim mrežnim uređajima, potrebno je da ima dovoljan broj mrežnih adaptera. U okviru simulacionog softvera "GNS3" moguće je upotrebljavati više vrsta adaptera, a za potrebe ovog projekta izabran je adapter marke Intel i tipa Eternet. Adapter je gigabitnog opsega što znači da ima veliku propusnu moć, posebno ukoliko će spektar njegovog korišćenja biti proslijeđivanje poslovnih prepiski, elektronske pošte i izvršavanje sličnih poslova koji se ne tiču transporta izuzetno velikih multimedijskih fajlova koji bi mogli dovesti do zagušenja ostvarene mrežne topologije.

Budući da svič mora da izvrši konekciju sa tri hosta, susjednim svičem i ruterom radi izlaska na globalnu mrežu i intermrežnog saobraćaja, adapter mora da ima najmanje 5 portova. Na identičan način se podešava i drugi svič, samo što, budući da mora da ostvari konekciju sa 5 hostova i jednim susjednim svičem, za ovaj svič potrebno dodijeliti 6 mrežnih adaptera.

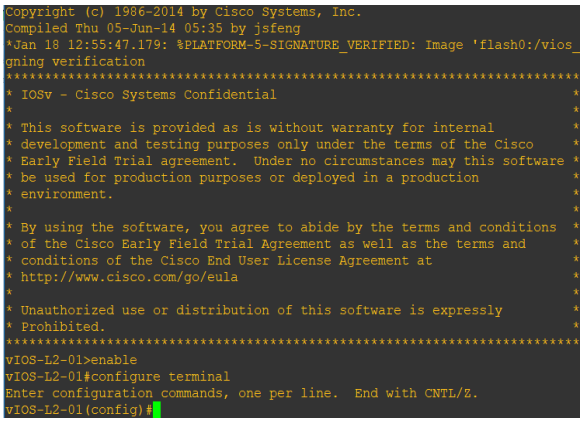
Po prostornom raspoređivanju mrežnih uređaja u virtuelizacionoj ravni potrebno je čitavu topologiju povezati medijumima prenosa podataka, u konkretnom slučaju Eternet kablovima. Nakon kabliranja topologije, potrebno je pokrenuti svaki uređaj pritiskom na taster „Start/Resume all nodes".

Ovaj postupak čini da se slike mrežnih uređaja pokrenu i izvrše funkcije podizanja sistema, na isti način na koji to rade stvarni uređaji u realnom okruženju. Vrijeme podizanja sistema zavisi direktno od mogućnosti i memorijskih kapaciteta mašine i operativnog sistema domaćina i dodijeljenih kapaciteta virtuelnim uređajima u okviru sistema gosta. Budući da su u prikazanom primjeru kapaciteti i sistema domaćina i dodijeljeni kapaciteti gosta dovoljno visoki da mogu bez problema da podrže manipulisanje virtuelnim operativnim sistemima, podizanje sistema mrežnih uređaja drugog i trećeg sloja OSI sistema se svodi na nekoliko sekundi – od pokretanja mrežnog čvora do osposobljavanja „User EXEC" moda da primi prve komande. Ovaj mod podržava unošenje svega nekoliko najosnovnijih komandi koji se tiču prikazivanja osnovnih podešavanja mrežnog uređaja koje ne nose nikakav bezbjedonosni rizik. Da bi ušli u „Privileged EXEC" mod kojim se nude šira ovlašćenja potrebno je izvršiti komandu `enable`. Da bi ušli u „Global configuration" mod koji nudi sva ovlašćenja za upravljanje mrežnim uređajem potrebno je unijeti komandu configure terminal.

Radi shvatanja sledećih koraka potrebno je razlučiti operativne sisteme koji su konfigurisani na način da imaju grafički interfejs i operativne sisteme koji naredbe za izvršavanje određenih akcija dobijaju putem neke vrste terminala ili konzole u koju se upisuju komande u obliku komandnih riječi određenog jezika kojim se taj operativni sistem koristi. Operativni sistem koji se nalazi u okviru Cisco mrežnih uređaja ne sadrži grafički interfejs, što znači da nisu osposobljeni za upotrebu pokazivača upravljanog određenim periferijskim uređajima. Umjesto upotrebe pokazivača za odabir željenih opcija, svaka željena akcija se izvršava ispisivanjem tačno određene komande u jezičkoj sintaksi koji razumije Cisco operativni sistem na tom određenom mrežnom uređaju. Sintaksa komandi je identična među svim Cisco mrežnim uređajima, tako da se uređajima različitih serija, modela i različitog mjesta u sedmoslojnoj OSI arhitekturi upravlja koristeći se identičnim komandama. Virtuelni računari virtuelizacionog softvera "GNS3" dolaze sa operativnim sistemom drugačijeg porijekla od operativnih sistema „Cisco" porodice uređaja. Iako sintaksa komandnog jezika ovih uređaja nije identična sintaksi „Cisco" uređaja, logički slijed komandi je u velikoj mjeri sličan. Jedna od osnovnih komandi koja prikazuje vrijednosti naziva hosta, IP adrese, subnet maske, default gateway-a, adrese DNS servera, MAC adrese i još par informacija koje ne utiču na rad u konkretnom primjeru jeste – `show ip`. Da bi se podesili željeni mrežni parametri potrebno je unijeti komandu – `ip` x.x.x.x/24 x.x.x.x. U ovom slučaju, prva adresa predstavlja željenu IP adresu virtuelnog računara nakon čega slijedi oznaka subnet maske koja u ovom slučaju iznosi 255.255.255.0, budući da u adresnom prostoru IPv4 protokola veličine 32 bita, 24 bita

označavaju veličinu mrežnog prefiksa, dok ostalih 8 označava veličinu host prefiksa. Druga adresa sastavljena od četiri okteta određuje adresu default gateway-a. Ova adresa podrazumijeva adresu koju će host koristiti ukoliko želi poslati pakete podataka van svoje (virtuelne) lokalne mreže.

Podešavanja IP adrese, subnet maske i default gateway-a potrebno je ponoviti na svakom računaru, dodijelivši svakom hostu jedinstvenu IP adresu, identičnu subnet masku – budući da su u konkretnom primjeru svi računari jednog segmenta konfigurisani kao pripadnici jedinstvene podmreže i vrijednost default gateway-a koji je identičan za svaku pojedinačnu virtuelnu lokalnu mrežu, ali koji se razlikuje među mrežama, da bi mrežni uređaji znali koju adresu da koriste za transport paketa trećim slojem OSI modela. Nakon podešavanja virtuelnih računara potrebno je ući u konzolu sviča i početi sa podešavanjem ovog mrežnog uređaja. Na sl. 4. prikazan je izgled podignutog sistema na sviču (drugog sloja) Cisco porijekla. Pri dnu slike se vide tri nivoa ovlašćenja – „User EXEC“ mod koji se prepoznaje po promptu „>“; „Privileged EXEC“ mod sa promtom „#“ i Global configuration mod sa promptom „(config)“ i komandi za podizanje ovlašćenja na sledeći viši nivo. Svi Cisco mrežni uređaji imaju mogućnost postavljanja lozinke između svakog moda, štiteći time podešavanja od neautorizovanog rukovanja.



Slika 4 - Prikaz konzole „Cisco“ mrežnog uređaja

Da bi svič imao svoju funkciju segmentisanja lokalne mreže na virtuelne djelove, potrebno je kreirati virtuelne mreže u internoj memoriji sviča. To se postiže ulaskom u globalni konfiguracioni mod i unošenjem komande – `vlan #`, pri čemu # predstavlja jedinstveni heksadecimalni identifikator vlan mreže. Po izvršenju ove komande vlan mreža je stvorena i automatski je iz globalnog konfiguracionog moda korisnik uveden u mod konfiguracije vlan mreže. U tom modu je potrebno unijeti komandu – `name xxx`, pri čemu xxx predstavlja ime vlan mreže, u ovom slučaju „SALES“. Po izvršavanju ove komande stvorili smo virtuelnu lokalnu mrežu pod nazivom „SALES“ u sviču. Komandu treba ponoviti za svaku virtuelnu mrežu u lokalnoj mreži budući da će saobraćaj svih mreža putovati kroz ovaj svič.

Nakon kreiranja virtuelne lokalne mreže, potrebno je povezati hostove sa interfejsima na sviču i dodijeliti im vlan segment. Za prikaz svih interfejsa na sviču koristi se komanda – `show ip interface brief`.

Da bi svakom hostu dodijelili određeni VLAN segment potrebno je iz globalnog konfiguracionog moda ući u mod konfiguracije svakog interfejsa pojedinačno komandom – `interface xxx #/#`. Nakon ulaska u mod konfiguracije interfejsa potrebno je odrediti ulogu interfejsa u okviru vlan mreže. Uloga može biti pristup i prenos (access/trunk). Ona se određuje komandom – `switchport mode x`. U ovom slučaju, x predstavlja ulogu access. Komandu je potrebno ponoviti za sve interfejse koji povezuju hostove sa svičem.

Postupak dodjeljivanja hostova VLAN mreži je potrebno uraditi i na drugom sviču. Pri tome je potrebno voditi pažnju o ulozi koji interfejs ima u okviru VLAN mreže, da interfejs koji je zadužen za povezivanje više VLAN mreža greškom ne bi bio konfigurisan na način da ima ulogu pristupa informacijama.

Nakon konfigurisanja svih interfejsa koji bi trebali da imaju access ulogu, potrebno je konfigurisati interfejse na kojima se vrši povezivanje više VLAN mreža. Ova uloga se naziva „trunk“ i konfiguriše se ulaskom u konfiguracioni mod interfejsa koji je namijenjen za tu funkciju i prvo ispisivanjem komande – `switchport trunk encapsulation dot1q`, čime se postiže usaglašavanje standarda enkapsulacije. U ovom slučaju potrebno je unijeti standard IEEE 802.1Q. Nakon usaglašavanja standarda enkaspulacije podataka, još je potrebno samo dodijeliti ulogu trunk-a interfejsu komandom – `switchport mode trunk`. Ovim činom smo završili konfiguraciju sviča. Nakon konfiguracije ovog sviča potrebno je na isti način konfigurisati i preostale svičeve, u našem primjeru svič broj 1. Takođe, obratiti pažnju da se tačno određenim interfejsima dodijeli prava uloga.

Nakon obavljenog posla na sviču 1 i sviču 2 potrebno je konfigurisati ruter čija je funkcija da prosljeđuje pakete podataka između nezavisnih mreža, ako tako konkretna situacija zahtijeva između različitih vlan mreža ili među mrežama i globalnom mrežom. Konfigurisanje rutera i učlanjivanje informacija o vlan mrežama u okvir njegovog poslovanja se vrši uspostavljanjem zajedničkog protokola enkapsulacije za svaku vlan mrežu posebno i pružanju informacija o default gateway-ima koje hostovi planiraju da koriste za određenu vlan mrežu kojoj pripadaju. Ovo se postiže kreiranjem podsloja interfejsa za svaku vlan

mrežu kojom će ruter morati da rukuje. Sintaksa komande za kreiranje podsloja jeste – `interface xxx #/#.vlan#`. Pri ovoj sintaksi xxx podrazumijeva naziv interfejsa rutera, #/# broj interfejsa rutera, a vlan# identifikator vlan mreže. Komande u okviru konkretnog primjera su sledeće:

```
interface fastEthernet 0/0.10
 encapsulation dot1Q 10
  ip address 10.10.10.101 255.255.255.0
  no shut
  exit
interface fastEthernet 0/0.20
 encapsulation dot1Q 20
  ip address 10.10.20.102 255.255.255.0
  no shut
  exit
interface fastEthernet 0/0.30
 encapsulation dot1Q 30
  ip address 10.10.30.103 255.255.255.0
  no shut
  exit
```

Komanda „no shut“ – skraćeno od „no shutdown“ je način kojim se koristi sintaksa jezika operativnog sistema pomoću kojih se koristi logička negacija komande da bi se ostvario željeni efekat, u ovom smislu da dođe do obustave stanja ugašenog interfejsa.

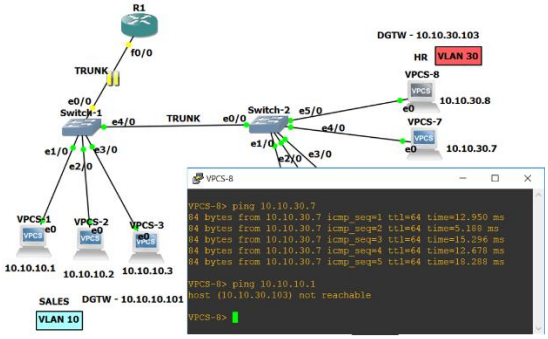
Ova sintaksa se može iskoristiti da bi negirali bilo koju logičku komandu koja se može negirati. Takođe, negiranjem određenih unijetih parametara možemo da poništimo neku komandu ukoliko smo pri upisivanju željenih parametara napravili grešku.

5. PROVJERA FUNKCIONALNOSTI VLAN

Ukoliko su sve navedene komande unijete uspješno i interfejsima pravilno dodijeljeni hostovi i uloge svakog hosta smještene u ispravnu vlan mrežu možemo biti sigurni da je mreža uspješno segmentisana. Konektivnost mreže se provjerava otvaranjem konzole nekog krajnjeg uređaja i upisivanjem komande – `ping x.x.x.x`, pri čemu je x.x.x.x adresa hosta na drugoj strani mreže.

Komanda „ping“ podrazumijeva slanje specijalno konfigurisanih ICMP paketa kojima se provjerava dostupnost pozivanih hostova i njihova mogućnost da pročitaju poslate podatke. Konektivnost među vlan mrežama obezbjeđena je posredstvom rutera kao mrežnog uređaja trećeg sloja OSI modela.

Ukoliko obustavimo rad rutera, možemo primjetiti da hostovi nisu u stanju da kontaktiraju hostove van svoje virtuelne lokalne mreže, iako su fizički priključeni na jednu istu realnu lokalnu mrežu. Dokaz ovome se vidi na slici br. 5.:



Slika 5 - Prikaz uspješno segmentisane mreže

6. UTICAJ SEGMENTACIJE NA NIVO OPTIMIZOVANOSTI MREŽE

Dizajniranje računarske mreže podrazumijeva mnogobrojne procese koji direktno zavise od konkretnih potreba preduzeća u čiju korist se kreira mreža. Različite potrebe preduzeća diktiraju opus preduzimanih akcija i tok kojim će se dizajn mreže odvijati. Uopšteno gledano, dizajn računarske mreže se ogleda u planiranju potrebnog broja elemenata računarske mreže poput krajnjih pristupnih uređaja i mrežnih uređaja, traženja najpovoljnije arhitekture uređaja, konfigurisanja elemenata radi uspostavljanja najvišeg nivoa optimizovanosti arhitekture. Nivo optimizovanosti se može smatrati poput skupa kvalitativnih odrednica mreže koje će klijentima omogućiti da što poptunije iskorišćavaju mogućnosti upotrebljenih računarskih elemenata.

Optimizacija računarske mreže u primjeru jednog preduzeća se može svoditi na procese poput segmentisanja lokalne računarske mreže, upošljavanja različitih elemenata kvaliteta servisa u cilju postizanja klasifikacije saobraćaja i uvođenja pravila prioriteta, uspostavljanja zaštitnih barijera, pružanja najefikasnijeg modela arhitekture pristupnih i distributivnih uređaja i uređaja jezgra mreže, odabira optimalnijeg konkretnog mrežnog uređaja za svaku logičku poziciju u okviru arhitekture mreže, pružanja različitih nivoa pristupa, uspostavljanja mogućnosti daljinskog upravljanja mrežom i slično.

VLAN segmentacija izvršavajući svoje akcije segmentisanja isključivo u okviru logičkog prostora, a ne upotrebom dodatne opreme, značajmo smanjuje troškove u odnosu na procese segmentacije fizičkim uređajima. Ima i značajan uticaj na stepen zagušenosti mreže.

Nivo optimizovanosti računarske mreže direktno zavisi od veličina kolizionih i broadcast domena. Što su kolizioni domeni veći, u smislu zahvatanja većeg broja učesnika koji dijele zajednički medijum, dolazi do veće šanse za pojavom kolizije paketa što će pokrenuti ponovnu transmisiju izgubljenih paketa. Što su broadcast domeni veći, dolazi do veće gustine

saobraćaja u okviru mreže izazvano dužim putanjama broadcast poruka i značajnijeg ispunjavanja memorijskih prostora poput ARP tabela i slično. Upotreba rutera kao nosilaca segmentacije LAN je neefikasno i neekonomično rješenje, pri čemu dolazi do smanjenja kolizionih i broadcast domena. Upotreba svičeva za potrebe segmentacije mreže se trenutno uprkos pristupačnosti ovih uređaja smatra neefikasnim i neekononičnim rješenjem budući da ne podržavaju fleksibilno upravljanje segmentima i ne ograničavaju broadcast domene. Njihovom upotrebom dolazi do ograničavanja kolizionih domena.

Upotreba VLAN-ova pri segmentaciji mreže konvergira sve prednosti dvaju prethodnih metoda svodeći kolizione i broadcast domene na nivo pojedinačnih uređaja, pri čemu pruža izuzetnu podršku dinamičnoj rekonfiguraciji postojeće LAN arhitekture. Uvrštavanjem samo 4 bajta informacija više u odnosu na VLAN neoznačeni frejm ostvaruje se značajno povećanje efikasnosti mreže preraspodjelom resursa dodijeljenih broadcast porukama.

VLAN mreže su izuzetno skalabilne i olakšavaju upravljanje u promjenjivim okruženjima gdje može doći do uključivanja novih hostova na mrežu ili isključivanja postojećih hostova sa mreže. Bez upotrebe VLAN-ova, ovakvi procesi bi tražili mnogo obimnije resurse ljudskog rada, promjenu postojeće arhitekture mrežnih uređaja i ponovno kabliranje radi konfigurisanja mreže po trenutnim zahtjevima. Koncept upotrebe virtuelnih lokalnih mreža nije bezbjednosno neprobojan sistem. Faktori rizika najčešće predstavljaju situacije poput imitiranja „Trunk“ sviča radi dobijanja pristupa svičevima van napadnute virtuelne lokalne mreže, višestruko dot1q označavanje pomoću kojih paketi podataka mogu da zaobiđu sigurnosne mehanizme i preskoče sa jedne VLAN na drugu, [6] ali kao i u svim oblastima bezbjednosti računarskih mreža, deviza stoji da nivo bezbjednosti mreže zavisi od količine uloženih intelektualnih i finansijskih sredstava i predstavlja konstantnu utrku između dvaju zaraćenih strana.

7. ZAKLJUČAK

Konstruisanje računarske mreže donosi mnogobrojne prednosti poslovanju svakom preduzeću. Budući da računarska mreža, kao najefikasniji vid čuvanja i dijeljenja podataka od važnosti za poslovanje preduzeća pruža mogućnosti da se povjerljive informacije čuvaju isključivo u elektronskom formatu i da se pristup takvim informacijama ograničava samo na osobe koje imaju privilegiju za to, stoga ona predstavlja veoma pogodnu metu pojedincima sa malicioznom namjerom.

Ovi pojedinci koristeći profesionalno znanje o funkcionisanju računarskih mreža ostvaruju mogućnost pristupa eventualno povjerljivim podacima preduzeća. Jedna od osnovnih barijera protiv ovakvih akcija jeste segmentacija mreže na virtuelne lokalne mreže i izmještavanje osjetljivih podataka van dostupnih krugova dometa subjektima koji ne posjeduju privilegiju da rukuju tim podacima.

Pored podizanja nivoa sigurnosti, korišćenje VLAN-ova poboljšava skalabilnost i efikasnost upravljanja mrežom, povećava se fluidnost saobraćaja i smanjuje zagušenje ograničavajući broadcast pakete na izolovane segmente umjesto njihovog preplavljivanja čitave mreže.

LITERATURA

[1] The Cisco Learning Network - Broadcast and a Collision Domains, DOC-30227 [Internet]. Dostupno na: https://learningnetwork.cisco.com/-docs/DOC-30227 [citirano 10.05.2018]

[2] IEEE Std 802.1Q-2011 - IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks, 2012.

[3] IEEE Standard for Ethernet, 802.3-2015, 2016., str. 108., ISBN 978-1-5044-0078-7

[4] ANSI/IEEE 802.1ad-2005 – IEEE Standard for Local and Metropolitan Area Networks, 2006.

[5] IEEE Standard for Local and metropolitan area networks, Virtual Bridged Local Area Networks – IEEE Computer Society, 2006.

[6] SANS Institute InfoSec – Virtual LAN Security: weaknesses and countermeasures [Internet]. Dostupno na: https://www.sans.org/reading-room/whitepapers/networkdevs/virtual-lan-security-weaknesses-countermeasures-1090 [citirano 10.05.2018]

SUMMARY

LOCAL AREA NETWORK SEGMENTATION MODEL

This paper conveys the basic aspects of designing and segmenting the local area network of a multisectoral enterprise. The main focus of the paper is centered around the practical work of creating and configuring independent virtual network segments within one physically connected computer network using the „Cisco IOS" command line interface. Practical steps of network configuration were simulated and represented by the virtualization software simulating the real world surrounding and interactions made between the network components. The structure of the protocols that shape the segmentation of a computer network to virtual local computer networks is presented as the most efficient segmentation method. The benefits of segmentation of the local computer network are explained. Special focus is given to the use of the Cisco IOS command language syntax as the most common programming language among network devices.

Key words: *Frame, dot1q, encapsulation, segment, Ethernet, collision domain*