KAKO POBOLJŠATI POSTOJEĆU MREŽNU INFRASTRUKTURU

Muharem Redžibašić, MA dipl. ing., email: r.muharem@gmail.com
Prof. dr. Mladen Radivojević; email: radivojevicmladen60@gmail.com
Internacionalni univerzitet Travnik u Travniku

Sažetak: S brzim razvojem tehnologije, mnogi poslovni procesi preneseni su na elektronsku obradu podataka što je podrazumijevalo i razvoj lokalnih mreža u mnogim firmama i organizacijama.Većina mrežnih infrastruktura razvijala se inkrementalno, proširivala se prema potrebama i u većini slučajeva to je bio ad-hoc pristup bez puno planiranja i brige o sigurnosti. Mrežni implementatori, uglavno nisu bili stručnjaci, tako da su česti problemi na mreži i sigurnosni rizici. Mnoge današnje mrežne infrastrukture imaju zastarjelu mrežnu opremu koja je konfigurisana na protokole koji su postali još nesigurniji, a fizička implementacija mreže je često jedna velika kolizijska domena. Ovaj rad će predstaviti pristup, tj. k možemo poboljšati postojeću mrežnu infrastrukturu i koji su ključni koraci u identificiranju slabih tačaka mrežne infrastrukture.
Ključne riječi: Mrežna infrastruktura, informacijska sigurnost, mrežna oprema, kolizijska domena, sigurnosni rizici

HOW TO IMPROVE EXISTING NETWORK INFRASTRUCTURE

Abstract: With the rapid development of technology, many business processes were transferred to the electronic processing of data which implied development of local networks in many companies and organizations. Most network infrastructures have been developed incrementally, spread to the needs and in most cases these was an ad-hoc approach without a lot of planning and review about security. Network implementers, generally, have not been professionals so failures on the network and security risks are often. Many of today's network infrastructures have obsolete network equipment which has configured protocols that have become more insecure and physical implementation of the network is often a big collision domain. This paper will present approach, i.e. How can we improve the existing infrastructure and what are the key steps in identifying the weak points of the network infrastructure.
Key words: Network Infrastructure, Information Security, Network Equipment, Collision Domain, Security Risks

1. Mrežna infrastruktura

Računarska mreža se može posmatrati kao komunikacijski sistem gdje se informacija generisana na jednoj strani dostavlja na drugu stranu. U ovom radu ćemo se uglavnom baviti lokalnim LAN (Local Area Network) mrežama koje svi imamo u našim kućama, firmama, institucijama.

Definicija koju ćemo izdvojiti prema Hrvatskoj akademskoj i istraživačkoj mreži CARNET je: *„Mrežu računala čini skupina međusobno povezanih računala. Mreže se mogu razvrstati prema veličini, načinu povezanosti, funkcionalnoj vezi i arhitekturi.“ (CARNet, 2009.)*

LAN mreže se koriste za povezivanje računara i ostalih mrežnih uređaja u cilju dijeljenja resursa (npr. Printera) i razmjene informacija putem mreže. [9]

Implementacija svake mreža mora proći kroz određene etape a to su najčešće: network design faza, faza implementacije mreže, dokumentacija mreže itd. Svaka mreža je sistem koji se sastoji iz određenih dijelova i koji se vremenom razvija. Postavlja se pitanje kada možemo reći da je proces implementacija mreže završen. Odgovor je nikada, mreža u svom životnom vijeku trpi konstantne modifikacije i proširenja te je svaku promjenu potrebno propratiti kroz navedene faze, zato je vrlo važno da pratimo nove trendove u tehnologiji i mrežama kako bi mogli na vrijeme prepoznati manjkavosti naše mreže i unaprijediti. Jako je bitno ako uspijemo spriječiti neke stvari na vrijeme prije nego postavljati sve iznova.

1.1. Faza dizajna mreže

Kada dizajniramo LAN mreže za srednja i velika preduzeća najbolje se odlučiti za troslojni hijerarhijski model. Hijerarhijski model podrazumijeva dijeljenje mreže u diskretne slojeve. Svaki sloj osigurava specifične funkcije koje definišu njegovu ulogu u cjelokupnoj mreži. Ovim se postiže modularan dizajn što na kraju rezultuje boljim performansama i većoj mrežnoj skalabilnosti.

Hijerarhijski mrežni model se sastoji iz 3 sloja, a to su:

1. Acces sloj (pristupni sloj)
2. Distribution sloj (distribucijski sloj)
3. Core sloj (jezgreni sloj)

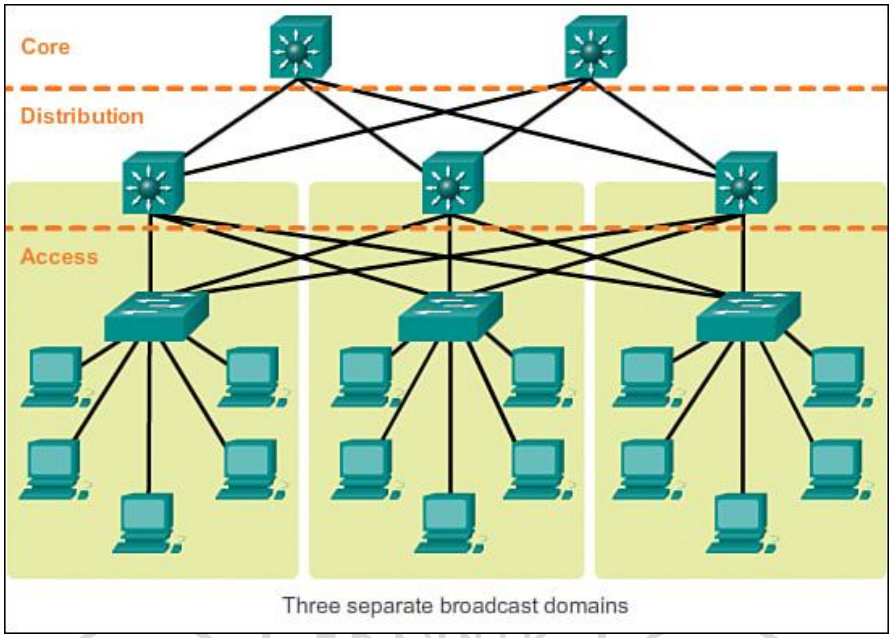
Primjenom ovog modela dobivamo mnogo prednosti kao što su prije svega **skalabilnost mreže** koja se odnosi na mogućnost jednostavne proširivosti sistema. Ako pogledamo sa slike ispod dovoljno je da se doda switch uređaj, spoji na distribucijski sloj i naša mreža je jednostavno proširiva – skalabilna.

Redudantnost – ova osobina je bitna pogotovo kada imamo mrežu koja pruža usluge za tzv. „mission critical„ aplikacije gdje je konektivnost imperativ. Redudantni linkovi osiguravaju alternativne linkove do destinacije tako da je mreža otporna na iznenadne padove dijelova mreže.

Sigurnost – troslojni hijerarhijski model nam omogućava da kreiramo određene sigurnosne politike na svakom od ovih slojeva. Sigurnost može biti implementirana na nivou portova, VLAN-ova[77], Access lista i sl.

Upravljivost – ovakve mreže su jednostavnije za upravljanje, potrebne intervencije možemo uraditi i fokusirati na pojedine dijelove ili na nivou određenog sloja bez utjecaja na ostatak sistema.

[77] Virtual Local Area Network, Virtual LAN – dijenačin za logičku segmentaciju mreže neovisno o fizičkoj topologiji mreže



Slika 1: Hijerarhijsko mrežni model [3]

Ukoliko dizajniramo našu računarsku mrežu kao jednu novu onda se svakako trebamo držati ovog modela, međutim ukoliko imamo slučaj da rekonstruišemo postojeću mrežu onda trebamo učiniti što je moguće više izmjena kako bi postojeće stanje približili ovom hijerarhijskom modelu isključivo radi prednosti koje smo gore spomenuli.

Jako je bitno pomenuti da je dokumentacija mreže dokument koji nastaje u trenutku dizajniranja mreže, dopunjava se elementima koji se odnose na implementaciju[78], sadrži informacije koje su obuhvaćene određenom klasom administriranja[79], i ostale informacije koje se odnose na funkcionalnost mreže. U zavisnosti od obima mreže može se koristiti papir, neki program sa automatskom podrškom za tablice, a ako je složenija mreža postoje čak i specijalizirana softverska rješenja. Dakle svaki podatak koji se odnosi na rad i funkcionisanje mreže treba biti dio mrežne dokumentacije. Dokumentacija je dokument koji se razvija i održava tokom životnog vijeka mreže. Na žalost danas u BiH ima jako malo kompanija koje se mogu pohvaliti sa mrežnom dokumentacijom. Ako dokumentacija nije ažurna može predstavljati veći problem nego da je uopšte nema jer korisnika te dokumentacije može dovesti do pogrešnih zaključaka.

1.2. Strukturno kabliranje

Pojava velikog broja različitih proizvođača mrežne opreme dovela je vremenom do potrebe definisanja standarda koji bi pokrili generalne aspekte umrežavanja. Skup standarda koji se odnose na

[78] Implementacija je faza kada se izvode radovi u cilju implementacije mreže koja je definisana u projektu. Obuhvata polaganje kablova, montažu konektora i spajanje na patch panele, označavanje kablova i utičnica, implementacija vodilica i kanalica za kablove, implementacija uzemljenja i sl.
[79] Sama administracija je definisana standardima ANSI/TIA/EIA 606-A. Ovaj standard definiše nekoliko klasa administracije, kolor kod terminacijskih područja, te označavanje, povezivanje i načine kreiranja izvještaja.

umrežavanje naziva se jednim imenom strukturnim kabliranjem. Strukturno (generičko) kaliranje obuhvata sve moguće vrste kabliranja.

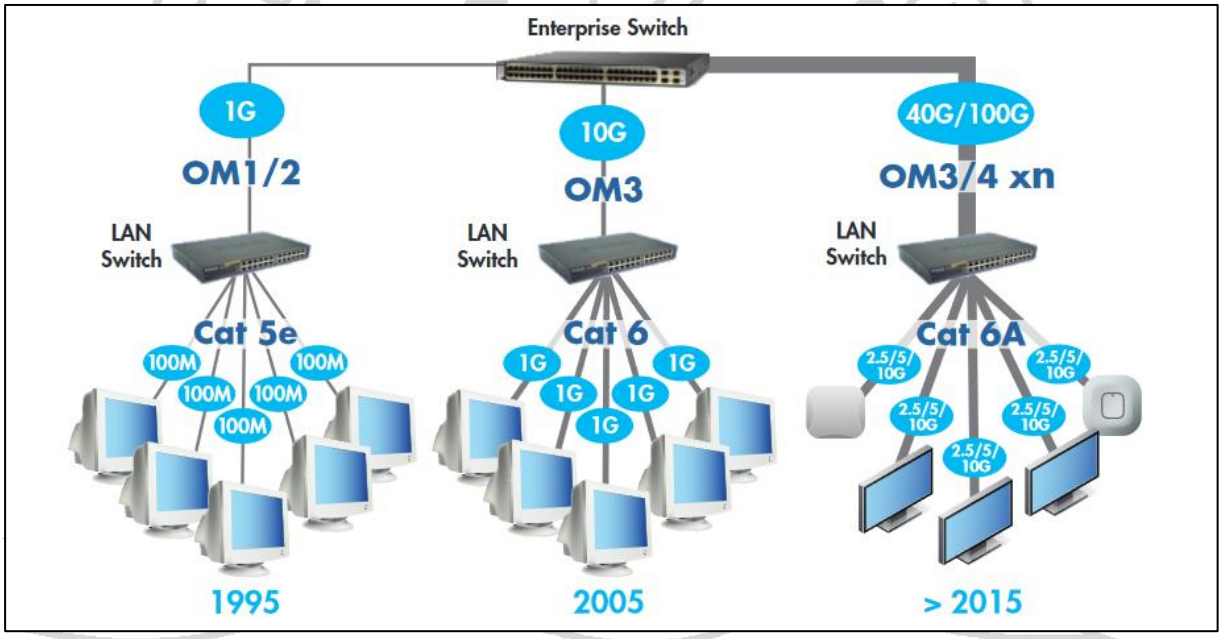
Svrha strukturnog kabliranja jeste uvesti pravila u planiranju i implementaciji računarskih mreža. Kao primjer navest ćemo strukturno kabliranje koje obuhvata zasićeno kabliranje (Saturated cabling) koja predviđa postavljanje dva priključka na svaka 2 – 3 m^2 radnog prostora. Ovaj pristup se koristi kod umrežavanja u objektima u kojima se ne zna tačan raspored računara i druge IT infrastrukture.

Strukturno kabliranje podrazumijeva crossconnections (čvorišta) i patch panels (prespojne ploče), a sve u cilju jednostavnog restruktuiranja računarske mreže

Standardi koji se odnose na strukturno kabliranje su:

- ISO / IEC IS11801 – međunarodni standardi
- EN 50173 – Evropski standardi [6]
- EIA / TIA 568 – Američki standardi

Vrlo je važno napomenuti da se pri kabliranju držimo jednog od standarda i poštujemo sve elemente strukturnog kabliranja gdje posebnu pažnju pridajemo **backbone kabliranju** gdje pomoću ove vrste kabliranja spajamo MDF[80] sa IDF[81]. Backbone kabliranje treba izvesti tako da se koristi mrežni mediji sa što većom propusnosti (npr. optički kablovi)



Slika 2: LAN kabliranje kroz vrijeme [4]

Radi poboljšanja postojeće mrežne infrastrukture trebamo analizirati stanje naše mreže te ukoliko imamo resursa svakako popraviti propusnost na tom dijelu mreže.

[80] Main distribution facilities (po evropskim standardima Building distribution)
[81] Intermedia Distribution Facilities (po evropskim standardima Floor distribution)

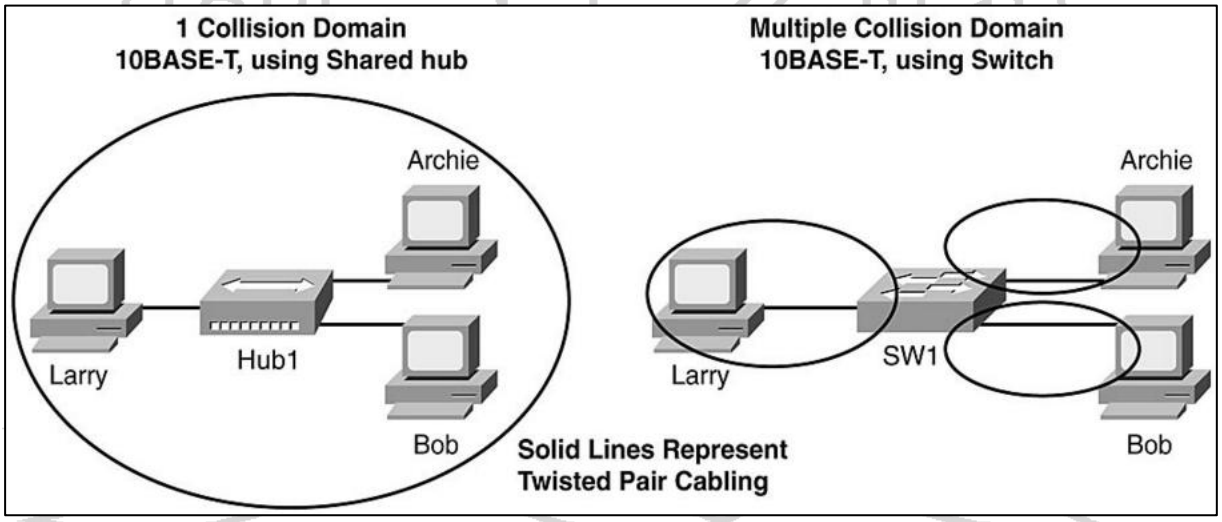
2. Koraci za poboljšanje mrežne infrastrukture

U ovom poglavlju će biti obrađene neke od ključnih stvari na koje trebamo paziti pri sagledavanju neke mrežne infrastrukture, bilo da pravimo novu ili rekonstruišemo postojeću. Stvari obrađene u ovom poglavlju ustvari će predstavljati ključne stvari na koje treba obratiti pažnju u cilju poboljšanja ili identificiranja slabih tačaka određene mrežne infrastrukture.

2.1. Kolizijska domena

Kolizijska domena je dijeljeni mrežni segment gdje može doći do kolizije, odnosno područje mreže koje bi bilo pogođeno pojavom kolizije. Kada govorimo o uređajima prvog sloja (OSI referntnog modela)[82], takvi uređaji zbog načina djelovanja, pojačavanja signala i njegovog prosljeđivanja, povećavaju kolizijsku domenu. Uređaji drugog nivoa rade segmentaciju (djeljenje) kolizijske domene te imaju jako dobru osobinu, a to je segmentacije kolizijske domene. Switch s druge strane radi mikrosegmentaciju, gdje svaki port na switchu i svaki uređaj spojen na switch, predstavljaju zasebnu kolizijsku domenu, a ako je u pitanju full duplex komunikacija, onda je to collision less okruženje, okruženje bez mogućnosti da dođe do kolizije.

Upravo zbog ove karakteristike switch je skoro u potpunosti izbacio upotrebu hub-ova u računarskim mrežama.



Slika 3: Kolizijske domene [2]

U praksi bi ovo značilo da gdje god imamo *hub* uređaj, iste zamijenimo sa *switch* uređajem, to nije velika investicija ali po pitanju performansi naše mreže je jako značajno.

[82] Open Systems Interconnection Basic Reference Model je apstraktni i slojeviti model koji služi kao preporuka stručnjacima za razvoj računarskih mreža i protokola

2.2. IP adresiranje i podmreže

IP adresa nam omogućava jedinstvenu identifikaciju hosta na mreži. Bez odgovarajuće adresne šeme komunikacija između računara ne bi bila moguća. Da bi se lakše upravljalo adresama, sve adrese su podijeljene u određene klase IP adresa. U originalnoj Internet routing shemi razvijenoj 1980 godine, IPv4 adrese su podijeljene u 5 klasa. U pitanju su A klasa, B klasa, C klasa, D klasa i E klasa. Posljednje dvije klase su klase specijalne namjene, te se rjeđe koriste.

Uglavnom u institucijama i organizacijama imamo loše urađeno adresiranje sa bespotrebnim gubitkom IP adresa, da bi to izbjegli potrebno je koristiti podmreže (subnetiranje). Kada govorimo o subnetiranju to znači da jednu cijelu klasu (A, B, C) podijelimo u nekoliko manjih te na taj način minimiziramo gubitak IP adresa. Subnetiranje prepoznajemo po tome što se od host dijela određeni biti dodjeljuju network dijelu. Da li je neka mreža subnetirana najbolje vidimo po subnet masci, ako je vrijednost subnet maske drugačija od default-ne, onda se može reći da imamo subnetiranu mrežu.

Subnetiranje omogućava administratoru da određenu mrežu podijeli u nekoliko manjih kako bi ispunio zadatak adresiranja uređaja u mreži.

Ukoliko našu mrežu izdijelimo na podmreže time ćemo dobiti mnoge koristi, kao npr.

- smanjit ćemo mrežni saobraćaj
- optimizirati mrežne performanse
- olakšati uočavanje i rješavanje mrežnih problema
- povećati mrežnu sigurnost

2.3. Ažuriranje firmware-a

Firmware je program koji se trajno ugrađuje u hardverski uređaj kao što su routeri. Programiran je da daje stalne upute za komunikaciju s drugim uređajima i obavlja funkcije kao što su osnovni ulazni / izlazni zadaci. Firmware se obično pohranjuje u flash ROM-u (samo za čitanje memorije) hardverskog uređaja. Može se izbrisati i prepisati. [5]

Firmware je izvorno dizajniran za softver visoke razine i može se mijenjati bez zamjene hardvera za noviji uređaj. Firmware također zadržava osnovne upute za hardverske uređaje koji ih čine operativnim. Bez firmware-a, hardverski uređaj bi bio nefunkcionalan. [7]

Ažuriranje firmware-a „flashing“ uključuje prepisivanje postojećih firmware-a ili podataka, sadržanih u EEPROM ili flash memorijskim modulima prisutnim u elektroničkom uređaju s novim podacima. [10]

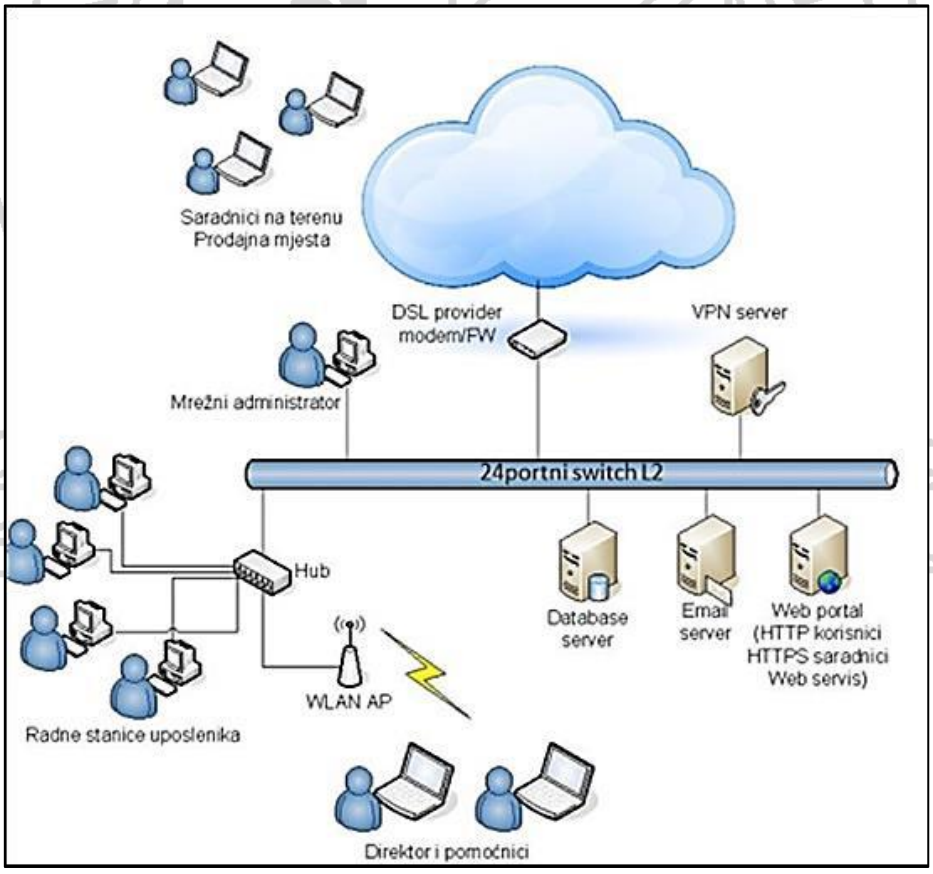
Neki firmware se ne mogu prepisati dok su drugi nadogradivi, što znači da je moguće nadograditi firmware uređaja spajanjem na računar u određenoj konfiguraciji, a zatim pokrenuti software proizvođača. Taj se proces naziva "flashing firmware“ ili jednostavno

"flashing". To postaje neophodno kada uređaj postane inkompatibilan sa novijim operativnim sistemima ili jednostavno kada trebamo poboljšati performanse uređaja.[8]

Ukoliko uzmemo za primjer mrežne uređaje kao što su routeri i modemi jako je bitno da provjerimo na službenoj web stranici proizvođača koja je posljednja verzija firmware-a dostupna i uporedimo sa našom trenutnom verzijom na uređaju. Ukoliko ima dostupna nova verzija obavezno trebamo nadograditi svoju postojeću. Prije nadogradnje uvijek se preporučuje da se snimi rezervna kopija postojećeg firmware-a i konfiguracije uređaja te ukoliko bi se desio neki problem da isto možemo vratiti u prvobitno stanje. Nadogradnja fimware-a se uglavnom izvodi radi poboljšanja performansi ali ukoliko su u pitanju mrežni uređaji onda je jako bitno da se to učini i radi aspekta sigurnosti istih. Često neki uređaji sa starijim verzijama firmware-a postanu ranjivi na određene maliciozne tipove koda te u cilju zaštite i prevencije da se ne desi nešto neočekivano sa velikim posljedicama na našoj mreži trebamo raditi ažuriranje firmware-a na zadnju dostupnu sigurnu verziju.

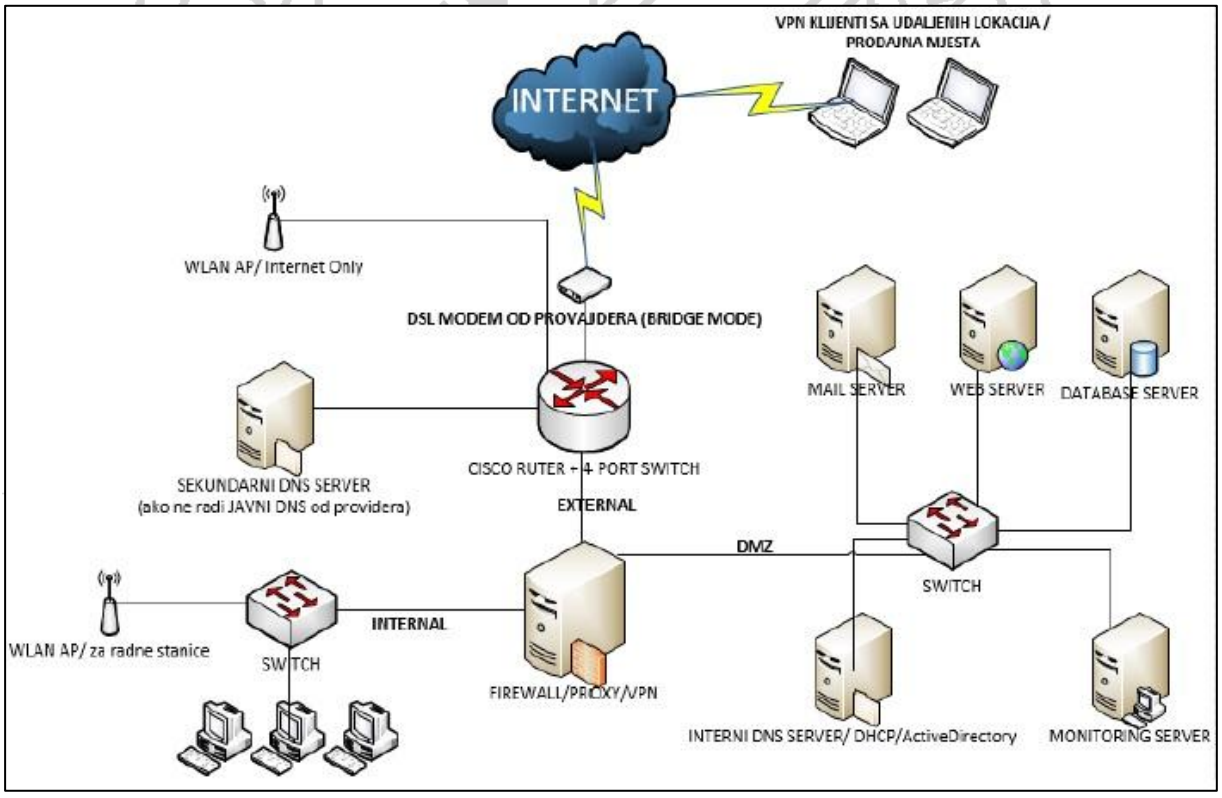
3. Primjer iz prakse

U ovom dijelu ćemo predstaviti jedan tipičan mrežni dijagram gdje je računarska mreža nastajala inkrementalno, a u nastavku ćemo predstaviti rekonstruisan mrežni dijagram sa prijedlozima za poboljšanje.



Slika 4: Primjer slabe mrežne infrastrukture(izvor: autori)

Ukoliko bolje pogledamo prethodnu sliku na prvi pogled možemo uočiti mnoge nedostatke. Prije svega možemo da uočimo hub uređaj koji proširuje kolizijsku domenu i koji je jako spor. Dakle, radi smanjenja potencijalnog broja kolizija, hub uređaj trebamo da zamijenimo sa switch uređajem čime ćemo povećati broj kolizijskih domena, a smanjiti broj potencijalnih kolizija u mreži i samim tim dobiti na brzini. Nadalje da se primijetiti da se korsiti DSL modem od providera koji je ujedno i ruter. Za profesionalniji pristup potrebno je da se uređaj zadrži od providera ali da se na njemu koristiti samo funkciju modema, ostale servise i postavke raditi na drugim sofisticiranijom uređajima sa više mogućnosti i većim kvantitetom memorije kao što je zaseban ruter. Time ćemo postići osim sigurnosti, performansi dobiti i osobinu skalabilnosti koja je propisana hijerarhijskim mrežnim modelom opisanim u prvom poglavlju ovog rada. Također je jako uočljivo da se serveri, uposlenici, administratori i svi ostali nalaze u istoj podmreži. Sa aspekta sigurnosti to nije zadovoljavajuće te se predlaže da se postavi sigurnosni mrežni uređaj (firewall) te da se odvoje podmreže prema tipu opreme i korisnika koji se nalaze u istim. Također za bežični pristup postoji samo jedna bežična pristupna tačka (access point) što se smatra sigurnosnim propustom jer se svi spajaju putem iste pristupne tačke. Obzirom da je potrebno da odvojimo različite tipove korisnika u različite podmreže, dobar potez bi bio da se ugradi još jedna bežična pristupna tačka (access point) koja će služiti samo za posjetioce/goste te će biti odvojen pristup od interne mreže.
Nakon svega opisanog možemo predstaviti poboljšan dijagram mrežne infrastrukture.



Slika 5: Primjer poboljšane mrežne infrastrukture(izvor: autori)

ZAKLJUČAK

Obzirom da nam je jasno da mnoge današnje mrežne infrastrukture imaju zastarjelu mrežnu opremu sa fizičkim implementacijama mreže koje su dosta loše i vrlo često jedna velika kolizijska domena..

Od same faze dizajna mreže jasno je da se treba držati troslojnog hijerarhijskog modela mrežne infrastrukture. Ukoliko imamo situaciju da rekonstruišemo postojeću mrežnu infrastrukturu onda ćemo nastojati da uradimo stvari koje će što više pribjegavati hijerarhijskom modelu mrežne infrastrukture. Također velika važnost je usmjerena i na strukturno kabliranje gdje je mnogo bitno da se stvari rade po unaprijed definisanim standardima i da se uradi kvalitetna mrežna dokumentacija gdje svaki podatak koji se odnosi na rad i funkcionisanje mreže treba biti dio mrežne dokumentacije.

Za nesmetano funkcionisanje računarske mreže jako je bino da se smanji područje mreže koje bi moglo biti pogođeno pojavom kolizije. Ovo možemo postići na način da zamjenom mrežnih uređaja povećavamo broj kolizijskih domena i samim tim smanjujemo područje mreže koje bi moglo biti pogođeno pojavom kolizije.

Također radi optimizacije mrežnih performansi i povećanja sigurnosti potrebno je da uradimo kvalitetno IP adresiranje u našoj mreži. Jedan od načina postizanja tih ciljeva jeste uvođenje podmreža (subnet-a). Povećanje sigurnosti također možemo postići adekvatnim praćenjem verzija firmware-a na mrežnim uređajima i njihovim ažuriranjem.

Kroz ovaj rad smo identifikovali ključne stvari vezane za stvaranje kvalitetne mrežne infrastrukture i predložili korake koje bi trebali da budu primarni ukoliko želimo poboljšati postojeću mrežnu infrastrukturu.

LITERATURA

[1] CARNet Hrvatska akademska i istraživačka mreža, (2009.), „Sigurnosni model mreže računala“, str. 6
[2] CCIE Study Blog (2016.), „Ethernet: Collision Domains and Switch Buffering“, https://bethepacketsite.wordpress.com/2016/02/10/ethernet-collision-domains-and-switch-buffering/ pristupljeno 08.11.2018. godine
[3] Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design (2018.), Article 2014., http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4, pristupljeno 30.10.2018. godine
[4] COMMSCOPE White Paper (2015.), „Fiber Backbone Cabling in Buildings“https://gfoeurope.it/download-news/8/fiber-backbone-cabling (strana 3), pristupljeno 28.11.2018. godine

[5] Halonja A, Milica M, (2009.) „Računalni nazivi sa elementom –WARE u engleskome i hrvatskome jeziku“, Rasprave Instituta za hrvatski jezik i jezikoslovlje
[6] Službena Internet stranica Instituta za standardizaciju Bosne i Hercegovine (2018), http://www.bas.gov.ba/standard/?natstandard_document_id=306061 pristupljeno 02.11.2018. godine
[7] Službena Internet stranica od TACHOPEDIA, (2018.), https://www.techopedia.com/definition/2137/firmware, pristupljeno 25.10.2018. godine
[8] Službena Internet stranica TECH-FAQ (2018.), „Flashing Firmware“, http://www.tech-faq.com/flashing-firmware.html, pristupljeno 12.11.2018. godine
[9] Tanenbaum A., Wetherall D., (2013.) „Computer Networks“, fifth edition, University of Washington , str. 19
[10] Wikipedia slobodna enciklopedija (2018.), https://en.wikipedia.org/wiki/Firmware, pristupljeno 29.11.2018. godine