



FAKULTET INFORMACIONIH TEHNOLOGIJA RAČUNARSKI SISTEMI I MREŽE

PROJEKAT UGRADNJE MREŽE U MALIM I SREDNJIM PREDUZEĆIMA

Predmet: **Završni rad**

Mentor: Prof. Dr. Mladen Radivojević

Student:
Vahid Bilić
FIT-15/15-I

Travnik, juli 2019.

SADRŽAJ

1.	UVOD	4
2.	DIZAJN MREŽE	5
2.1.	JEDNOSTOVNA MREŽNA TOPOLOGIJA	6
2.2.	MAGISTRALA TOPOLOGIJA.....	7
2.3.	HIJERARHIJSKA TOPOLOGIJA MREŽE	8
3.	SIGURNOST MREŽE.....	9
3.1.	SIGURNOST.....	9
3.2.	OSIGURANJE RAČUNALNE MREŽE.....	11
3.3.	ANTI-VIRUSI	11
3.4.	KRIPTIRANJE.....	12
3.5.	PRIJETNJE PO MREŽU	12
3.5.1.	LJUDSKA POGREŠKA	12
3.5.2.	PRIRODNI UZROCI	13
3.5.3.	VIRUSI	13
3.5.4.	SPAM	13
4.	WLAN and LAN	13
4.1.	TOPOLOGIJA DIZAJN I IMPLEMENTACIJA	13
4.2.	IP ADRESIRANJE	15
4.3.	PROTOKOL USMJEREVANJA.....	16
4.4.	VLANs.....	16
4.5.	NAT/PAT.....	17
4.6.	DHCP	17
4.7.	IZBOR UREĐAJA	19
4.8.	KONFIGURACIJA PC.....	20
4.9.	SIGURNOSNA KONFIGURACIJA.....	20
5.	POSTAVLJANJE MREŽE	21
5.1.	KONFIGURACIJA UREĐAJA I SISTEMA.....	21
5.2.	FIZIČKA TOPOLOGIJA	21
5.3.	HARDWERSKI ZAHTJEVI I KONFIGURACIJA	22
5.3.1.	RAČUNALO RADNE STANICE	24

5.3.2.	KONFIGURACIJA	25
5.3.3.	KONFIGURACIJA NIC.....	26
5.3.4.	SERVER.....	26
5.3.5.	KONFIGURACIJA SERVERA.....	26
5.3.6.	MREŽNI PRINTER	27
5.3.7.	KONFIGURACIJA MREŽNOG PRINTERA	27
5.3.8.	ADSL MODEM.....	27
5.3.9.	BACKUP.....	28
5.3.10.	UPS	28
5.3.11.	VENTILATORI ZA HLAĐENJE.....	28
5.3.12.	ORMARIĆ	29
5.4.	SOFTWERSKI ZAHTJEVI I KONFIGURACIJA	29
5.4.1.	SISTEMSKI SOFTWER	29
5.4.2.	APLIKACIJSKI SOFTWER	29
5.5.	INSTALACIJA SISTEMSKOG SOFTWERA WINDOWS 7 NA HOSTOVE.....	30
5.6.	INSTALACIJA WINDOWS SERVERA 2008 R2.....	33
5.7.	MREŽNA PROTOK (BANDWICH)	35
5.7.1.	IZRAČUN KOLIČINE PROTOKA PODATAKA	36
6.	PLANIRANJE LAN ADRESIRANJA ZA MALA PREDUZEĆA.....	36
6.1.	IP ADRESIRANJE	37
6.2.	TESTIRANJE KONEKCIJE.....	39
7.	ZAKLJUČAK	42
8.	LITERATURA.....	43

1. UVOD

U današnjem međusobno povezanom svijetu je naivno vjerovati da je sistem računarske mreže zaštićen i stabilan pored svih izazova sa kojim se susrećemo u današnjem svjetu. Većina vlasnika preduzeća misli da njihove mreže nisu ranjive vanjskim utjecajima pod izlikom da su oni još mala firma i da nikom nisu posebno zanimljivi. S druge strane imamo direktore preduzeća koji ulažu u svoju računarsku mrežu jer znaju da je to jedan od najbitnijih resursa u današnjem preduzeću koji održava stabilnost u radu. Svrha ovo projekta je da dizajniramo lokalnu mrežu (LAN) za malu kompaniju i da tu mrežu implementiramo i zaštitimo njene resurse. Svako preduzeće danas potrebu za stabilnom unutrašnjom mrežom koja neizostavan dio današnjeg posla.¹ Obzirom da se sva komunikacija pretežno obavlja preko e-maila da se podacima pristupa preko interneta itd. Projekat ugradnje i implementacije mreže je proces koji ne zahtjeva mnogo vremena niti novca a dugorčno je dobit velika. Raspored našeg projekta ce teći idućim rasporedom.

- ISPITIVANJE ZAHTJEVA KORISNIKA -7 DANA
- ANALIZA MREŽE- 20 DANA
- DIZAJNIRANJE MREŽE – 15 DANA
- KONFIGURACIJA MREŽE- 19 DANA
- TESTIRANJE MREŽE- 5 DANA
- IMPLEMENTACIJA MREŽE- 5 DANA
- PUŠTANJE U RAD MREŽE- 1 DAN

¹ Cisco, Inter-Switch Link and IEEE 802.1Q Frame Format,Cisco, Tech. Rep

2. DIZAJN MREŽE

Danas većina preduzeća gradi vlastitu LAN infrastrukturu s posebnom paznjom na sigurnosne mjere kako bi zaštitili svoje resurse od neovlaštenih pristupa. Projektovanje sigurne i stabline mreže zahtjeva projektovanje mrežne topologije prije odlučivanja koje ćemo uređaje i tehnologije koristiti za implementaciju. **Topologija mreže** određuje raspored mrežnih uređaja. Četiri najpoznatije LAN topologije su: *magistrala, zvijezda, prsten i razgranata*.

Ove topologije su logičke arhitekture što ne znači da se uređaji moraju fizički identično organizovati. U osnovi, projektovanje mreže je jedna od četiri faze PDIUO (Planiranje Dizajna, Implementacija, Upravljanje, Optimizacija).

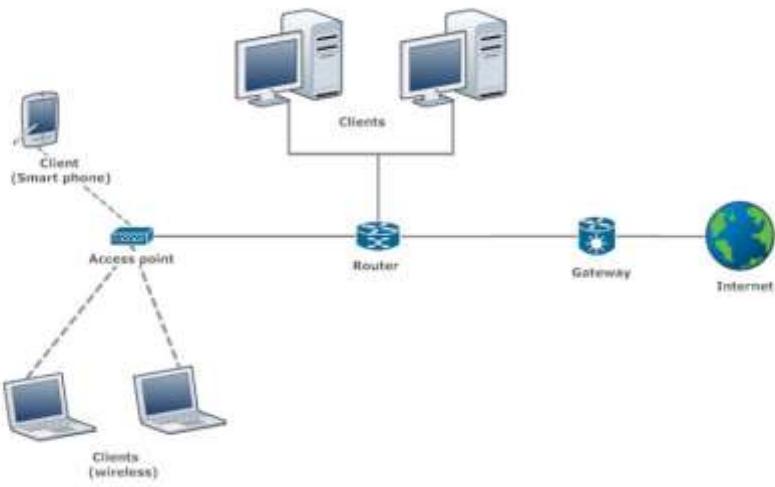
U ovoj fazi životnog ciklusa mreže, zadatak dizajnera će biti razvoj fizičkog i logičkog dizajna projekta mreže. Fizički dizajn mreže se bavi identifikacijom LAN i WAN tehnologija i mrežnih uređaja koji treba da ostvare performanse logičkog dizajna u cjelini. Tokom ove faze, projektant mreže je odgovoran za odabir uređaja poput kablovske žice, prekidača, mostova, rutera, AP i drugi. Kao što vidimo, logička faza projektovanja je temelj za fizičku mrežu, dizajner razvija hijerarhijsku i modularnu mrežu.²

Ova faza uključuje projektiranje adresiranja mrežnog sloja, izbor protokola za komutiranje i usmjeravanje, planiranje sigurnosti i dizajn upravljanja mrežom. Takođe složenost topologije zavisi od veličine mreže i karakteristika prometa.

² Cisco Systems, Inc. 2004. Cisco IOS Network Address Translation. PDF file

2.1. JEDNOSTOVNA MREŽNA TOPOLOGIJA

U slici ispod možemo da vidimo kako izgleda jednostavna mrežna topologija koja možemo da iskoristimo i kao pojašnje i opis svakog uređaja u topologiji.



Slika 1
Jednostvana
mrežna
topologija

Klijent: Je

zadnji korisnik

mreže može da bude racunčar ili mobitel itd. Uredzaj koji šalje zahtevе za podacima u mreži u koji ih dobiva.

Router je računarski uređaj koji služi za međusobno povezivanje računarskih mreža. On ima funkciju da za svaki paket podataka odredi putanju - rutu kojom treba taj paket da ide i da taj isti paket proslijedi sljedećem uređaju u nizu.³

Acces point: je uređaj koji omogućava bežičnim uređajima priključivanje na računalnu mrežu koristeći Wi-Fi, Bluetooth ili neki drugi bežični standard. BPT obično se uključuje u usmjerivač ako se želi omogućiti pristup žičanoj mreži, i koristi se kao relej za druge bežične uređaje unutar radijusa dometa BPT-a.

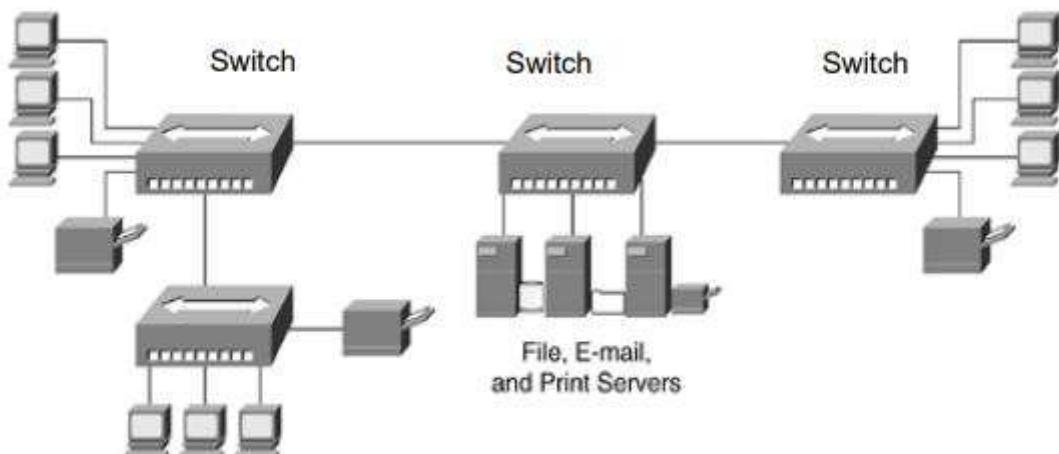
Gateway: je hardverski uređaj čija osnovna uloga je prevođenje iz jednog protokola u drugi protokol, odnosno vrši prilagođavanje električnog signala jednog protokola u električni signal drugog protokola. Sama definicija Gateway-a bila bi da je to mesto na mreži koje služi kao ulaz na drugu mrežu. Mogu biti i softverskog tipa kada su implementirani u ruter uređaje ili kombinacija hardversko-softverskog uređaja. Za razliku od ruteru koji prosleđuju pakete najkraćom putanjom za njima poznate protokole, Gateway uređaji poznaju različite protokole na osnovu čega rade prevođenje iz jednog u drugi protokol. Najpoznatiji Gateway uređaji su PSTN modem, ADSL modem, kablovski modem, itd. Kada je softverska verzija Gateway-a u

³ <https://mrezniredjaji.wordpress.com/>

pitanju može biti primenjena kroz računare, servere ili mrežne uređaje što je i najčešći slučaj kada su u pitanju poslovne ili enterprise konekcije. Zbog toga računar (ili server ili mrežni uređaj), koji je konfigurisan da radi kao Gateway uređaj, nazivamo i Default Gateway.

2.2. MAGISTRALNA TOPOLOGIJA

Magistralna topologija mreže je nestrukturirani tip mreže koja projektuje topologiju, koja je adekvatna za dizajniranje male mreže. To je nehijerarhijski model dizajniranja mreže gdje svaki inter-mrežni uređaj obavlja isti zadatak. Ovaj model je jednostavan za planirati, dizajnirati i implementirati u malim mrežama, kada bi došla potreba za rastom mreže došlo bi to poteškoća i može da dođe do toga da mreža ne funkcioniše ispravno osim toga manjak hijerarhije otežava mogućnost održavanja i proširenja mreže.



Slika 2 prikazuje dizajn mreže magistralne topologije

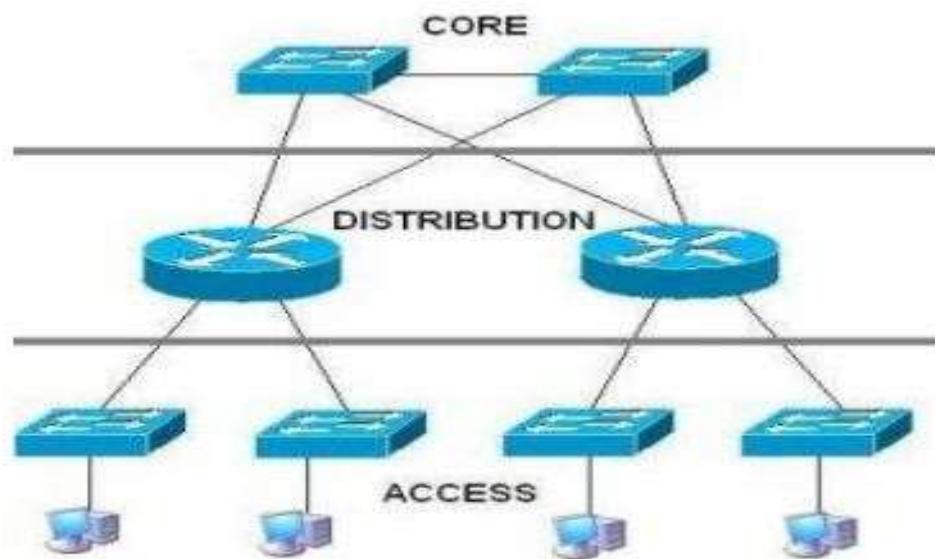
Dizajn prikazan na slici 2 sastoji se od radnih stаница, štampačа, servera i switch koji pripadaju istoj emitovanoj domeni i dijele istu širinu pojasa zajedno.⁴ Magistralna topologija koristi proces kontrole pristupa medijima kao što je višestruki nosac detekcija sudara pristupa (CSMA / CD) ili tehnologija propuštanja tokena za kontrolu propusta podataka. Nepostojanje modularnosti u magistralnoj mrežnoj topologiji dolazi do toga da svim mrežnim uređajima u

⁴ IEEE Computer Society. LAN/MAN Standards Committee, Institute of Electrical and Electronics Engineers, and IEEE-SA Standards Board, IEEE standard for information technology telecommunications and information exchange between systems : local and metropolitan area networks specific requirements. Part 11, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. New York: Institute of Electrical and Electronics Engineers, 2012. [Online]. Available: <http://ieeexplore.ieee.org/servlet/opac?punumber=6178209>

istoj podmreži da primaju prima kopiju svake poslane poruke.Osim toga, u slučaju kvara veze je teško dobiti alternativni put do odredišta.

2.3. HIJERARHIJSKA TOPOLOGIJA MREŽE

Kao što je objašnjeno u odeljku 2.2, kada mreža raste i postaje sve veća i kompleksnija; model magistarlane topologije mreže ne bi funkcionirao.Zbog toga projektanti mreže pribjegavaju rješenju izgradnje modularne mreže. Modularno projektiranje pomaže da se podjeli ogroman i složen zadatak specifičnom funkcijom i napravi dizajn koji je više upravlјiv. Na primjer, mrežni sistem kompanije može uključivati:LAN-ovi kompanije, sistem daljinskog pristupa, sistem bežične veze i WAN funkcionalnosti, u takvom scenariju hijerarhijske metode modeliranja dobro se uklapaju.U osnovi, hijerarhijski model je troslojna tehnika modularnog i strukturnog projektovanja koji se koristi za dizajniranje LAN ili WAN mreže. Takav model dizajna pomaže da se izgradi mreža kompanije u diskrette slojeve koji se sastoje od mnogih međusobno povezanih komponenti. Tehnički gledano, hijerarhijski dizajn modela ima tri sloja, sloj jezgre ,distributivni sloj i sloj pristupa, kao što je prikazano na slici 3 ispod. Svaki sloj ima svoje funkcije i oni su izgrađeni pomoću mrežnih uređaja kao što su ruteri ili switch.



Slika 3 Hjerarhijski model mreže

Postoje mnoge prednosti u korištenju hijerarhijskog modela dizajniranja mreže,među onima koji donose uštedu troškova, skalabilnost, fleksibilnost, prilagodljivost, jednostavnost, poboljšanje izolacija kvarova i jednostavnije upravljanje mrežom.

SLOJ JEZGRE:

Sloj jezgre je glavna osnovica i treba da bude dizajnirana da sto brže prebacuje pakete. Ovaj sloj mreže ne treba da provodi bilo kakave manipulacije sa paketima kao sto su pristupanje listama ili filtriranje koji bi mogli da uspore prebacivanje paketa.

DISTRIBUTIVNI SLOJ:

Distributivni sloj mreže je točka razgraničenja između slojeva pristupa i jezgarE i pomaže definirati i razlikovati jezgru. Svrha ovog sloja je da obezbjedi definiciju granica i mjesto na kojem se može izvršiti manipulacija paketima. U okruženju kampusa, sloj distribucije može uključivati nekoliko funkcija, kao što su sljedeće:

- Agregacija adrese ili područja
- Pristup odjeljenja ili radne grupe
- Definicija domene emitovanja / multicast domena
- Rutiranje virtualnog LAN-a (VLAN)
- Bilo kakvi medijski prijelazi koji se trebaju pojaviti
- Sigurnost

U okruženju bez kampusa, distribucijski sloj može biti točka preraspodjele između domena usmjeravanja ili razgraničenja između statičkih i dinamičkih protokola usmjeravanja. To može biti i točka na kojoj s udaljene lokacije pristupaju korporativnoj mreži. Sloj distribucije se može sažeti kao sloj koji obezbeđuje politiku povezivanja

3. SIGURNOST MREŽE

3.1. SIGURNOST

Ljudi u društvu naučili su da čuvaju svoje skladište gdje čuvaju svoju imovinu i vrijedno blago. Odsutnost takve sigurnosti može uzrokovati gubitak imovine. Isto tako, računalne resurse treba zaštititi iznutra i izvana od uljeza ili sabotera. Jedini način osiguravanja kompletног računarnog sustava je ograničavanje svih fizičkih i logičkih pristupa sustavu. Očito, ukupno razdvajanje računala jednog od drugog stvara sigurnu zonu; no na drugu stranu sustav gubi podatkovnu komunikaciju, što sustav čini beskorisnim.⁵

⁵ <http://www.saylor.org/site/wp-content/uploads/2012/02/Computer-NetworkingPrinciples-Bonaventure-1-30-31-OTC1.pdf> Referred 18.11.2016.

Kao što je nam poznato, računalo je korisnije kada je dio mrežnog sustava. Umreženo okruženje pomaže povećati produktivnost čovjeka, kao i stvoriti pogodno okruženje za napredak tvrtke na globalnoj razini. Međutim, važno je poduzeti neke sigurnosne mjere kako bi se smanjilo ili, ako je moguće, izbjegli sigurnosni rizici uzrokovani neovlaštenim pristupom resursima i uslugama sustava koji mogu ugroziti produktivnost i napredak tvrtke.

Tvrtke neumorno rade kako bi povećale zaradu. Za to koriste najbrže načine komunikacije. Danas je internet najjeftiniji, najbrži i najlakši način komunikacije za vođenje poslovanja na globalnoj razini. Internet je promijenio način kako ljudi žive i rade i čak je i revolucionirao način poslovanja. Osim toga internet nije sigurno okruženje a samim i time mreža koja je spojena na interneta bez odgovarajuće zaštite čini veliki rizik za sigurnost resursa i imovine .

Prijetenje ne dolaze samo izvana već i iznutra npr od sadašnjih i bivših uposlenika kompanije.Zato kompanija u današnje vrijeme mora da implementira efekтивне sigurnosne mjere da bi zaštitili svoje mrežne resurse od napada.U ovom trenutku vrijedi definisati sta je sigurnost mreže;postoji mnogo definicija sta je sigurnost mreže al jedna od preciznijih po mom mišljenju je: da sigurnost mreže znači osigurati konzistentnost i funkcionalnost sustava, te integritet i pouzdanost podataka, a zaštita mreže znači zaštitu od aktivnosti nedobronamjernih osoba koji mogu, ali ne moraju biti ovlašteni korisnici resursa lokalne mreže, kao i od nedovoljno upućenih ili neobrazovanih korisnika čije pogreške mogu na bilo koji način ugroziti rad sustava.⁶

Glavni razlog za implementaciju mrežne sigurnosti je osiguranje mreže i sustava i resursa povezanih s mrežom. Informacije u bilo kojem obliku smatraju se vrijednim podacima mreže i gubitk ili curenje informacija može dovesti kako do finacijski tako i drugi gubitaka.Uvođenje sigurnosnih kontrola u mreženom okruženju omogućuje mreži kako bi ispravno funkcionirala kako je dizajnirana. Zbog toga, tvrtke, vlade i druge organizacije su dale prednost mrežnoj sigurnosti i potrošile milijarde eura na planiranje i uvođenje novih tehnologija.

U današnjem otvorenom okruženju, organizacije koje žele pružiti javni pristup mrežnim resursima trebaju analizirati sigurnosne prijetnje koje mogu rezultirati napadom na sustav. U ovom trenutku, vrijedi podsjetiti da se napad može dogoditi iznutra mreže od strane pouzdanih

⁶ <http://www.saylor.org/site/wp-content/uploads/2012/02/Computer-NetworkingPrinciples-Bonaventure-1-30-31-OTC1.pdf> Referred 18.11.2016.

radnika. Sigurnosni analitičar je zabrinut o otkrivanju bilo kakvih ranjivosti i napada koji bi mogli uzrokovati prijetnje za djelovanja sustava, ali i opstanka tvrtke.

3.2. OSIGURANJE RAČUNALNE MREŽE

Kao čovjek uvijek smo imali potrebu zaštite osjetljivih podataka, a time i dokumenata s takavim podacima. Tokom historije razvijeno je mnogo metoda kojima su ljudi pokušavali i uspijevali očuvati tajnost važnih podataka. Mnoge metode su bile jednostavne i nisu pružale dovoljnu zaštitu. U takvim slučajevima tajnost je često bila narušena. Razvojem nauke kriptografije i modernih tehnologija otkriveni su vrlo dobri načini kriptovanja i zaštite dokumenata. Kriptiranje je dobar način sprječavanja neovlaštene osobe od pregledavanja sadržaja osjetljivog dokumenta. Ali kada se dokument dekriptira tajnim ključem, ovlaštena osoba loših namjera može spremiti, kopirati, ispisati ili prosljediti dokument.⁷

Ograničavanje pristupa dokumentu nekolicini pojedinaca jedan je od pristupa zaštite dokumenta, no uvijek postoji mogućnost da jedna od osoba kojoj je povjeren pristup oda podatke. U tom slučaju treba se pronaći osobu koja je odala informacije, što nije uvijek jednostavan zadatak. Rješenje koje osigurava zaštitu osjetljivih informacija ne može ovisiti o samo jednoj tehnologiji. Mnogi sigurnosno zaštitni mehanizmi, ko sto su anti-virusni programi, protokoli sigurnosti mreža računala (npr. IPSec), kontrola pristupa, kriptiranje, vodeni žigovi, mogu se upotrijebiti za zaštitu dokumenata. No efikasna zaštita ne primjenjuje samo jedno rješenje, već kombinaciju spomenutih metoda zaštite.

3.3. ANTI-VIRUSI

Antivirusni softver, antivirusni program ili antivirus je računalni softver koji se koristi za zaštitu, identifikaciju i uklanjanje računalnih virusa, kao i drugih štetnih programa koji mogu uzrokovati probleme u korištenju računala ili oštetiti podatke.

Za razliku od prvobitnih antivirusnih programa koji su bili temeljeni isključivo na tretiranju računalnih virusa, moderni antivirusni program se dizajnira tako da sustav štiti od što većeg

⁷ 37 Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 13 38 CERT, LSS (2010) Metode zaštite dokumenata, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb

broja različitih mogućih štetnih programa (crva, virusa, trojanskih konja, rootkita, špijunske i reklamske modula, phishing napada itd.). Prvi antivirusni programi pojavili su se 1983. godine.

3.4. KRIPTIRANJE

Šifriranje podataka odnosi se na ograničavanje pristupa sadržaju diska neželjenim korisnicima. Šifriranje (encryption) je pretvaranje izvornog teksta (plaintext) u šifrirani tekst (ciphertext) pomoću određene šifre (algoritma – AES, 3DES). Postupak se sastoji od izmjene dijelova teksta, npr. na način da sva slova u abecedi pomaknemo za tri mesta naprijed u abecedi (tzv. Cezarova šifra), tako da riječ INFORMACIJA postaje LQIRUPDFLMD. Moderni postupci su naravno mnogo komplikiraniji. Obrnuti postupak – dešifriranje (decryption) – odnosi se na omogućavanje čitanja šifriranih podataka korisnicima koji posjeduju ključ. Time su podaci zaključani na način da je tijelo informacije (tekst) nečitljivo korisnicima koji ne posjedu ključ (password) – u primjeru je ključ informacija da su slova pomaknuta za tri mesta.⁸

Moderni alati za šifriranje diska podatke šifriraju u pravom vremenu (on-the-fly-encryption, real-time encryption), tj. podatke šifriraju dok ih spremaju (kopiraju) u šifrirani spremnik, ili u slučaju čitanja, dešifriraju dio datoteke koji se čita. Uobičajeni način šifriranja je blokovski, tj. podaci se u radnoj memoriji šifriraju u blokovima te se tek onda spremaju na disk ili čitaju.

3.5. PRIJETNJE PO MREŽU

3.5.1. LJUDSKA POGREŠKA

Ljudska pogreška može biti posljedica izravnih napada na računalni sustav ili bilo koji mrežni uređaj kao rezultat namjernog djelovanja korisnika. Ljudska pogreška se smatra internom greškom i može biti rezultat kvara hardvera, krađe opreme, neograničenog pristupa poslužitelju, vandalizma i pristupa poslužitelju od strane ne-administratora. Podaci se također mogu ukrasti davanjem povlastica korisnicima čime im se omogućuje preuzimanje, izmjena i kopiranje osobnih datoteka koje pripadaju drugim korisnicima na mreži.⁹

⁸ 37 Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 13 38 CERT, LSS (2010) Metode zaštite dokumenata, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb,

⁹ <https://www.schalley.eu/>

3.5.2. PRIRODNI UZROCI

Osim ljudski pogreški prijetnje također mogu biti posljedica ekoloških katastrofa poput uragana, tornada, požara, poplava, potresa, i grmljavinskih oluja. Nedostatak aparata za gašenje požara u uredima, zgradama koje se nalaze u blizini područja poplava ili potresa, izlaganje mreže intenzivnoj ili nepovoljnoj temperaturi i još mnogo toga su mnogi uzroci prirodnih prijetnji mreži.

3.5.3. VIRUSI

Virusi se mogu smatrati dijelom koda koji se učitava na glavno računalo bez znanja korisnika, no taj se program pokreće protiv želja korisnika i uzrokuje veliku štetu korisničkom računalu. Virus se može primijetiti kada se računalo korisnika zamrzne kao rezultat preuzimanja zlonamjernog programa ili kada korisnik otvorí zlonamjernu e-poštu Ove prijetnje mogu biti ograničene instaliranjem antivirusnog softvera kao što su Microsoft Defender, Norton i još mnogo toga.¹⁰

3.5.4. SPAM

Neželjena pošta preplavljuje internet s mnogo kopija iste poruke, u pokušaju prisile poruke na korisnika koji inače ne bi otvorili tu poruku. Neželjena pošta nema fizički učinak na mrežu stoga ne može uništiti mrežne elemente. Spam filteri mogu se koristiti za suzbijanje učinka neželjene pošte i većina spam filtera dolazi uključena sa email klijentima.

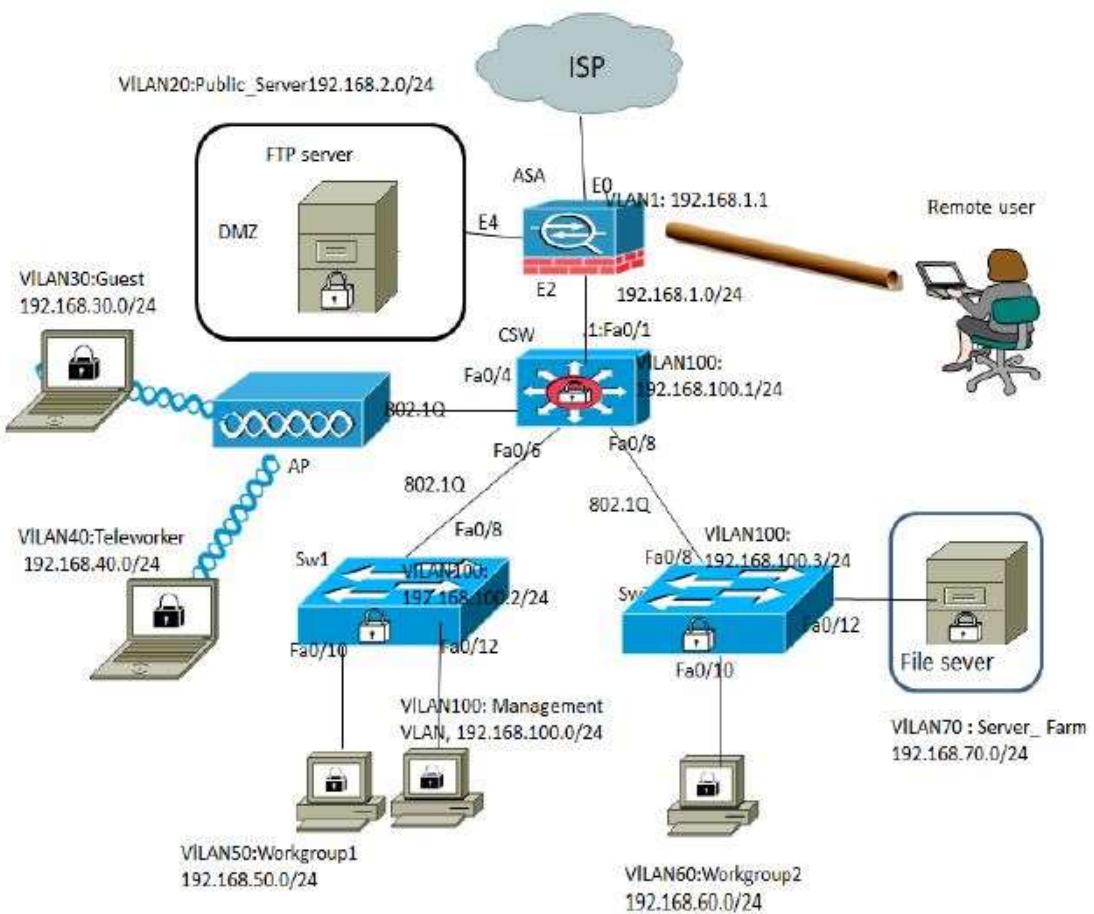
4. WLAN and LAN

Očekuje se da čitatelji ovog rada imaju osnovno znanje o računalnim mrežama. Ovo poglavlje će opisati uređaje koji tvore mreže i koji su povezani s mrežom, kako su uspostavljene veze, i različite sigurnosne protokole koji se mogu koristiti za osiguravanje bežične veze računalne mreže.

4.1. TOPOLOGIJA DIZAJN I IMPLEMENTACIJA

¹⁰ Meghanathan, N 2014. Network Security: Attacks and Control. PDF file.
<https://arxiv.org/ftp/arxiv/papers/1412/1412.6017.pdf>

Topologija projekta, prikazana na slici 4, dizajnirana je uzimajući u obzir karakteristike i značajke male tvrtke. Pretpostavljamo da topologija ima tri odjela s mogućom budućom ekspanzijom i planiranom ponudom fleksibilnije, pouzdanije, sigurne i brze mrežne usluge. Osmisljena je tako da ima sedam podmreža, od kojih su dvije podmreže radnih grupa u kojima se nalaze zaposlenici i jedna podmreža za mrežu tima koji upravlja mrežom, dvije podmreže su za DMZ i interne poslužitelje i preostale dvije podmreže su za bežičnu mrežu.



Slika 4 Prepostavljeni dizajn LAN mreže

Topologija prikazana na slici 4 je proširena topologija zvijezda gdje je CSW preklopnik koristi se kao središnji prekidač za centraliziranje svih priključaka koji idu na sklopke radne stanice (SW1 i SW2), vatrozid (ASA) i pristupna točka (AP). Proširena topologija zvijezde jamči da će se sustav moći proširiti kad god bude to trebalo. Mrežni uređaji su međusobno povezani pomoću kabela Cat 5 (neoklopljena upletena parica) i konektorima RJ-45.

Prema slici 4, vatrozid je gateway prema vanjskoj mreži usmjeravanjem IP- prometa u oba smjera. Vatrozid je povezan s internetom putem testne mreže s fixnom IP adresom. Javni poslužitelj povezan je s vatrozidom s vlastitom podmrežem koja je u osnovi planirana za pružanje usluga dijeljenja datoteka javnim korisnicima. Vatrozid se koristi za prevođenje privatnih IP adresa unutar i podmreže Public_Server na javnu IP adresu vanjskog sučelja vatrozida i obrnuto. Iznad svega, glavni zadatak vatrozida je poslužiti kao kontrolna točka za filtriranje dolaznog i odlaznog saobraćaja u svrhu zaštite interne mreže od napada koji dolaze iz vanjske mreže.

Prekidači sloja pristupa (Sw1 i Sw2) prikazani na slici 4 koriste se za povezivanje radne stanice i internog poslužitelja za prekidač jezgre. Podmreža Workgroup1 i upravljačka podmreža su povezani na Sw1 prekidač, a radna grupa2 na podmrežu i na Serverfarmu povezana je preko prekidača Sw2. Podmreža Workgroup1 i workgroup2 namijenjene su zaposlenicima, a korisnicima u tim podmrežama je dopušteno komuniciranje putem Interneta i vanjskog svijeta. Podmreža za upravljanje je namijenjen za administraciju i upravljanje mrežom. Podmreža farme konfigurirana je za pružanje usluga dijeljenja datoteka samo internom korisniku.

Pristupna točka (AP) prikazana na slici 4 izravno je povezana s prekidačem jezgre (CSW) i konfiguriran je za pružanje bežične veze posjetiteljima i ovlaštenim korisnicima unutar dometa radio signala.

4.2. IP ADRESIRANJE

IPv4

IP adresa je logička adresa čvora u TCP/IP skupu protokola. Sastoji se od četiri decimalna broja razdvojena tačkama (tzv.decimalna notacija sa tačkom) tj. četiri okteta od po osam bita – ukupno 32 bita. npr - 147.91.177.97

Klase IP adresa IP adrese su podijeljene u klase. Podjela IP adresa u klase precizno definiše koji dio adrese se koristi za adresiranje čvorova (host), a koji za adresiranje mreže (net).

Clasa A	0	NET 7 bita	HOST 24 bita
Clasa B	10	NET 14 bita	HOST 16 bita
Clasa C	110	NET 21 bit	HOST 8 bita
Klasa A	128 mreža – 16,78M čvorova	1.0.0.0 – 126.0.0.0	
Klasa B	16.385 mreže – 65.536 čvorova	128.1.0.0 – 191.255.0.0	
Klasa C	2 miliona mreža – 254 čvora	192.0.1.0 – 223.255.255.0	
Klasa D	grupne adrese (1110)	224.0.0.0 – 239.255.255.255	
Klasa E	eksperimentalne adrese (1111)	240.0.0.0 – 255.255.255.254	

4.3. PROTOKOL USMJEREVANJA

U ovom dijelu moje teze usredotočujem se na definiciju usmjeravanja protokola i protokola koji se danas široko koriste u različitim vrstama okruženja. Prvo, važno je razumjeti što je protokol usmjeravanja. Usmjeravanje je proces pronalaženja puta od početne točke do odredišta - kao put od kuće do škole. Usmjeravanje se sastoji od pronalaženja svih mogućih puteva i odabira najkraćeg (ili najmanje vremenskog) puta. Također se koristi za odabir drugog puta ako je najkraći zatvoren. Stoga, protokol usmjeravanja zadužen je za podatke koji teku između hostova. Protokol usmjeravanja čini tablicu usmjeravanja za hostove u mreži(routing table).Kao što naslov sugerira, postoji niz različitih protokola usmjeravanja za različite prigode.¹¹

4.4. VLANs

Virtualna lokalna mreža je skupina uređaja koji dijele istu domenu kao da su spojeni na istu žicu, ali zapravo nisu. VLAN-ovi se koristi za grupiranje mrežnih uređaja i druge opreme prema vrsti podataka ili prema sigurnosnim pravila koje dijele. Isprva su se usmjerivači koristili za odvajanje VLAN-ova, ali taj pristup se pokazao spor, skup i dugotrajan.¹² Umjesto toga, sada su VLAN-ovi distribuiraju putem mreže pomoću mrežnih prekidača. Prednosti korištenja switch VLAN nego preko usmjerivača su brojni. Jedna od najvažnijih značajki su performanse: dok su switch-evi brzi za proslijedivanje podataka, usmjerivači su stvorili uska grla u mrežama, usporavajući proces. Druga korist je kako lako virtualno formiraju se grupe i koliko brzo se podaci prosljeđuju između članova iste skupine. Osim toga, s VLAN-ovima lako je primjeniti različita sigurnosna pravila i pristup politikama korisnicima, ako su u istoj virtualnoj grupi.

¹¹ Meghanathan, N 2014. Network Security: Attacks and Control. PDF file.

<https://arxiv.org/ftp/arxiv/papers/1412/1412.6017.pdf>

¹² Allied Telesis 2015. Virtual LANs. PDF file.

Veliku fleksibilnost sa ovim pristupom korisnicima omogućuje slobodno kretanje i kada su priključeni na novu lokaciju, i dalje će biti u istom VLAN-u s istim pravilima i privilegijama.

4.5. NAT/PAT

Sve dok postoji samo jedna javna IP adresa koja se daje tvrtki, potrebno je primijeniti prijevod mrežne adrese (NAT) ili prijevod adrese porta(PAT). Prevođenje mrežne adrese je tehnologija koja omogućuje određenom uređaju kao što je vratnik ili usmjerivač koji predstavlja drugi uređaj u privatnoj mreži da djeluje u javnoj mreži. Uz NAT moguće je koristiti jednu javnu IP adresu čak i ako na LAN-u postoji više od jednog uređaja. Ova tehnika mapira IP adresu u jednoj mreži (u našem slučaju, LAN) na IP adresu na drugoj mreži (javna IP adresa na internetu)

Postoje dvije vrste prijevoda mrežne adrese. Prva vrsta je statična NAT, najjednostavniji od svih tipova. Statički NAT koristi jedan-na-jedan prevođenje IP adrese. Drugim riječima, postoji jedna specifična IP adresa u lokalnoj mreži koja je mapirana na određenu IP adresu na Internetu. Drugi, dinamički NAT omogućuje konfiguriranje statične NAT automatski, on-the-go stvarajući tabelu adresa unutar LAN-a i sličnu tabelu na vanjskom LAN-u. Na taj način, mapiranja jedan na jedan se stvaraju automatski i stoga se puno vremena štedi u slučaju da postoje brojni unosi u tabelama adresa

Napredniji alat je NAT preopterećenje ili Port Address Translation. Ovaj alat omogućuje više korisnika unutar LAN-a koristi jednu IP adresu na vanjskoj mreži. Za to, NAT preopterećenje ne koristi samo unutarnje IP adrese nego i brojeve portova razlikovati jednog korisnika od drugog. Svakom domaćinu unutar LAN-a dodijeljen je port koji služi kao izvor i odredišni port

4.6. DHCP

Dynamic Host Configuration Protocol (DHCP) je skup pravila za komunikacijske uređaje, kao što su računar, router ili ostale vrste mrežnih adaptera, pomoću kojih uređaj može zahtijevati i dobiti odgovarajuću IP adresu sa servera.

DHCP je protokol korišten od strane mrežnih računara za dobijanje IP adresa i ostalih mrežnih postavki kao što su pretpostavljeni gateway, subnet maska, i IP adrese DNS servera sa DHCP servera. Olakšava konfiguriranje mreže jer eliminiše ručno dodavanje osnovnih postavki za jednu računarsku mrežu. DHCP server osigurava da su dodijeljene IP adrese posebne, i brine se da u mreži nema sukoba. DHCP je prihvacen kao standardni protokol u oktobru 1993. godine.

Posljednja definicija datira iz marta 1997. godine. Najnovija nestandardna verzija protokola koja opisuje DHCPv6 u novom IPv6 okruženju je predstavljena u julu 2003. godine.

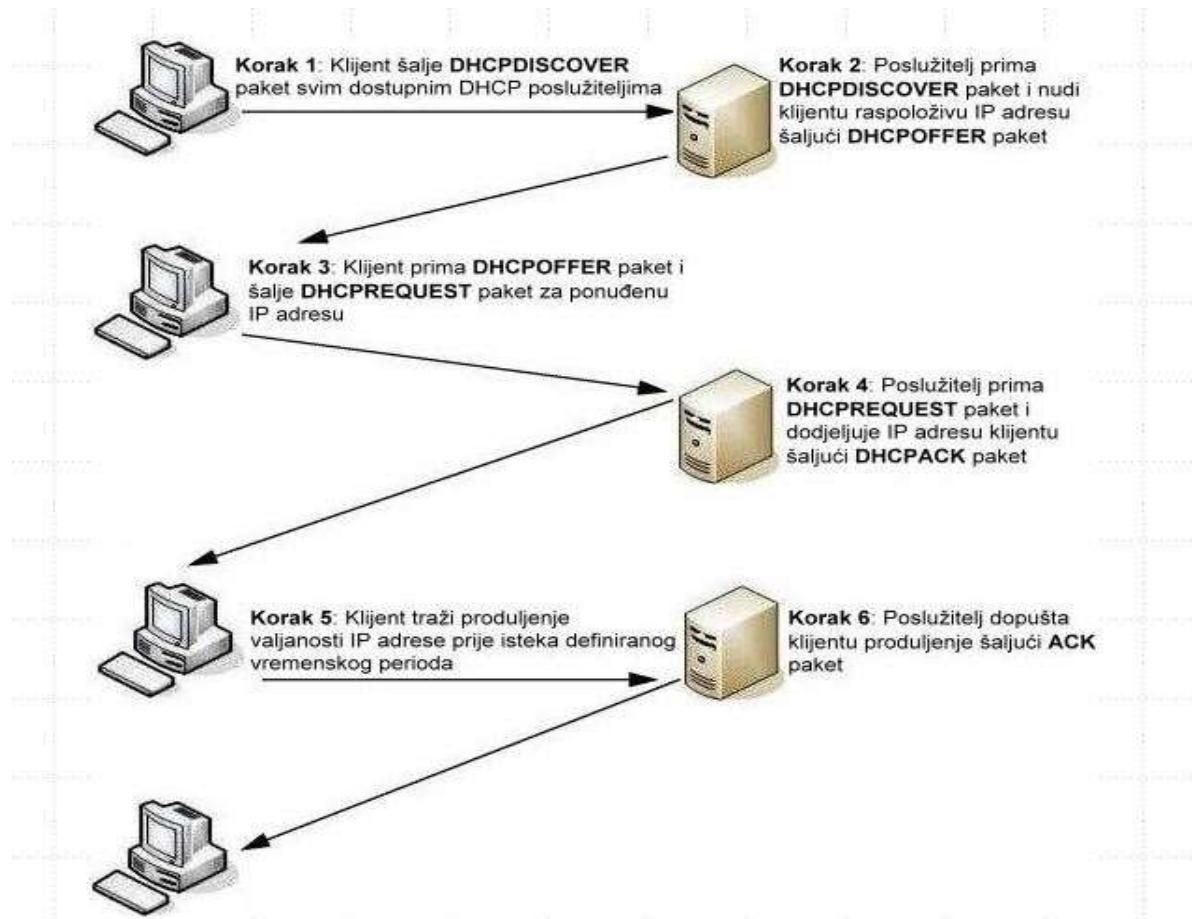
Klijenti šalju upit poslužitelju, koji im osim IP adrese može dodijeliti mrežnu masku, adresu predefiniranog izlaza, adresu WINS poslužitelja, domenu i adresu DNS poslužitelja. Postoje tri načina dodjele IP adresa:

- Automatska dodjela - DHCP poslužitelj trajno dodjeljuje IP adresu klijentu
- Ručna dodjela - Adresa se dodjeljuje od strane administratora mreže
- Dinamička dodjela - DHCP dodjeljuje, odnosno iznajmljuje, IP adresu klijentu na određeni vremenski period.

Adrese se dodjeljuju iz određenog raspona adresa. Postupak dodjele adrese prolazi kroz nekoliko faza. Klijent mora imati instaliranu DHCP podršku da bi pri spajanju na mrežu mogao poslati zahtjev za dodjelu IP adrese.¹³

Zahtjev se šalje razašiljanjem kao DHCPDISCOVER paket. Kad poslužitelj primi zahtjev pogleda u svoju bazu može li pružiti uslugu te ako može šalje "unicast" odgovor kao DHCPOFFER. Paket DHCPOFFER može sadržavati i sve ostale postavke koje poslužitelj može dodijeliti. Ukoliko klijent ponudu smatra prihvatljivom šalje "broadcast" DHCPREQUEST tražeći da mu se dodijeli baš ta adresa. Ovaj zahtjev se razašilje jer na mreži može postojati više DHCP poslužitelja pa tako svi ostali znaju čija je ponuda prihvaćena. Poslužitelj odgovara "unicast" paketom DHCPACK. Ukoliko je klijent primijetio da je ponuđena adresa već u uporabi, šalje DHCPDECLINE poruku i postupak kreće ispočetka. Postupak kreće ispočetka i u slučaju kada poslužitelj pošalje DHCPNACK. Ukoliko nakon nekog vremena klijent više ne treba dodijeljenu adresu šalje poruku DHCPRELEASE. Proces je prikazan na slici 5.

¹³ Bonaventure, Olivier, 2011. Computer Networking. PDF file.



Slika 5

4.7. IZBOR UREĐAJA

Iako su protokoli usmjeravanja i kabliranje važni, pravi mrežni uređaj može olakšati klijentu korištenje mreže i održavanje u radnom stanju. Uobičajeno je da u malim poslovnim mrežama ljudi pokušavaju uštedjeti novac gotovo na svim mogućim načinima ako je to moguće. Međutim, s tim pristupom ponekad završe s uređajima koji ne odgovaraju brzini ili sigurnosnim zahtjevima. Cijena uređaja obično se povećava što je više opcija uređaja. Iako nije svaka je tvrtka spremna potrošiti stotine ili čak tisuće eura za mrežne uređaje, to ne znači da su preostali samo oni uređaji koji bolje rade u kući. S druge strane, moguće je kupiti usmjerivač ili prekidač s brojnim značjkama kao što je veza s konzolom, PortFast, DHCP za pristojnu cijenu.

4.8. KONFIGURACIJA PC

Očito je da što je veća tvrtka, to je više razlika među radnim stanicama za zaposlenike. Međutim, uobičajena je praksa ukloniti što više moguće razlike kako bi korisnicima olakšali rad na različitim radnim stanicama i za administratore - održavanje i rješavanje problema s računalima. Na primjer, a dobro rješenje je smanjiti količinu različitih verzija operacijskih sustava instaliran na računalima - na taj način administrator mreže znatno troši manje vremena za podešavanje računala, primjenu potrebnih postavki i instaliranje ažuriranja. Isto vrijedi i za softver i upravljačke programe - računala možda ne podržavaju najnovije verzije ili je korisnici ne trebaju za svoj rad. Ipak, kada je većina radnih stanica tvrtke ista (ili, barem, određena grupa) koristi isti softver, krećući se između računala ili rješavanje problema neće biti problem niti za korisnike niti za administratore.

Upravljački programi, međutim, dovode nas do hardverskih konfiguracija. Važno je shvatiti da hardver možda ne zahtijeva česte nadogradnje, ali to ne znači da je ne zahtijeva nikakve nadogradnje. Dok nove tvrtke kupuju moderna ili najnovija računala, starije tvrtke često nisu spremne finacijski nadograditi radne stanice koje već imaju. Ipak, u nekom trenutku softver koji tvrtka koristi će se ažurirati i trebat će više snage iz CPU-a ili više memorije s tvrdih diskova. Alternativno, jedna od komponenti radne stanice može se pokvariti i pokvariti važne podatke. Stoga su nadogradnje hardvera neizbjegljive i ponekad presudne za sigurnost podataka i tempo rada tvrtke.

4.9. SIGURNOSNA KONFIGURACIJA

U ovom dijelu govorit ću o načelima sigurnosti koja su najčešća u okruženju male poslovne mreže. Namjeravam navesti najčešće korištene prijetnje i napade na mrežu i njihove komponente te objasniti metode koje sprječavaju te napade.

Neophodno je reći da „mrežnom sigurnošću“ mislim ne samo na sigurnost krajnjih uređaja koji razmjenjuju informacije, nego i na mrežu između njih, mrežne opreme i njegovih postavki i medija. Osim toga, sljedeće čimbenike treba uzeti u obzir: pristup - mogućnost ovlaštenih osoba za korištenje mreža; povjerljivost - podaci u mreži nisu dostupni onima koji to žele; autentifikacija - korisnici moraju dokazati da su oni koji jesu; integritet - podaci nisu izmijenjeni tijekom tranzita; ne-odbacivanje – korisnik ne odbija njene ili njegove akcije u mreži. Slijedeći ove izjave, znatno je lakše shvatiti kako bi trebala izgledati mrežna sigurnost za svako

pojedinačno poduzeće i njegovu svrhu. Također je važno da dizajn mreže ima nekoliko uobičajenih metoda koje odgovaraju gotovo svim vrstama mreža, dizajn sigurnosti je više individualan zbog vrste podataka koje tvrtka koristi i razinu sigurnosti koju ova tvrtka želi imati. Iako se mrežne prijetnje i napadi stalno razvijaju, još je moguće razlikovati nekoliko njih.

5. POSTAVLJANJE MREŽE

5.1. KONFIGURACIJA UREĐAJA I SISTEMA

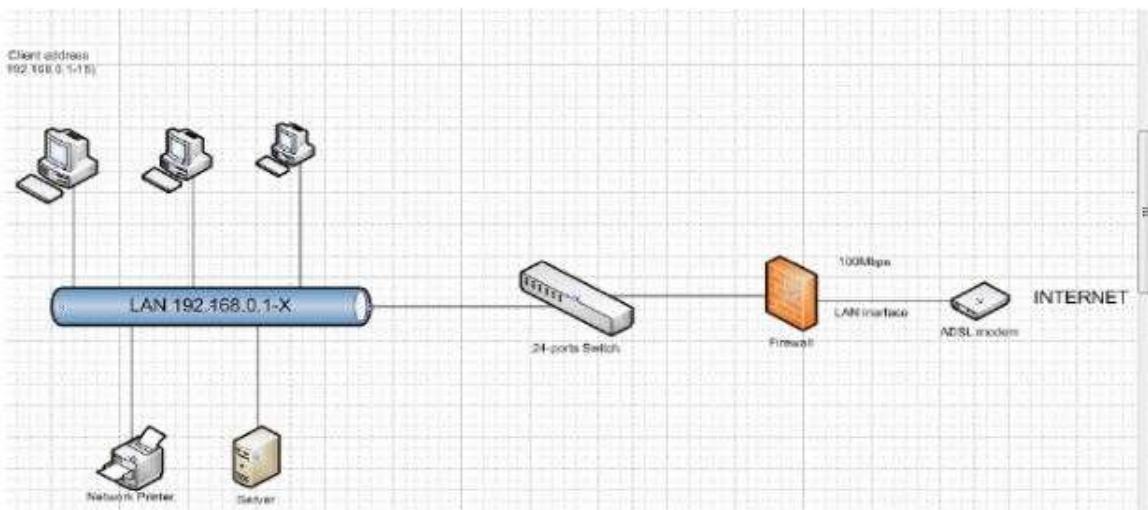
Prije uvođenja LAN strukture za bilo koju poslovnu operaciju postoji potreba da se utvrdi vrsta usluga koje će se pružati u lokalnoj mreži. Moja teza predviđa mali računarski centar za obuku, čiji je fokus upoznavanje / osposobljavanje studenata na osnovnim IT tečajevima. Ove usluge i operacije određuju vrstu hardvera i softvera koji će se koristiti na topologiji. Također je bolje pripremiti osnovnu mapu topologije koja će se koristiti u slučaju poslovnog rasta koji zahtijeva dodavanje više mrežnih uređaja. Karta će olakšati integraciju dodatnih uređaja s obzirom na postojeću topologiju na terenu i pomoći u rješavanju problema. Međutim, važno je uzeti u obzir broj slojeva kojima podaci moraju putovati prije dolaska na odredište sa izvora. Važno je zadržati broj slojeva što je moguće manjim, čime se povećava učinkovitost. Mrežna oprema zaslužuje ulaganje u, s obzirom na prosječan vijek trajanja mrežnih uređaja kao što su prekidači, vratoredi, računala, koji je oko 4-5 godina, ovisno o korištenju, ali svaka organizacija nastoji maksimizirati svoje korištenjem opreme na duže vrijeme. Moglo bi doći do kvara na portovima i neispravnosti napajanja ako bi se kupili jeftiniji uređaji u komercijalne svrhe. Budući da će svi podaci i komunikacije poslovanja koristiti opremu isplati se dugoročno.

5.2. FIZIČKA TOPOLOGIJA

Učinkovita mreža zahtijeva adekvatno planiranje kako bi se osiguralo da će mreža podržati poslovne potrebe i zahtjeve, stoga su naglašena sljedeća ključna pitanja pri projektiranju LAN-a za mala i srednja poduzeća:

- Koje su potrebe tvrtke?
- Koja važna pitanja treba razmotriti kao podršku trenutnim i budućim potrebama poslovanja?
- Koja je financijska implikacija / razmatranje troškova?

SCENARIO



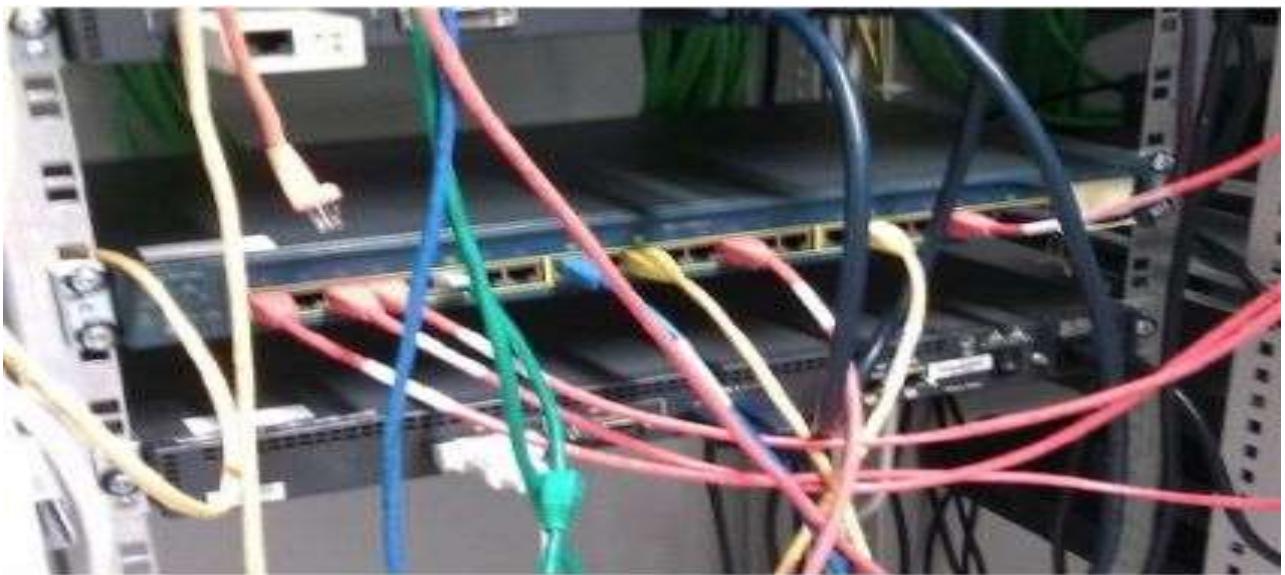
Slika 6

Laboratorijski rad podrazumijeva izradu gornje topologije (vidi slika 6) i konfiguraciju mrežnih uređaja za učinkovito funkcioniranje. Ethernet LAN sastoji se od 15PC-a, 24-portnog swticha, ADSL modema, mrežnog pisača, vatrozida i kablova kako je prikazano u dijagramu topologije.

5.3. HARDWERSKI ZAHTJEVI I KONFIGURACIJA

Potrebni hardverski uređaji za dizajn LAN-a su sljedeći:

- 24 PORTNI SWITCH
- 15 MREŽNI RAAČUNARA ZA ZAPOSLENIKE, STUDENTE, ADMINISTRACIJU,
- PRINTER SA PODRŠKOM ZA MREŽU
- ADSL MODEM
- SERVER
- MREŽNE KARTE
- KABLOVI
- VENTILATORI ZA HLAĐENJE
- ORMARIĆ
- UPS NAPAJANJE



Slika 7

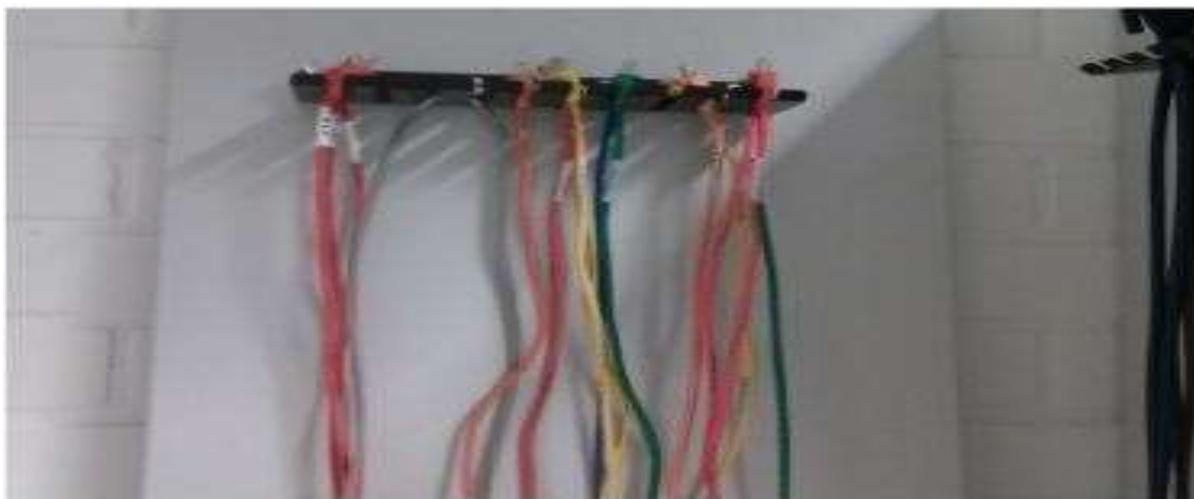
SLIKA 7 24 PORTNI CISCO Catalyst 2950 SWITCH

Switch je uređaj koji upravlja protok podataka između dijelova lokalne mreže (LAN). Za razliku od hub-a, switch dijeli mrežni promet te ga šalje na određena odredišta, dok hub šalje podatke na sve uređaje koji su u mreži. Koristi se za mreže srednje veličine, jer je bolji i efikasniji od hub-a. Switch daje računaru punu brzinu jedne konekcije (recimo 10 Mbps) ako je to moguće, dok računari prikopčani na hub dobijaju samo dio te konekcije što bi bilo neupotrebljivo ako bi se radilo o većem broju računara, pogotovo ako se radi o prijenosu većih datoteka. Ovaj uređaj funkcioniše na drugom nivou (Layer 2 uređaj) što znači da je svijestan svojih klijenata. Identifikator uređaja povezanog na switch je njegova fizička tzv. MAC (engl. Media Access Control) adresa.¹⁴

KONFIGURACIJA SWITCHA

Nije bilo potrebne posebne konfiguracije na switchu. Međutim, switch je dizajniran kako bi osigurao različite kanale od mreže preko ADSL modema do interneta.

¹⁴ Cisco, Inter-Switch Link and IEEE 802.1Q Frame Format,Cisco, Tech. Rep



Slika 8 Spajanje kablova

Kabliranje je provedeno kako je prikazano u topologiji. Kablovi su se izvodili od prekidača do mreže na zidu gdje se svaki domaćin može lako povezati putem Ethernet kabela i konektora. Svi Ethernet kabeli sastoje se od 4 para žica obojenih zajedno: smeđe, smeđe i bijele, zelene i zelene i bijele. Ethernet kabeli i konektori uključuju kategoriju 5 (CAT5), poboljšanu kategoriju 5 (CAT5e) ili kategoriju 6 (CAT6), ovisno o količini prijenosa podataka i osjetljivosti na smetnje. U svrhu moje teze CAT5e korišten je zbog svoje pouzdanosti, troškova i performansi u maloj mreži.¹⁵

5.3.1. RAČUNALO RADNE STANICE

Odabir računala koja će se koristiti kao radna stanica temeljio se na aktivnostima / zadatcima na mreži. Računala koje će se koristiti za radnu stanicu mora ispunjavati zahtjeve i biti kompatibilan sa softverom koji se instalira na njega. Računalo je sa sljedećim specifikacijama:

Processor: Intel core i3-2120 processor (3MB Cache, 3.30GHz)

Memory: 2GB*2 dual channel DDR3 SDRAM at 1333MHz

Hard drive: 250GB* 2 SATA hard drive (7200RPM)

Video Card: Intel HD Graphics (VGA, HDMI)

Optical Drive: 16x DVD+ /RW Drive

¹⁵ Cisco, Inter-Switch Link and IEEE 802.1Q Frame Format,Cisco, Tech. Rep

5.3.2. KONFIGURACIJA

Što se tiče računala za radnu stanicu, osnovna je konfiguracija bila da se učini učinkovitim kako bi bio kompatibiln s mrežom. Osnovna konfiguracija je osigurati da računalo sadrži utore za karticu NIC (mrežna kartica) koja omogućuje pristup računalima mreži. MAC Adresa (Media Access Control) jedinstveno identificira sustav na mreži preko MAC adrese koja je jedinstvena za svaki uređaj spojen u mrežu.

NIC (Network Interface Card)



Slika 9 Cisco mrežna karta

NIC je važna komponenta u umrežavanju i to je zasebna kartica za proširenje koja se nalazi u utoru za proširenje na matičnoj ploči unutar kućišta računala. On osigurava fizičku vezu između računala i mrežnog kabela, uključujući drugi prijenosni medij, a računalo ne može komunicirati na mreži bez kartice mrežnog sučelja slanjem podataka, NIC pretvara računalne podatke u energetske impulse i prenosi ih na mrežni medij. Funkcionira u podatkovnoj vezi i fizičkoj vezi OSI modela.

5.3.3. KONFIGURACIJA NIC

Konfiguracija se radi u 3 sljedeće faze:

IRQ (interrupts request) setting: Ova postavka omogućava direktnu komunikaciju između procesora i uređaja

I/O (input/output) ports: Ova opcija vrši identifikaciju memorijskog prostora koji koristimo za protok informacija i podataka između procesora i NIC.

Base Memory Address: Ova opcija dodjeljuje memorijski buffer prostor za spremanje dolaznih i odlaznih podatkovni paketa.

Uglavnom u današnje vrijeme svi ovi uređaji dolaze sa instalacijskim CD koji omogućava da ameteri instaliraju sve postavke bez većeg stručnog znanja o mrežama.

5.3.4. SERVER

Nije ništa drugo nego osobno računalo s većom funkcionalnošću od računala koja se koriste kao radne stanice. Server računalo je više prikladan za obavljanje poslova za koje je napravljen. To je središnje računalo odgovorno za upravljanje mrežom i hostom pomoću NOS-a (mrežni operativni sustav) i svih aplikacijskih softvera. Sadrži programe i podatke te ih čini dostupnim domaćinima na mreži. Poslužiteljsko računalo se razlikuje od računala radne stanice u smislu da mora biti pouzdaniji. Termin poslužitelj ili server se vrlo često koristi u informacijskoj tehnologiji. Poslužitelji su obično računala koja služe za dijeljenje sadržaja te izgradnju internetskih stranica. Poslužitelji su otvoreni i preko domene (internetske adrese) ili IP adrese svatko može s bilo kojega računala pristupiti nekome poslužitelju i nekoj internetskoj stranici ili preuzeti neki sadržaj s njih. Na poslužiteljima, ovisno o kakvim je poslužiteljima riječ, obično bude po nekoliko korisnika te poslužitelji sve njih poslužuju primajući zahtjeve i šaljući povratne baš kao i vaše računalo, samo za više korisnika istovremeno.

5.3.5. KONFIGURACIJA SERVERA

Točna konfiguracija SERVERA ovisi o broju korisnika, količini podataka koji se pohranjuju i obrađuju, brzini koja je potrebna i velicini zadatka koje planiramo izvršiti. Računalo koje će se koristiti kao poslužitelj mora biti konfiguirano tako da uključuje dvostruki procesor, redundantne tvrde diskove ili napajanja, skalabilno kako bi zadovoljilo trenutne i buduće potrebe kako bi moglo obraditi podatke brže i učinkovitij

5.3.6. MREŽNI PRINTER

Mrežni printer je uređaj kao i normlani printer samo što posjeduje opciju spajanja na mrežu gdje mu se može dodjileti IP adresa pomoću koje kasnije svi ostali korisnici pristupaju printeru i koriste njegove značajke. Osim toga mrežne printere odlikuje i veći kapacitet koji se održava zbog toga da više ljudi koriste resurse jednog uređaja koji mora zadovoljiti sve potrebe.

5.3.7. KONFIGURACIJA MREŽNOG PRINTERA

Se vrši veoma jednostavno tako sto printer spojimo preko etehert kabla na mrežu gdje kasnije preko hosta isntaliramo njegov driver koji kasnije dopusta svim racunarima da se spoje na njega.

5.3.8. ADSL MODEM

ADSL (Asymmetric Digital Subscriber Line) Modem



Slika 10 ADSL Modem CISCO

ADSL modem je uređaj koji povezuje računalo ili mrežni usmjerivač s digitalnom pretplatničkom linijom (Asynchronous Digital Subscriber Line, ADSL) kako bi se računala u lokalnoj mreži spojila s Internetom. ADSL modem modulira tonove visoke frekvencije za prijenos do multipleksera s kojim je izravno spojen i koji je smješten u centrali telekomunikacijske mreže. On je zapravo neka vrsta transivera i ima istu ulogu kao i običan modem za spajanje na telefonsku liniju ali se primijenjena tehnologija bitno razlikuje. ADSL modemi mogu prenosi podatke vrlo velikim brzinama koje se mjere desecima megabita u sekundi a za prijenos podataka koriste istu telekomunikacijsku liniju koja se koristi i za prijenos glasa. Za razliku od uobičajenih modema, ADSL modemi mogu prenositi podatke u isto vrijeme kada se linija koristi za glasovnu komunikaciju. Većina ADSL modema omogućava

konfiguriranje preko internog Web poslužitelja kojem se pristupa kroz Web preglednik. Na računalo se spajaju putem Ethernet ili USB priključka.

Neki ADSL modemi konstruirani su tako da pored spajanja na telekomunikacijsku mrežu omogućavaju i dijeljenje ADSL usluge u mreži koja je na njih spojena. U tom slučaju nazivaju se ADSL usmjerivači i mogu pružati mogućnost spajanja više računala izravno na modem putem Ethernet priključka ili WiFi pristupne točke. Pored toga ADSL modemi/ruteri mogu pružati i usluge prevodenja mrežnih adresa (Network Address Translation, NAT), dinamičkog konfiguriranja umreženih računala (Dynamic Host Configuration Protocol, DHCP), virtualne privatne mreže te funkcionalnost za prijenos glasa preko IP mreža (VoIP).

5.3.9. BACKUP

Je proces u kojem помоћу неког екстеријерног уређаја вршимо сигурносно копирање садржаја са нашеј сервера или рачунара на екстеријерни медиј. Ово радимо у случају ако би дошло до не очекиваних проблема и губитка садржаја са сервера да имамо резервне копије свих података.

5.3.10. UPS

Уредјај за беспрекидно напајање UPS (Uninterruptable power supply) је систем чији је основни задатак да обезбеди ненасметано електрично напајање потрошача. Потрошачи су најчешће лични рачунари са припадајућом опремом, управљачки системи у процесној индустрији, телекомуникацијама и остали системи код којих проблем у регуларном напајању електричном енергијом може изазвати озбиљне последице, безбедносне, финансијске или функционалне.

5.3.11. VENTILATORI ZA HLAĐENJE

Су у суштини обични вентилатори које користимо да би rashaldili систем и довели га до оптималне радне температуре у случајима интензивнијег користења уређаја.

5.3.12. ORMARIĆ



Slika 11 Ormarić sa mrežnim printerom

5.4. SOFTWERSKI ZAHTJEVI I KONFIGURACIJA

Softverski zahtjevi i instalacija važan su aspekt rada u mom radu jer podrazumijevaju instalaciju različitog softvera, koji se smatra skupom uputa u obliku programa, podataka ili koda za učinkovito funkcionisanje hardvera u mreži i za obradu podataka. Neki od hardvera su dizajnirani s ugrađenim operativnim sustavom koji omogućuje da hardver radi učinkovito u mreži. Vrsta zadataka i operacija u organizaciji određuje vrstu softvera koji će se instalirati na radnoj stanici i koji se razlikuju za različite organizacije. Softver se može podijeliti u dvije kategorije koje su:

5.4.1. SISTEMSKI SOFTWER

Sistemske softver je opći naziv za svaki računarski program kojem je namjena da omogući računaru samo pokretanje i izvršavanje osnovnih funkcija. Sistemske softver je zadužan za upravljanje pojedinačnim hardverskim dijelovima. Sistemske softver izvršava zadatke kao što je prijenos podataka sa memorije na disk, ispisivanja teksta na ekranu i tako dalje. To su operativni sistemi, državni, programske alatne, kompjajleri, asembleri i ostali slični alati. Sistemske softver se može i smjestiti u čip, obično se koristi termin firmware.

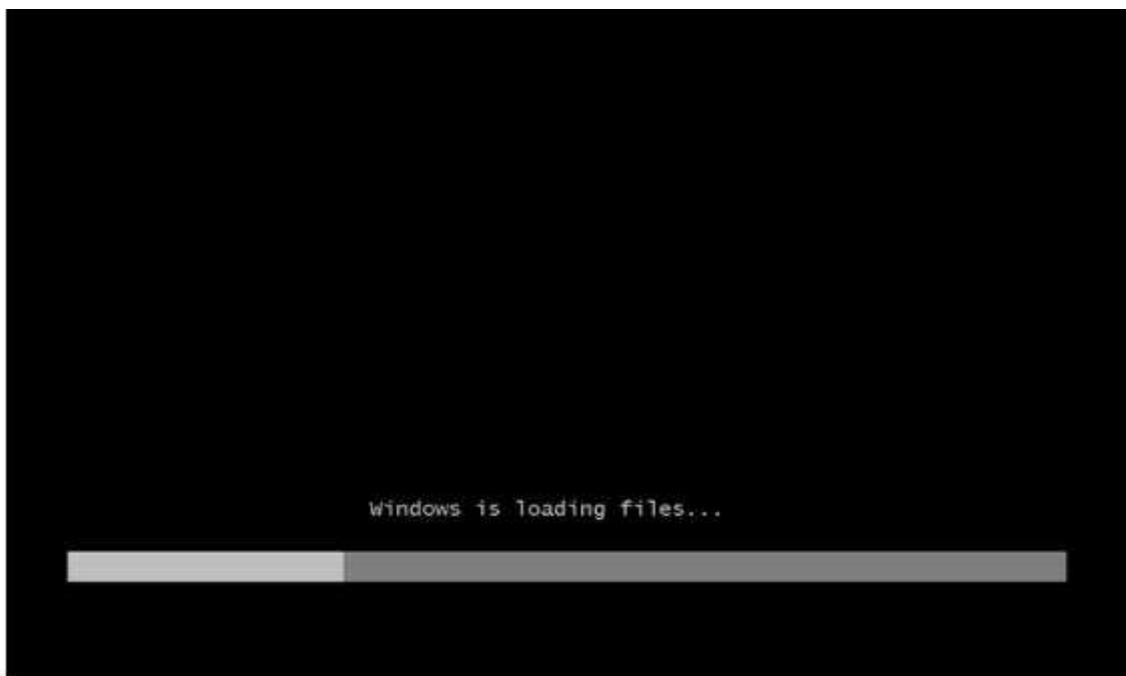
5.4.2. APLIKACIJSKI SOFTWER

Aplikacijskim softverom smatra se programi koji stvarno rade za korisnike. Oni uključuju Microsoft Office, sustave za upravljanje bazama podataka, PDF čitače, 7-zip, internetski preglednik, Skype i još mnogo toga. Aplikacijski softver jednostavno se smatra aplikacijom za

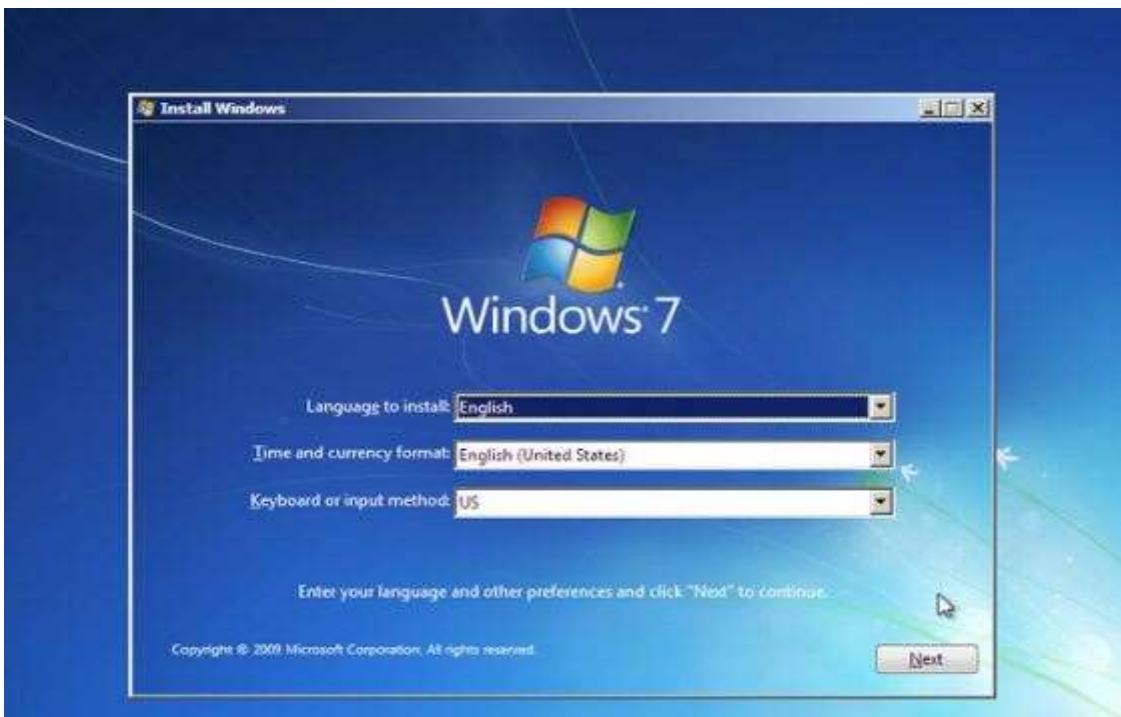
krajnje korisnike. Aplikacijski softver se ne može pokrenuti bez rada sistemskog softwera. Za potrebe ovog rada raspvaljat ćeemo o softwerima koji se smatraju značajnima a to su:

- OPERACIJSKI SISTEM WINDOWS 7
- UPRAVLJAČKI SOFTWER UREĐAJA
- WINDOWS SERVER 2008 R2
- PROGRAMSKI KOMPAJLERI (Eclipse, NetBeans)
- OFFICE PAKET,7 ZIP,CHROME,PDF READER, FOG, CLONEZILA, ALTRIS, SYMENTC GHOST

5.5. INSTALACIJA SISTEMSKOG SOFTWERA WINDOWS 7 NA HOSTOVE



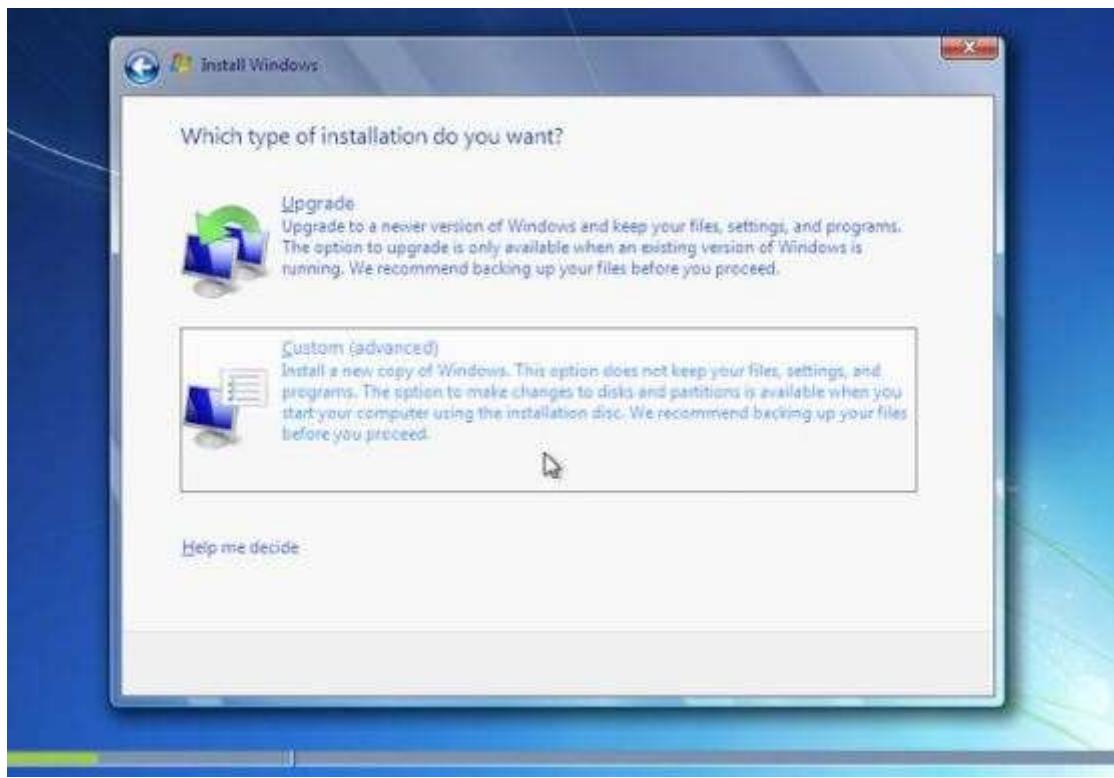
Ubacimo bootabilni Windows 7 DVD. Ako Windowsi već postoje na računalu, računalo će ispisati: Press any key to boot from CD... (pritisnite bilo koju tipku na tipkovnici). Ako ne postoje, računalo će samo ući u Setup. Pričekajte trenutak dok se učitaju podaci potrebni za početak instalacije.



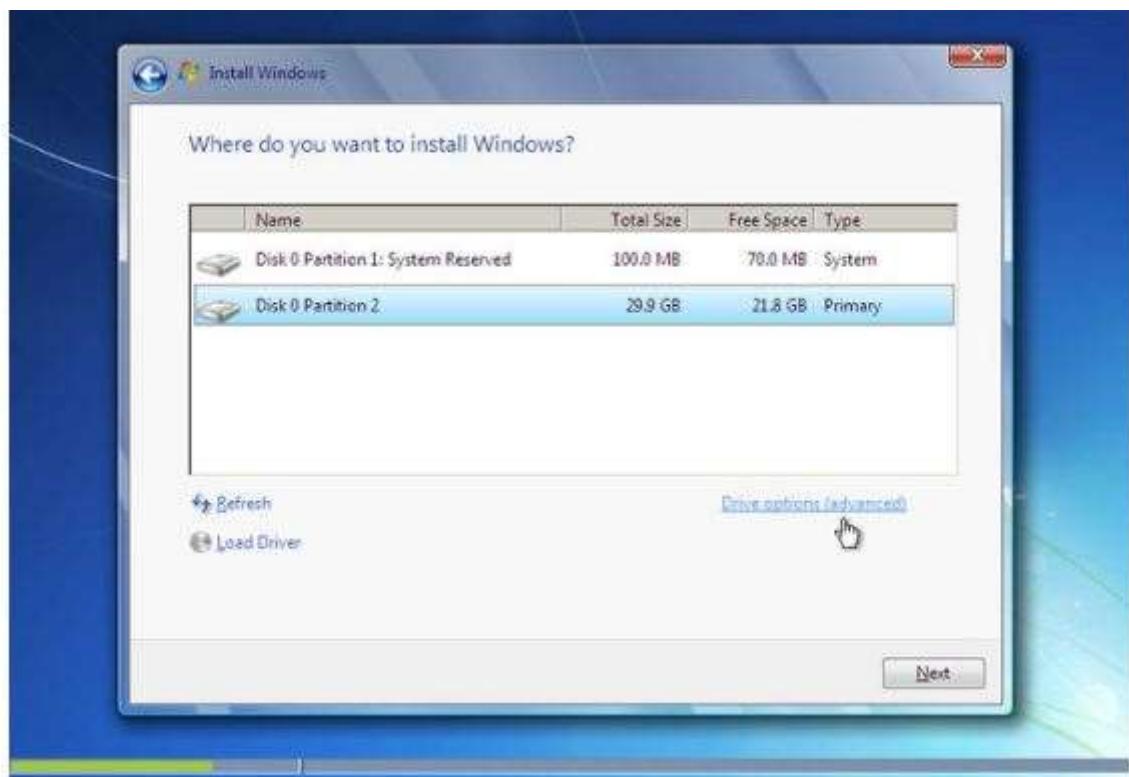
Prvo što moramo napraviti je odabir jezika instalacije kao i samih Windows -a. Kao Languge to install ostavite English ukoliko vam ništa drugo ne nudi, a pod Time and currency format odaberite Croatian kao pod Keyboard or input method. Kliknite "Next" za nastavak



Odaberite "Install now" kako biste započeli instalaciju. Kako biste nastavili instalaciju morate se složiti sa Ugovorom. Kliknite u kućicu pored "I accept the license terms", a zatim kliknite na "Next".



U ovom dijelu instalacije odabiremo koju vrstu instalacije želimo napraviti. "Upgrade" kao ažuriranje stare instalacije tj. instalacija preko postojeće Windows instalacije. Pokazalo se da instalacija preko Windows Vista-e prolazi bez ikakvih problema, što nije slučaj s Windows XP-om. Odaberite "Custom" ako radite "čistu" instalaciju tj. instalaciju prvi puta.



Odaberite particiju na koju želite instalirati Windows. Ovdje imate opciju kreiranja i brisanja particija ako kliknete na "Drive options (advanced)". Preporučamo vam da za Windows instalaciju imate odvojenu particiju veličine najmanje 20gb. Odaberite "Next" za nastavak. Instalacija je započela i možete pratiti po koracima koliko je daleko stigla. Ovdje će vam se računalo ponovno pokrenuti (možda više puta).

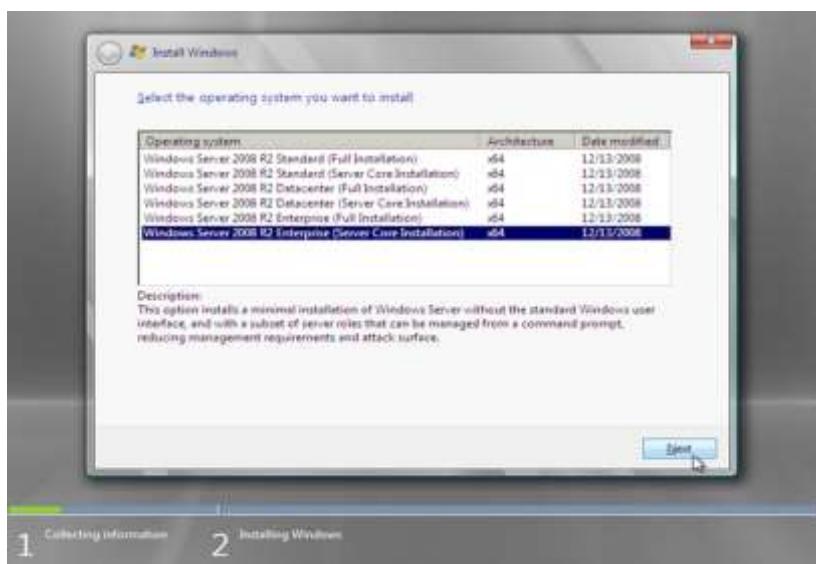
5.6. INSTALACIJA WINDOWS SERVERA 2008 R2



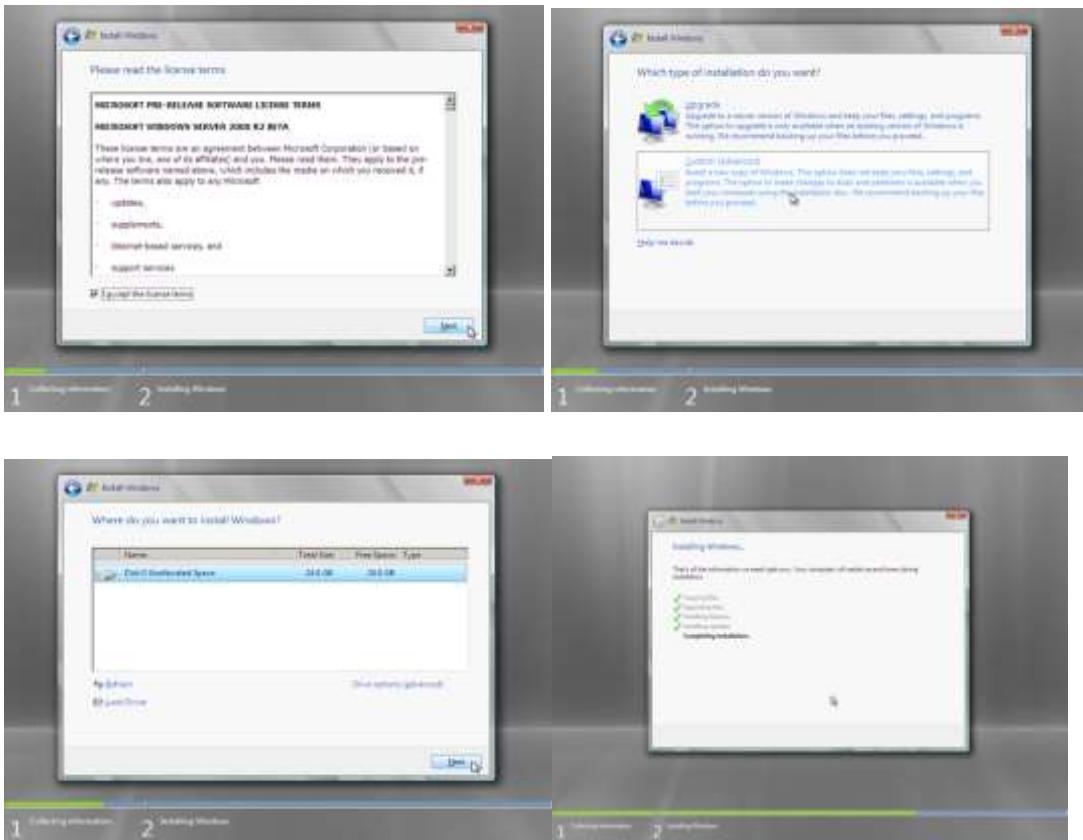
Sistem prvo zahteva da odaberete jezik za instalaciju, vreme i valutu i tip tastature. Kada ste gotovi sa podešavanjem kliknite na next.



Osim ako ne želite da popravite sistem od nekih grešaka, kliknite na Install now opciju.



Sledeći ekran prikazuje vrste instalacija: Možete da izaberete koju će verziju Windows Servera 2008 R2 da instalirate. Disk vam nudi tri različite vrste operativnog sistema i za svaku od njih full verziju sistema ili server core instalaciju. Razlika između ove dve verzije je u tome što server core instalacija sadrži manje servisa od full instalacije. Full instalacija sadrži neke servise koji su možda ređe korišćeni u praksi, pa smo se zato odlučili u ovom slučaju za Server Core instalaciju.



Sada trebate izabrati gde ćeete smestiti instalaciju servera, preporučujem Vam da to bude na C: particiji, naravno. Kada kreirate novu particiju za instalaciju, Windows Server 2008 R2 će vam automatski kreirati dodatnu particiju od 200MB koji koristi za skladištenje nekih sistemskih drajvera.

Instalacioni wizard će vam sada instalirati operativni sistem i restartovati kompjuter kada bude završio.

Četvrti korak - Startovanje po prvi put. Kada instalacioni wizard završi svoje, sistem će vam se boot-ovati po prvi skoro isto kao i na Windows-u 7.

5.7. MREŽNA PROTOK (BANDWICH)

Kao opšteprihvaćena definicija za pojam bandwith se često navodi da je u pitanju količina podataka koja u tačno definisanom vremenskom periodu treba da bude prenesena preko globalne mrže, to jest interneta. Dakle, ovaj pojam se slobodno može prevesti kao opseg ili propusni opseg, ali se neretko događa da se on u oblasti informacionih tehnologija ne upotrebljava uvek pravilno. Obično se smatra da je bandwith količina podataka koji se mogu preneti preko servera, odnosno konkretnе web stranice u tačno definisanom vremenskom roku,

te se iz tog razloga često u praksi može čuti da je mesečni opseg tačno definisan. Ipak, ako bismo želeli da preciznije odredimo pomenuti pojam, rekli bismo da je u pitanju maksimalna količina podatka koji mogu da budu preneti na opisane načine, ali u tačno određenom vremenskom roku.¹⁶

Uzimajući u obzir činjenicu da moja teza pruža jednostavno umreženo rješenje za mali ured, a to je tradicionalna konfiguracija LAN-a s jednim 24-portnim switchom, uključujući 15 hostova i ADSL modem koji djeluje kao usmjerivač za spajanje na mrežu. Utvrđeno je da će širina pojasa biti zajednička svim uređajima i hostovima na mreži, za razliku od VLAN-a (Virtual Local Area Network) koji se sastoji od različitih LAN segmenata i može ponuditi veću propusnost. LAN je dizajniran tako da je sav hardver na mreži bespriječoran, kao i kabeli za povezivanje, Ethernet adapteri su bez grešaka jer bilo koji problem s LAN hardverom može rezultirati sporom ili nefunkcionalnom mrežom.

5.7.1. IZRAČUN KOLIČINE PROTOKA PODATAKA

Imamo 15 računara za koje ćemo uzeti u prosjek da svaki dan downloadaju po 1 GB podataka uzememo li u obzir da je radno vrijeme 8 sati kalkulaciju vršimo na sljedeći način: $15 * 1\text{GB} = 15\text{ GB}$ prometa za 8 sati gdje onda $15\text{GB}/8 = 1.875\text{ GB PROMETA PO SATU}$ ZATIM TAJ BROJ DIJELIMO SA 3600 SEKUNDI KOJI IMAMO U JEDNOM SATU $1.875\text{GB} * 1024 = 1920\text{MB}/3600 = 0.533\text{MBps}$ posto je jedan 1Bajt 8 bita idemo na $0.533 * 8 = 4.26\text{ Mbps}$. Pomoću ove formule smo došli do izračuna da nam je potrebna minimalna brzina interneta od 4.26Mbps. Ako uzmemmo da u BHTELEKOMU imamo paket NET FLAT 10 koji ima pristupnu brzinu do 10 Mbps/1 Mbps uploada po cijeni od 29.90 KM mjesечно.

6. PLANIRANJE LAN ADRESIRANJA ZA MALA PREDUZEĆA

Važnost i bit svake mreže je sposobnost mrežnih uređaja i domaćina da komuniciraju i budu u mogućnosti dijeliti resurse unutar i preko mreže. Da bi komunikacija bila učinkovita mora postojati poruka poslana odredištu iz izvora i obratno. Sve mreže prepoznaju dvije vrste adresa koje su logične (mrežni sloj) i fizička (ili Mac ili hardverska) adresa. MAC adresa je dodijeljena uređaju NIC (kartica mrežnog sučelja) proizvođača uređaja dok se logička adresa ručno ili automatski dodjeljuje nakon nekih određenih setova protokola. U TCP / IP protokolima IP je

¹⁶ Dean, T. 2009. Network+ guide to networks. Fifth edition. Boston, MA: Cengage learning.

osnovni protokol koji je odgovoran za logično adresiranje, stoga je adresiranje mreže u osnovi poziv IP adrese.

Više uređaja povezuje se s internetom budući da je napredak tehnologije neizbjegjan predloženo je da će se u trenutku kada IPv4 adrese iscrpe i pri rješavanju ovog problema otvoriti nova verzija IP adrese pod nazivom IPv6 koja će nadopuniti IPv4. Međutim, IPv4 adrese su još uvijek u upotrebi i koegzistiraju s IPv6 većim dijelom vremena kroz određeni prijelazni mehanizam. IPv4 adrese mogu biti predstavljene u obliku točkastih 32 bitova dok IPv6 ima veličinu od 128 bita i ima velik adresni prostor u odnosu na IPv4.

U dizajnu LAN mreže za male tvrtke, svaki domaćin mora komunicirati s resursom na drugom hostu ili na drugoj mreži izvan ili unutar organizacije. Komunikacija može biti obavijest o slanju i primanju e-pošte, pristupanju novim proizvodima na web-lokaciji, instant poruke, dijeljenje datoteka i još mnogo toga. Predmet planiranja adresa je sinonim za poštansku proceduru dostave pisama, u kojoj se mora utvrditi adresa pošiljatelja. Međutim, da bi se poruka poslala na mrežu, potrebno je pravilno planiranje adresiranja, a uz ove planove može se uspostaviti učinkovita internetska i interna komunikacija. Adresiranje je ključna značajka u protokolima mrežnog sloja koji omogućuje učinkovitu komunikaciju između domaćina na istoj ili različitim mrežama.¹⁷

Informacije na mreži su u obliku paketa ili okvira koji se moraju identificirati s izvornim i odredišnim adresama na krajevima okvira. Uređaj na mreži mora razumjeti koncept TCP / IP-a za razmjenu informacija na mreži. Sva mala poduzeća osmišljena su s ciljem zadovoljavanja budućih izazova novih aplikacija kako se poslovanje povećava, a ključni čimbenik je postizanje tog cilja stvaranjem fleksibilne i skalabilne strukture IP adresiranja koja može podržati rast.

6.1. IP ADRESIRANJE

IP adresiranje je važan čimbenik u prijenosu paketa / okvira između domaćina na istom LAN-u i preko interneta. To je metoda identificiranja hostova i uređaja na mreži, no za slanje i primanje poruka na IP mreži, svakom domaćinu mora biti dodijeljena jedinstvena adresa veličine 32 bita koja je obično predstavljena u obliku koji se naziva decimalni decimal. Adresa duljine 32 bita može se podijeliti na četiri okteta (1 oktet = 8 bita), a svaki oktet se pretvara u

¹⁷ Dean, T. 2009. Network+ guide to networks. Fifth edition. Boston, MA: Cenage learning.

decimalni broj i razdvaja točkama. Uzimajući u obzir, na primjer, IP koji je predstavljen u točkastom obliku decimalnog naziva okteta u obliku

10.10.16.1 koja je povezana samo s IP-v4. Vrijednost u svakom oktetu se kreće od 0-255 Decimala, što je isto kao i 00000000-11111111 u binarnom; stoga je gornja IP adresa ista kao i 00001010.00001010.00010000.00000001 u binarnom. Po dogovoru, prvih nekoliko bitova adrese označavaju klasu kojoj adresa pripada. Klase IP adresiranja u IPV4 protokolu su:

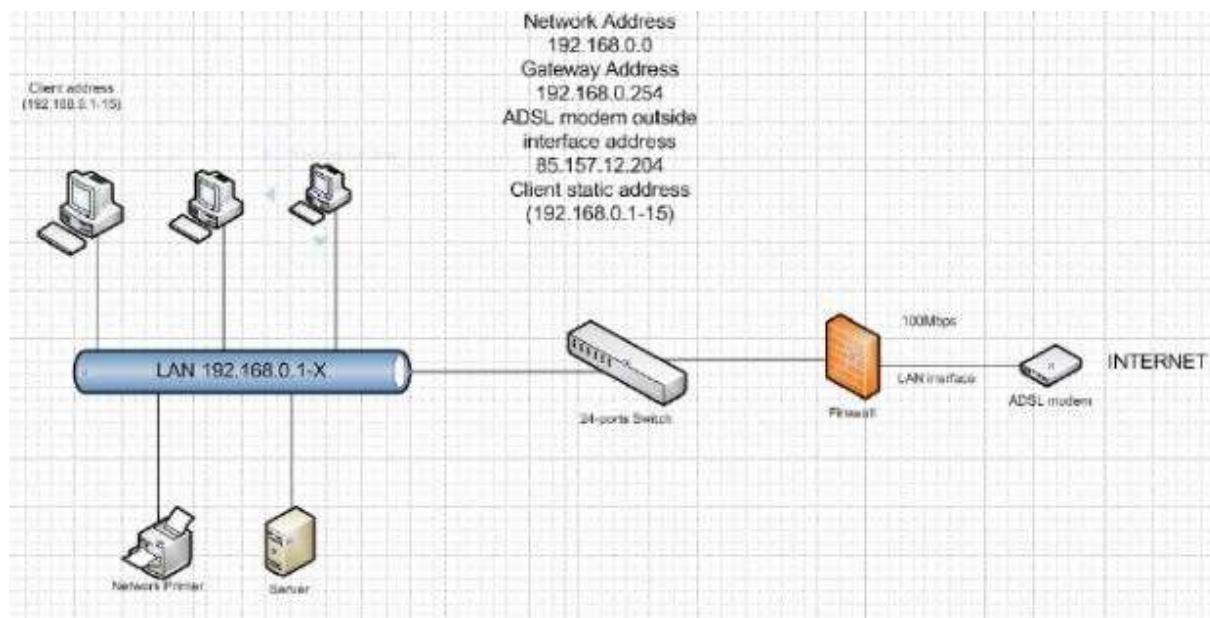
Klase A 10.0.0.0 - 10.255.255.255

Klase B 172.16.0.0 - 172.31.255.255

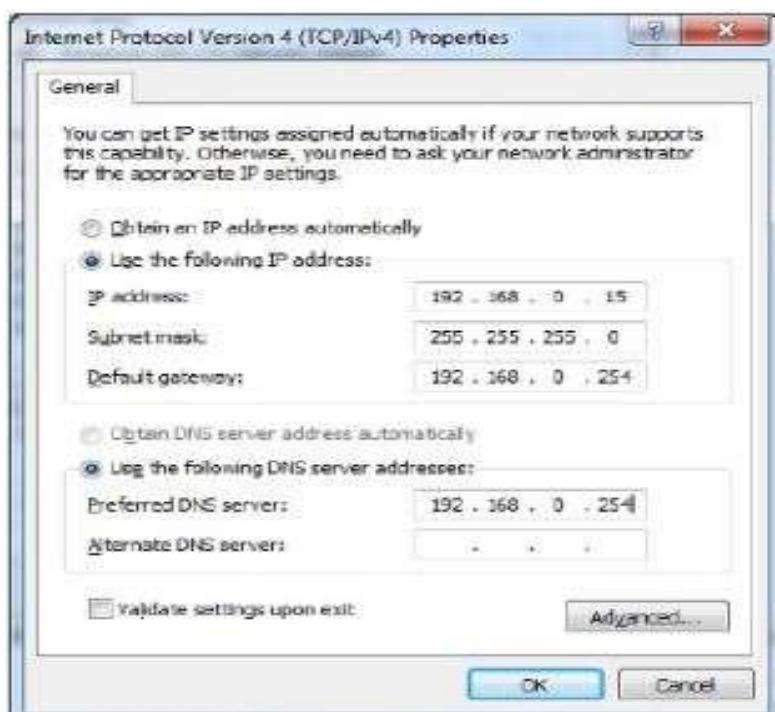
Klase C 192.168.0.0 - 192.168.255.255

Scenario:

Adresiranje mrežnih uređaja izvršeno je nakon što je kabliranje završeno. To smo uradili kako bi se osiguralo da host može komunicirati jedn s drugim i također s ADSL modemom, koji je bio mrežno sučelje. Ping naredba korištena je za testiranje povezanosti unutar LAN-a i izvan LAN-a tako što je pingirala slučajnu web-lokaciju. Za prikaz sažetka mrežnih informacija korištena je naredba ipconfig / all.



Slika 12 Prikaz mrežne topologije sa planom ip adresiranja



Slika 13 IP Adresiranje

Slika 12 i 13 ilustrira IPv4 adresnu postavku za IP adresu hosta 192.168.0.15, masku podmreže 255.255.255.0 i zadani gateway od 192.168.0.254 koja je bila adresa ADSL modema u mreži.

6.2. TESTIRANJE KONEKCIJE

Nakon adresiranja svakog hosta s pojedinačnom jedinstvenom IP adresom, veza s ADSL-om testirana je pomoću naredbe ping 192.168.0.254 i rezultat je prikazan u Slici 14 što pokazuje da je veza s internetom i natrag na host bila uspješna. Povezivanje s pojedinim hostom također je testirano pingiranjem njihove jedinstvne IP adrese naredbom ping host IP adresa. Pingovanje hosta 192.168.0.2 dobivamo rezultat prikazan u slici 15. Rezultat pokazuje da je pingiranje bio uspješno, jer smo ostvarili komunikaciju između domaćina i mreže. Također smo pingirala na slučajne web stranice preko naredbe ping websitename i rezultat je prikazan u Slici 16, koji pokazuju da host može komunicirati s drugim hostom na različitim mrežama. Na Slici 17 prikazan je sažetak mreže s hosta na mrežu, rezultat pokazuje da je u mreži uspjesno implementirana IPv4 adresa, adresa pristupnika, Mac adresa hosta i maska podmreže.

```
cmd C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\LASISI>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:
Reply from 192.168.0.254: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\LASISI>
```

Slika 14 Pingovanje modema

```
cmd C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\LASISI>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time=2ms TTL=128
Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\LASISI>
```

Slika 15 Pingovanje hosta 192.168.0.2

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\LASISI>ping www.coolfm.com

Pinging www.coolfm.com [82.98.86.161] with 32 bytes of data:
Reply from 82.98.86.161: bytes=32 time=227ms TTL=55
Reply from 82.98.86.161: bytes=32 time=267ms TTL=55
Reply from 82.98.86.161: bytes=32 time=305ms TTL=55
Reply from 82.98.86.161: bytes=32 time=249ms TTL=55

Ping statistics for 82.98.86.161:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 227ms, Maximum = 305ms, Average = 262ms.

C:\Users\LASISI>
```

Slika 16 Pingovanje nasumične web stranice

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\LASISI>ipconfig /all

Windows IP Configuration

Host Name . . . . . : LASISI-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address . . . . . : E8-11-32-67-DA-58
    DHCP Enabled . . . . . : No
    Autoconfiguration Enabled . . . . . : Yes
    IPv4 Address . . . . . : 192.168.0.12(Preferred)
        Subnet Mask . . . . . : 255.255.255.0
        Default Gateway . . . . . : 192.168.0.254
        DNS Servers . . . . . : 192.168.0.254
    NetBIOS over Tcpip . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Bluetooth Device (Personal Area Network)
    Physical Address . . . . . : B4-74-9F-D3-E9-16
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter isatap.regionline.fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft ISATAP Adapter
    Physical Address . . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled . . . . . : No
    Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter 6TO4 Adapter:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft 6to4 Adapter
    Physical Address . . . . . : 0A-0A-0A-0A-0A-0A-E0
    DHCP Enabled . . . . . : No
    Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter isatap.{3CB40107-2E80-4907-9B4A-660PA7860A88}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
```

Slika 17 Infomracije hostova u mreži

7. ZAKLJUČAK

Ovaj tezom možemo zaključiti da plansko postavljanje mreže u samim početcima preduzeća može dovesti do unaprijeđenja poslovanja a isto tako i u budućnosti kada budemo trebali nadograditi mrežu za veće potrebe posao će biti mnogo lakši.Ovim radom smo uvidjeli koje sve izazove i rezultate nosi plansko planiranje mreže i sa čime se sve možemo susresti prilikom dizajna i implementacije.Za sad po svim standardima i našim testiranjima mreža funkcioniše bezprijekorno, međutim pravi test za mrežu će donjeti njenu korištinje što može da izazove neke nove probleme na koje moramo biti spremni da na vrijeme rjesimo.Obzirom da smo preduzeli određene korake da zaštitimo našu mrežu trebala bi biti sigurna od vanjskih napada,ali kako napadi svaki dan postaju sve softiciranjem tako i mi moramo našu mrežu održavati i updateovati po najnovijm standardima i rješenjima.Da bi naša mreža što bolje funkcionsala potrebno je da izvršimo osnovnu edukaciju korisnika mreže da bi naša mreža što bolje bila zaštićena od ljudske greške koja je među najvećim postocima uzroka pada svake mreže.S toga pravilna edukacija korsnika mreže i redovito održavanje trebalo bi da dovede do toga da naša mreža bez problema radi 24 sata na dan u svim uslovima.

8. LITERATURA

- [1] <https://mrejniuredjaji.wordpress.com/>
- [2] <http://etutorials.org/>
- [3] <https://www.schalley.eu/>
- [4] 37 Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 13 38
CERT, LSS (2010) Metode zaštite dokumenata, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str.
- [5] <http://mreze.layer-x.com/>
- [6] <https://repozitorij.fpz.unizg.hr/islandora/object/fpz:458/preview>
- [7] <https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-04-296.pdf>
- [8] Barman, S. 2001. Writing Information Security Policies. Sams publishing.
- [9] Network bandwidth . University of California. Available: <http://www.ucsc.edu/security/bandwidth.html>. UC Santa Cruz, 1156 High Street, Santa Cruz
- [10] Dean, T. 2009. Network+ guide to networks. Fifth edition. Boston, MA: Cenage learning.
- [11] Networking, . Available: http://en.wikipedia.org/wiki/network_topology
- [12] IEEE Computer Society. LAN/MAN Standards Committee, Institute of Electrical and Electronics Engineers, and IEEE-SA Standards Board, IEEE standard for information technology telecommunications and information exchange between systems : local and metropolitan area networksspecific requirements. Part 11, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. New York: Institute of Electrical and Electronics Engineers, 2012. [Online]. Available: <http://ieeexplore.ieee.org/servlet/opac?punumber=6178209>

- [13] S. Karris, Networks: Design and Management. Orchard Publications, Jan. 2009.
- [14] Cisco, Inter-Switch Link and IEEE 802.1Q Frame Format, Cisco, Tech. Rep
- [15] Cisco Systems, Inc. 2004. Cisco IOS Network Address Translation. PDF file,
- [16]https://www.cisco.com/en/US/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.pdf Referred 22.11.2016.
- [17] Bonaventure, Olivier, 2011. Computer Networking. PDF file.
- [18] <http://www.saylor.org/site/wp-content/uploads/2012/02/Computer-NetworkingPrinciples-Bonaventure-1-30-31-OTC1.pdf> Referred 18.11.2016.
- [19] Allied Telesis 2015. Virtual LANs. PDF file.
- [20] https://www.alliedtelesis.com/sites/default/files/vlan_feature_config_guide_revb.pdf
- [21] Meghanathan, N 2014. Network Security: Attacks and Control. PDF file.
<https://arxiv.org/ftp/arxiv/papers/1412/1412.6017.pdf>