SVEUČILIŠTE J. J. STROSSMAYERA U OSIJEKU

**FAKULTET ELEKTROTEHNIKE
RAČUNARSTVA I INFORMACIJSKIH
TEHNOLOGIJA OSIJEK**

SIGURNOST INFORMACIJA U PRAKTIČNIM PRIMJENAMA

Priručnik za laboratorijske vježbe

Višnja Križanović, Krešimir Grgić, Ana Pejković

Osijek, 2026.

Izdavač
Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek

Za izdavača
prof. dr. sc. Tomislav Matić

Autori
izv. prof. dr. sc. Višnja Križanović
prof. dr. sc. Krešimir Grgić
Ana Pejković, univ. mag. ing. el.

Recenzenti
prof. dr. sc. Mario Kušek
Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva
prof. dr. sc. Slavko Rupčić
Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek

Lektor
izv. prof. dr. sc. Dragana Božić Lenard
Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek

Srpanj, 2026. godine

ISBN 978-953-8184-11-6

Sveučilište Josipa Jurja Strossmayera u Osijeku

Suglasnost za izdavanje ovog sveučilišnog priručnika
donio je Senat Sveučilišta Josipa Jurja Strossmayera u Osijeku
na 10. sjednici održanoj 15. srpnja 2026. godine pod brojem 20/26.

Sadržaj:

Vježba 1. - Sigurnosni aspekti bežične komunikacije:
Sigurnosne postavke za pristup bežičnoj lokalnoj mreži (WLAN)

UVOD

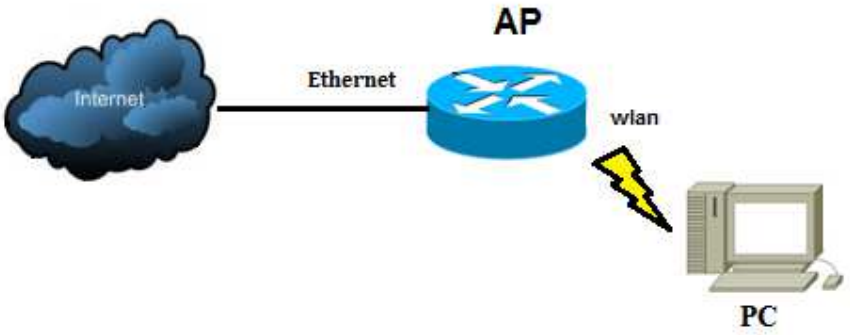
Bežična lokalna mreža (eng. *Wireless Local Area Network*, WLAN) sastoji se od bežično povezanih mrežnih sučelja, pri čemu se bežična komunikacija odvija u određenim frekvencijskim područjima (npr. 2.4 GHz, 3.7 GHz, 5 GHz i 60 GHz). Način komunikacije između bežično povezanih sučelja definira se kroz odgovarajuće standarde bežičnih lokalnih mreža. Među osnovnim standardima bežičnih lokalnih mreža izdvaja se IEEE 802.11 skup standarda koji definira bežičnu komunikaciju na fizičkom sloju te na sloju podatkovne veze. Ovaj skup standarda obuhvaća IEEE 802.11a/n/ac (5GHz) i 802.11b/g/n (2.4GHz) inačice standarda.

Pojedine inačice navedenog standarda koje koriste različita frekvencijska područja su međusobno nekompatibilne. Stoga neki proizvođači mrežne opreme proizvode hibridna rješenja. Međutim, pri implementaciji takve opreme svaki od povezanih uređaja mora koristiti samo jedan od podržanih standarda. Razlike između pojedinih inačica postoje i u dostupnim brzinama prijenosa podataka (802.11a: 54Mbps / 802.11b: 11Mbps / 802.11g: 54Mbps / 802.11n (2.4/5GHz): 300/600Mbps). Rješenja koja rade u nižim frekvencijskim područjima u pravilu imaju veći domet signala (npr. ona u 2.4GHz u odnosu na ona u 5GHz). Pri radu bežičnih kouminkacijskih uređaja može doći do interferencije s uređajima koji rade u istom frekvencijskom području (npr. kao kod 802.11b/g/n), pa usklađivanje frekvencija sprječava interferenciju (npr. kao kod 802.11a/n/ac).

Komunikacijski uređaji u bežičnim lokalnim mrežama koji se ponašaju kao središnji predajnik i prijemnik bežičnih signala nazivaju se pristupnim točkama (eng. *Access Point*, AP). Pristupne točke komuniciraju s bežičnim klijentima, žičnom mrežom te s drugim pristupnim točkama. Na pristupnu točku može se povezati do 255 klijenata. Standardne bežične pristupne točke podržavaju prethodno navedene standarde i koriste se za pokrivanje određenog područja bežičnim signalom. U slučaju primjene više bežičnih pristupnih točaka područje pokrivenosti signalom je veće. Dok je u kućnim mrežama najčešće potrebna samo po jedna pristupna točka, poslovne se mreže najčešće sastoje od više pristupnih točaka. Utvrđivanje optimalne lokacije na kojoj je potrebno postaviti pristupne točke je važno je za kvalitetno pokrivanje određenog područja signalom.

Pristupne točke mogu biti konfigurirane kako bi radile na jedan od sljedećih načina:

- korijenski (u slučaju kada je pristupna točka na koju se bežično povezuju klijenti povezana sa žičnom mrežom preko jednog od svojih žičnih sučelja),
- umošćeni (u slučaju kada se na pristupnu točku ne povezuju klijenti već se ona koristi za povezivanje više mrežnih segmenata bežičnim putem)
- obnavljački (u slučaju kada neka pristupna točka koja se povezuje na korijensku pristupnu točku služi kao bežični mrežni obnavljač).



Slika 1.1. *Povezivanje krajnjeg uređaja (PC) na bežičnu pristupnu točku (AP)*

Pri povezivanju uređaja koristi se:

- *ad hoc* način rada – povezivanje više bežičnih uređaja čiji se položaj može mijenjati, a koji ne koriste neki centralni uređaj pri komunikaciji već svaki povezani uređaj izravno prosljeđuje podatke bilo kojem od ostalih uređaja u meži;
- infrastrukturni način rada – pri komunikaciji klijenti koriste bežičnu pristupnu točku povezanu na žičnu mrežu, i pristupna točka i klijenti koriste istu oznaku mreže.

Primjena *ad hoc* konekcija pogodna je kada je potrebno omogućiti izravnu komunikaciju između uređaja, međutim ograničenje *ad hoc* načina rada predstavlja činjenica da u određenim primjerima primjene nije prikladan za ukupne prometne zahtjeve. U usporedbi s *ad hoc* bežičnim mrežama, infrastrukturni način rada omogućuje centralizirano upravljanje mrežom, a primjena dodatnih pristupnih točaka može smanjiti prometno zagušenje te proširiti domet same mreže.

PRIPREMA ZA VJEŽBU

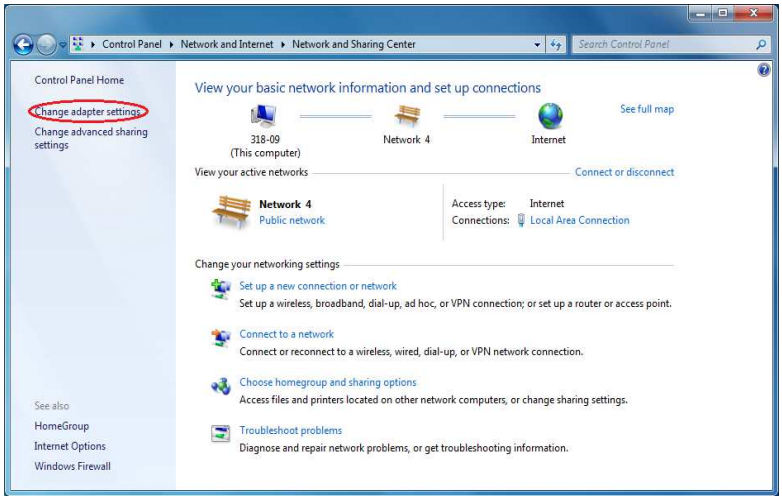
- Proučiti navedena načela prema kojima se omogućuje sigurna komunikacija u bežičnim mrežama uz primjenu postojećih inačica protokola zaštićenog pristupa Wi-Fi-ju (*Wi-Fi Protected Access,* skr. WPA).

KREIRANJE ODABRANOG TESTNOG SCENARIJA:

Kroz korake (A)-(D) definiran je postupak uspostave testnog okruženja. Ovaj postupak obuhvaća deaktivaciju svih mrežnih konekcija na računalu PC1 osim lokalne mreže, isključivanje vatrozida (eng. *firewall*) **te resetiranje postavki usmjerivača** (eng. *router*). Preostali koraci (I)-(V) vezani su uz konfiguraciju postavki usmjerivača i klijenta (PC1) i testiranje mogućnosti (ne)ovlaštenog pristupa kreiranoj mreži.

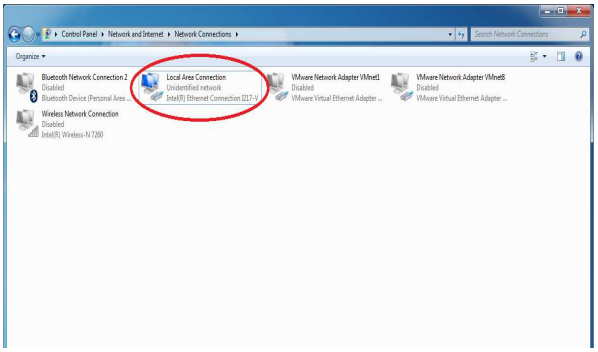
(A) DEAKTIVIRANJE POJEDINIH MREŽNIH KONEKCIJA NA KLIJENTIMA

(1) Na računalu otvorite prozor upravljačke ploče (eng. *Control Panel*), zatim odaberite poveznicu vezanu uz postavke mreže i Interneta (eng. *Network and Internet*), te zatim poveznicu vezanu uz opcije središta za umrežavanje i dijeljenje (eng. *Network and Sharing Center*).



Slika 1.2. *Prikaz opcija promjene postavki mrežnog adaptera (eng. Change Adapter Settings) središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

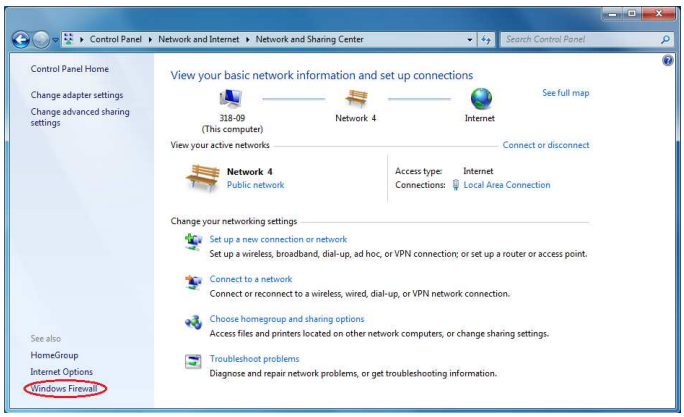
(2) Kliknite na opciju promjene postavki mrežnog adaptera (eng. *Change Adapter Settings*). Omogućena (eng. *enabled*) treba ostati samo **lokalna žična konekcija** (eng. *Local Area Connection*, LAN). Deaktivirajte (eng. *disable*) sve ostale mrežne konekcije na računalima (za pojedina bežična, žična i virtualna sučelja), osim navedenih, tako što ćete pritisnuti desnu tipku miša nad odgovarajućom konekcijom i odabrati opciju za onemogućavanje (*Disable*).



Slika 1.3. *Prikaz postavki mrežnih konekcija (Network Connections) na računalu u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

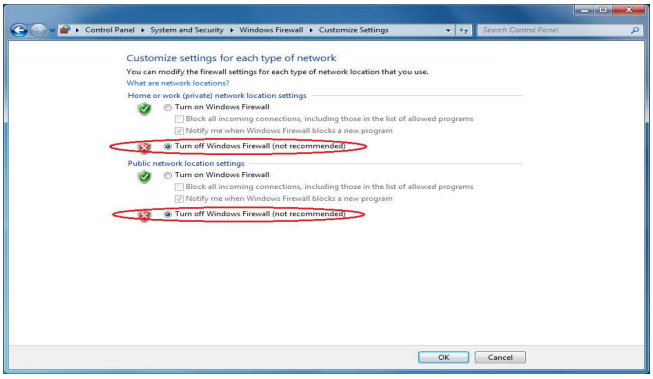
(B) ISKLJUČIVANJE VATROZIDA NA KLIJENTIMA

(3) Na računalu otvorite prozor upravljačke ploče (*Control Panel*), zatim odaberite poveznicu vezanu uz postavke mreže i Interneta (*Network and Internet*), te zatim poveznicu vezanu uz opcije središta za umrežavanje i dijeljenje (*Network and Sharing Center*).



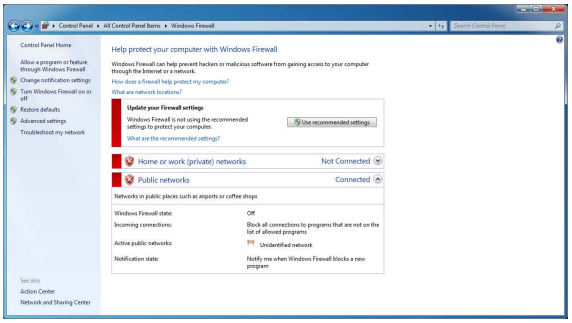
Slika 1.4. *Prikaz opcije za pristup postavkama Windows vatrozida (Windows Firewall) središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

(4) Isključite vatrozid ukoliko je pokrenut na računalu prema sljedećem postupku. Odaberite poveznicu koja otvara prozor s postavkama središta za umrežavanje i dijeljenje (*Network and Sharing Center*), zatim otvorite prozor s postavkama vatrozida (*Windows Firewall*), odaberite izbornik za uključivanje i isključivanje vatrozida (*Turn Windows Firewall on or off*) i isključite vatrozid (*Turn off Windows Firewall*).



Slika 1.5. *Prilagođavanje postavki (Customize Settings) za isključivanje Windows vatrozida (Windows Firewall)*

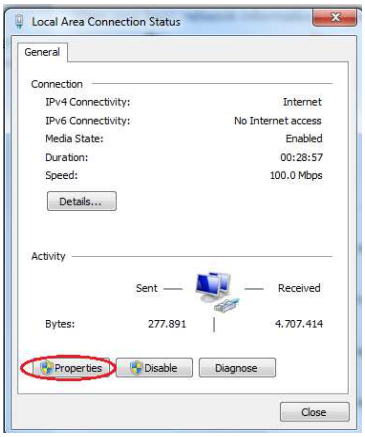
(5) Prikaz nakon deaktivacije vidljiv je na slici.



Slika 1.6. *Prikaz nakon deaktivacije Windows vatrozida*

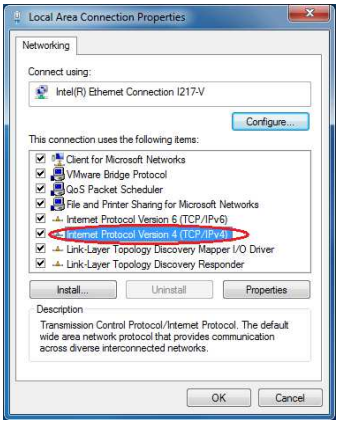
(C) DINAMIČKO ADRESIRANJE KLIJENATA

(6) U prozoru s opcijama središta za umrežavanje i dijeljenje (*Network and Sharing Center*) odaberite opciju promjene postavki mrežnog adaptera (*Change Adapter Settings*), zatim odaberite lokalnu mrežnu konekciju (*Local Area Connection*) i zatim njene postavke (*Properties*).



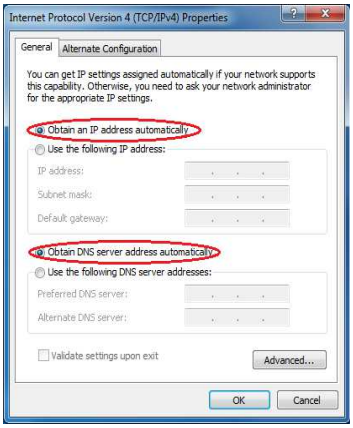
Slika 1.7. *Provjera postavki lokalne mreže (Local Area Connection Status) na računalu*

(7) Odaberite opciju prikaza postavki protokola IPv4 (*Internet Protocol Version 4 (TCP/IPv4)*).



Slika 1.8. *Provjera postavki lokalne konekcije (Local Area Connection Properties) na računalu*

(8) Provjerite jesu li odabrane sljedeće opcije prema prikazu sa slike: automatska dodjela IP adrese (*Obtain an IP address automatically*) te automatska dodjela adrese DNS poslužitelja (*Obtain DNS server address automatically*), te ih odaberite ukoliko već nisu odabrane.



Slika 1.9. *Provjera postavki na računalu za automatsku dodjelu IPv4 adrese i adrese DNS servera*

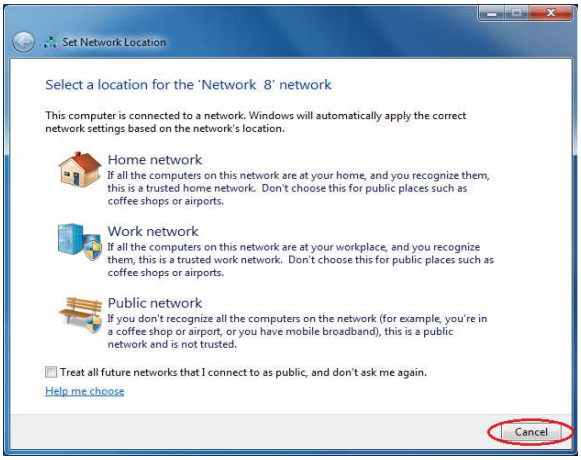
(D) RESETIRANJE POSTAVKI USMJERIVAČA

(9) Uključite usmjerivač. Povežite računalo PC1 na *Ethernet2* sučelje usmjerivača pomoću *patch* kabela, prema *shemi* na donjoj slici.

a) b)

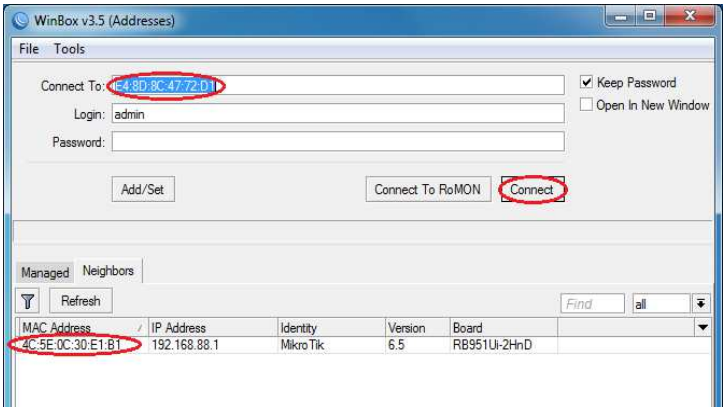
Slika 1.10. *a) Način povezivanja PC1 uređaja i MikroTik usmjerivača i b) MikroTik usmjerivač sa označenim Ethernet2 portom*

(10) Nakon što se otvori izbornik postavki lokacije mreže (*Set Network Location*) odaberite opciju izuzeća (*Cancel*).



Slika 1.11. *Izbornik postavki lokacije mreže* (*Set Network Location*)

(11) Pokrenite *WinBox* aplikaciju čija se ikona nalazi na radnoj ploči (eng. *Desktop*) računala. Prvo označite MAC adresu (eng. *MAC Address*) usmjerivača koja se nalazi na popisu u donjem dijelu prozora, a zatim kliknite na opciju za povezivanje (*Connect*).



Slika 1.12. *Sučelje WinBox aplikacije*

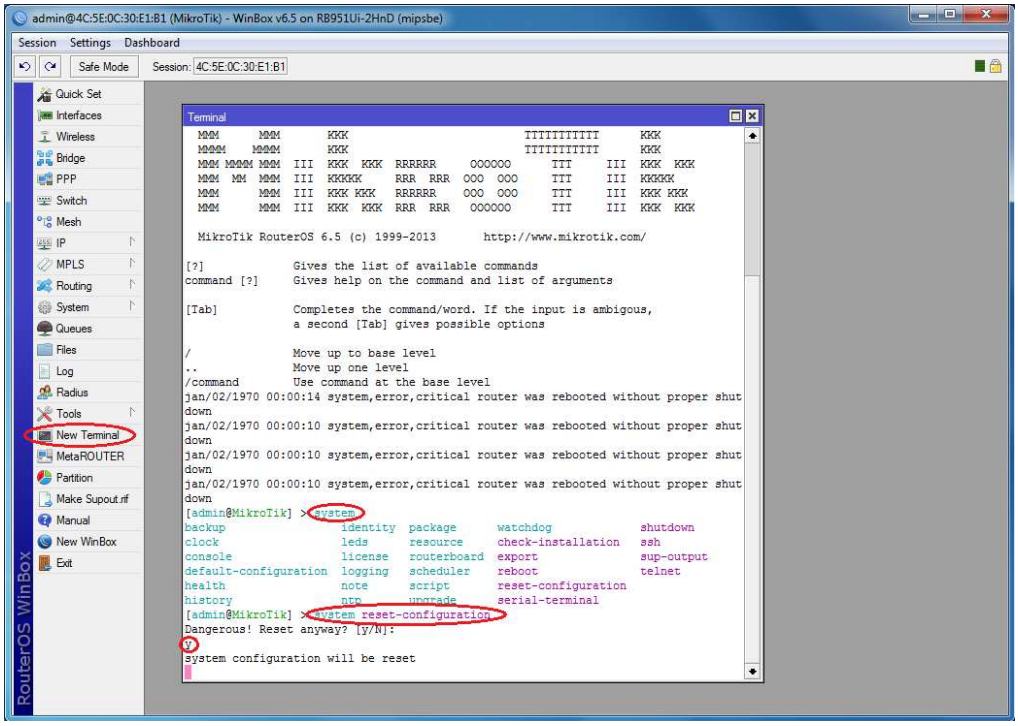
(12) Unutar otvorenog sučelja aplikacije *WinBox* odaberite opciju za otvaranje novog terminala (*New Terminal*). Otvara se terminal prikazan na donjoj slici.
Resetirajte postavke na usmjerivaču upisivanjem naredbe:

system reset-configuration

i pomoću tipkovnice potvrdite upis odabirom tipke *Enter* te još jednom potvrdite izbor upisivanjem naredbe:

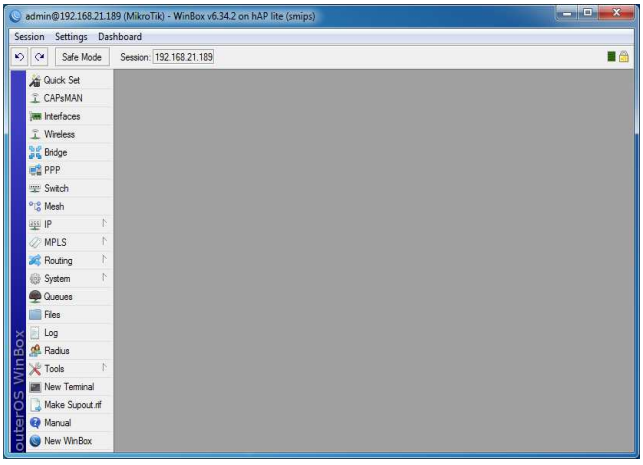
y

te odabirom tipke *Enter*. Ovime se pokreće resetiranje postojeće konfiguracije te se konfiguracija usmjerivača vraća na tvornički definiranu.



Slika 1.13. *Prikaz terminala WinBox aplikacije*

(13) Nakon ponovnog otvaranja *WinBox* aplikacije, prikaz bi trebao odgovarati prikazu na slici 1.14.



Slika 1.14. *Početno sučelje WinBox aplikacije*

Zadaci:

U vježbi je potrebno testirati mogućnosti primjene usmjerivača kao bežične pristupne točke. Potrebno je kreirati topologiju u kojoj će se krajnji uređaji povezati na Internet preko konfigurirane pristupne točke te testirati komunikaciju u kreiranoj mreži.

UPUTE ZA RAD:

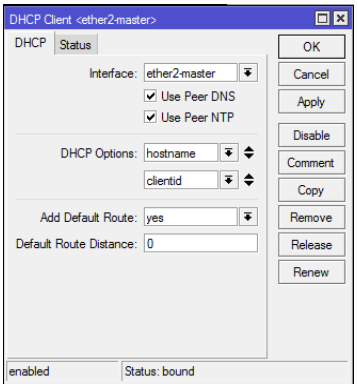
(I) ODREĐIVANJE ADRESA AKTIVNIH SUČELJA

Zadatak 1. Pokrenite naredbeni redak (***Command Prompt***) upisivanjem naredbe ***cmd*** unutar *Windows*-ovog *Start* izbornika i provjerite IP adresu koja je automatski dodijeljena računalu PC1 upisivanjem naredbe ***ipconfig*** u naredbeni redak (*Command Prompt*). Ispišite sljedeće:

- adresu računala PC1 (*IPv4 Address*): _____
- adresu maske podmreže (*Subnet Mask*): _____
- adresu aktivnog *Ethernet2* sučelja usmjerivača (*Default Gateway*): _____

(14) U nastavku je opisan osnovni postupak konfiguriranja protokola za dinamičku konfiguraciju klijenta (eng. *Dynamic Host Configuration Protocol*, DHCP) na *Ethernet2* sučelju usmjerivača. Iz izbornika odaberite tip protokola (*IP*), zatim vrstu klijenta (*DHCP Client*) te opciju dodavanja novog klijenta (*Add New*). Postavke DHCP klijenta načinite prema slici:

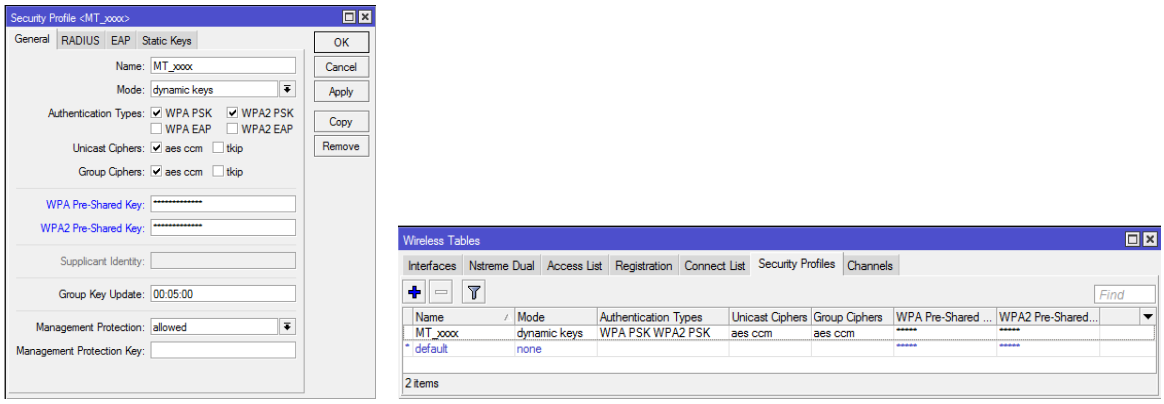
- definirajte sučelje (eng. *Interface*): *Ethernet2*
- definirajte sljedeće DHCP opcije (eng. *DHCP Options*): ime hosta (*hostname*) te identifikator klijenta (*clientid*). Potvrdite izbor (*OK*).



Slika 1.15. *Prikaz unutar Winbox-a opcija DHCP klijenta (DHCP Client) na Ethernet2 sučelju*

(II) KONFIGURIRANJE POSTAVKI BEŽIČNE MREŽE

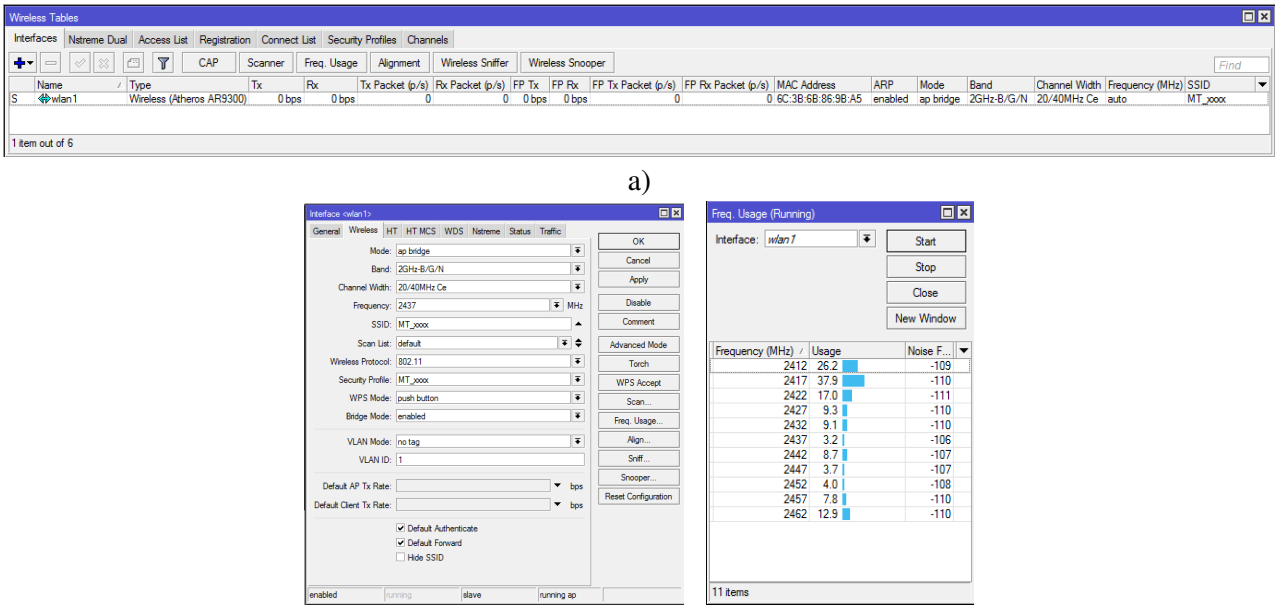
(15) Kroz sljedećih nekoliko koraka potrebno je konfigurirati bežični pristup putem kojeg bi se trebala ostvariti bežična konekcija između usmjerivača i klijenata. Nakon otvaranja izbornika za postavke bežične mreže (*Wireless*) unutar kartice (eng. *tab*) sigurnosnih profila (*Security profiles*) te izbora opcije dodavanja (*Add*) potrebno je odabrati ime i lozinku profila koju pristupna točka koristi. Pri definiranju naziva potrebno je koristiti sljedeću oznaku: *MT_xxxx*, pri čemu umjesto simbola '*xxxx*' treba upisati vlastiti broj indeksa. Pod opcijom načina rada (*Mode*) potrebno je odabrati dinamičke ključeve (*dynamic keys*), označiti polja *WPA PSK* i *WPA2 PSK* te upisati željenu *WPA* i *WPA2* lozinku (*Pre-Shared Key*).



a) b)

Slika 1.16. *a) Prikaz kartice za definiranje sigurnosnog profila (Security Profile) i b) izbornika za definiranje tablica s postavkama bežičnog pristupa (Wireless Tables)*

(16) U izbornika za postavke bežične mreže (*Wireless*) unutar kartice sučelja (*Interfaces*) potrebno je odabrati postojeću *wlan1* konekciju. Pri konfiguraciji je potrebno za način rada (eng. *Mode*) odabrati umošćivanje pristupne točke (*ap bridge*), što znači da usmjerivač služi kao pristupna točka. Izabran je frekvencijski pojas (*Band*) 2GHz B/G/N. Frekvencija (eng. *Frequency)* koja je izabrana iznosi 2437 MHz, jer se ona u ovom slučaju najmanje koristi, a do informacije o najčešće korištenoj frekvenciji se dolazi odabirom opcije koja prikazuje korištenje frekvencija (*Freq. Usage*). Pod naziv bežične mreže (*SSID*) se treba upisati naziv pristupne točke. U opciji sigurnosnog profila (*Security Profile*) označen je prethodno kreirani profil '*MT_xxxx*'.



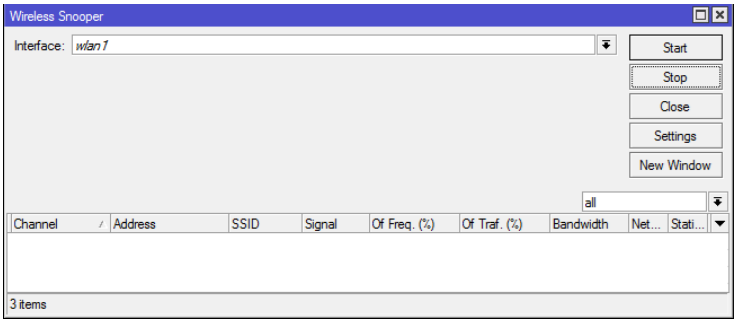
a)

b) c)

Slika 1.17. *a) Konfiguriranje tablica s postavkama bežičnog pristupa (Wireless Tables) i b) wlan1 sučelja (Interface) te c) prikaz primjene frekvencija (Freq. Usage) aktivnog wlan1 sučelja*

(17) Neki od dodatnih alata koji se nalaze unutar *wlan1* sučelja su *Torch, Scanner, Sniffer* te *Snooper.* Za razliku od alata *Torch* koji se koristi za praćenje prometa koji prolazi kroz *wlan* sučelje te za njegovu klasifikaciju (ovisno o protokolima, izvorišnoj i odredišnoj adresi te portovima), alat *Snooper* nadgleda frekvencijske kanale koji se primjenjuju pri komunikaciji, kao i same uređaje koji koriste određeni frekvencijski kanal.

Zadatak 2. U predviđeni prostor na slici upišite nekoliko zapisa dobivenih nakon pokretanja alata *Snooper*.



Slika 1.18. *Prikaz zapisa alata Snooper*

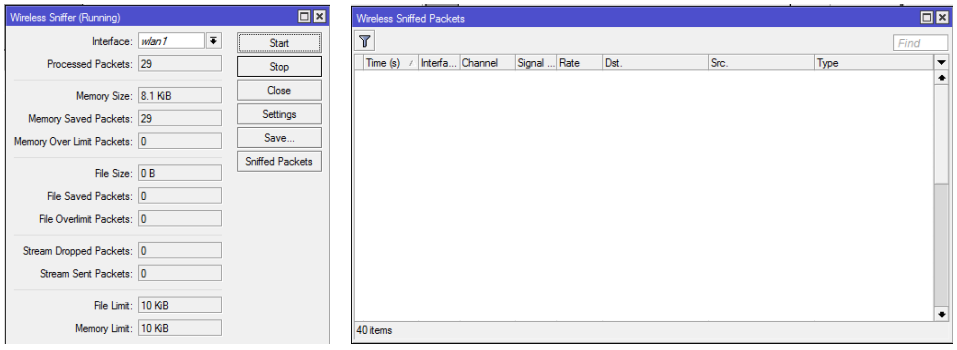
(18) Alat *Scanner* omogućuje pregled svih pristupnih točaka u frekvencijskom dometu koje su definirane u listi skeniranja. Ta naredba će prikazivati pristupne točke sve dok korisnik ne zaustavi proces skeniranja.

Zadatak 3. U predviđeni prostor na slici upišite nekoliko zapisa dobivenih nakon pokretanja alata *Scanner*.

Slika 1.19. *Prikaz zapisa alata Scanner*

(19) Alat *Scanner* omogućuje prikaz dodatnih informacija.

Zadatak 4. U predviđeni prostor na slici upišite nekoliko zapisa dobivenih nakon pokretanja alata *Sniffer*.



Slika 1.20. *Prikaz zapisa alata Sniffer*

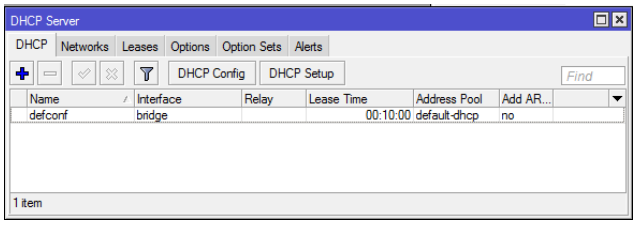
Zadatak 5. Navedite koje dodatne informacije su prikazane:

_____

_____

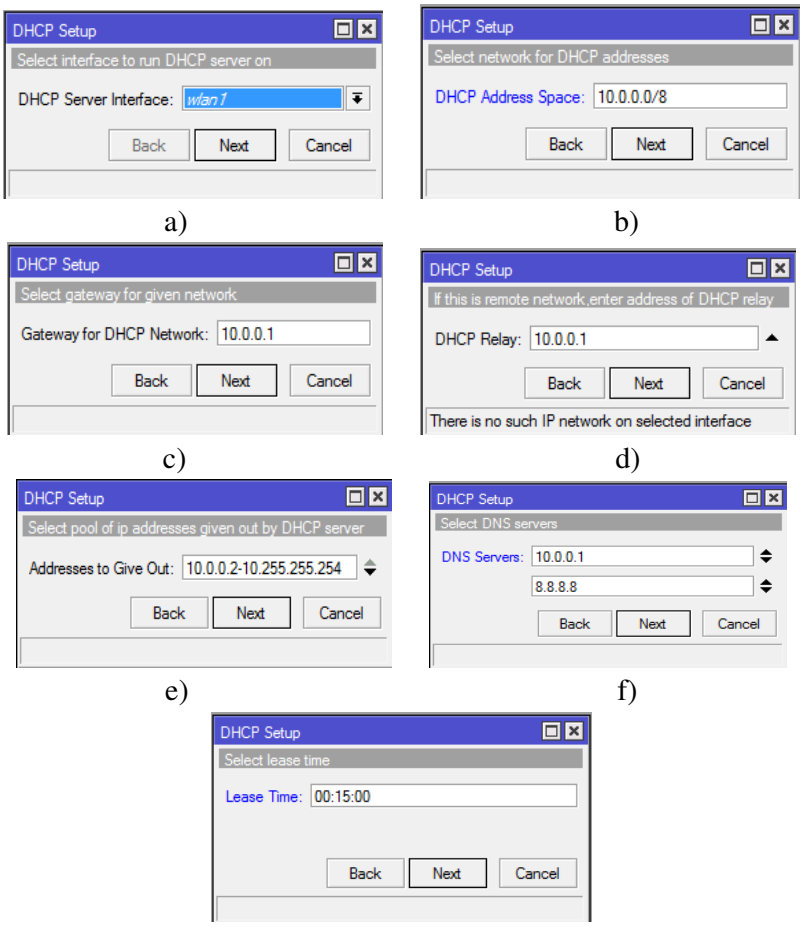
(III) KONFIGURIRANJE DHCP POSLUŽITELJA NA SUČELJU USMJERIVAČA

(20) Idući korak je kreiranje DHCP poslužitelja (*DHCP Server*) na *wlan1* sučelju odabirom sljedećih opcija: tipa protokola (*IP*), DHCP poslužitelja (*DHCP Server*), vrste protokola (*DHCP*), te postavki DHCP-a (*DHCP Setup*).



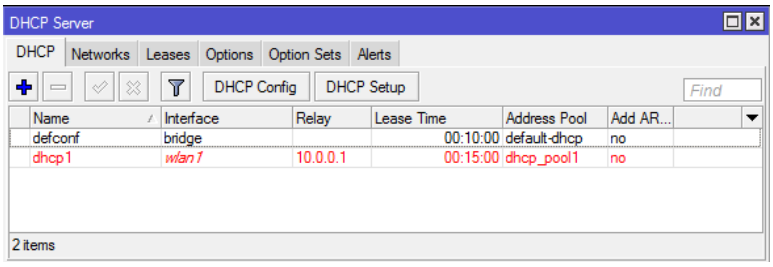
Slika 1.21. *Prikaz izbornika s opcijama za definiranje DHCP poslužitelja (DHCP Server)*

(21) Opcije koje se u ovom koraku konfiguriraju na *wlan1* sučelju su DHCP adresni prostor, pristupnik (eng. *gateway*) za DHCP mrežu, raspon adresa koje se mogu koristiti, te DNS poslužitelji. Raspon adresa korišten pri konfiguraciji je blok privatnih IP adresa za lokalno adresiranje: 10.0.0.2-10.255.255.254. Dodatni DNS poslužitelj je *Google* koji omogućuje pristup Internetu u slučaju da to konfigurirani DNS poslužitelj ne može.

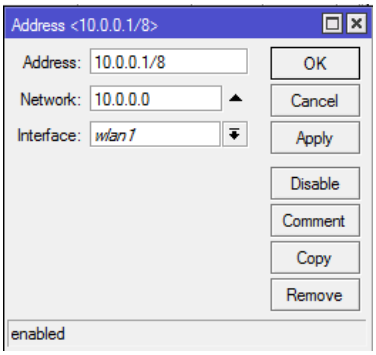


Slika 1.22. a) *Postavke sučelja DHCP poslužitelja (DHCP Server Interface), b) definiranje DHCP adresnog prostora (DHCP Address Space), c) postavljanje pristupnika za DHCP mrežu (Gateway for DHCP Network), d) definiranje DHCP prijenosa (DHCP Relay), e) definiranje adresa za dodjelu (Addresses to Give Out), f) definiranje DNS poslužitelja (DNS Servers) i g) definiranje vremena dodjele (Lease Time)*

(22) U idućem koraku potrebno je postaviti IP adresu *wlan1* sučelja odabirom izbornika tipa protokola (*IP*), adrese (*Addresses*) i njenog dodavanja (*Add*) te upisivanjem odgovarajuće adrese 10.0.0.1/8.



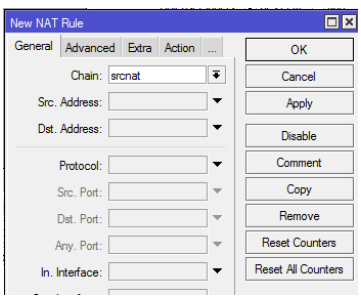
a)



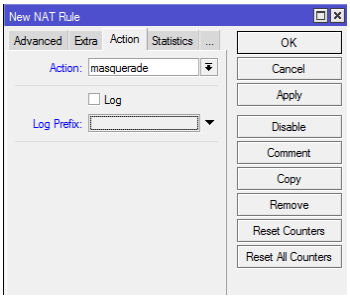
b)

Slika 1.23. *a) Prikaz definiranih postavki DHCP poslužitelja (DHCP Server) i b) adrese (Address) wlan1 sučelja te mreže (Network)*

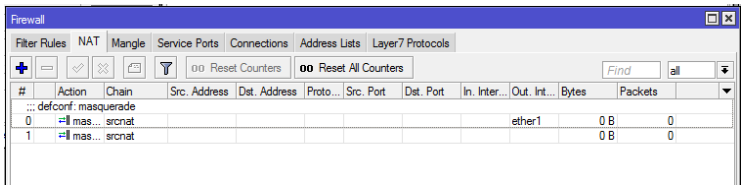
(23) Na poslijetku je potrebno omogućiti prevođenje mrežnih adresa odabirom izbornika tipa protokola (*IP*), vatrozida (*Firewall*), prevođenja mrežnih adresa (*NAT*) te opcije dodavanja (*Add*). Unutar kartice s općim postavkama (*General*) potrebno je postaviti lanac (*Chain*) za prevođenje izvorne mrežne adrese (*srcnat*), a unutar kartice aktivnosti (*Action*) odabrati opciju maskiranja (*masquerade*).



a)



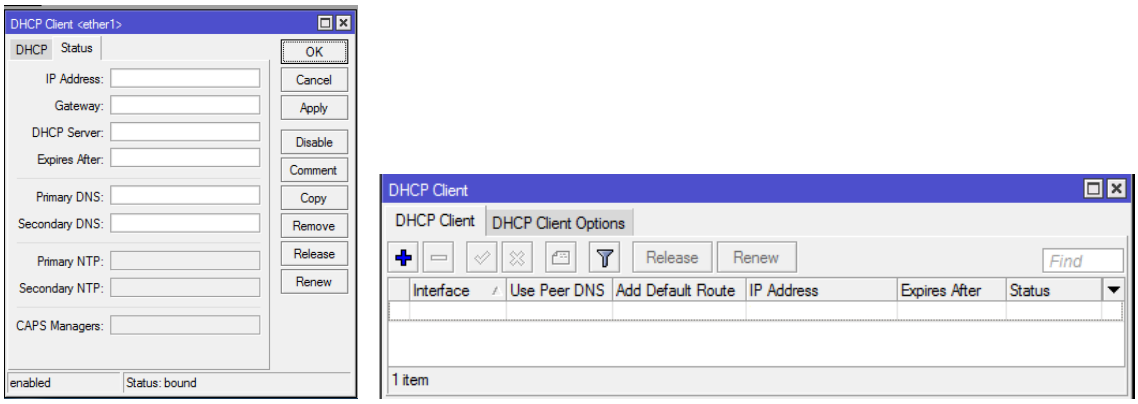
b)



c)

Slika 1.24. *a) Dodavanje novog NAT pravila (New NAT Rule) za prevođenje mrežnih adresa, b) definiranje postupka (Action) maskiranja adresa (masquerade) i c) prikaz izbornika s definiranim opcijama prevođenja mrežnih adresa*

Zadatak 6. U predviđeni prostor na slikama upišite sve dodijeljene oznake i adrese.

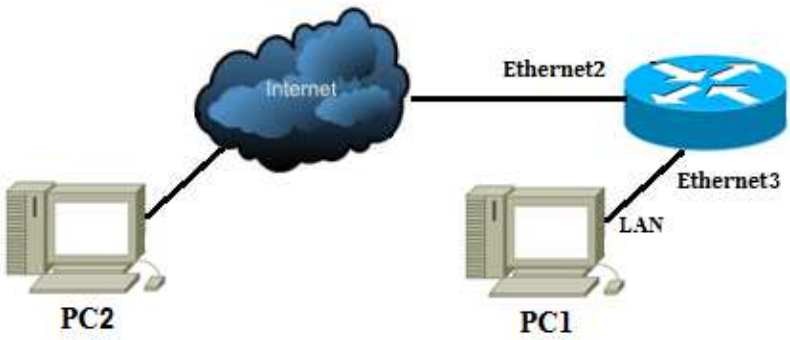


a) b)

Slika 1.25. *a) Prikaz statusa (Status) adresa dodijeljenih kreiranom DHCP klijentu (DHCP Client) i b) prikaz podataka o aktivnom DHCP klijent sučelju (Interface)*

(IV) KREIRANJE TESTNE MREŽE

(24) Računalo je potrebno prespojiti na sučelje *Ethernet3*, a sučelje *Ethernet2* povezati na Internet (preko kojeg je tada moguće pristupiti i drugim računalima, npr. nekom računalu PC2 povezanom na Internet).



Slika 1.26. *Pikaz kreirane mrežne topologije u testnom okruženju*

Zadatak 7. U konzolu računala PC1 unesite redom sljedeće naredbe za otpuštanje i obnovu IP adresa:

ipconfig /release

ipconfig /renew

Nakon unošenja naredbe ***ipconfig /all*** u konzole računala PC1 i PC2 potrebno je ispisati sljedeće adrese:

- adresu računala PC1 (*IPv4 Address*): _____
- adresu maske podmreže (*Subnet Mask*): _____
- adresu aktivnog *Ethernet3* sučelja usmjerivača (*Default Gateway*): _____

Zadatak 8. Provjerite postoji li konekcija između računala PC1 te:

a) *Ethernet3* sučelja usmjerivača: _____

b) *Ethernet2* sučelja usmjerivača: _____

Zadatak 9. Provjerite je li računalo PC1 povezano na Internet i može li komunicirati sa sljedećim uređajima na Internetu:

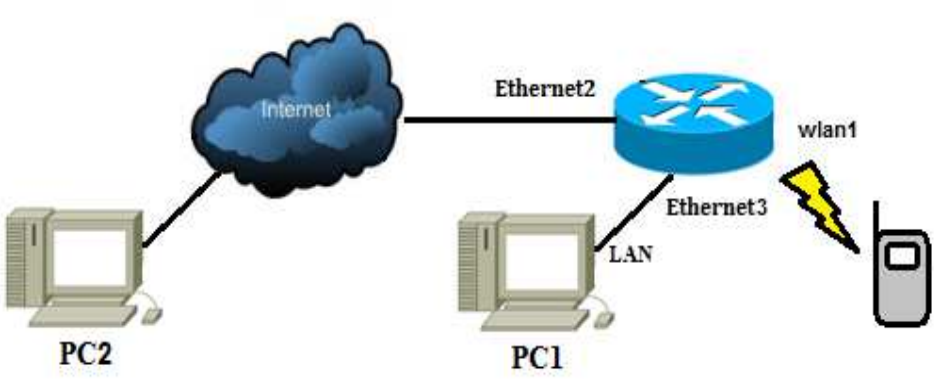
a) sa PC2 (u konzolu računala PC1 unesite naredbu *ping* te adresu jednog od susjednih računala koje je povezano na Internet):

_____

b) sa poslužiteljem (u konzolu računala PC1 unesite naredbu: *ping www.etfos.unios.hr*):

_____

(25) U prethodno kreiranu topologiju prikazanu na donjoj slici povežite bežični uređaji putem Wi-Fi mreže koristeći se lozinkom koja je definirana pri konfiguraciji.



Slika 1.27. *Prikaz proširene mrežne topologije u testnom okruženju*

Zadatak 10. Provjerite koja je adresa dodijeljena uređaju:

_____

Zadatak 11. Iz kojeg raspona je odabrana ta adresa:

Zadatak 12. Provjerite je li uređaj povezan u mrežu i postoji li mogućnost komunikacije prema Internetu:

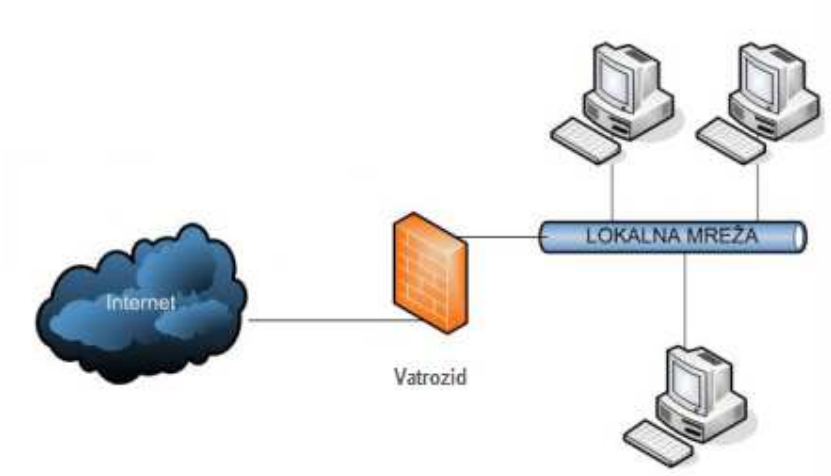
_____

_____

Vježba 2. - Primjena zaštitnih mehanizama u lokalnim mrežama: *Konfiguriranje vatrozida*

UVOD

Pojam sigurnosti lokalne mreže usko je vezan uz mogućnost adekvatne zaštite dostupnih mrežnih resursa – informacija, aplikacija i opreme. Propusti u primjeni odgovarajućih zaštitnih mehanizama mogu rezultirati narušavanjem povjerljivosti lokalno pohranjenih podataka, kao i određenih informacija koje se razmjenjuju u mreži, te onemogućiti primjenu pojedinih mrežnih usluga, odnosno funkcija pojedinih mrežnih uređaja. Ranjivost mreže moguće je smanjiti primjenom zaštitnih mehanizama koji se mogu konfigurirati na različite načine - ovisno o potrebi krajnjih korisnika, ali i o vrstama lokalnih mreža u koje se postavljaju.



Slika 2.1. *Prikaz zaštite lokalne mreže uz primjenu vatrozida*

Vatrozid (eng. *firewall*) je zaštitni mehanizam koji kontrolira proces razmjene mrežnih paketa između pojedinih mrežnih segmenata sa različitim definiranim sigurnosnim razinama. Provjera mrežnog prometa se izvodi prema točno definiranim kriterijima i pravilima te se na osnovu njih filtrira neželjeni promet. Kako se vrste sigurnosnih rizika neprestano mijenjaju, kako bi vatrozidi mogli pratiti promjene, nova se pravila moraju kontinuirano ažurirati.

Osnovna uloga vatrozida vezana je uz kontrolu informacijskog toka te filtriranje mrežnog prometa. Filtriranje mrežnog prometa obuhvaća postupke analize dolaznih i odlaznih tokova podataka. Filter otvara svaki pojedini podatkovni paket i provjerava njegov sadržaj, odnosno provjerava odgovara li takav sadržaj unaprijed postavljenim pravilima. Filtriranje se može provoditi statički, pri čemu se pravila prema kojima se vrši filtriranje mogu ručno mijenjati, te dinamički, pri čemu se pravila prema kojima se vrši filtriranje mogu mijenjati na osnovu određenih vanjskih procesa.

S obzirom na primijenjene koncepte filtriranja paketa, razlikuje se filtriranje podatkovnih paketa na mrežnom, transportnom te aplikacijskom sloju. Primjenjuju se sljedeći koncepti filtriranja:

- filtriranje paketa ovisno o vrsti protokola - odluka o prosljeđivanju paketa donosi se na osnovu zapisa o korištenim komunikacijskim protokolima u zaglavlju paketa;
- filtriranje paketa u ovisnosti o IP adresama - odluka o prosljeđivanju paketa donosi se na osnovu zapisa o izvorišnim ili odredišnim IP adresama paketa (na taj je način moguće npr.: onemogućiti prosljeđivanje paketa sa definiranim odredišnim IP adresama prema pojedinom odredištu, ili samo paketima s određenim IP adresama omogućiti prosljeđivanje prema odredištu);
- filtriranje paketa u ovisnosti o portovima - odluka o prosljeđivanju paketa donosi se na osnovu zapisa o portovima (ovakvo filtriranje zasniva se na činjenici da se od ukupno 65536 portova, prvih 1024 koristi samo za određene aplikacije, pa je u ovisnosti o aplikacijskim portovima pojedinim mrežnim paketima moguće ograničiti pristup mreži - ovo je vrlo korisna opcija s obzirom na činjenicu da su neki aplikacijski portovi, iznimno osjetljivi na napade te ih je potrebno posebno zaštititi);
- filtriranje paketa u ovisnosti o putu usmjeravanja paketa - odluka o prosljeđivanju paketa donosi se na osnovu puta kojim se paket usmjerava od izvora prema odredištu;
- filtriranje paketa u ovisnosti o veličini fragmentiranog paketa - odluka o prosljeđivanju paketa donosi se na osnovu procijenjene veličine paketa (velike poruke moguće je fragmentirati u manje pakete, pa je početni fragment moguće odbaciti ukoliko je potrebno naznačiti da će i ostali paketi biti beskorisni budući da prvi paket nosi informaciju o aplikacijskom portu).

Vatrozid je potrebno ispravno konfigurirati kako bi onemogućio različite vrste sigurnosnih rizika, tj. napada. Neki od najčešćih rizika su:

- *IP address spoofing* - zlonamjerno lažiranje IP adrese kojim se zaobilaze zaštitni mehanizmi koji se temelje na filtriranju prometa prema IP adresama (ovakva vrsta napada može se spriječiti onemogućavanjem prosljeđivanja paketa koji kao izvorišnu adresu imaju neku od lokanih adresa, a kao ulazno okruženje ono koje je povezano na Internet);
- *Smurf* - ciljano onemogućavanje rada pojedinih krajnih uređaja (poslužitelja ili računala) u mreži, pri čemu napadač odašilje ICMP zahtjev (*echo request*) na *broadcast* adresu cijele lokalne mreže, dok se kao odredišno računalo navodi ono koje se želi onesposobiti velikim brojem paketa s odgovorom (*echo reply*); ovakva vrsta napada može se spriječiti onemogućavanjem prosljeđivanja paketa za emitiranje (*broadcast*);
- *SYN flooding* - slanje velikog broja TCP paketa koji su označeni SYN zastavicom, pri čemu se zloupotrebljava postojeći mehanizam uspostave TCP konekcije - uspostavlja se veliki broj poluotvorenih konekcija, a kako poslužitelj može omogućiti samo ograničeni broj istovremenih konekcija, krajnji korisnici u tom slučaju ne mogu pristupiti sadržajima na poslužitelju (ovakva vrsta napada može se spriječiti ograničavanjem ukupnog broja dolaznih paketa);
- *Ping of death* - onemogućavanje rada operacijskog sustava zbog velikog broja ICMP *echo* zahtjeva (ovakva vrsta napada može se spriječiti ograničavanjem broja ICMP *echo* zahtjeva);
- *Port scanning* - skeniranje portova odredišnog računala pomoću aplikacija koje osluškujući portove detektiraju koju su od njih otvoreni i detektiraju procese koje bi mogli iskoristiti za ulaz u sustav.

Postoji više različitih načina konfiguracije vatrozida u mreži, a među najpoznatijima su:

- *Screening router* - usmjerivač analizira dolazni i odlazni promet, te propušta ili odbacuje određene pakete u ovisnosti o pravilima koja su unaprijed postavljena;
- *Bastion host* - poslužitelj postavljen u lokalnoj mreži koja je od Interneta odvojena vatrozidom (u tzv. demilitariziranoj zoni), pa je pristup iz te mreže prema vanjskoj moguć je samo preko *bastion hosta*;

• *Dual homed host* - konfiguracija slična prethodnoj, međutim *host* u ovom slučaju ima dva odvojena sučelja - jedno prema unutrašnjoj i jedno prema vanjskoj mreži;
• *Screened host* - konfiguracija nastala kombinacijom *screening routera* i *bastion hosta* pri čemu se između njih nalazi demilitarizirana zona, dok je razina sigurnosti povećana dodavanjem unutrašnjeg *screening* usmjerivača - unutrašnji i vanjski usmjerivač uvijek komuniciraju preko *bastion hosta*, a ne izravno.

Načini filtriranja mrežnog prometa uz primjenu *MikroTik* usmjerivača

MikroTik RouterOS omogućuje konfiguriranje postavki za filtriranje mrežnog prometa i provedbu inteligentne analize toka podataka te evidentiranje stanja pojedinih mrežnih konekcija. *MikroTik* usmjerivač omogućuje klasifikaciju prometa prema: izvorišnim MAC adresama, IP adresama, portovima, protokolima, opcijama protokola, sadržaju paketa, veličini paketa, redoslijedu paketa te dolaznom vremenu paketa. Filtriranje se vrši prema predefiniranim pravilima. Pravila odlučuju hoće li usmjerivač prihvatiti određene IP pakete te što će s njima učiniti. Filter se sastoji iz pravila sljedećeg oblika:

AKO (IF) < uvjet (condition) > TADA (THEN) < akcija (action) >

Prilikom obrade podataka filteri obrađuju pakete redom prema kojem su pravila navedena. Ukoliko paket podliježe određenim pravilima izvršavaju se određene akcije, dok u suprotnom paket prelazi na iduće pravilo. Akcije obuhvaćaju sljedeće:
• *accept* - paket se prihvaća i prolazi kroz usmjerivač te se dodatna pravila na njemu ne primjenjuju
• *add-dst-to-address-list* - dodaje odredišnu IP adresu paketa na popis određen *address list* parametrom
• *add-src-to-address-list* - dodaje izvorišnu IP adresu paketa na popis određen *address list* parametrom
• *drop* - odbacuje paket
• *jump* - predstavlja skok na lancu određen vrijednošću parametra koji definira odredišni skok (*jump target)*
• *log* - dodaje zapis u sistemski *log*
• *passthrough* - ignorira trenutno pravilo i prelazi na sljedeće
• *reject* - odbacuje paket i šalje ICMP poruku o odbacivanju
• *return* – paket se iznova prosljeđuje kroz provjeru u lancu
• *tarpit* - prihvaća i pohranjuje dolazne TCP veze.

Pravila su organizirana u lance koji omogućuju bolje upravljanje i obradu paketa koji izlaze iz usmjerivača kroz jedno od njegovih sučelja. Odgovorni su za sav promet koji ide od, kroz i na usmjerivač. Razlikuju se sljedeće vrste lanaca:

- ulazni (eng. *input*) – koristi za obradu paketa koji ulaze u usmjerivač preko jednog od njegovih sučelja, a čija je odredišna IP adresa jedna od adresa sučelja usmjerivača
- izlazni (eng. *output*) – koristi za obradu podataka koji idu na izlaz usmjerivača
- prosljeđivanje (eng. *forward*) – koristi za obradu paketa koji prolaze kroz usmjerivač

Lanci se koriste zbog smanjenja prosječnog broja pravila kroz koja paketi prolaze - kako bi vatrozid bio brži te kako bi se lakše upravljalo strukturom vatrozida. Novi lanci se mogu dodavati ovisno o potrebama.

PRIPREMA ZA VJEŽBU

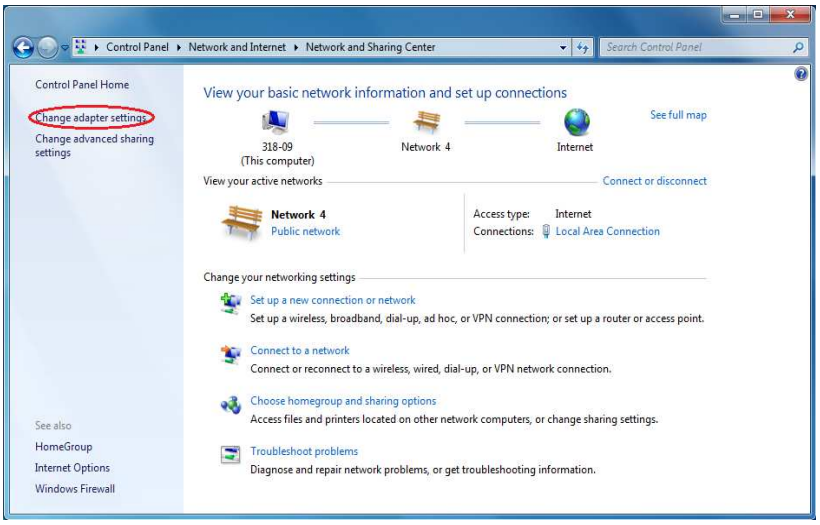
- Proučiti navedena načela prema kojima vatrozidi vrše filtriranje mrežnog prometa.

KREIRANJE ODABRANOG TESTNOG SCENARIJA:

Kroz korake (A)-(D) definiran je postupak uspostave testnog okruženja. Ovaj postupak obuhvaća deaktivaciju svih mrežnih konekcija na računalu PC1 osim lokalne mreže, isključivanje vatrozida te resetiranje postavki usmjerivača. Preostali koraci (I)-(V) vezani su uz konfiguraciju postavki usmjerivača i klijenta (PC1) i testiranje mogućnosti (ne)ovlaštenog pristupa kreiranoj mreži.

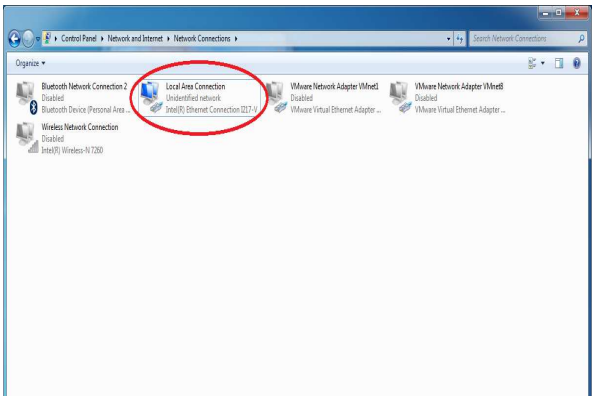
(A) DEAKTIVIRANJE POJEDINIH MREŽNIH KONEKCIJA NA KLIJENTIMA

(1) Na računalu otvorite prozor upravljačke ploče (*Control Panel*), zatim odaberite poveznicu vezanu uz postavke mreže i Interneta (*Network and Internet*), te zatim poveznicu vezanu uz opcije središta za umrežavanje i dijeljenje (*Network and Sharing Center*).



Slika 2.2. *Prikaz opcija promjene postavki mrežnog adaptera (eng. Change Adapter Settings) središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

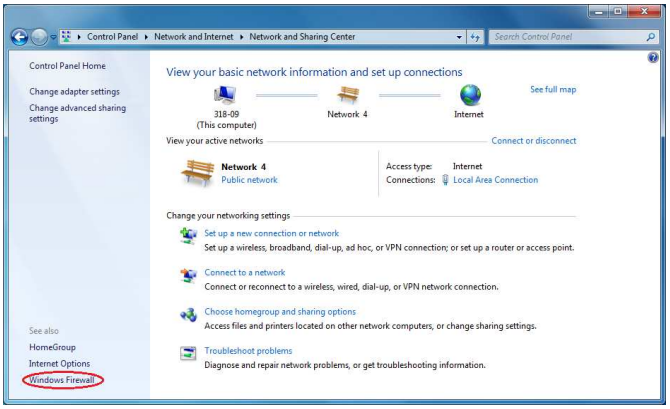
(2) Kliknite na opciju promjene postavki mrežnog adaptera (*Change Adapter Settings*). Omogućena treba ostati samo **lokalna žična konekcija** (*Local Area Connection*, LAN). Deaktivirajte sve ostale mrežne konekcije na računalima (za pojedina bežična, žična i virtualna sučelja) osim navedenih – odaberite desnom tipkom miša odgovarajuću konekciju i odaberite opciju za deaktiviranje (*Disable*).



Slika 2.3. *Prikaz postavki mrežnih konekcija (Network Connections) na računalu u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

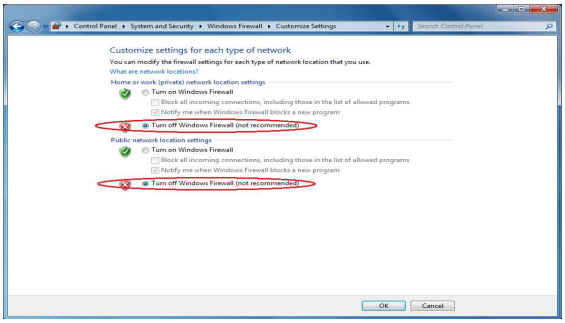
(B) ISKLJUČIVANJE VATROZIDA NA KLIJENTIMA

(3) Na računalu otvorite prozor upravljačke ploče (*Control Panel*), zatim odaberite poveznicu vezanu uz postavke mreže i Interneta (*Network and Internet*), te zatim poveznicu vezanu uz opcije središta za umrežavanje i dijeljenje (*Network and Sharing Center*).



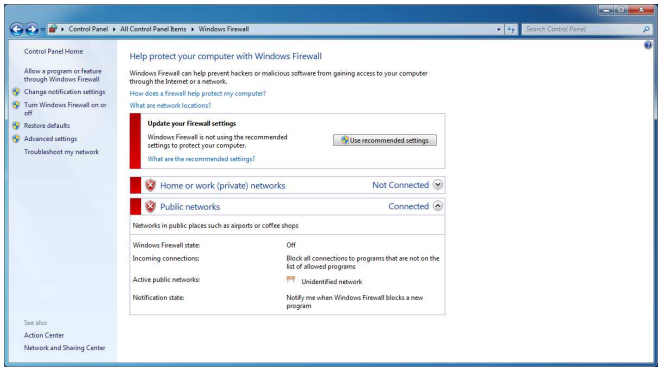
Slika 2.4. *Prikaz opcije za pristup postavkama Windows vatrozida (Windows Firewall) središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

(4) Isključite vatrozid ukoliko je pokrenut na računalu prema sljedećem postupku. Odaberite poveznicu koja otvara prozor s postavkama središta za umrežavanje i dijeljenje (*Network and Sharing Center*), zatim otvorite prozor s postavkama vatrozida (*Windows Firewall*), odaberite izbornik za uključivanje i isključivanje vatrozida (*Turn Windows Firewall on or off*) i isključite vatrozid (*Turn off Windows Firewall*).



Slika 2.5. *Prilagođavanje postavki (Customize Settings) za isključivanje Windows vatrozida (Windows Firewall)*

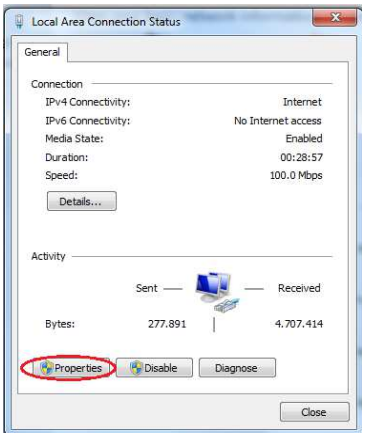
(5) Prikaz nakon deaktivacije vidljiv je na slici.



Slika 2.6. *Prikaz nakon deaktivacije Windows vatrozida*

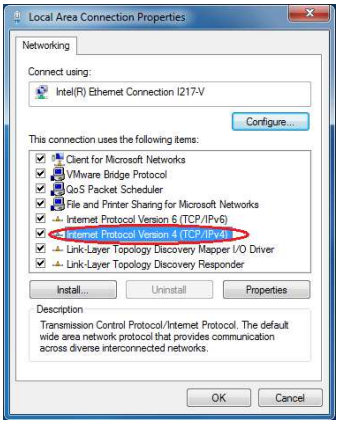
(C) DINAMIČKO ADRESIRANJE KLIJENATA

(6) U prozoru s opcijama središta za umrežavanje i dijeljenje (*Network and Sharing Center*) odaberite opciju promjene postavki mrežnog adaptera (*Change Adapter Settings*), zatim odaberite lokalnu mrežnu konekciju (*Local Area Connection*) i zatim njene postavke (*Properties*).



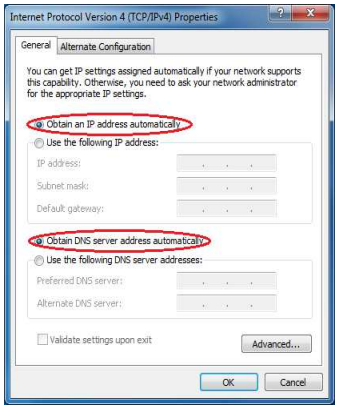
Slika 2.7. *Provjera postavki lokalne mreže (Local Area Connection Status) na računalu*

(7) Odaberite opciju prikaza postavki IPv4 protokola (*Internet Protocol Version 4 (TCP/IPv4)*).



Slika 2.8. *Provjera postavki lokalne konekcije (Local Area Connection Properties) na računalu*

(8) Provjerite jesu li odabrane sljedeće opcije prema prikazu sa slike: automatska dodjela IP adrese (*Obtain an IP address automatically*) te automatska dodjela adrese DNS poslužitelja (*Obtain DNS server address automatically*), te ih odaberite ukoliko već nisu odabrane.



Slika 2.9. *Provjera postavki na računalu za automatsku dodjelu IPv4 adrese i adrese DNS servera*

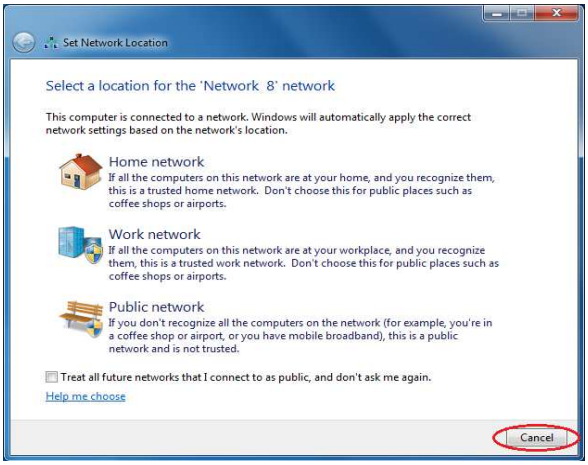
(D) RESETIRANJE POSTAVKI USMJERIVAČA

(9) Uključite usmjerivač. Povežite računalo PC1 na *Ethernet2* sučelje usmjerivača pomoću *patch* kabela, prema *shemi* na slici.

a) b)

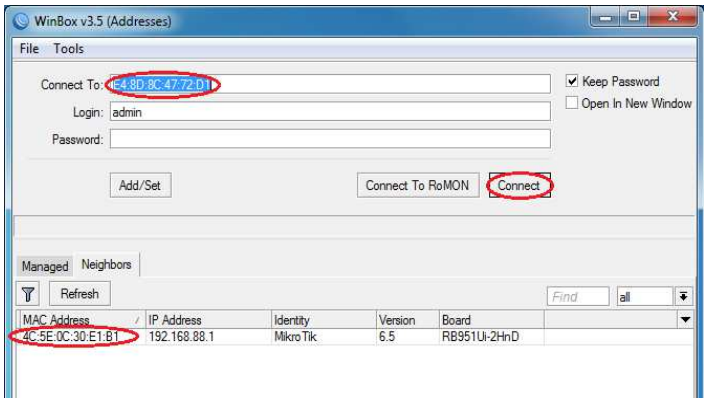
Slika 2.10. *a) Način povezivanja PC1 uređaja i MikroTik usmjerivača i b) MikroTik usmjerivač sa označenim Ethernet2 portom*

(10) Nakon što se otvori izbornik postavki lokacije mreže (*Set Network Location*) odaberite opciju izuzeća (*Cancel*).



Slika 2.11. *Izbornik postavki lokacije mreže* (*Set Network Location*)

(11) Pokrenite *WinBox* aplikaciju čija se ikona nalazi na radnoj ploči (*Desktop*) računala. Prvo označite MAC adresu (*MAC Address*) usmjerivača koja se nalazi na popisu u donjem dijelu prozora, a zatim kliknite na opciju za povezivanje (*Connect*).



Slika 2.12. *Sučelje WinBox aplikacije*

(12) Unutar otvorenog sučelja aplikacije *WinBox* odaberite opciju za otvaranje novog terminala (*New Terminal*). Otvara se terminal prikazan na donjoj slici.

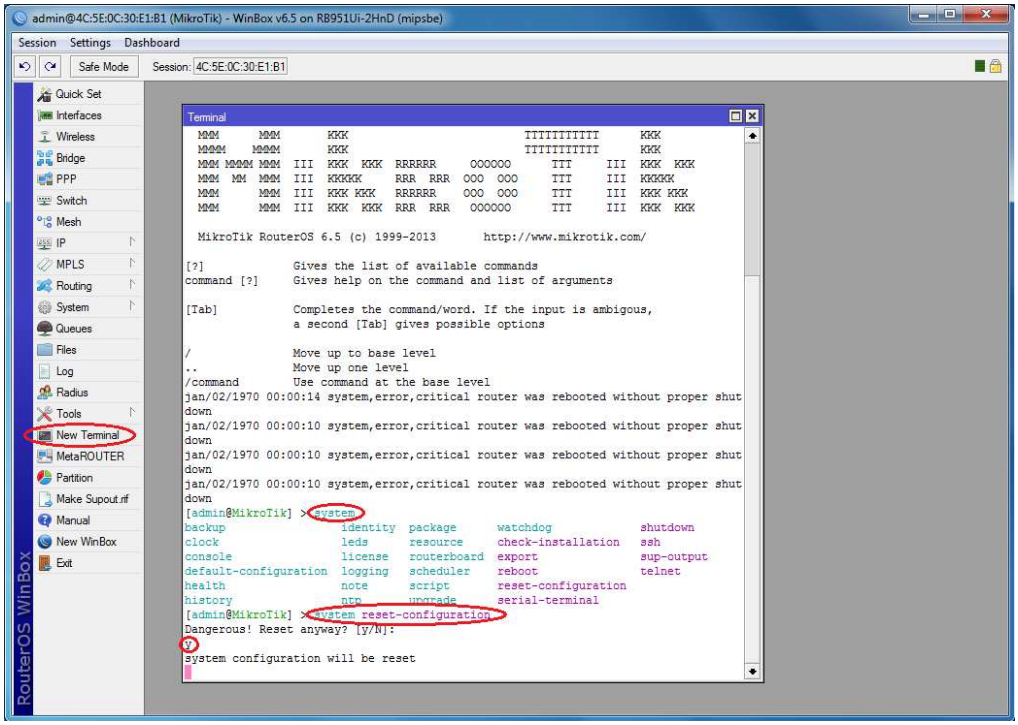
Resetirajte postavke na usmjerivaču upisivanjem naredbe:

system reset-configuration

i pomoću tipkovnice potvrdite upis odabirom tipke *Enter* te još jednom potvrdite izbor upisivanjem naredbe:

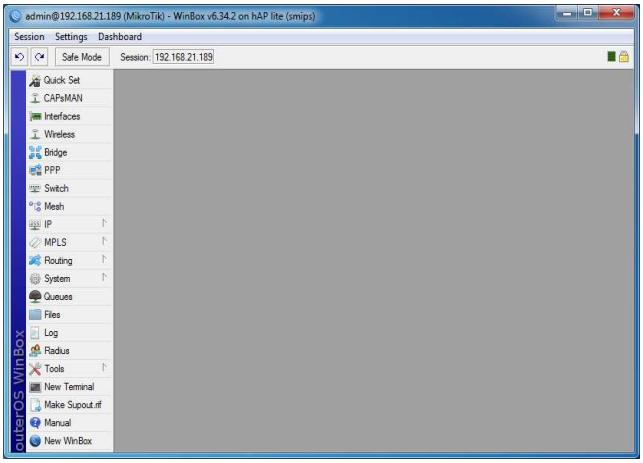
y

te odabirom tipke *Enter*. Ovime se pokreće resetiranje postojeće konfiguracije te se konfiguracija usmjerivača vraća na tvornički definiranu.



Slika 2.13. *Prikaz terminala WinBox aplikacije*

(13) Nakon ponovnog otvaranja *WinBox* aplikacije, prikaz bi trebao odgovarati prikazu na slici 2.14.



Slika 2.14. *Početno sučelje WinBox aplikacije*

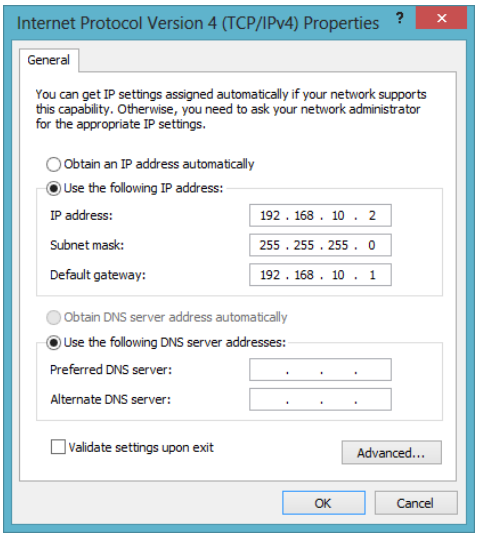
Zadaci:

U testnom scenariju potrebno je definirati i postaviti pravila za filtriranje prometa i zaštitu pristupa usmjerivaču iz lokalne računalne mreže. Potrebno je koristiti usmjerivač *MikroTik RouterOS* koji implementira značajke vatrozida - omogućuje analizu i klasifikaciju mrežnog prometa te njegovo filtriranje. Potrebno je načiniti konfiguraciju vatrozida koja omogućuje filtriranje paketa prema IP adresama, rasponu IP adresa, protokolima te portovima.

UPUTE ZA RAD:

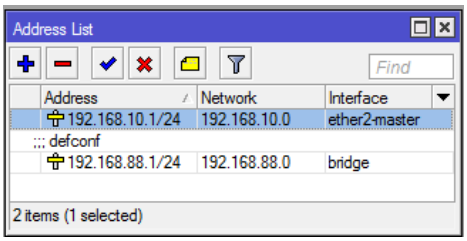
(I) ADRESIRANJE RAČUNALA I AKTIVNOG SUČELJA USMJERIVAČA

(14) Računalu je potrebno dodijeliti IP adresu 192.168.10.2/24. Prema prikazu sa slike 2.15., postavite adresu računala, adresu maske podmreže te pristupnika (*gateway*).



Slika 2.15. *Postavljanje IPv4 adrese računala (IP address), maske podmreže (Subnet mask) i predefiniranog pristupnika (Default gateway)*

(15) Sučelju *Ethernet2* potrebno je dodijeliti IP adresu. Iz izbornika tipa protokola (*IP*) potrebno je odabrati opciju za adresiranje (*Addresses*) te unutar izbornika s popisom adresa (*Address List*) kliknuti na oznaku '+' i dodijeliti sučelju *Ethernet2* adresu 192.168.10.1/24 te postaviti 192.168.10.0 za adresu mreže.



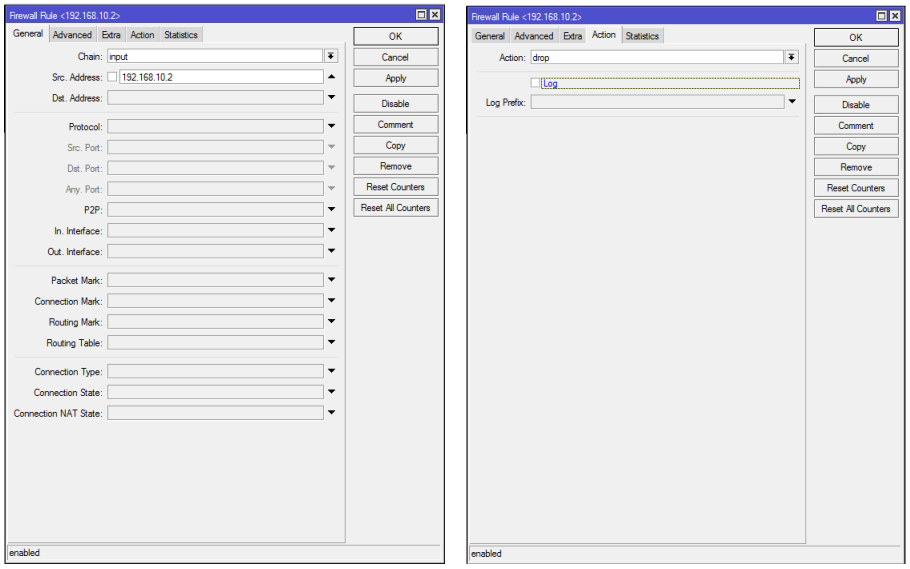
Slika 2.16. *Popis adresa (Address List) aktivnih sučelja usmjerivača*

Zadatak 1. Provjerite postoji li konekcija između računala i usmjerivača upisivanjem naredbe *ping* na konzoli računala. _____

A) Blokiranje pristupa računalu prema IP adresi

(II) KONFIGURIRANJE SUČELJA USMJERIVAČA

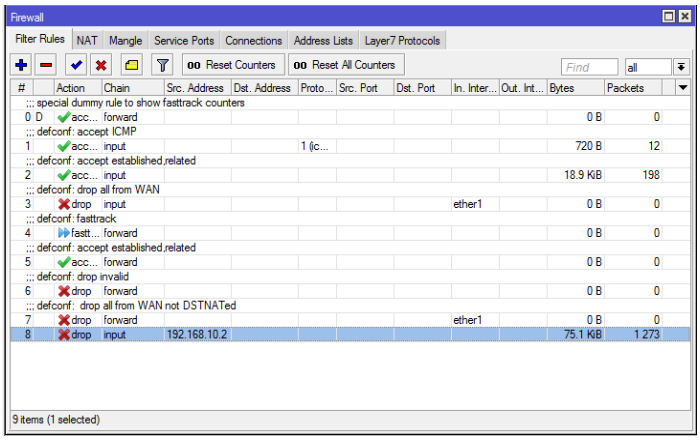
(16) Cilj ovog zadatka je računalu blokirati pristup. Iz početnog izbornika *WinBox* aplikacije prikazanog na slici 2.14. odaberite izbornik protokola (*IP*) te opciju vatrozid (*Firewall*). U izborniku vezanom uz postavke pravila filtriranja mrežnog prometa (*Firewall Filter Rules*) potrebno je odabrati odgovarajuću akciju. Lanac koji je potrebno odabrati je ulaz (*input*), što podrazumijeva da će se obrađivati paketi koji ulaze na usmjerivač, a čije odredišne IP adrese odgovaraju adresi aktivnog sučelja usmjerivača. Potrebno je unijeti adresu koju želimo blokirati, tj. IP adresu računala, te odabrati akciju koja podrazumijeva ispuštanje paketa koji ulaze na usmjerivač (*drop*). Odabir odgovarajućeg lanca i adrese vidljiv je na slici 2.17.



a) b)

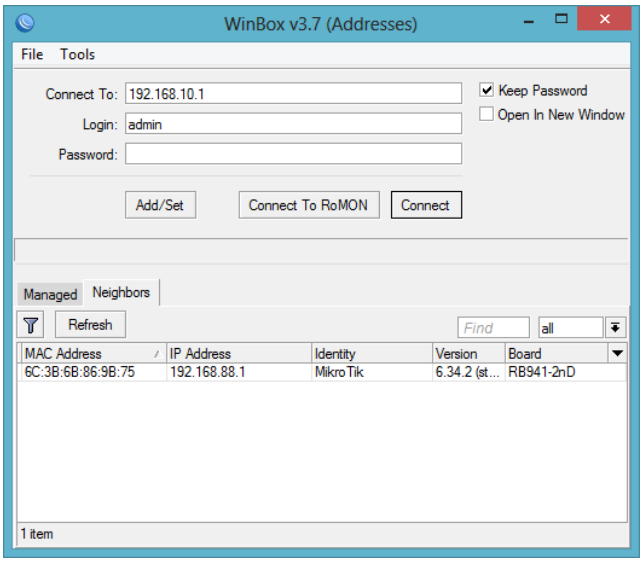
Slika 2.17. *a) Postavljanje IP adrese s koje će pomoću postavljenih pravila vatrozida (Firewall Rule) biti blokiran mrežni promet i b) izbor radnje (Action) blokiranja prometa (drop)*

(17) Prikaz svih definiranih pravila za filtriranje prometa, uključujući i prethodno, nalazi se na slici 2.18.



Slika 2.18. *Prikaz svih postavljenih pravila za filtriranje prometa (Filter Rules) pomoću vatrozida (Firewall)*

(18) Nakon definiranja pravila filtriranja, potrebno je upisati IP adresu *MikroTik* usmjerivača u izbornik za pokretanje *WinBox* aplikacije (*WinBox Loader*), prema prikazu na slici 2.19.



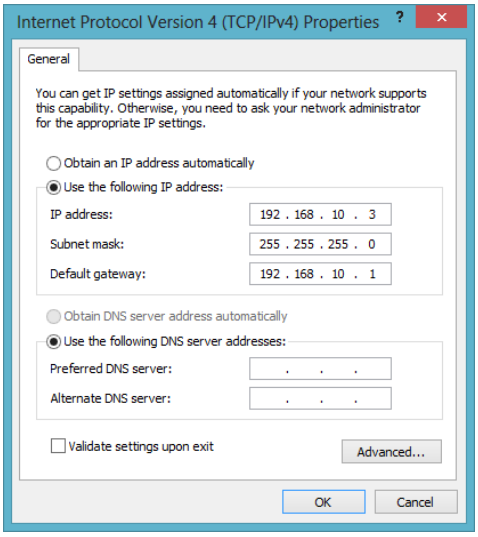
Slika 2.19. *Pristupanje Winbox aplikaciji upisivanjem IP adrese aktivnog Ethernet2 sučelja usmjerivača*

Zadatak 2. Provjerite postoji li mogućnost pristupanja konfiguratoru usmjerivača i objasnite odgovor.

_____

(III) PROMJENA IP ADRESE RAČUNALA

(19) Promjenite IP adresu računala prema prikazu sa slike 2.20., te ponovite postupak opisan pod (18).



Slika 2.20. *Promjena IPv4 adrese računala*

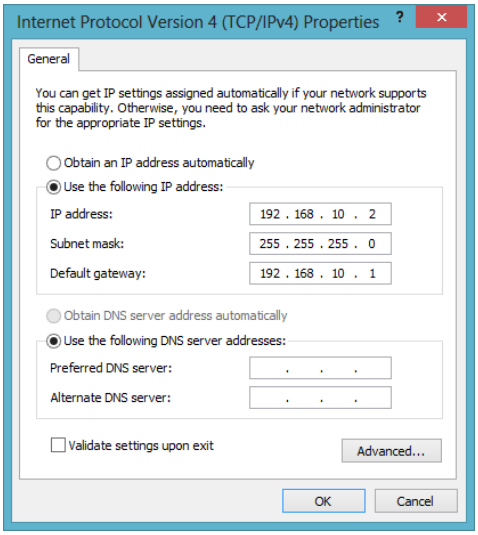
Zadatak 3. Provjerite postoji li mogućnost pristupanja konfiguratoru usmjerivača i objasnite odgovor.

_____

B) Filtriranje paketa prema listi IP adresa

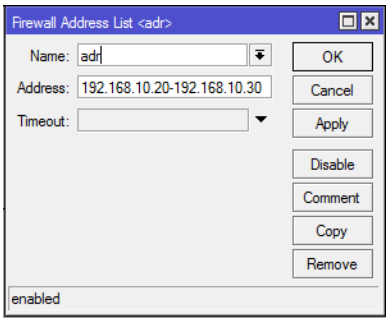
(IV) KONFIGURIRANJE POSTAVKI RAČUNALA I USMJERIVAČA

(20) U ovom primjeru promet je potrebno filtrirati prema definiranoj listi IP adresa. Za početak je potrebno vratiti IP adrese računala prema prikazu sa slike 2.21. i obrisati prethodno definirano pravilo filtriranja prometa označeno na slici 2.18.



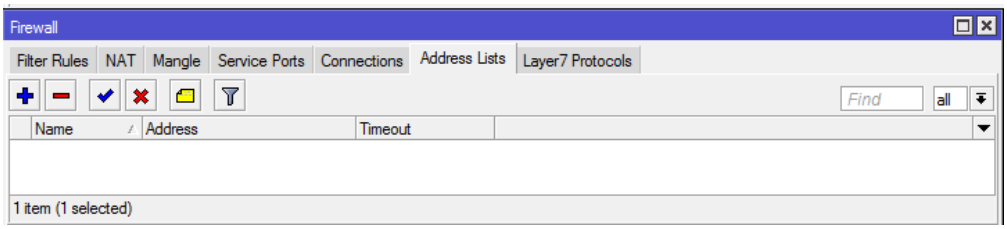
Slika 2.21. *Vraćanje IPv4 adrese računala na početno odabranu*

(21) Nadalje, potrebno je kreirati listu adresa pod nazivom *adr* u kojoj se nalazi određeni raspon IP adresa koje će imati pristup *MikroTik* usmjerivaču. Koristeći izbornik za dodavanje nove adresne liste vatrozida (*New Firewall Address List*) dodajte naziv popisu adresa i raspon prema prikazu sa slike 2.22.



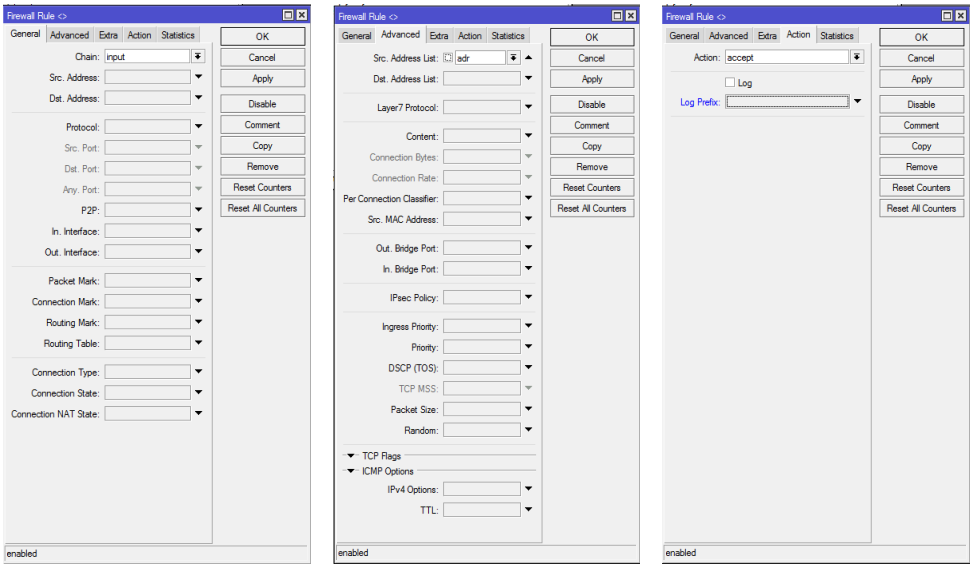
Slika 2.22. *Dodavanje naziva (Name) adresne liste vatrozida (Firewall Address List) i dodavanje raspona adresa (Address)*

Zadatak 4. U prostor na slici 2.23. upišite prikazane oznake adresa kojima se dopušta pristup usmjerivaču te naziv liste.

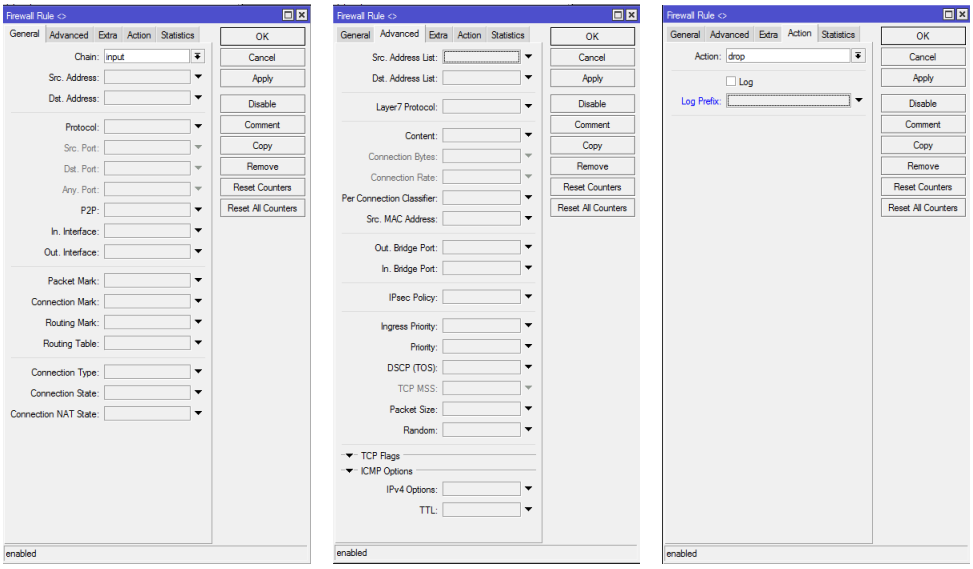


Slika 2.23. *Prikaz kreirane liste adresa (Address List)*

(22) Sada je potrebno definirati dodatna pravila filtriranja koristeći izbornik za dodavanje pravila filtriranja mrežnog prometa vatrozidu (*Firewall Filter Rules*) prema prikazu sa slike 2.24.



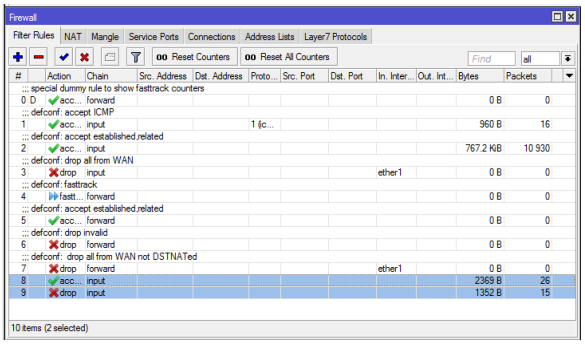
a) prvo pravilo



b) drugo pravilo

Slika 2.24. *Postavljanje pravila za filtriranje mrežnog prometa pomoću vatrozida (Firewall Rule)*

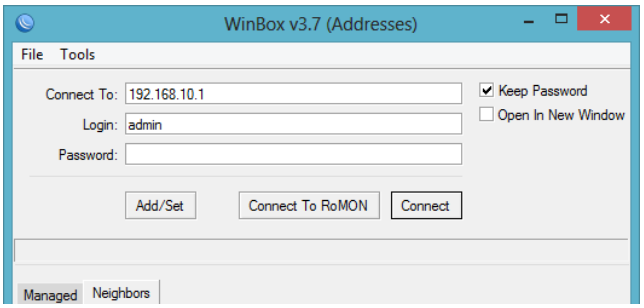
(23) Prikaz svih definiranih pravila za filtriranje prometa, uključujući i prethodna, nalazi se na slici 2.25.



Slika 2.25. *Prikaz svih postavljenih pravila za filtriranje mrežnog prometa (Filter Rules) pomoću vatrozida (Firewall)*

Zadatak 5. Objasnite redom značenje postavljenih pravila:
prvo pravilo: _____
drugo pravilo: _____

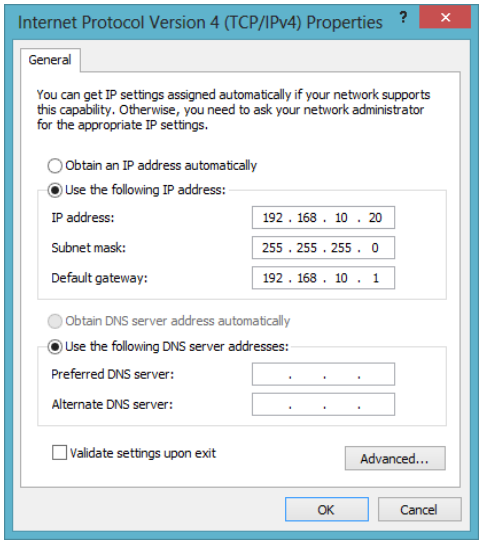
(24) Potrebno je upisati IP adresu *MikroTik* usmjerivača u izbornik za pokretanje *WinBox* aplikacije (*WinBox Loader*), prema slici 2.26.



Slika 2.26. *Pristupanje Winbox aplikaciji upisivanjem IP adrese aktivnog Ethernet2 sučelja usmjerivača*

Zadatak 6. Provjerite postoji li sada mogućnost pristupanja konfiguratoru usmjerivača i objasnite odgovor. _____
_____

(25) Promjenite IP adresu računala prema prikazu sa slike 2.27.



Slika 2.27. *Promjena IPv4 adrese računala*

Zadatak 7. Ponovite postupak naveden pod (24) i provjerite postoji li sada mogućnost pristupanja konfiguratoru usmjerivača i objasnite odgovor.

_____
_____
_____

C) Filtriranje paketa prema portovima i protokolima

(V) KONFIGURIRANJE POSTAVKI RAČUNALA I USMJERIVAČA

U ovom primjeru promet je potrebno filtrirati prema definiranim portovima i protokolima. Usmjerivač je potrebno konfigurirati tako da dinamički dodaje zapis o IP adresama u adresnu listu, dok bi zapis trebao vrijediti unutar ograničenog vremenskog perioda. To je tzv. „*port knocking*“.

Postupak konfiguracije usmjerivača obuhvaća sljedeće korake:

1.) klijent (računalo) šalje pakete usmjerivaču na port 8039

- usmjerivač dodaje adresu klijenta u adresnu listu „*knock*“ uz definirani vremensko ograničenje (*timeout*) od 20 sekundi

2.) klijent šalje pakete usmjerivaču na port 9308

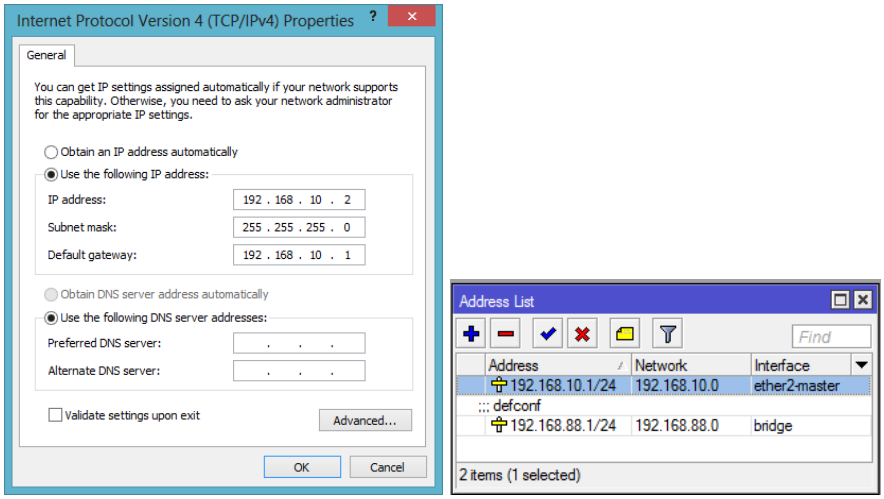
- usmjerivač provjerava nalazi li se adresa klijenta u adresnoj listi

3.) ako se adresa klijenta nalazi na popisu, usmjerivač dodaje IP adresu klijenta u adresnu listu „*safe*“ uz vremensko ograničenje (*timeout*) od 15 minuta

- klijent ima puni pristup konfiguratoru usmjerivača 15minuta

4.) blokira se pristup u svim drugim slučajevima.

(26) IP adresa računala treba ostati 192.168.10.2/24, a adresa usmjerivača 192.168.10.1/24. Potrebno je obrisati dva prethodno definirana pravila filtriranja prometa označena na slici 2.28.

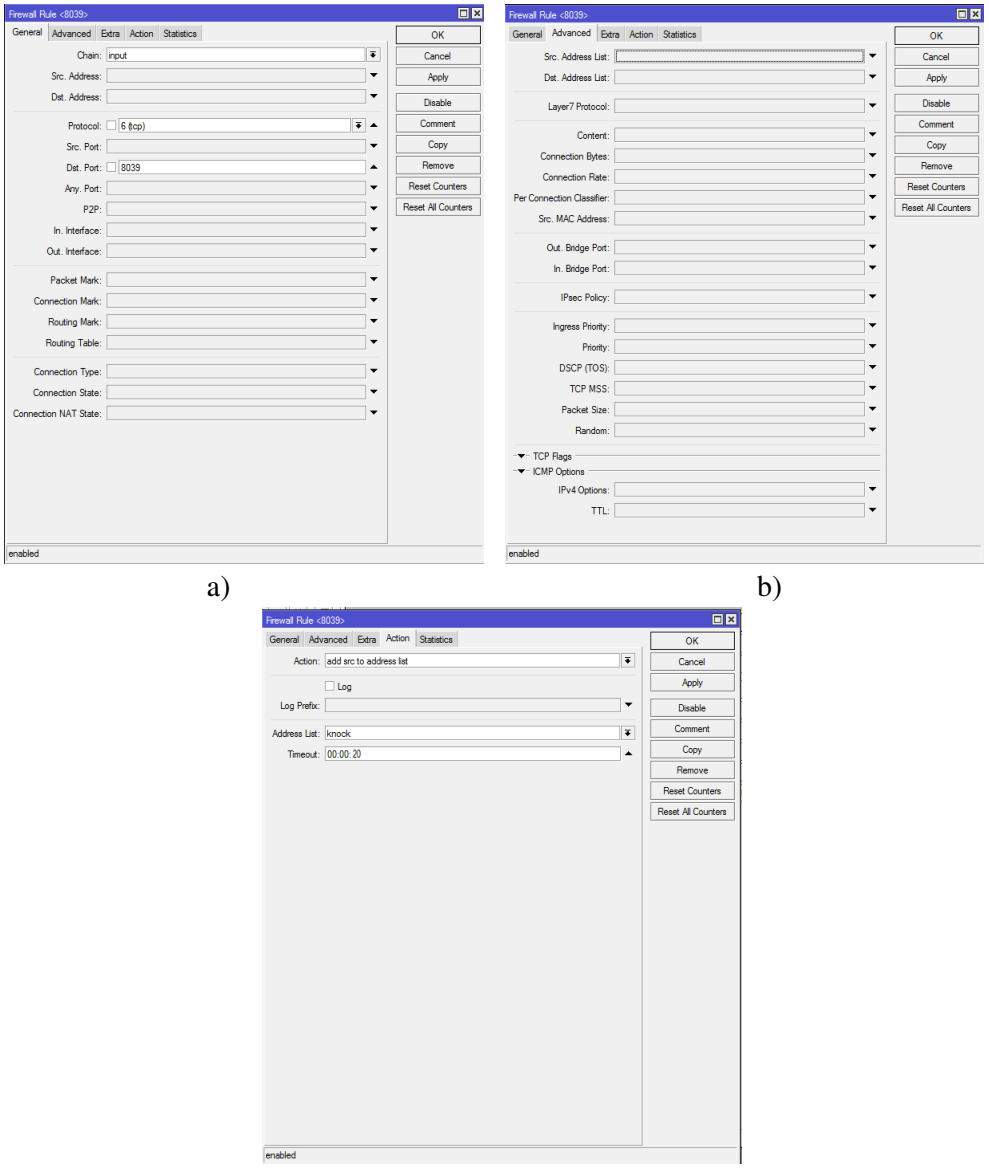


a) b)

Slika 2.28. *a) Postavljanje IPv4 adrese računala i b) prikaz IPv4 adrese aktivnog Ethernet2 sučelja usmjerivača*

Prvo pravilo

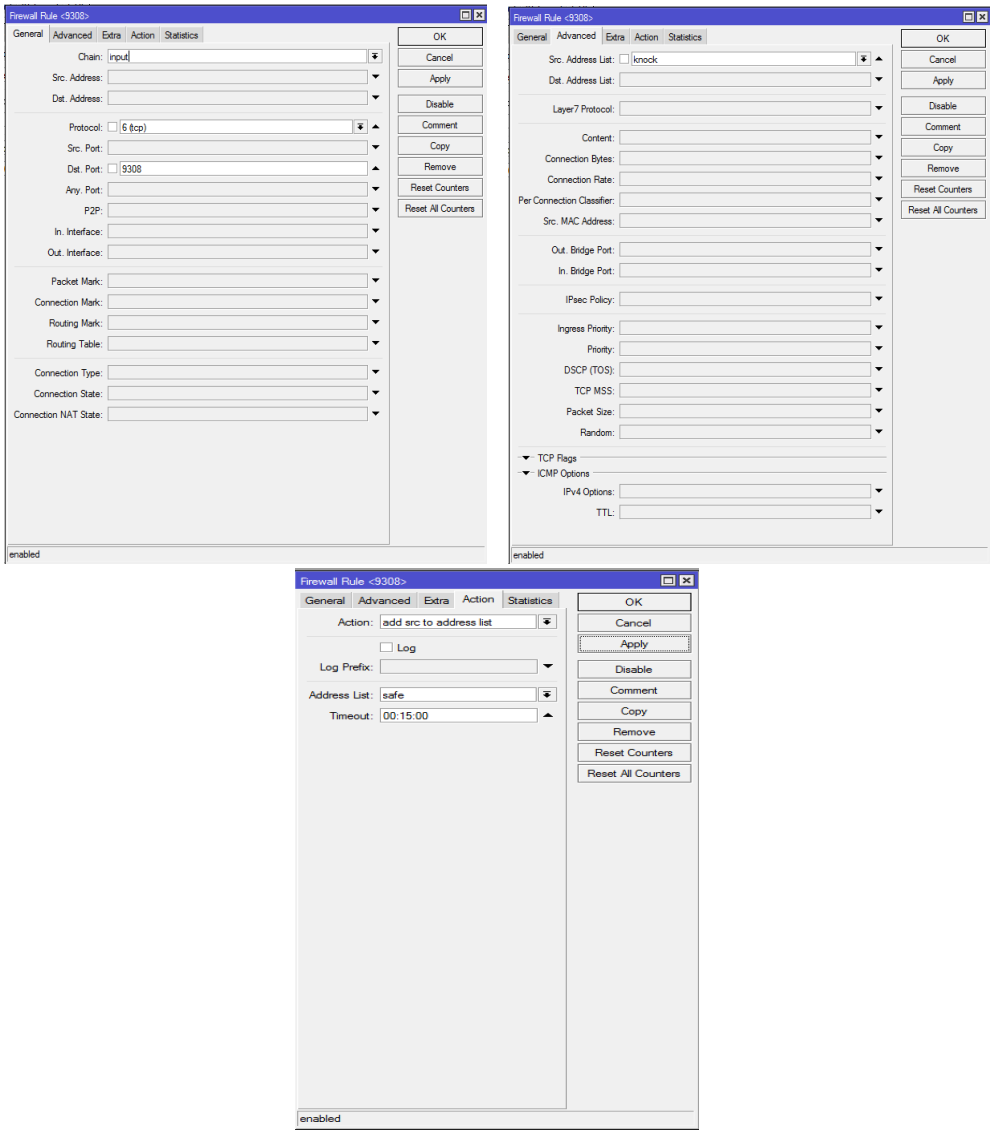
(27) Koristeći izbornik za dodavanje novog pravila vatrozida za filtriranje mrežnog prometa (*New Firewall Rule*) potrebno je zadati određeni protokol i broj porta, odnosno blokirati sav promet osim onog na portu 8039. Odabrani lanac je ulazni (*input*) što podrazumijeva obradu podataka koji se šalju na usmjerivač. U izborniku aktivnosti (*Action*) bira se dodavanje izvora na adresnu listu (*add-src-to-address-list*) da bi se bilježile sve izvorišne adrese paketa unutar liste „*knock*“. U izbornik vremenskog ograničenja (*Timeout*) postavlja se vremenski interval na 20 sekundi.



Slika 2.29. *Postavljanje pravila za filtriranje mrežnog prometa na vatrozidu (Firewall Rule) u prvom koraku prema sljedećem: a) izbor protokola, broja porta i blokiranje svog mrežnog promet osim onog na portu 8039, b) prikaz naprednih (Advanced) opcija filtriranja i c) dodavanje izvora na adresnu listu (add-src-to-address-list) da bi se bilježile sve izvorišne adrese paketa unutar adresne liste (Address List) „knock“ te postavljanje vremenskog ograničenja (Timeout) na zadani vremenski interval*

Drugo pravilo

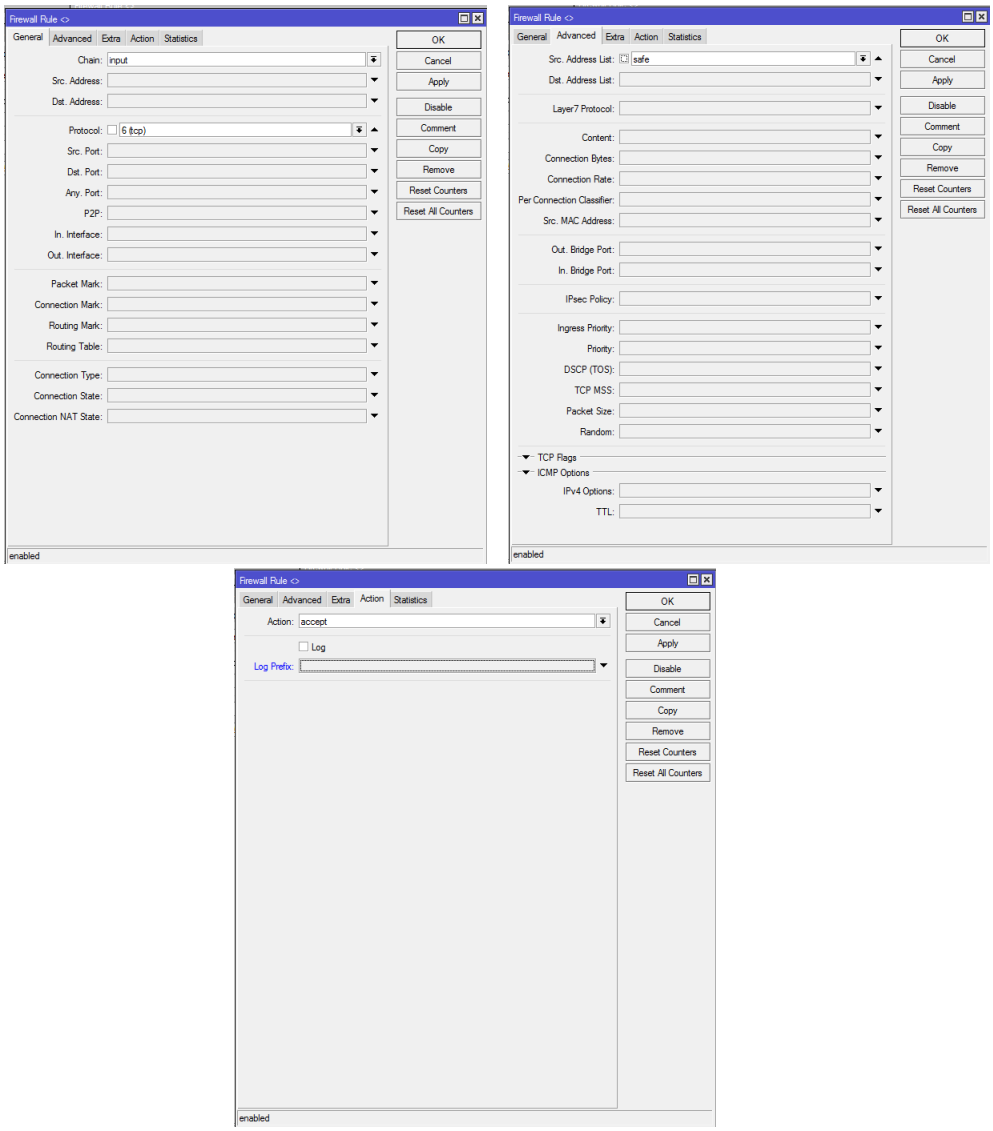
(28) U drugom pravilu vatrozidu također potrebno je zadati određeni protokol i broj porta, odnosno blokirati sav promet osim onog na portu 9308. Odabrani lanac je ulazni (*input*) što podrazumijeva obradu podataka koji se šalju na usmjerivač. U izborniku s naprednim postavkama (*Advanced*) odabire se lista „*knock*“, a u izborniku aktivnosti (*action*) bira se da se dodavanje izvora na adresnu listu (*add-src-to-address-list*) da bi se bilježile sve izvorišne adrese paketa unutar liste „*safe*“. U izbornik s vremenskim ograničenjem (*timeout*) postavlja se vremenski interval na 15 minuta.



Slika 2.30. *Postavljanje pravila za filtriranje mrežnog prometa na vatrozidu (Firewall Rule) u drugom koraku prema sljedećem: a) izbor protokola, broja porta i blokiranje svog mrežnog promet osim onog na portu 9308, b) prikaz naprednih (Advanced) opcija filtriranja prema izvorišnoj adresnoj listi (Src. Address List) „knock“ i c) dodavanje izvora na adresnu listu (add-src-to-address-list) da bi se bilježile sve izvorišne adrese paketa unutar adresne liste (Address List) „safe“ te postavljanje vremenskog ograničenja (Timeout) na zadani vremenski interval*

Treće pravilo

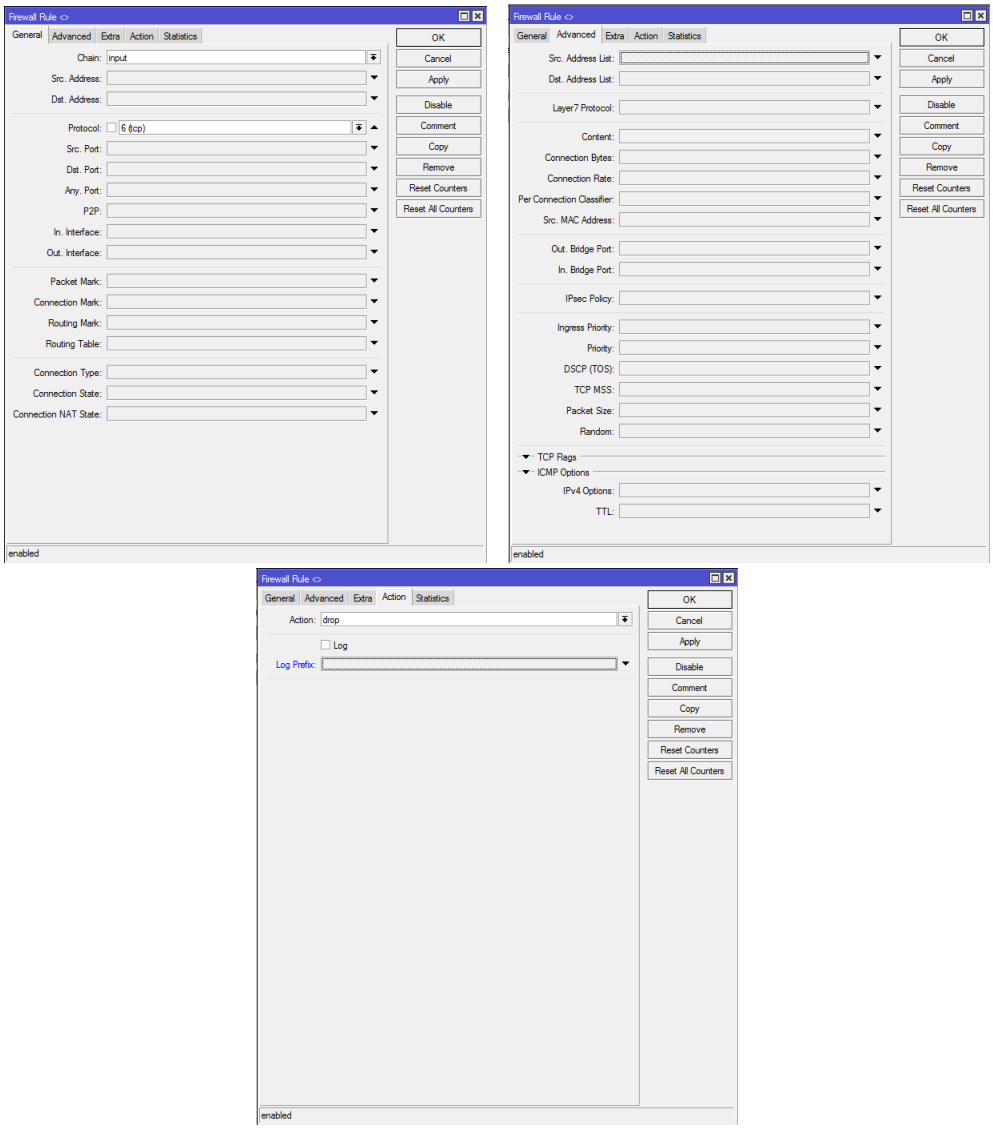
(29) U trećem koraku potrebno je dopustiti jedino adresama s liste „*safe*“ pristup usmjerivaču.



Slika 2.31. *Postavljanje pravila za filtriranje mrežnog prometa na vatrozidu (Firewall Rule) u trećem koraku prema sljedećem: a) izbor protokola, b) prikaz naprednih (Advanced) opcija filtriranja prema izvorišnoj adresnoj listi (Src. Address List) „safe“ i c) dopuštanje (accept) jedino adresama s liste „safe“ pristup usmjerivaču*

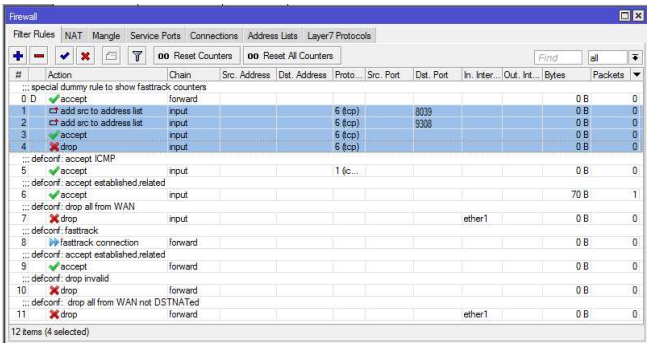
Četvrto pravilo

(30) U četvrtom koraku potrebno je blokirati pristup svemu što se ne uklapa u prethodna pravila.



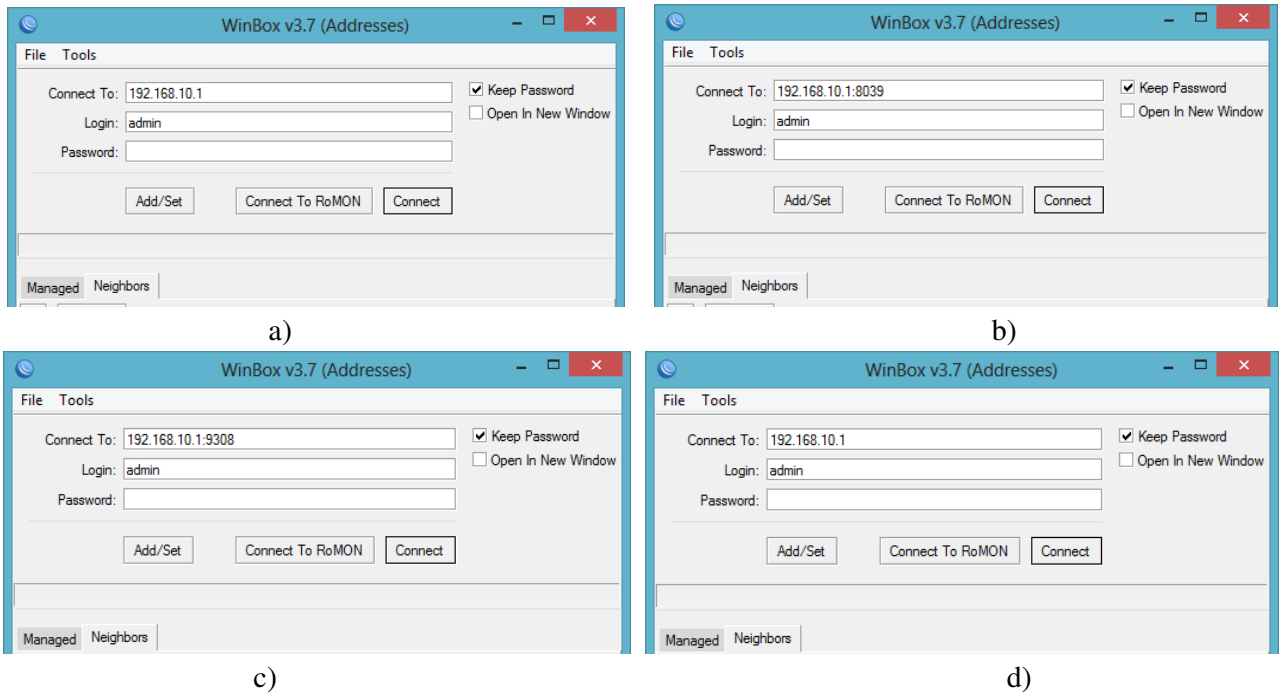
Slika 2.32. *Postavljanje pravila za filtriranje mrežnog prometa na vatrozidu (Firewall Rule) u četvrtom koraku prema sljedećem: a) izbor protokola, b) prikaz naprednih (Advanced) opcija filtriranja i c) blokiranje (drop) pristupa svemu što se ne uklapa u prethodna pravila*

(31) Sva prethodno defnirana pravila prikazana su na slici 2.33. (označena plavo). Njih je potrebno premjestiti kako bi redoslijed svih pravila odgovarao prikazu sa slike 2.33.



Slika 2.33. *Poredak svih konfiguriranih pravila filtriranja prometa (Filter Rules) vatrozida (Firewall)*

(32) Sad je potrebno u izbornik za pokretanje *WinBox* aplikacije (*WinBox Loader*) redom upisati oznake prema prikazu sa slike 2.34.



Slika 2.34. *Poredak upisivanja naredbi u početni prozor za pokretanje Winbox aplikacije (WinBox Loader) i pristupanje usmjerivaču prema sljedećem: a) IP adresa aktivnog Ethernet2 sučelja usmjerivača, b) IP adresa aktivnog Ethernet2 sučelja usmjerivača i broj porta 8039, c) IP adresa aktivnog Ethernet2 sučelja usmjerivača i broj porta 9308 i d) IP adresa aktivnog Ethernet2 sučelja usmjerivača*

Zadatak 8. Provjerite postoji li sada mogućnost pristupanja konfiguratoru usmjerivača i objasnite prethodno provedeni postupak upisa naredbi.

Vježba 3. - Prevencija neovlaštenog pristupa lokalnoj mreži:

Primjena protokola DHCP i ARP pri ograničavanju pristupa lokalnoj mreži

UVOD

U cilju adekvatne zaštite lokalne računalne mreže (eng. *Local Area Network*, skr. LAN) od neovlaštenog pristupa često je potrebno kombiniranti više različitih sigurnosnih rješenja. Jedan od načina koji omogućuje implementiranje kombiniranog pristupa u zaštiti računalne mreže zasniva se na primjeni posebne konfiguracije rubnog mrežnog usmjerivača koji povezuje određenu lokalnu mrežu s drugim mrežama. Takav usmjerivač štiti pristup lokalnoj mreži jer samo određenim klijentima dopušta povezivanje na tu lokalnu mrežu.

Zaštitu od neovlašetnog pristupa mreži moguće je realizirati na više načina. Neki od načina su:

- zaštita pristupa lokalnoj mreži putem autorizacije klijenata
- inicijalno ograničavanje pristupa mreži svim klijentima te naknadno dopuštanje pristupa samo nekim klijentima
- inicijalno dopuštanje pristupa mreži svim klijentima te naknadno blokiranje nekih klijenata.

Ovakve postupke zaštite moguće je realizirati konfiguriranjem određenih pravila koja usmjerivaču omogućuju provjeru ovlasti pristupa mreži za pojedine klijente te naknadnu dodjelu lokalnih IP adresa klijentima kojima se dopusti pristup mreži.

Kako se postavke definirane na sučeljima takvog usmjerivača mogu razlikovati, bitno je voditi računa o tome na koji će se način klijenti povezivati na pojedina sučelja usmjerivača (npr. žično ili bežično). Provjera smiju li klijenti pristupiti mreži ili ne provodi se ili na temelju autentifikacije klijenta pomoću lozinke i/ili na temelju jedinstvene oznake klijenta, tj. njegove MAC adrese. Navedeno je moguće provesti, uz ostalo, primjenom protokola ARP (*Address Resolution Protocol*) te protokola DHCP (*Dynamic Host Configuration Protocol*). Dok je protokol ARP namijenjen povezivanju fizičke MAC adrese uređaja s odgovarajućom mrežnom IP adresom, pri čemu se informacije o navedenoj kombinaciji adresa pohranjuju u ARP tablicu usmjerivača, namjena protokola DHCP vezana je uz dodjelu definiranih IP adresa uređaju. Ukoliko se nakon provjere utvrdi da se klijentu može dopustiti pristup lokalnoj mreži, DHCP poslužitelj konfiguriran na odgovarajućem sučelju usmjerivača dodjeljuje lokalnu IP adresu klijentu. Neki od načina implementacije kombiniranih zaštitnih rješenja uz primjenu navedenih metoda bit će prikazani u ovoj vježbi.

PRIPREMA ZA VJEŽBU

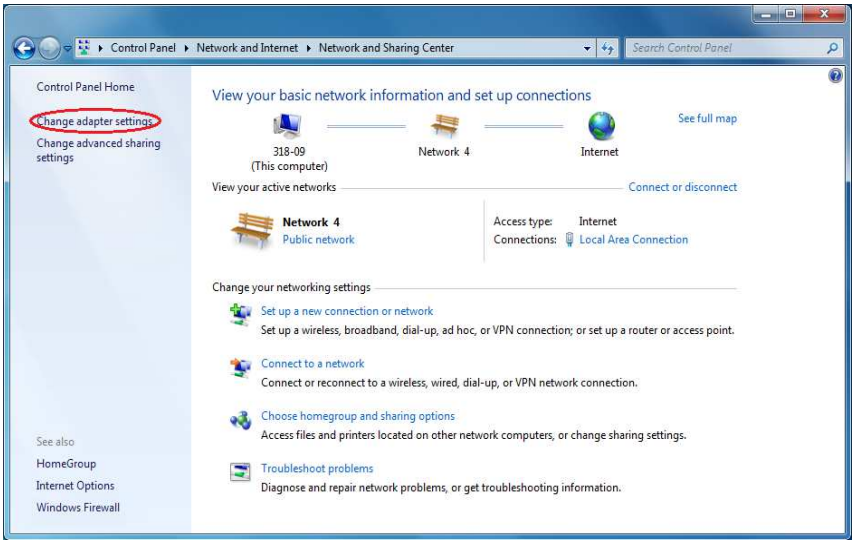
- Proučite namjenu **protokola DHCP i ARP**.
- **Provjerite** imate li svu mrežnu opremu potrebnu za **rad u paru**: računala, usmjerivač, *patch* kabele.

KREIRANJE ODABRANOG TESTNOG SCENARIJA:

Kroz korake (A)-(D) definiran je postupak uspostave testnog okruženja. Ovaj postupak obuhvaća deaktivaciju svih mrežnih konekcija na računalima osim lokalne mreže na PC1 te bežične mreže na PC2, isključivanje vatrozida te resetiranje postavki usmjerivača. Preostali koraci (I)-(VIII) vezani su uz konfiguraciju postavki usmjerivača i klijenata i testiranje mogućnosti (ne)ovlaštenog pristupa kreiranoj mreži.

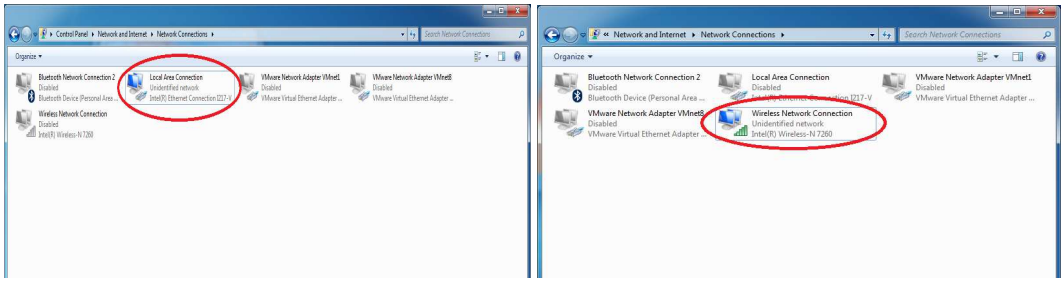
(A) DEAKTIVIRANJE POJEDINIH MREŽNIH KONEKCIJA NA KLIJENTIMA

(1) Na računalima otvorite prozor upravljačke ploče (eng. *Control Panel*), zatim odaberite poveznicu vezanu uz postavke mreže i Interneta (*Network and Internet*), te zatim poveznicu vezanu uz opcije središta za umrežavanje i dijeljenje (*Network and Sharing Center*).



Slika 3.1. *Prikaz opcija promjene postavki mrežnog adaptera (eng. Change Adapter Settings) središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

(2) Kliknite na opciju promjene postavki mrežnog adaptera (*Change Adapter Settings*). Na **PC1** omogućena treba ostati samo **lokalna žična konekcija** (*Local Area Connection*, LAN), a na **PC2** omogćena treba ostati samo **lokalna bežična konekcija** (*Wireless Network Connection*, WLAN). Deaktivirajte sve ostale mrežne konekcije na računalima (za pojedina bežična, žična i virtualna sučelja) osim navedenih - odaberite desnom tipkom miša odgovarajuću konekciju i odaberite opciju za deaktiviranje (*Disable*).

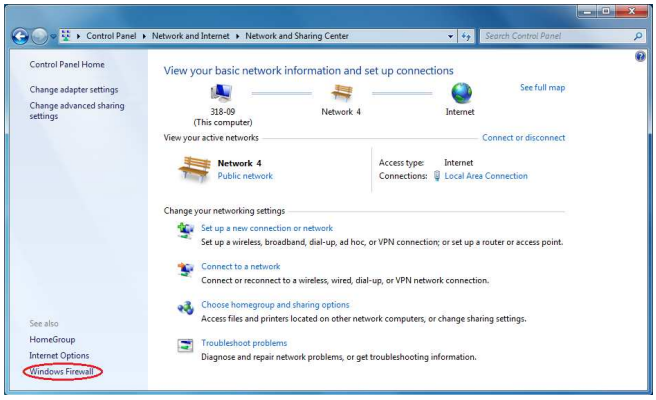


a) b)

Slika 3.2. *Prikaz postavki mrežnih konekcija (Network Connections) na računalima PC1 a) i PC2 b) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

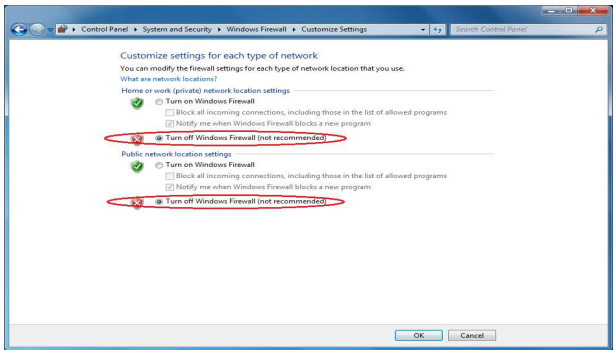
(B) ISKLJUČIVANJE VATROZIDA NA KLIJENTIMA

(3) Na računalima otvorite prozor upravljačke ploče (eng. *Control Panel*), zatim odaberite poveznicu vezanu uz postavke mreže i Interneta (*Network and Internet*), te zatim poveznicu vezanu uz opcije središta za umrežavanje i dijeljenje (*Network and Sharing Center*).



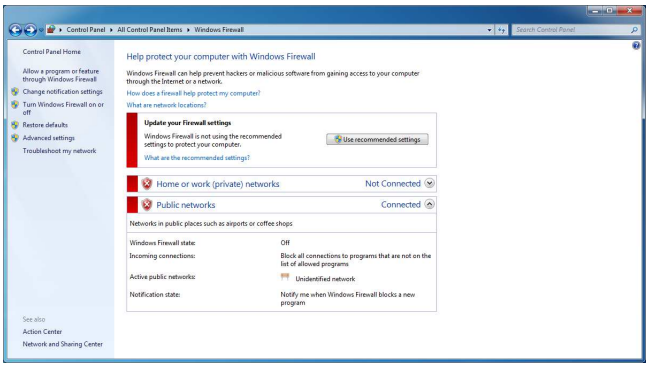
Slika 3.3. *Prikaz opcije za pristup postavkama Windows vatrozida (Windows Firewall) središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

(4) Isključite vatrozid ukoliko je pokrenut na računalu prema sljedećem postupku. Odaberite poveznicu koja otvara prozor s postavkama središta za umrežavanje i dijeljenje (*Network and Sharing Center*), zatim otvorite prozor s postavkama vatrozida (*Windows Firewall*), odaberite izbornik za uključivanje i isključivanje vatrozida (*Turn Windows Firewall on or off*) i isključite vatrozid (*Turn off Windows Firewall*).



Slika 3.4. *Prilagođavanje postavki (Customize Settings) za isključivanje Windows vatrozida (Windows Firewall)*

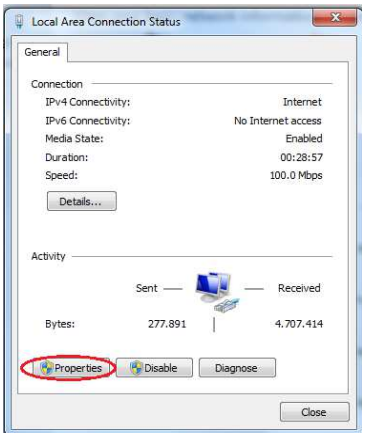
(5) Prikaz nakon deaktivacije vidljiv je na slici.



Slika 3.5. *Prikaz nakon deaktivacije Windows vatrozida*

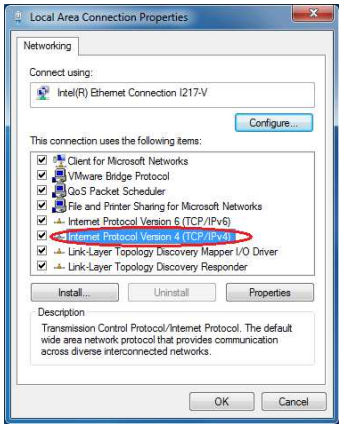
(C) DINAMIČKO ADRESIRANJE KLIJENATA

(6) U prozoru s opcijama središta za umrežavanje i dijeljenje (*Network and Sharing Center*) odaberite opciju promjene postavki mrežnog adaptera (*Change Adapter Settings*), zatim odaberite lokalnu mrežnu konekciju (*Local Area Connection*) i zatim njene postavke (*Properties*).



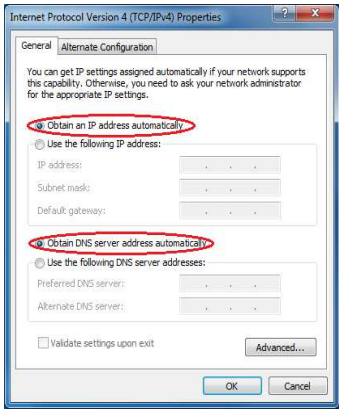
Slika 3.6. *Provjera postavki lokalne mreže (Local Area Connection Status) na računalu*

(7) Odaberite opciju prikaza postavki protokola IPv4 (*Internet Protocol Version 4 (TCP/IPv4)*).



Slika 3.7. *Provjera postavki lokalne konekcije (Local Area Connection Properties) na računalu*

(8) Provjerite jesu li odabrane sljedeće opcije prema prikazu sa slike: automatska dodjela IP adrese (*Obtain an IP address automatically*) te automatska dodjela adrese DNS poslužitelja (*Obtain DNS server address automatically*), te ih odaberite ukoliko već nisu odabrane.



Slika 3.8. *Provjera postavki na računalu za automatsku dodjelu IPv4 adrese i adrese DNS servera*

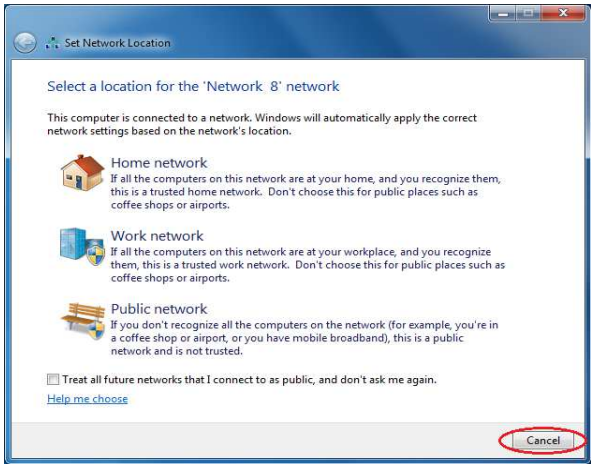
(D) RESETIRANJE POSTAVKI USMJERIVAČA

(9) Uključite usmjerivač. Povežite računalo PC1 na *Ethernet2* sučelje usmjerivača pomoću *patch* kabela, prema *shemi* na slici.

a) b)

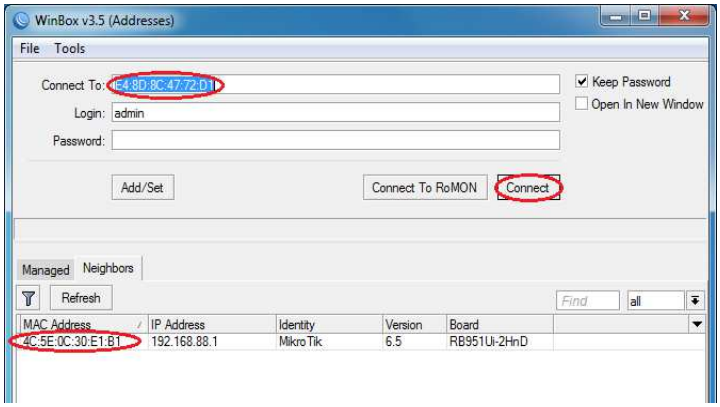
Slika 3.9. *a) Način povezivanja PC1 uređaja i MikroTik usmjerivača i b) MikroTik usmjerivač sa označenim Ethernet2 portom*

(10) Nakon što se otvori izbornik postavki lokacije mreže (*Set Network Location*) odaberite opciju izuzeća (*Cancel*).



Slika 3.10. *Izbornik postavki lokacije mreže* (*Set Network Location*)

(11) Pokrenite *WinBox* aplikaciju čija se ikona nalazi na radnoj ploči (*Desktop*) računala. Prvo označite MAC adresu (*MAC Address*) usmjerivača koja se nalazi na popisu u donjem dijelu prozora, a zatim kliknite na opciju za povezivanje (*Connect*).



Slika 3.11. *Sučelje WinBox aplikacije*

(12) Unutar otvorenog sučelja aplikacije *WinBox* odaberite opciju za otvaranje novog terminala (*New Terminal*). Otvara se terminal prikazan na donjoj slici.

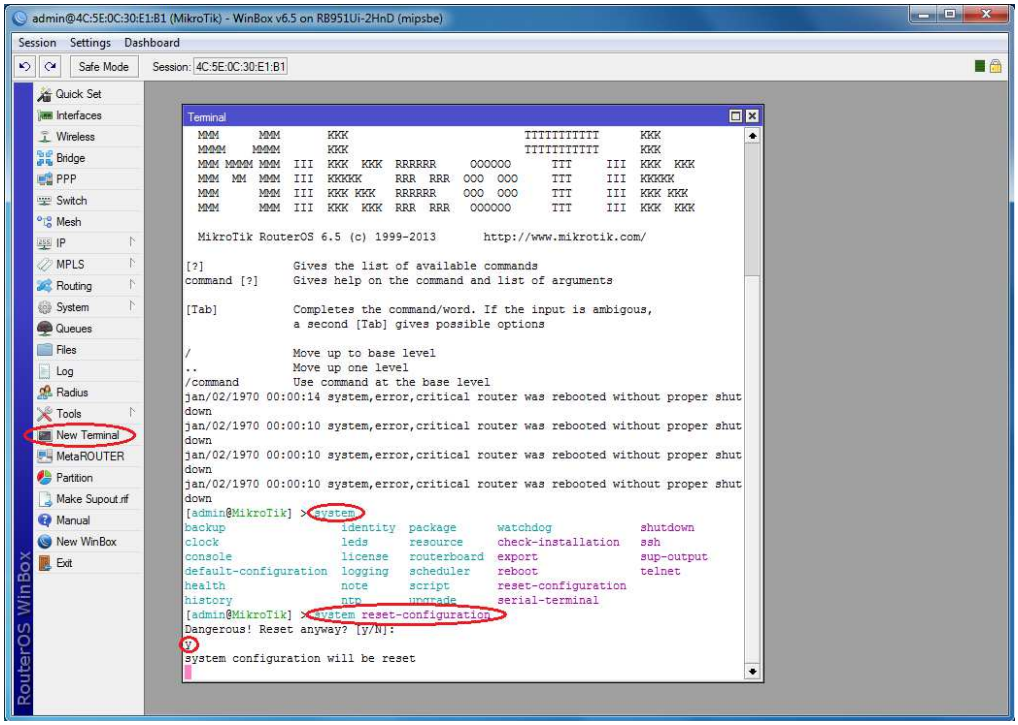
Resetirajte postavke na usmjerivaču upisivanjem naredbe:

system reset-configuration

i pomoću tipkovnice potvrdite upis odabirom tipke *Enter* te još jednom potvrdite izbor upisivanjem naredbe:

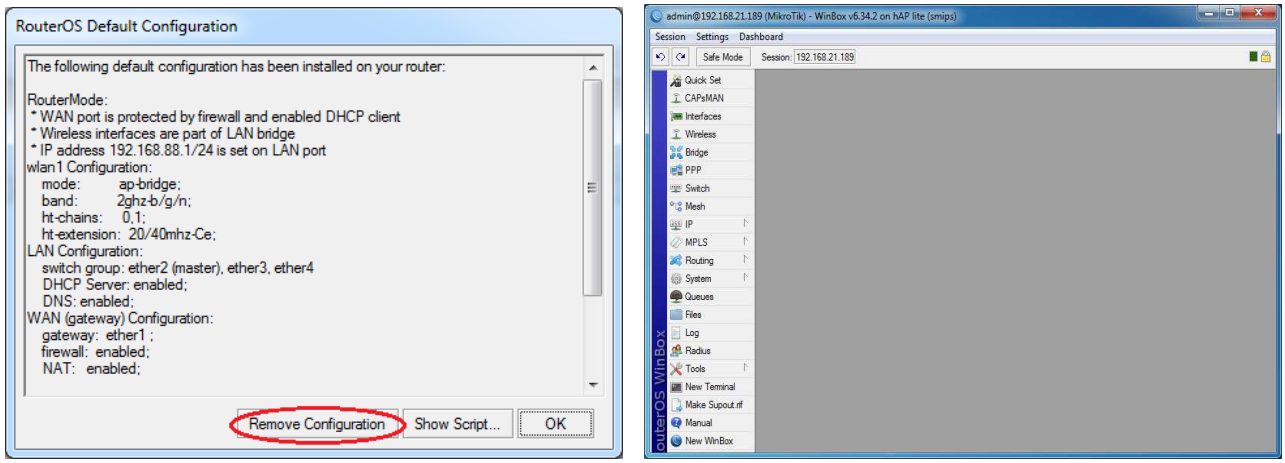
y

te odabirom tipke *Enter*. Ovime se pokreće resetiranje postojeće konfiguracije te se konfiguracija usmjerivača vraća na tvornički definiranu.



Slika 3.12. *Prikaz terminala WinBox aplikacije*

(13) Nakon ponovnog otvaranja *WinBox* aplikacije, potrebno je odabrati opciju brisanja konfiguracije (***Remove configuration***) kako bi postojeća tvornička konfiguracija bila u potpunosti obrisana.

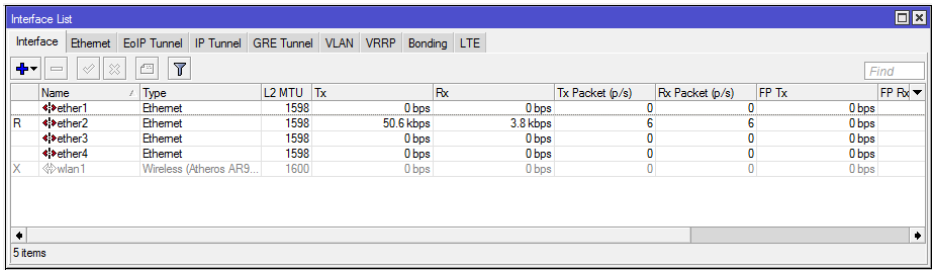


a) b)

Slika 3.13. a) *Brisanje postojeće tvorničke konfiguracije uređaja i b) početno sučelje WinBox aplikacije*

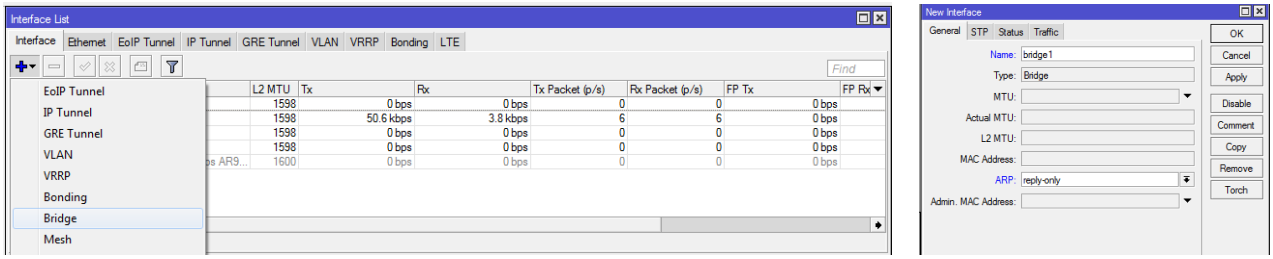
(I) KONFIGURIRANJE SUČELJA USMJERIVAČA

(14) Iz početnog *WinBox* izbornika prikazanog na slici odaberite opciju sučelja (*Interfaces*). Na slici su prikazana sva definirana sučelja koja se nalaze u ispisu unutar izbornika sučelja (*Interfaces*).



Slika 3.14. *Prikaz izbornika sučelja (Interfaces)*

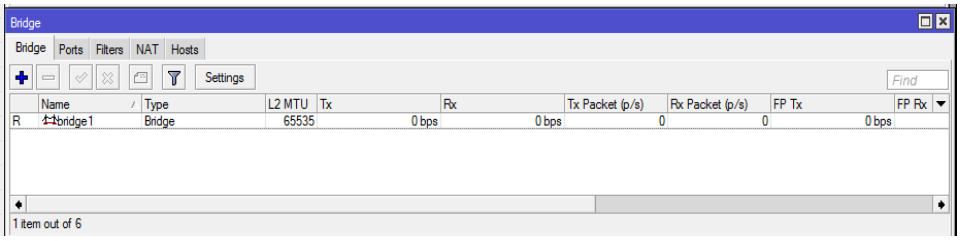
(15) Za kreiranje dodatnog sučelja potrebno je iz padajućeg izbornika odabrati opciju umošćivanja (*Bridge*). Za dodano sučelje potrebno je definirati naziv *bridge1* te unutar izbornika ARP odabrati opciju jedino odgovora (*reply-only*).



a) b)

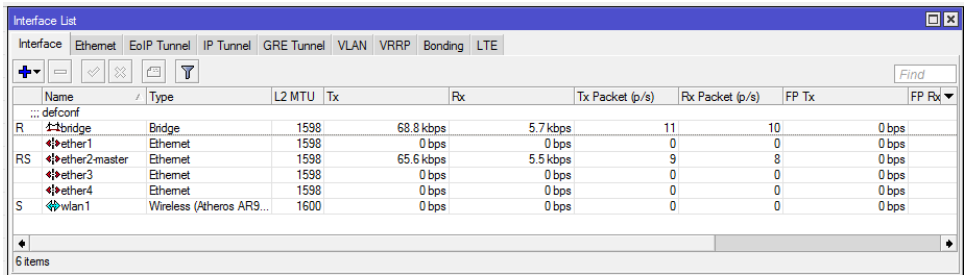
Slika 3.15. *a) Dodavanje novog sučelja mosta (Bridge) i b) konfiguriranje novog sučelja bridge1*

(16) Nakon dodavanja sučelja, prikaz bi trebao odgovarati prikazu sa donje slike.



Slika 3.16. *Prikaz novog kreiranog sučelja bridge1*

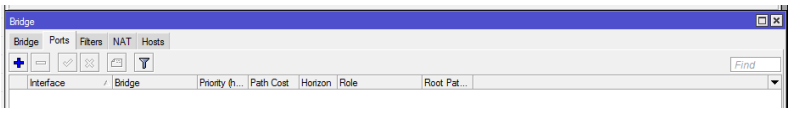
(17) Aktivirajte (*activate*) sučelje *wlan1* koje će se koristiti. Na slici se nalazi prikaz svih aktivnih sučelja.



Slika 3.17. *Prikaz svih aktivnih sučelja usmjerivača*

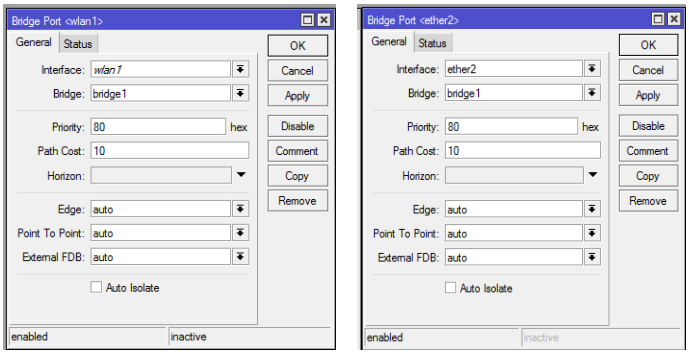
(II) DODAVANJE SUČELJA USMJERIVAČA U BRIDGE

(18) Kroz idućih nekoliko koraka bit će objašnjen postupak dodavanja sučelja u most (eng. *bridge*), tzv. umošćivanje (eng. *bridging)*. Prema prikazu sa slike, unuar izbornika mosta (*Bridge*) potrebno je otvoriti karticu portovi (*Ports*).



Slika 3.18. *Kartica portovi (Ports) unutar izbornika most (Bridge)*

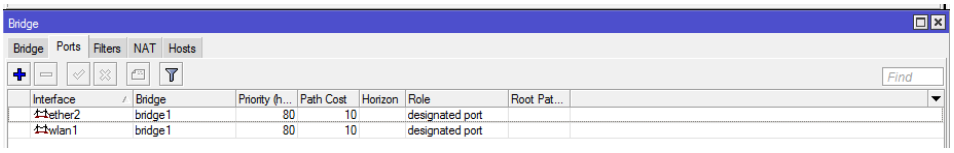
(19) Klikom na oznaku '+' potrebno je dodati sučelje *wlan1* u *bridge1*. Postupak je potrebno ponoviti za sučelje *Ethernet2*, tj. i sučelje *Ethernet2* dodati u *bridge1*. *Napomena*: Ukoliko se nakon dodavanja *Ethernet2* sučelja prekine komunikacija s *WinBox* aplikacijom, potrebno je odabrati opciju ponovnog povezivanja (*Reconnect*) i ponovno pokrenuti *WinBox*.



a) b)

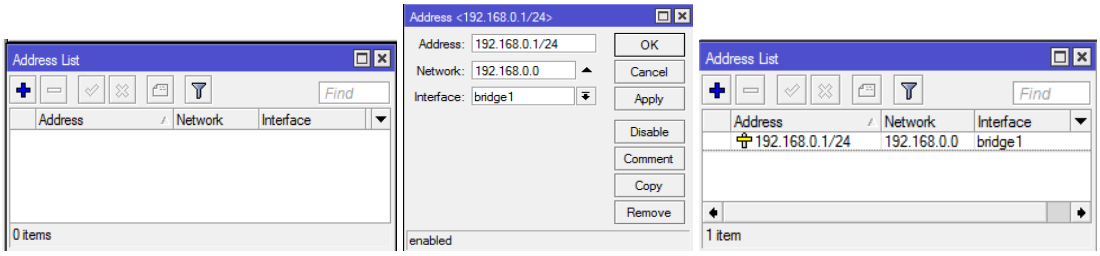
Slika 3.19. a) *Dodavanje sučelja wlan1 u most bridge1 i b) dodavanje ethernet sučelja u most bridge1*

(20) Sada bi se u izborniku *Bridge* trebale nalaziti oznake oba dodana sučelja.



Slika 3.20. *Prikaz sučelja dodanih u most bridge1*

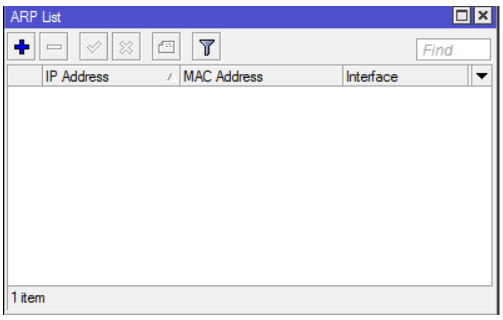
(21) Nakon kreiranja sučelja *bridge1*, tom je sučelju potrebno dodijeliti IP adresu. Iz izbornika tipa protokola (*IP*) potrebno je odabrati opciju za adresiranje (*Addresses*) te unutar izbornika s popisom adresa (*Address List*) kliknuti na oznaku '+' i dodijeliti sučelju *bridge1* adresu 192.168.0.1/24 te postaviti 192.168.0.0 za adresu mreže.



a) b) c)

Slika 3.21. *a) Dodavanje bridge1 sučelja u adresnu listu (Address List), b) dodjela IP adrese krieranom bridge1 sučelju i c) prikaz adrese doijeljene bridge1 sučelju*

Zadatak 1. Provjerite sadržaj ARP tablice. (Kako biste pristupili ARP tablici usmjerivača prikazanoj na slici, iz izbornika odaberite opciju protokola IP (*IP*) te protokola ARP (*ARP*).



Slika 3.22. *Prikaz sadržaja ARP tablica usmjerivača*

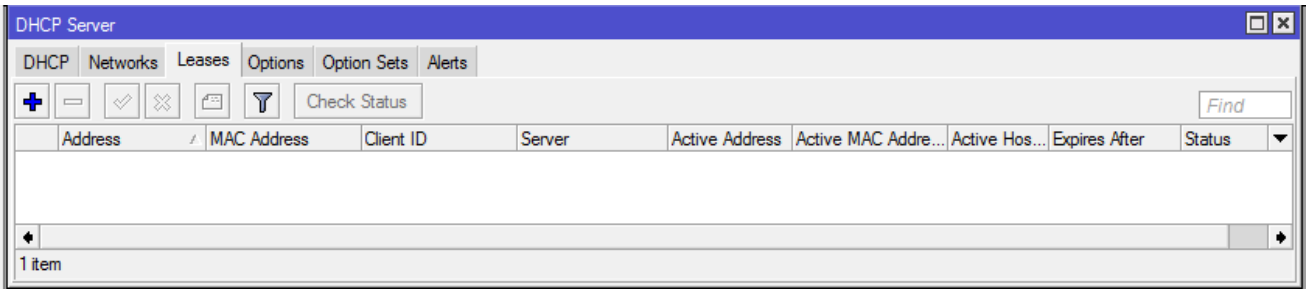
Zadatak 2. Objasnite što se može zaključiti na temelju sadržaja ARP tablice.

_____

_____

_____

Zadatak 3. U izborniku DHCP poslužitelja (*DHCP Server*) pod karticom rezervacija (*Leases*), prikazanom na slici, pogledajte popis trenutno dodijeljenih IP adresa.



Slika 3.23. *Popis adresa pod karticom rezervacija (Leases) u izborniku DHCP poslužitelja (DHCP Server)*

Zadatak 4. Objasnite što se može zaključiti iz navedenog prikaza.

_____

_____

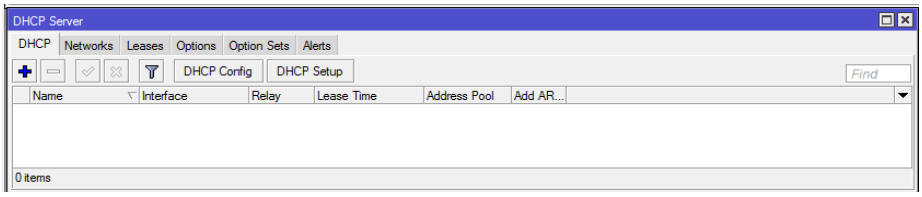
_____

Zadatak 5. Pokrenite naredbeni redak (***Command Prompt***) upisivanjem naredbe ***cmd*** unutar *Windows*-ovog *Start* izbornika i provjerite IP adresu koja je automatski dodijeljena računalu PC1 upisivanjem naredbe ***ipconfig*** u naredbeni redak (*Command Prompt*). Ispišite sljedeće:

- adresu računala PC1 (*IPv4 Address*): _____
- adresu maske podmreže (*Subnet Mask*): _____
- adresu aktivnog *Ethernet2* sučelja usmjerivača (*Default Gateway*): _____
- na koji način je računalu dodijeljena adresa: _____

(III) KONFIGURIRANJE DHCP POSLUŽITELJA NA BRIDGE SUČELJU USMJERIVAČA

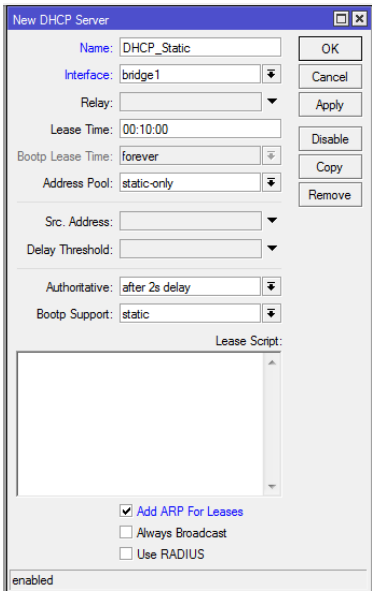
(22) U nastavku je opisan osnovni postupak konfiguriranja DHCP poslužitelja na *bridge1* sučelju usmjerivača.
Iz izbornika odaberite tip protokola (*IP*), zatim vrstu poslužitelja (*DHCP Server*), vrstu protokola (*DHCP*) te opciju dodavanja novog poslužitelja (*Add New*).



Slika 3.24. *Prikaz izbornika DHCP poslužitelja (DHCP Server)*

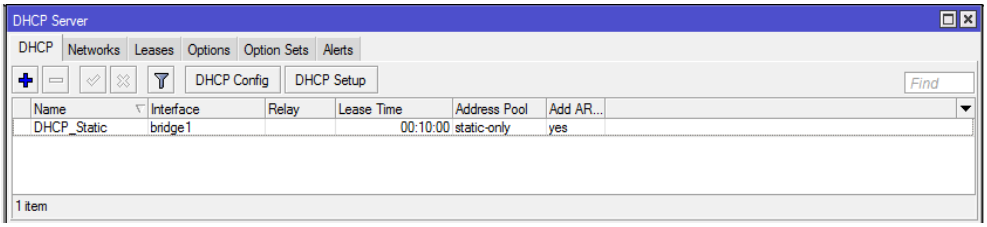
(23) Definirajte postavke DHCP poslužitelja:

- naziv poslužitelja (*Name*): *DHCP_Static*
- sučelje (*Interface*): *bridge1*
- statički raspon adresa (*Address pool*): *static-only*
- označite opciju dodavanja protokola ARP za rezervaciju IP adresa: *Add ARP For Leases*.



Slika 3.25. *Postavke novog DHCP poslužitelja (New DHCP Server)*

(24) Potvrdite izbor (*OK*). Prikaz bi trebao odgovarati sljedećem prikazu:

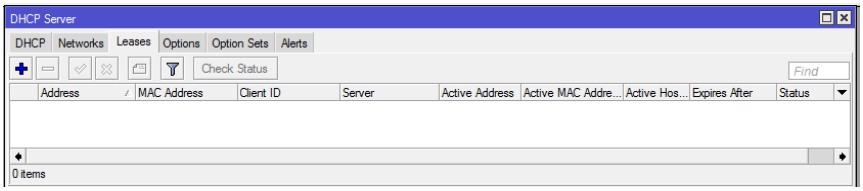


Slika 3.26. *Prikaz kreiranog DHCP poslužitelja (DHCP Server)*

Zadatak 6. Objasnite zašto je ARP tablica usmjerivača prazna.

(IV) STATIČKO ADRESIRANJE KLIJENATA

(25) Kako bi se samo točno određenim klijentima omogućio pristup lokalnoj mreži, unutar izbornika DHCP poslužitelja (*DHCP Server*) potrebno je odabrati karticu rezervacija (*Leases*) te dodati oznake uređaja kojima se želi omogućiti pristup. U ovom dijelu vježbe pristup će se omogućiti računalima PC1 i PC2.

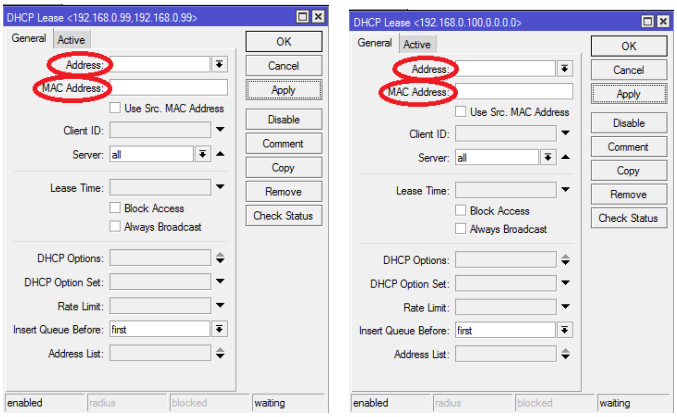


Slika 3.27. *Popis adresa pod karticom rezervacija (Leases) u izborniku DHCP poslužitelja (DHCP Server)*

Zadatak 7. Uređaje je moguće jednoznačno definirati preko njihove MAC adrese. Za informaciju o MAC adresi računala na oba je računala potrebno u naredbeni redak (*Command Prompt*) upisati naredbu ***ipconfig /all***. Upišite odgovarajuće MAC adrese računala:

MAC PC1:_____ MAC PC2:_____

(26) U izborniku DHCP rezervacije (*DHCP Lease*) je **uz oznaku MAC adrese** (*MAC Address*) **računala PC1**, koju svakako treba **upisati u taj izbornik**, potrebno upisati i sljedeću statičku **IP adresu** (*Address*): **192.168.0.100**
Isto tako, u dodatnom izborniku DHCP rezervacije (*DHCP Lease*) je **uz MAC adresu** (*MAC Address*) **računala PC2**, koju također svakako treba **upisati u izbornik**, potrebno upisati i statičku **IP adresu** (*Address*): **192.168.0.99**



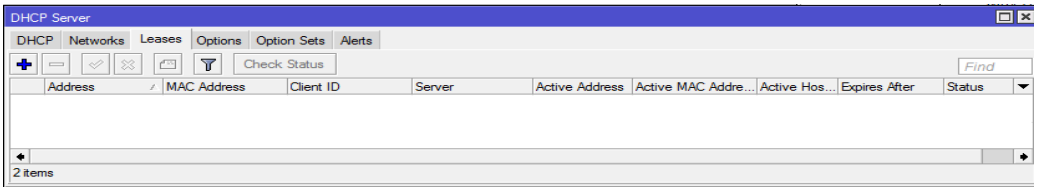
a) b)

Slika 3.28. *a) Unos adresa računala PC1 i b) unos adresa računala PC2 u izbornik DHCP Leases*

Zadatak 8. U konzolu računala PC1 unesite redom sljedeće naredbe za otpuštanje i obnovu IP adresa:

ipconfig /release
ipconfig /renew

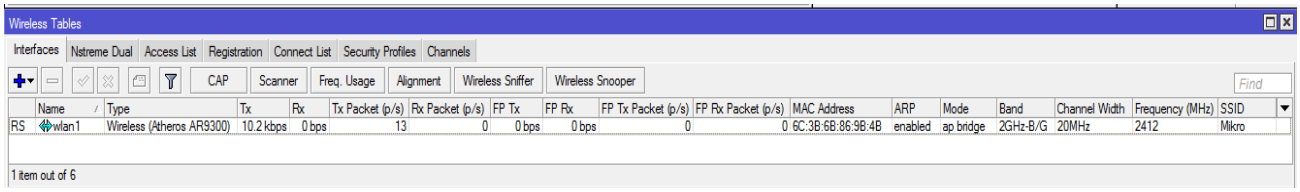
Oznake iz izbornika *Leases* upišite u prostor na slici.



Slika 3.29. *Prikaz definiranih statičkih adresa računala pod karticom rezervacija (Leases) u izborniku DHCP poslužitelja (DHCP Server)*

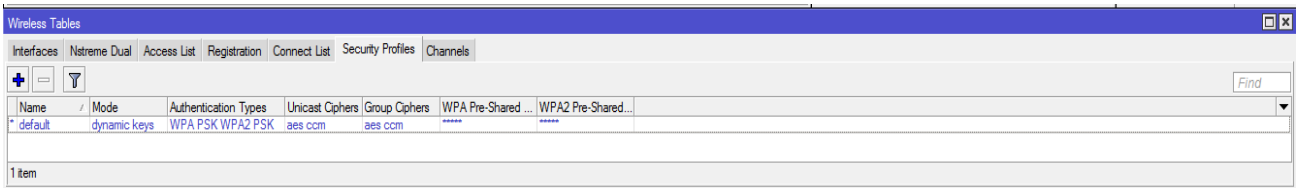
(V) KONFIGURIRANJE POSTAVKI BEŽIČNE MREŽE

(27) Kroz sljedećih nekoliko koraka potrebno je konfigurirati bežični pristup putem kojeg bi se trebala ostvariti bežična konekcija između usmjerivača i računala PC2. Nakon otvaranja izbornika bežične mreže (*Wireless*) unutar kartice sučelja (*Interfaces*) trebala bi biti vidljiva postojeća *wlan1* konekcija koju je potrebno dodatno kofigurirati.



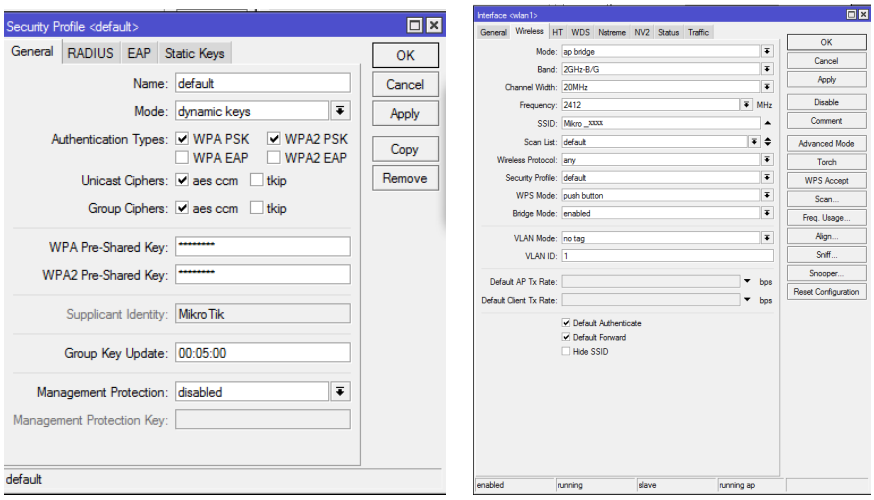
Slika 3.30. *Prikaz wlan1 konekcije unutar kartice aktivnih sučelja (Interfaces) u izborniku s popisom bežičnih konekcija (Wireless Table)*

(28) Za početak je potrebno odabrati karticu sigurnosnih profila (*Security Profiles*) te dodatno definirati predefinirani sigurnosni profil (*default*).



Slika 3.31. *Prikaz kartice sigurnosnih profila (Security Profiles) u izborniku s popisom bežičnih konekcija (Wireless Table)*

(29a) Pri konfiguriranju sigurnosnog profila pod opcijom načina rada (*Mode*) potrebno je odabrati dinamičke ključeve (*dynamic keys*), označiti polja *WPA PSK* i *WPA2 PSK* te upisati željenu *WPA* i *WPA2* lozinku (*Pre-Shared Key*).



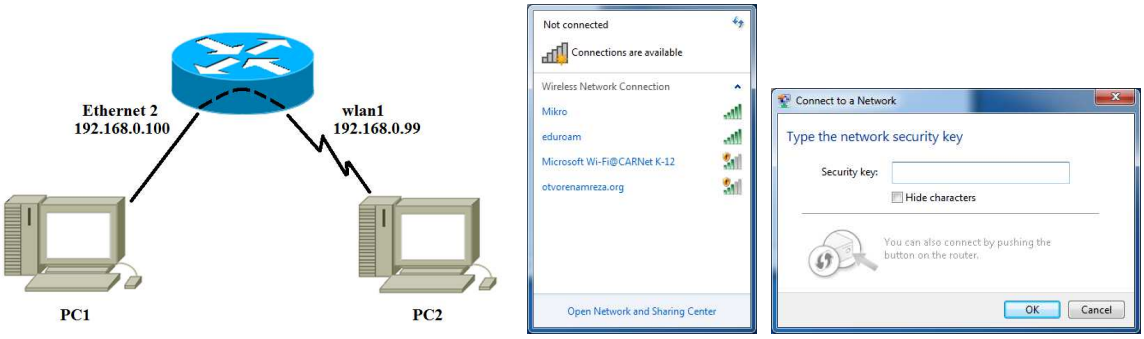
a) b)

Slika 3.32. *a) Konfiguriranje sigurnosnog profila (Security Profile) i b) postavke bežičnog pristupa (Wireless)*

(29b) U izborniku bežične mreže (*Wireless*) unutar kartice sučelja (*Interfaces*) potrebno je odabrati postojeću *wlan1* konekciju. Pri konfiguraciji je potrebno za način rada (*Mode*) odabrati *ap bridge*. Pri definiranju SSID-a potrebno je koristiti sljedeću oznaku: *Mikro_xxxx* pri čemu umjesto simbola „*xxxx*“ treba upisati vlastiti datum rođenja (dan i mjesec). Pod opcijom sigurnosnog profila (*Security Profile*) treba iz padajućeg izbornika odabrati zadani (*default*).

(VI) KREIRANJE TESTNE LOKALNE MREŽE

(30a) Sada je potrebno povezati uređaje i kreirati topologiju prema prikazu sa slike. Računalo PC1 treba ostati žično povezano na sučelje *Ethernet2* usmjerivača, dok je računalo PC2 potrebno bežično povezati s usmjerivačem preko sučelja *wlan1*.



a) b) c)

Slika 3.33. *a) Kreirana mrežna topologija, b) izbornik s popisom dostupnih bežičnih mreže za bežično povezivanje PC2 sa usmjerivačem i c) okvir za unos sigurnosnog ključa (Security key)*

(30b) Kako bi se računalo PC2 povezalo sa usmjerivačem, potrebno je unutar *Windows*-a na računalu PC2 provjeriti nalazi li se na popisu dostupnih bežičnih mreža definirana mreža sa odgovarajućom SSID oznakom: *Mikro_xxxx* (Napomena: Ukoliko postoji više mreža sličnog naziva treba odabrati mrežu sa odgovarajućom „*xxxx*“ oznakom.) Nakon klika na odgovarajući naziv potrebno je odabrati opciju za povezivanje (*Connect*) te upisati prethodno definiranu lozinku. Nakon uspješnog povezivanja trebala bi se pojaviti oznaka koja označava postojanje veze (*Connected*).

Zadatak 9. U konzolu računala PC2 unesite redom sljedeće naredbe za otpuštanje i obnovu IP adresa:

ipconfig /release
ipconfig /renew

Nakon unošenja naredbe ***ipconfig /all*** u konzole računala PC1 i PC2 potrebno je ispisati sljedeće adrese:

- adresu računala PC1 (*IPv4 Address*): _____
- adresu maske podmreže (*Subnet Mask*): _____
- adresu računala PC2 (*IPv4 Address*): _____
- adresu maske podmreže (*Subnet Mask*): _____

Zadatak 10. Navedite adresu mreže u kojoj se nalaze PC1 i PC2? _____/_____

Zadatak 11. Provjerite postoji li konekcija između:

- računala PC1 i usmjerivača upisivanjem naredbe *ping* na otvorenoj konzoli (*Command Prompt*) računala PC1: *ping 192.168.0.1*
- računala PC2 i usmjerivača upisivanjem naredbe *ping* na otvorenoj konzoli (*Command Prompt*) računala PC2: *ping 192.168.0.1*

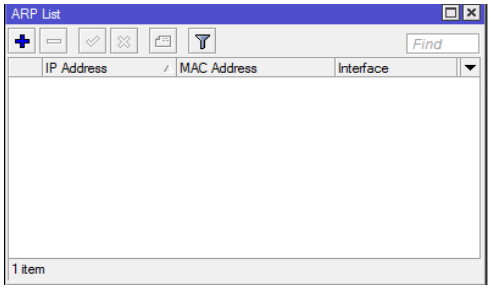
U tablicu upišite postoji li povezanost između pojedinih uređaja.

Tablica 3.1. *Testiranje međusobne povezanosti uređaja*

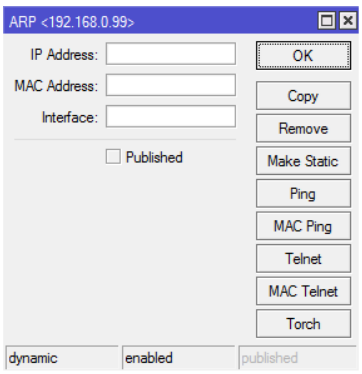
Provjera povezanosti između pojedinih uređaja (koristiti oznake: ✓ ako povezanost postoji ili × ako povezanost ne postoji)		
	PC2:	**USMJERIVAČ:**
PC1:		
USMJERIVAČ:		

(VII) ANALIZA SADRŽAJA ARP TABLICA

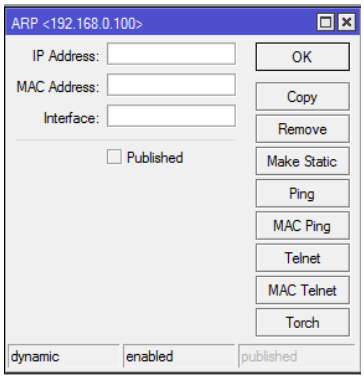
Zadatak 12. Pogledajte sadržaj ARP tablice usmjerivača. Prikaz upišite u odgovarajuće prostore na slikama:



a)



b)



c)

Slika 3.34. *a) Sadržaj ARP tablice usmjerivača, b) adrese računala PC2 i c) adrese računala PC1*

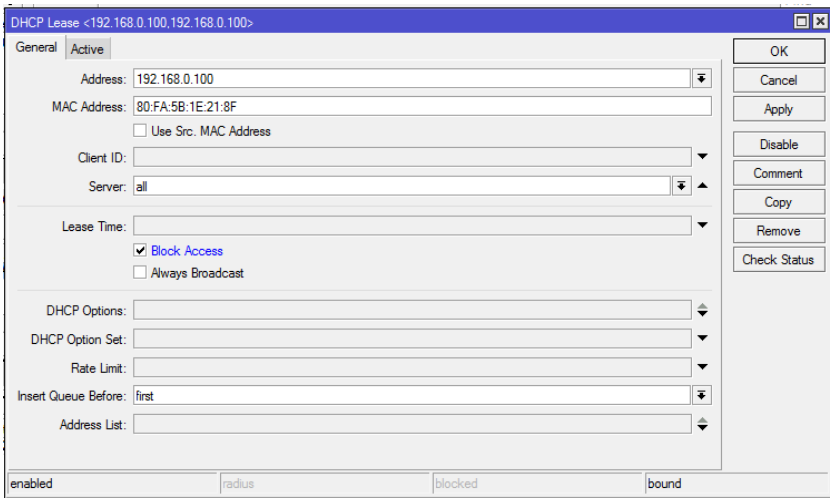
Zadatak 13. Objasnite što se sve može uočiti iz prikazanog sadržaja ARP tablice.

Zadatak 14. Za provjeru sadržaja ARP tablice klijenta (računala) potrebno je u naredbeni redak (*Command Prompt*) računala upisati naredbu: *arp –a*
Provjerite sadržaj ARP tablice računala PC1 i PC2 i objasnite što se sve može uočiti iz prikazanog sadržaja.

Zadatak 15. Provjerite i ukratko opišite koje se dodatne opcije mogu definirati upisivanjem naredbe *arp* u naredbeni redak (*Command Prompt*) računala.

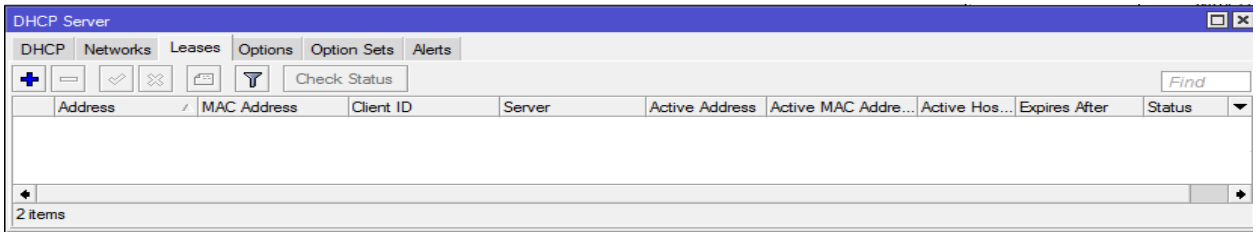
(VIII) NAKNADNO BLOKIRANJE PRISTUPA MREŽI

(31) U slučaju kada je klijentu potrebno blokirati pristup kreiranoj lokalnoj mreži, unutar izbornika rezervacija DHCP poslužitelja (*DHCP Server Leases*) potrebno je odabrati DHCP rezervacije (*DHCP Leases*) (npr. za računalo PC1, tj. ono s IP adresom 192.168.0.100) i označiti opciju blokiranja pristupa (*Block Access*). Sada se u izborniku rezervacija (*Leases*) uz adresu računala treba nalaziti i oznaka '*B*'.



Slika 3.35. *Blokiranje pristupa računalu PC1 lokalnoj mreži unutar izbornika DHCP rezervacija (DHCP Leases)*

Zadatak 16. Upišite podatke navedene u izborniku *Leases* u prostor na slici.



Slika 3.36. *Prikaz izbornika DHCP rezervacija (DHCP Leases) nakon blokiranja jednog klijenta (PC1)*

Zadatak 17. U konzolu računala PC1 unesite redom sljedeće naredbe za otpuštanje i obnovu IP adresa: ***ipconfig /release*** te ***ipconfig /renew***. Nakon provedbe prethodnog postupka objasnite što se dogodilo. Može li računalo PC1 pristupiti lokalnoj mreži?

Zadatak 18. U konzolu računala PC2 unesite redom sljedeće naredbe: ***ipconfig /release*** te ***ipconfig /renew*** Provjerite postoji li još uvijek konekcija između računala PC2 i usmjerivača upisivanjem naredbe *ping* na otvorenoj konzoli (*Command Prompt*) računala PC2: *ping 192.168.0.1*. Što zaključujete?

Vježba 4. - Sigurna razmjena podataka kroz javnu računalnu mrežu:
Konfiguriranje virtualne privatne mreže (VPN)

UVOD

Računalne mreže predstavljaju dijeljeni resurs kojeg u cilju razmjene podataka koristi veći broj korisnika. U takvom mrežnom okruženju često se javlja potreba za razmjenom povjerljivih informacija koje niti u kojem slučaju ne smiju postati dostupne neovlaštenim osobama. S porastom globalne svjetske mreže povećava se i broj pokušaja neovlaštenog pristupa i zlouporabe računalnih resursa i privatnih informacija. Zbog toga je iznimno bitno voditi računa o zaštiti računalnih mreža, kao i o zaštiti svakog pojedinog računala unutar mreže.

U praksi se često javlja potreba za razmjenom povjerljivih informacija između međusobno udaljenih računala koja se ne nalaze na zajedničkoj sigurnoj mreži, već ih je potrebno povezati preko javne nesigurne mreže (npr. Interneta). U takvim slučajevima koriste se virtualne privatne mreže (*Virtual Private Network*, VPN). VPN omogućuje kontrolirano i sigurno povezivanje udaljenih čvorova kroz javnu računalnu mrežu.

VPN mreže temelje se na konceptu IP tuneliranja, što podrazumijeva stvaranje virtualne veze između dvaju čvorova (*point-to-point*) koji su u stvarnosti razdvojeni nizom mreža. Virtualni tunel na svojim krajevima ima usmjerivače između kojih se zapravo kreira virtualna veza. Kada usmjerivač na početku tunela želi poslati paket putem virtualne veze on ga enkapsulira unutar IP datagrama čija je odredišna adresa adresa usmjerivača na kraju tunela. Kako bi se osigurala povjerljivost informacije prilikom slanja koristi se i odgovarajuća **enkripcija** (eng. *encryption*), tj. **šifriranje** odnosno **kriptiranje**. Na odredištu se vrši postupak **dekripcije** (eng. *decription*), tj. **dešifriranje** odnosno **dekriptiranje**.

PPTP (*Point-to-Point Tunneling Protocol*) je jedan od protokola koji se u VPN mrežama primjenjuje za tuneliranje podataka od točke do točke. Enkripciju i kompresiju podataka te autentikaciju korisnika protokol PPTP prepušta protokolu PPP (*Point-to-Point*) kojeg prenosi svojim tunelima. PPTP uspostavlja dvije paralelene veze između VPN klijenta i poslužitelja. Najprije uspostavlja kontrolnu TCP vezu na portu 1723, a zatim GRE (*Generic Routing Encapsulation*) tunel prema istom čvoru kroz koji se tada mogu prenositi paketi.

PRIPREMA ZA VJEŽBU

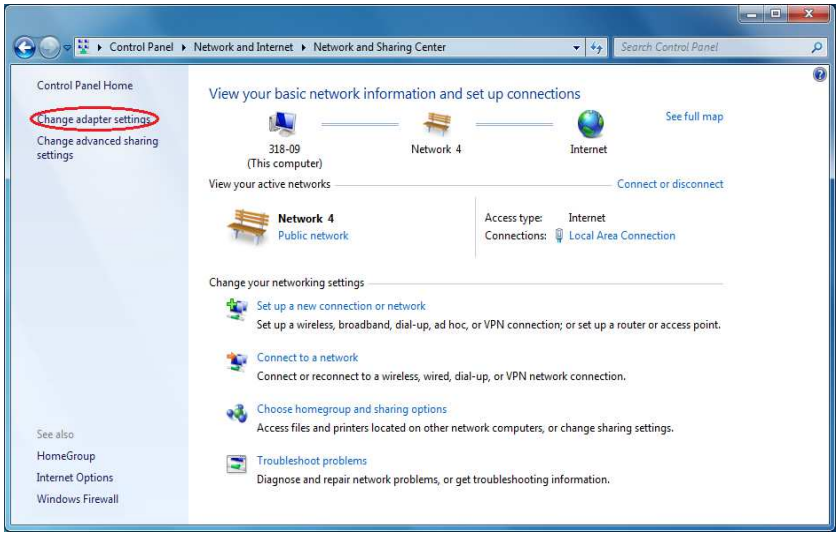
- Proučite namjenu **VPN mreža** te **protokola PPP i PPTP**.
- **Provjerite** imate li svu mrežnu opremu potrebnu za **rad**: računalo, usmjerivač, *patch* kabele.

KREIRANJE ODABRANOG TESTNOG SCENARIJA:

Kroz korake (A)-(D) definiran je postupak uspostave testnog okruženja. Ovaj postupak obuhvaća deaktivaciju svih mrežnih konekcija na računalu PC1 osim lokalne mreže, isključivanje vatrozida te resetiranje postavki usmjerivača. Preostali koraci (I)-(V) vezani su uz konfiguraciju postavki usmjerivača i klijenta (PC1) i testiranje mogućnosti (ne)ovlaštenog pristupa kreiranoj mreži.

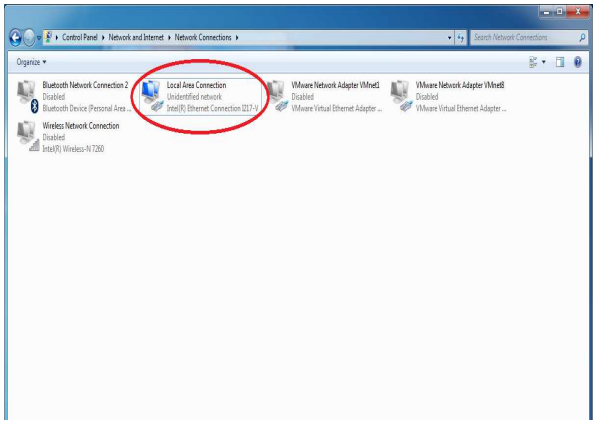
(A) DEAKTIVIRANJE POJEDINIH MREŽNIH KONEKCIJA NA KLIJENTIMA

(1) Na računalu otvorite prozor upravljačke ploče (*Control Panel*), zatim odaberite poveznicu vezanu uz postavke mreže i Interneta (*Network and Internet*), te zatim poveznicu vezanu uz opcije središta za umrežavanje i dijeljenje (*Network and Sharing Center*).



Slika 4.1. *Prikaz opcija promjene postavki mrežnog adaptera (eng. Change Adapter Settings) središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

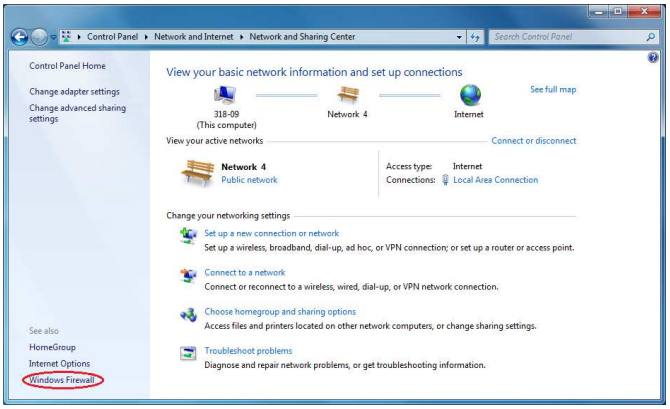
(2) Kliknite na opciju promjene postavki mrežnog adaptera (*Change Adapter Settings*). Omogućena treba ostati samo **lokalna žična konekcija** (*Local Area Connection*, LAN). Deaktivirajte sve ostale mrežne konekcije na računalima (za pojedina bežična, žična i virtualna sučelja) osim navedenih - odaberite desnom tipkom miša odgovarajuću konekciju i odaberite opciju za deaktiviranje (*Disable*).



Slika 4.2. *Prikaz postavki mrežnih konekcija (Network Connections) na računalu u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

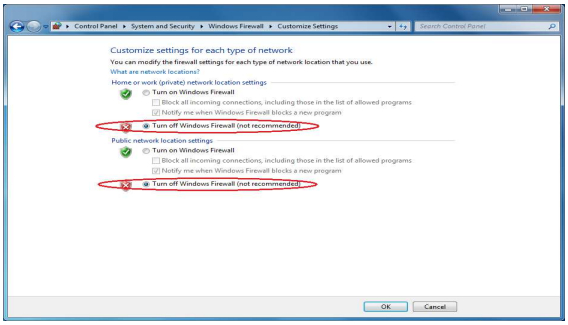
(B) ISKLJUČIVANJE VATROZIDA NA KLIJENTIMA

(3) Na računalu otvorite prozor upravljačke ploče (eng. *Control Panel*), zatim odaberite poveznicu vezanu uz postavke mreže i Interneta (*Network and Internet*), te zatim poveznicu vezanu uz opcije središta za umrežavanje i dijeljenje (*Network and Sharing Center*).



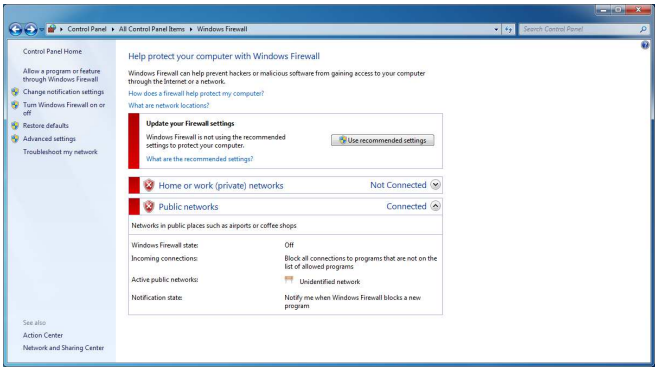
Slika 4.3. *Prikaz opcije za pristup postavkama Windows vatrozida (Windows Firewall) središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel)*

(4) Isključite vatrozid ukoliko je pokrenut na računalu prema sljedećem postupku. Odaberite poveznicu koja otvara prozor s postavkama središta za umrežavanje i dijeljenje (*Network and Sharing Center*), zatim otvorite prozor s postavkama vatrozida (*Windows Firewall*), odaberite izbornik za uključivanje i isključivanje vatrozida (*Turn Windows Firewall on or off*) i isključite vatrozid (*Turn off Windows Firewall*).



Slika 4.4. *Prilagođavanje postavki (Customize Settings) za isključivanje Windows vatrozida (Windows Firewall)*

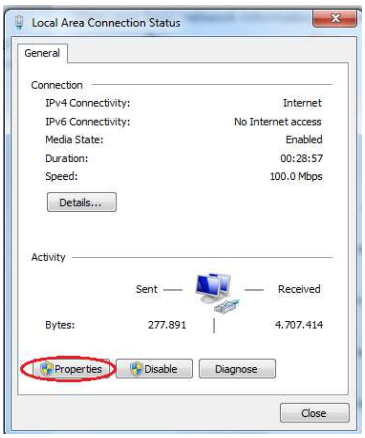
(5) Prikaz nakon deaktivacije vidljiv je na slici.



Slika 4.5. *Prikaz nakon deaktivacije Windows vatrozida*

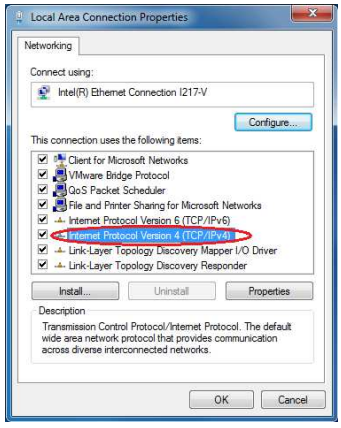
(C) DINAMIČKO ADRESIRANJE KLIJENATA

(6) U prozoru s opcijama središta za umrežavanje i dijeljenje (*Network and Sharing Center*) odaberite opciju promjene postavki mrežnog adaptera (*Change Adapter Settings*), zatim odaberite lokalnu mrežnu konekciju (*Local Area Connection*) i zatim njene postavke (*Properties*).



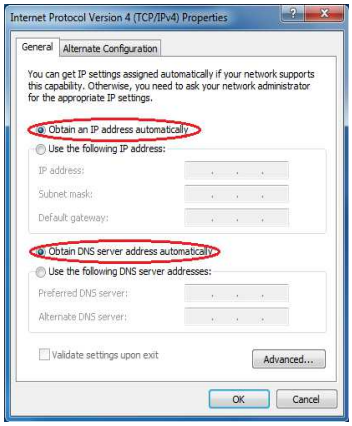
Slika 4.6. *Provjera postavki lokalne mreže (Local Area Connection Status) na računalu*

(7) Odaberite opciju prikaza postavki IPv4 protokola (*Internet Protocol Version 4 (TCP/IPv4)*).



Slika 4.7. *Provjera postavki lokalne konekcije (Local Area Connection Properties) na računalu*

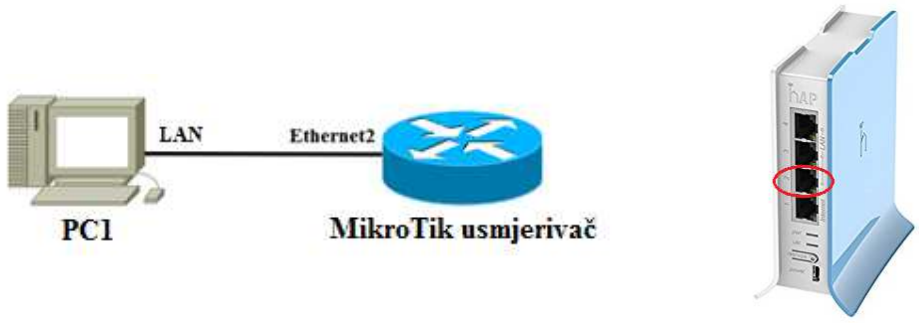
(8) Provjerite jesu li odabrane sljedeće opcije prema prikazu sa slike: automatska dodjela IP adrese (*Obtain an IP address automatically*) te automatska dodjela adrese DNS poslužitelja (*Obtain DNS server address automatically*), te ih odaberite ukoliko već nisu odabrane.



Slika 4.8. *Provjera postavki na računalu za automatsku dodjelu IPv4 adrese i adrese DNS servera*

(D) RESETIRANJE POSTAVKI USMJERIVAČA

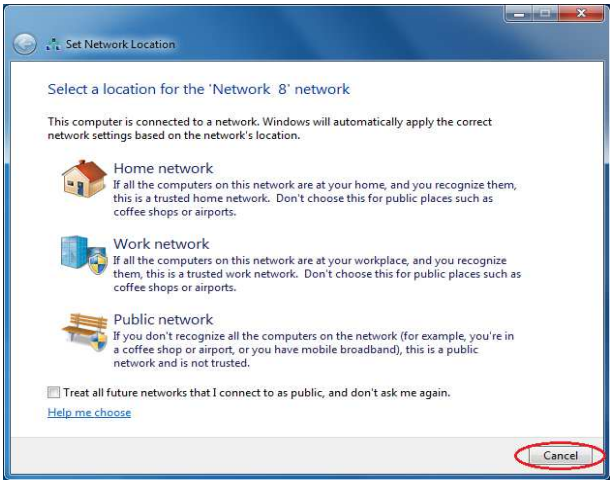
(9) Uključite usmjerivač. Povežite računalo PC1 na *Ethernet2* sučelje usmjerivača pomoću *patch* kabela, prema *shemi* na slici.



a) b)

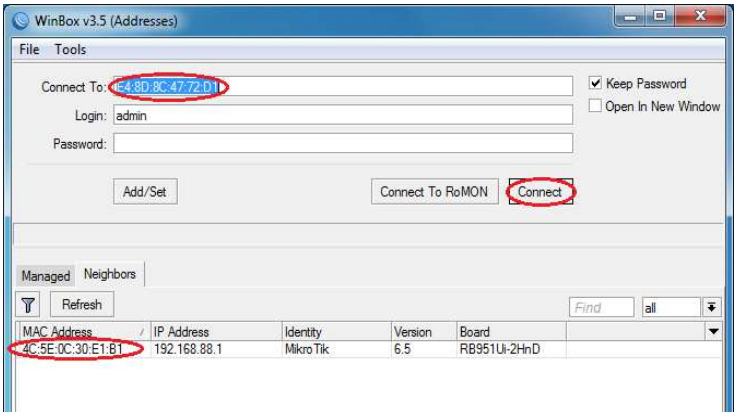
Slika 4.9. *a) Način povezivanja PC1 uređaja i MikroTik usmjerivača i b) MikroTik usmjerivač sa označenim Ethernet2 portom*

(10) Nakon što se otvori izbornik postavki lokacije mreže (*Set Network Location*) odaberite opciju izuzeća (*Cancel*).



Slika 4.10. *Izbornik postavki lokacije mreže* (*Set Network Location*)

(11) Pokrenite *WinBox* aplikaciju čija se ikona nalazi na radnoj ploči (*Desktop*) računala. Prvo označite MAC adresu (*MAC Address*) usmjerivača koja se nalazi na popisu u donjem dijelu prozora, a zatim kliknite na opciju za povezivanje (*Connect*).



Slika 4.11. *Sučelje WinBox aplikacije*

(12) Unutar otvorenog sučelja aplikacije *WinBox* odaberite opciju za otvaranje novog terminala (*New Terminal*). Otvara se terminal prikazan na donjoj slici.

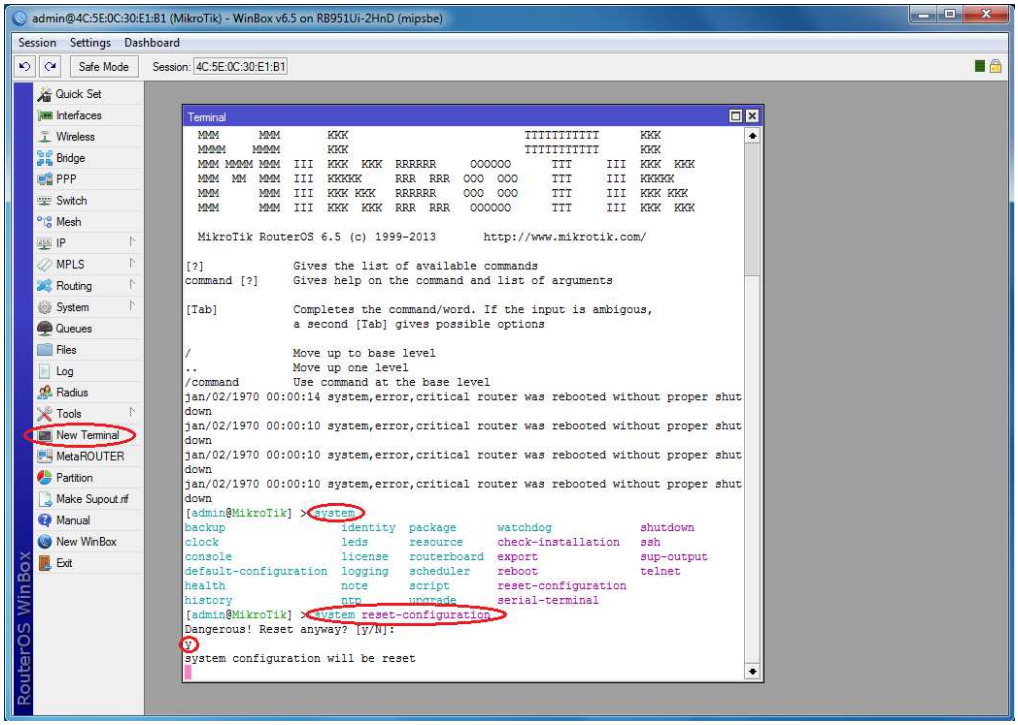
Resetirajte postavke na usmjerivaču upisivanjem naredbe:

system reset-configuration

i pomoću tipkovnice potvrdite upis odabirom tipke *Enter* te još jednom potvrdite izbor upisivanjem naredbe:

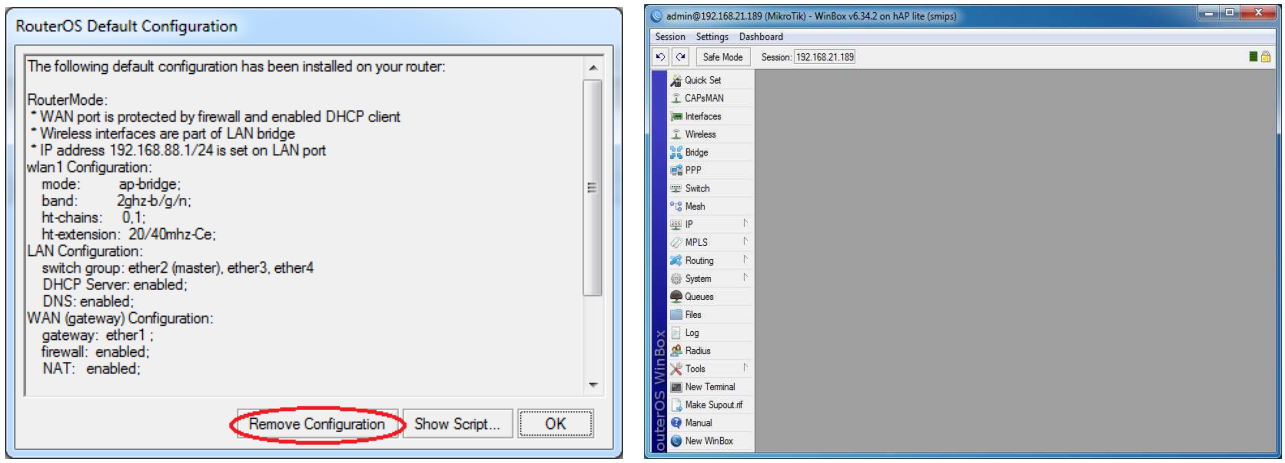
y

te odabirom tipke *Enter*. Ovime se pokreće resetiranje postojeće konfiguracije te se konfiguracija usmjerivača vraća na tvornički definiranu.



Slika 4.12. *Prikaz terminala WinBox aplikacije*

(13) Nakon ponovnog otvaranja *WinBox* aplikacije, potrebno je odabrati opciju brisanja konfiguracije (***Remove configuration***) kako bi postojeća tvornička konfiguracija bila u potpunosti obrisana (slika 4.13.).



a) b)

Slika 4.13. a) *Brisanje postojeće tvorničke konfiguracije uređaja i b) početno sučelje WinBox aplikacije*

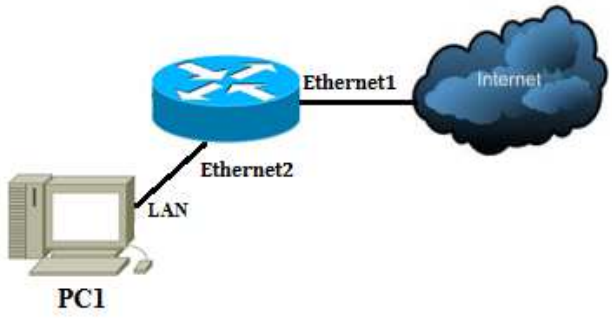
Zadaci:

U testnom scenariju potrebno je konfigurirati VPN. Potrebno je definirati osnovne postavke usmjerivača, načiniti PPTP konfiguraciju, konfigurirati postavke na klijentu te testirati kreirani VPN.

UPUTE ZA RAD:

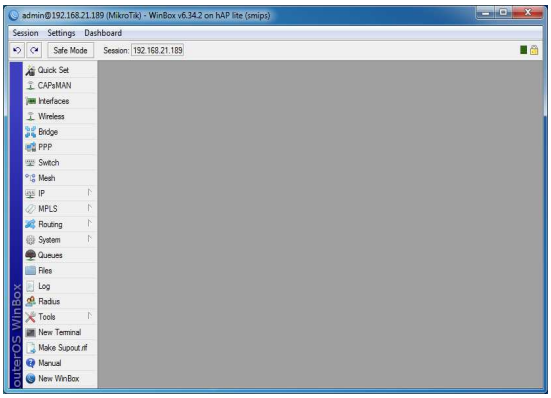
KREIRANJE TESTNE MREŽE

(14) U prvom koraku potrebno je kreirati topologiju prema prikazu sa slike 4.14.

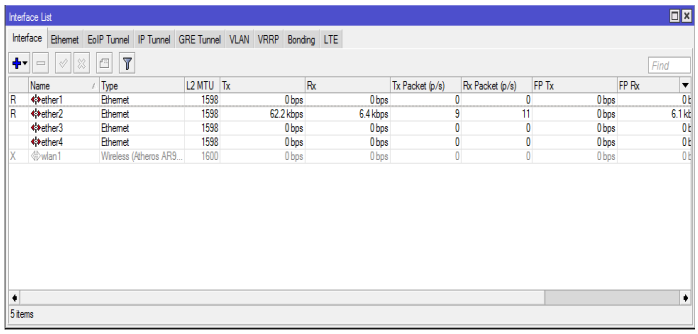


Slika 4.14. *Prikaz kreirane mrežne toplogije*

(15) Na slici se nalazi prikaz svih sučelja usmjerivača.



a)

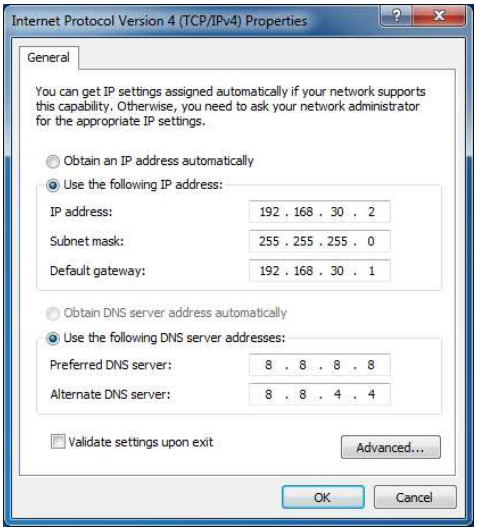


b)

Slika 4.15. a) *Početno sučelje WinBox aplikacije i b) prikaz svih aktivnih sučelja (Interfaces)*

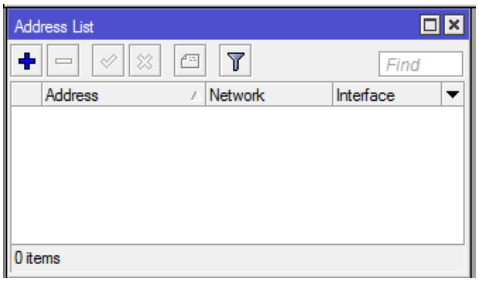
(I) ADRESIRANJE RAČUNALA I SUČELJA USMJERIVAČA

(16) Računalu je potrebno dodijeliti IP adresu 192.168.30.2/24. Prema prikazu sa slike 4.16., postavite adresu računala, adresu maske te pristupnika (*gateway*).



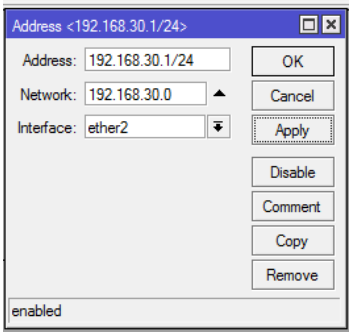
Slika 4.16. *Postavljanje IPv4 adrese računala (IP address), maske podmreže (Subnet mask) i predefiniranog pristupnika (Default gateway) te DNS adresa poslužitelja (DNS server addresses)*

(17) Sučelju *Ethernet2* potrebno je dodijeliti IP adresu. Iz izbornika tipa protokola (*IP*) potrebno je odabrati opciju za adresiranje (*Addresses*) te unutar izbornika s popisom adresa (*Address List*) kliknuti na oznaku '+'.



Slika 4.17. *Izbornik za dodavanje i prikaz popisa dodijeljenih IP adresa (Address List)*

(18) Dodijelite sučelju *Ethernet2* adresu 192.168.30.1/24 te postavite 192.168.30.0 za adresu mreže.



Slika 4.18. *Adresiranje aktivnog ethernet sučelja usmjerivača upisivanjem adrese sučelja (Address) i adrese mreže (Network)*

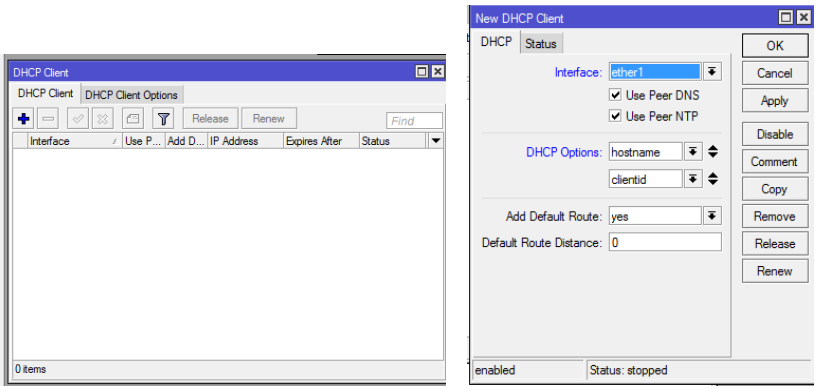
(II) KONFIGURIRANJE DHCP KLIJENTA NA USMJERIVAČU

(19) U nastavku je opisan osnovni postupak konfiguriranja DHCP klijenta na *Ethernet1* sučelju usmjerivača. Iz izbornika odaberite tip protokola (*IP*), zatim vrstu klijenta (*DHCP Client*) te opciju dodavanja novog klijenta (*Add New*).

(20) Postavke DHCP klijenta načinite prema slici:

- definirajte sučelje (*Interface*): *Ethernet1*
- definirajte sljedeće opcije (*DHCP Options*): ime hosta (*hostname*) te identifikator klijenta (*clientid*).

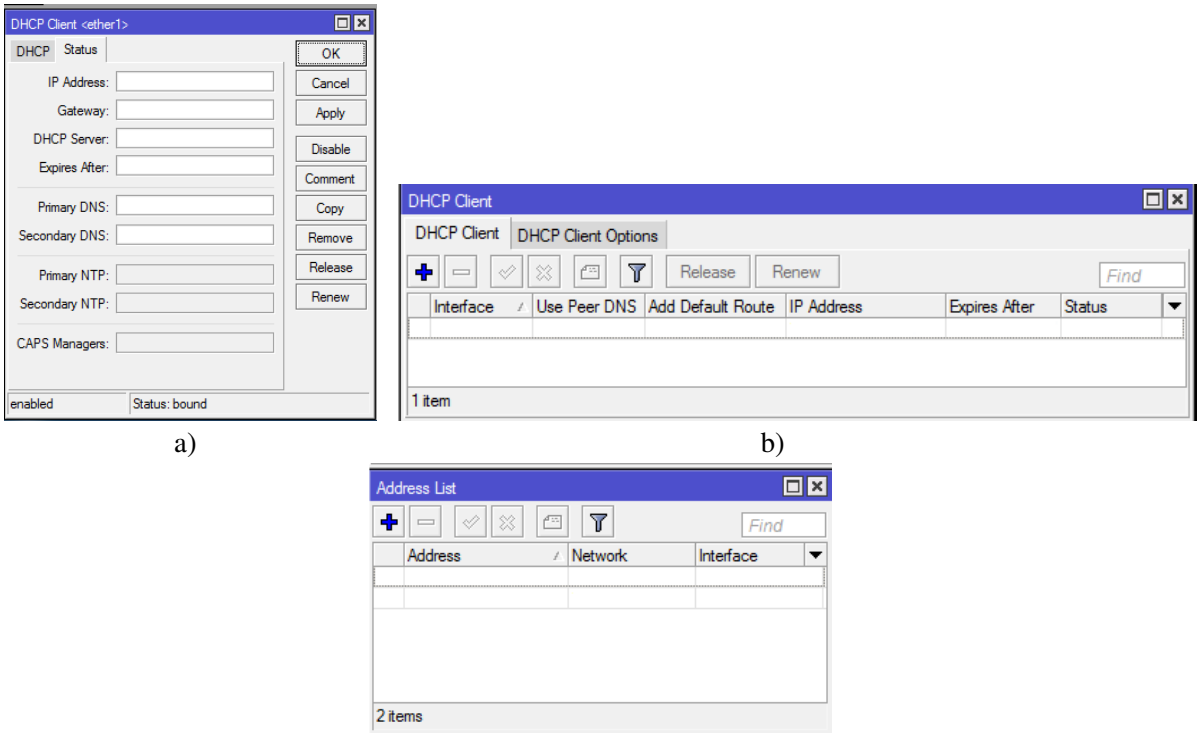
Potvrdite izbor (*OK*).



a) b)

Slika 4.19. a) *Prikaz izbornika DHCP klijenta (DHCP Client) i b) postavke novog DHCP klijenta (New DHCP Client)*

Zadatak 1. U predviđeni prostor na slikama upišite sve dodijeljene oznake i adrese.



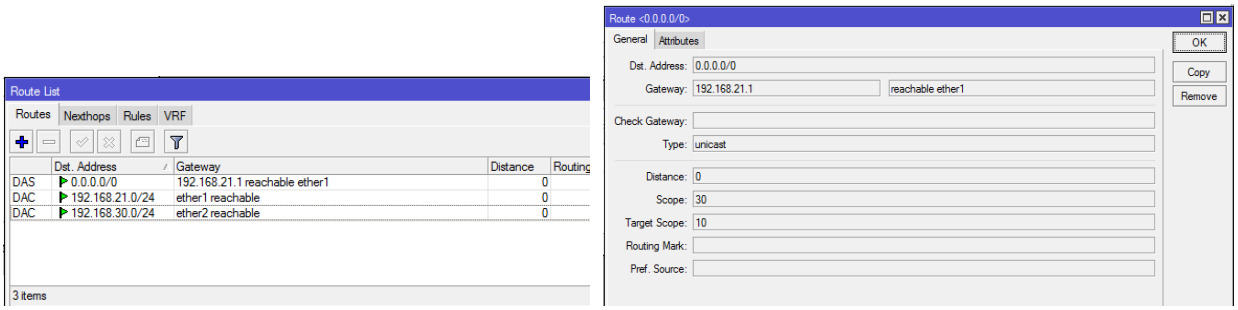
a) b)

c)

Slika 4.20. *a) Prikaz statusa (Status) adresa dodijeljenih kreiranom DHCP klijentu (DHCP Client), b) prikaz podataka o DHCP klijentu (DHCP Client) i c) popis adresa (Address List) aktivnih sučelja u mreži*

(III) KONFIGURIRANJE DODATNIH POSTAVKI NA USMJERIVAČU

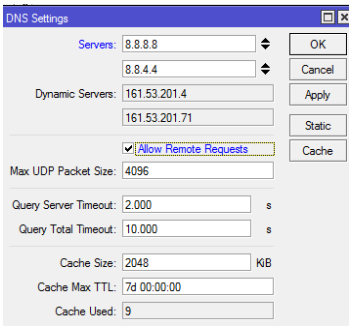
(21) Provjerite odgovara li sadržaj tablica usmjeravanja prikazu na slici 4.21.



a) b)

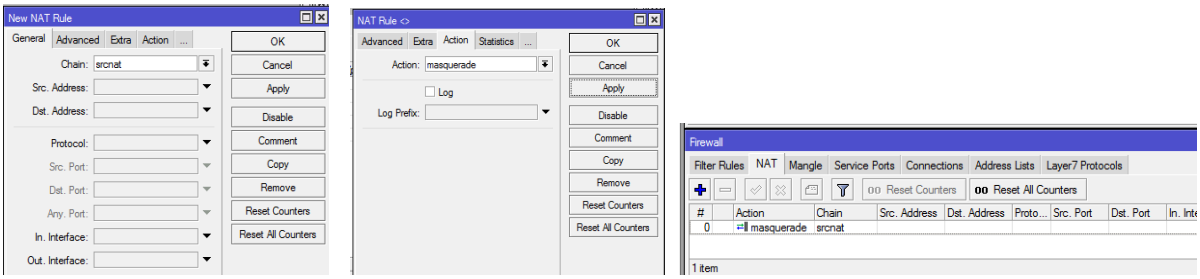
Slika 4.21. *a) Prikaz oznaka ruta (Route List) usmjerivača i b) sadržaj tablica usmjeravanja*

(22) U izbornik DNS postavki (*DNS Settings*) potrebno je unijeti oznake poslužitelja te označiti opciju za omogućavanje udaljenih zahtjeva (*Allow Remote Requests*).



Slika 4.22. *Prikaz DNS postavki* (*DNS Settings) poslužitelja*

(23) Za prevođenje IP adresa iz lokalnih u javne (NAT) potrebno je pokrenuti postupak maskiranja (*masquerade*) IP adresa. Iz izbornika tipa protokola (*IP*) potrebno je odabrati opciju vatrozid (*Firewall*) te karticu za prevođenje mrežnih adresa (*NAT*) i dodati novo pravilo (*Add*). Unutar kartice s općim postavkama (*General*) treba postaviti lanac (*Chain*) za prevođenje izvorne mrežne adrese (***srcnat***) i potvrditi (*Apply*). U idućem koraku unutar kartice aktivnosti (*Action*) odabrati opciju maskiranja (*masquerade*) i potvrditi (*OK*), čime započinje postupak prevođenja adresa.



a) b) c)

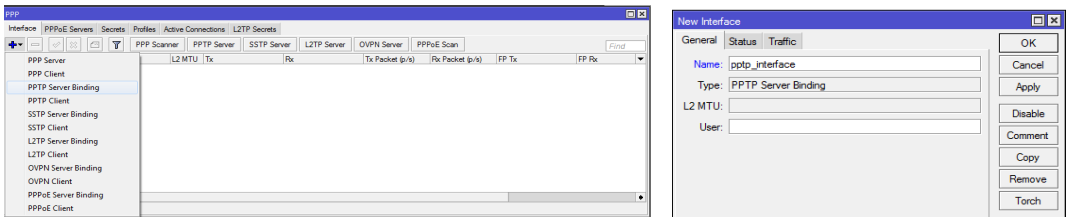
Slika 4.23. *a) Definiranje novog pravila za prevođenje IP adresa (New NAT Rule), b) opcija maskiranja (masquerade) adresa i c) prikaz zapisa o prevođenju IP adresa (NAT)*

Zadatak 2. Provjerite postoji li konekcija između računala i:

- sučelja *Ethernet2* usmjerivača: _____
- sučelja *Ethernet1* usmjerivača: _____

(IV) KONFIGURIRANJE PPTP POSLUŽITELJA NA USMJERIVAČU

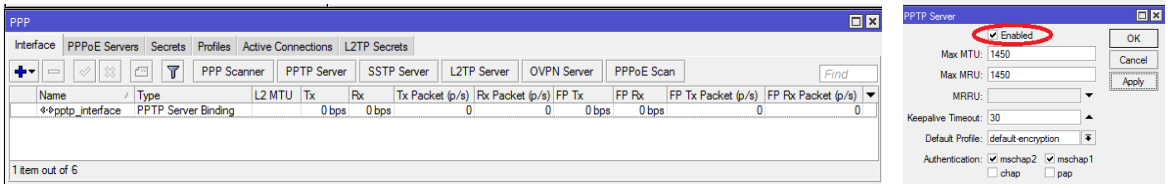
(24) Kroz sljedeće korake bit će prikazan postupak konfiguracije *PPTP* poslužitelja na usmjerivaču. Iz izbornika *PPP* odaberite opciju '+' te nakon toga PPTP povezivanje poslužitelja (*PPTP Server Binding*), prema prikazu sa slike 4.24. Naziv (*Name*) poslužitelja postavite na „*pptp_interface*“.



a) b)

Slika 4.24. *a) Definiranje postavki sučelja PPTP poslužitelja (PPTP Server Binding) i b) definiranje naziva (Name) poslužitelja*

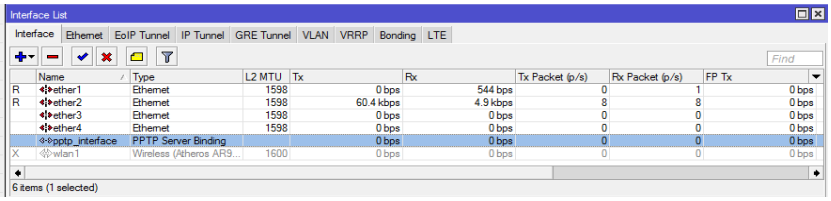
(25) Prikaz postavki kreiranog *PPTP* poslužitelja trebao bi odgovarati onom na slici 4.25. (označena opcija *Enabled*).



a) b)

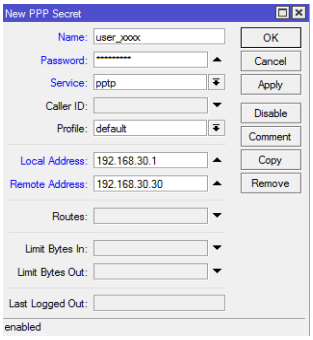
Slika 4.25. *a) Prikaz podataka o sučelju (Interface) kreiranog PPTP poslužitelja i b) aktiviranje PPTP poslužitelja (PPTP Server)*

(26) Novo kreirano *PPTP* sučelje (*pptp_interface*) trebalo bi biti navedeno na popisu uz sva ostala sučelja.



Slika 4.26. *Prikaz popisa aktivnih sučelja (Interface List) i označenog pptp sučelja*

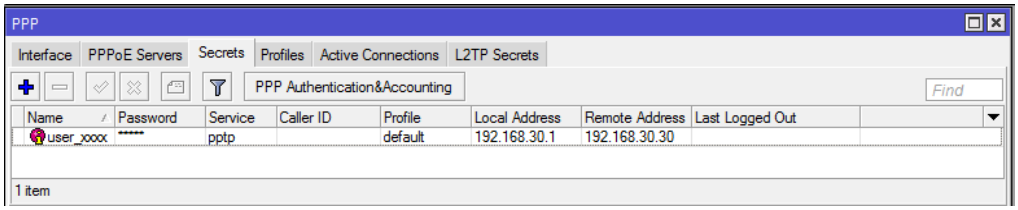
(27) Unutar izbornika *PPP* prikazanog na slici 4.25., odaberite karticu tajne (*Secrets*). Izbornik *PPP* tajna (*PPP Secret*) sadrži lokalnu bazu *PPP* korisnika i njihovih oznaka. U dodani izbornik upište postavke prema prikazu sa slike 4.27. Za naziv (*Name*): „*user_xxxx*“ te lozinku (*Password*): „*pass_xxxx*“ - umjesto oznaka „*xxxx*“ upišite vlastiti datum rođenja (dan i mjesec). Za uslugu (*Service*) postavite *pptp*, za lokanu adresu 192.168.30.1, a za adresu udaljenog (*Remote*) čvora 192.168.30.30.



Slika 4.27. *Prikaz postavki u izborniku PPP tajna (New PPP Secret)*

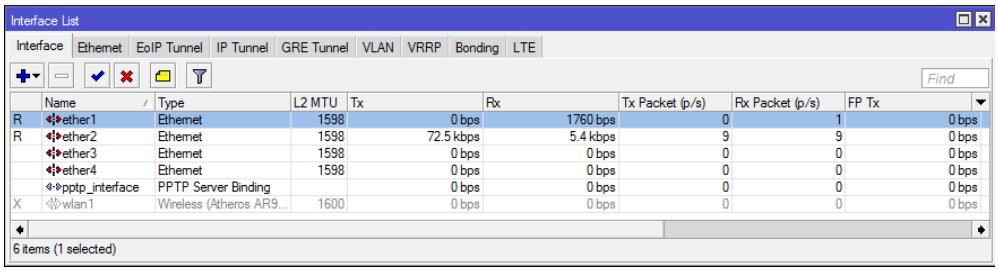
(V) KONFIGURIRANJE PROXY ARP-a

(28) Kroz sljedećih nekoliko koraka bit će prikazan postupak konfiguracije zamjenske ARP (*proxy arp*) funkcije na usmjerivaču, odnosno tehnike kojom se usmjerivač javlja na ARP zahtjeve koji su namijenjeni nekom drugom uređaju u mreži te preuzima zadaću daljnjeg usmjerivanja tih paketa kroz mrežu. Primjena ove funkcije je prikladna u slučaju povezivanja dviju mreža preko serijskog sučelja, višestrukog adresiranja unutar određene lokane mreže te pri filtriranju prometa.



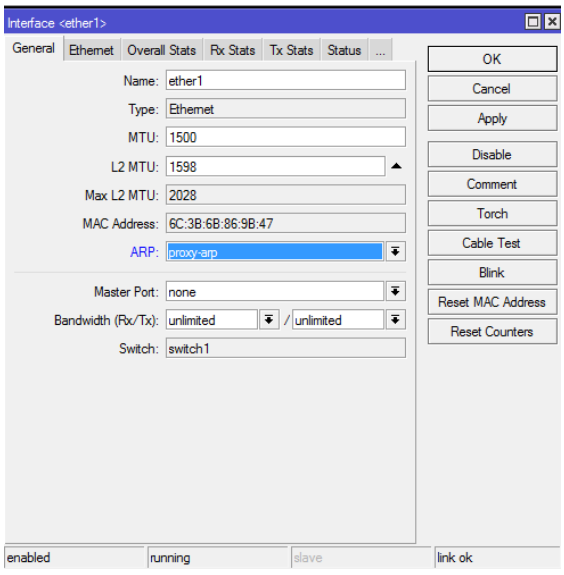
Slika 4.28. *Prikaz sadržaja kartice tajne (Secrets) u izborniku PPP*

(29) Unutar izbornika s popisom sučelja (*Interface List*) selektirajte *Ethernet1* sučelje usmjerivača.



Slika 4.29. *Prikaz popisa svih aktivnih sučelja (Interface List)*

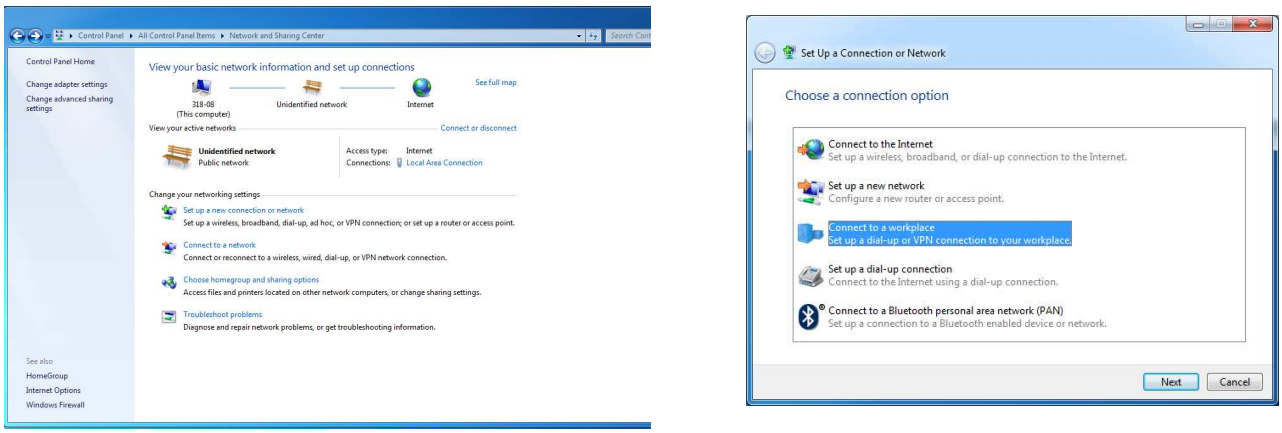
(30) Unutar izbornika za definiranje postavki *Ethernet1* sučelja odaberite opciju zamjenski ARP (*proxy arp*).



Slika 4.30. *Izbor postavki zamjenskog ARP (proxy arp) poslužitelja na Ethernet1 sučelju (Interface) usmjerivača*

(VI) KONFIGURIRANJE VPN KLIJENTA

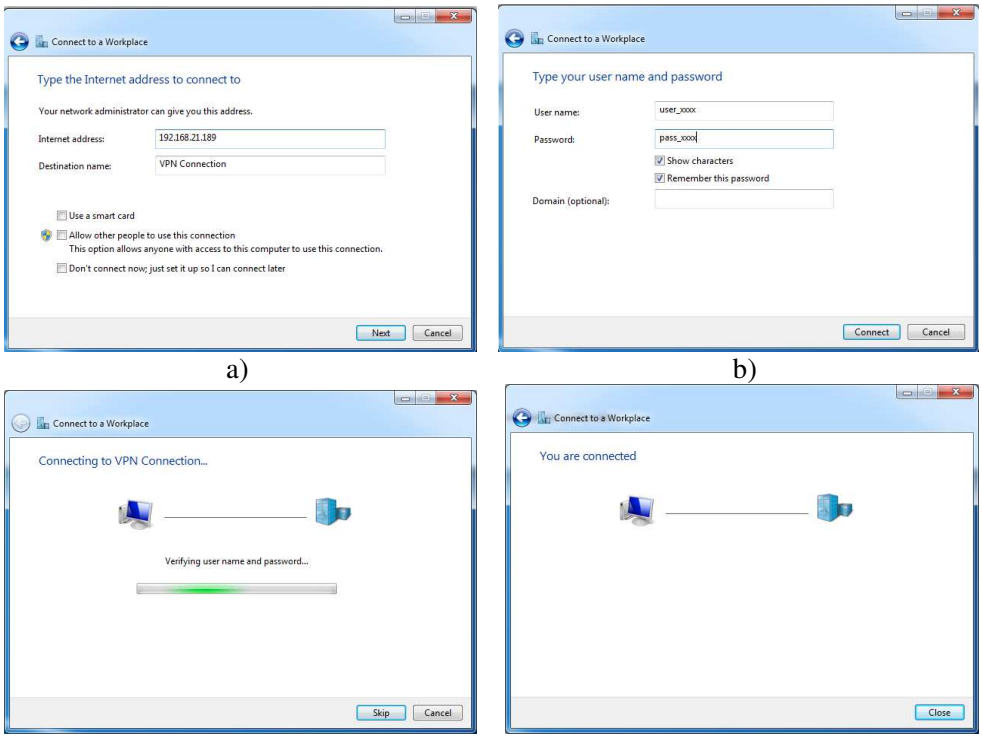
(31) Kroz sljedeće korake bit će prikazan postupak konfiguracije VPN klijenta. Na računalu otvorite prozor upravljačke ploče (*Control Panel*), zatim opcije umrežavanja i dijeljenja (*Network and sharing options*) te odaberite opciju kreiranja nove konekcije ili mreže (*Set up a new connection or network*) prema prikazu sa slike 4.31.



a) b)

Slika 4.31 *a) Prikaz središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel) i b) izbor opcije za postavljanje konekcije ili mreže (Set Up a Connection or Network)*

(32) Kroz sljedećih nekoliko koraka prikazan je postupak konfiguracije postavki na klijentu - postavke IP adrese, vrste konekcije, korisničkog imena i lozinke.



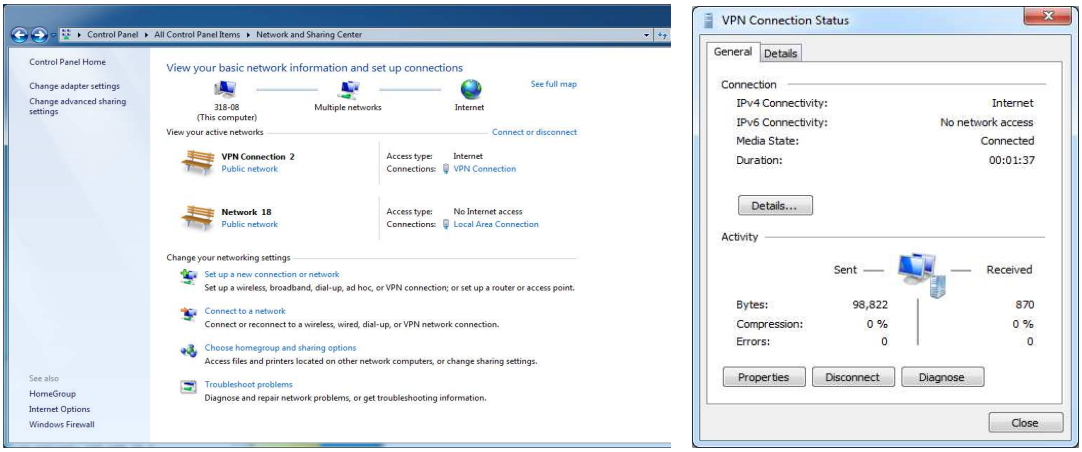
a) b)

b) d)

Slika 4.32. *Konfiguracija postavki na klijentu: a) postavke IP adrese i vrste konekcije, b) postavke korisničkog imena i lozinke, c) povezivanje na VPN mrežu i d) potvrda o povezanosti*

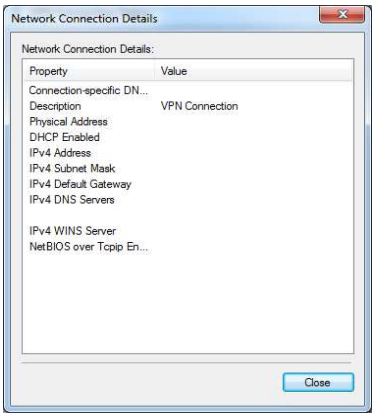
(VII) TESTIRANJE VPN KONEKCIJE

(33) U prozoru *upravljačke ploče* (*Control Panel*) odaberite oznaku VPN konekcije (*VPN Connection*).



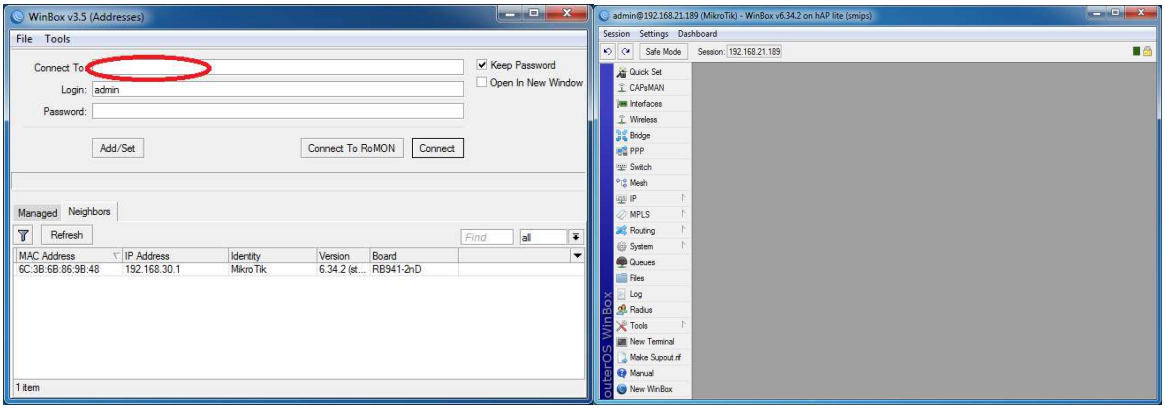
Slika 4.33. *a) Prikaz središta za umrežavanje i dijeljenje (Network and Sharing Center) u izborniku s postavkama mreže i Interneta (Network and Internet) prozora upravljačke ploče (Control Panel) i b) Prikaz s detaljima o uspostavljenoj VPN konekciji*

Zadatak 3. U izbornik na slici upišite oznake dodijeljene klijentu:



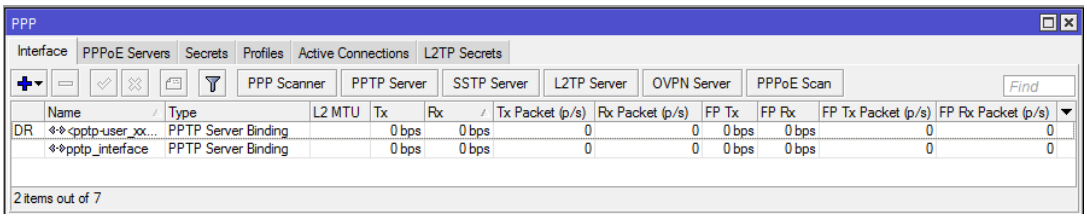
Slika 4.34. *Prikaz oznaka dodijeljenih klijentu*

(34) Otvorite izbornik za pokretanje *WinBox* aplikacije (*Winbox Loader*) i upišite IP adrese DHCP klijenta navedene na slici 4.35.

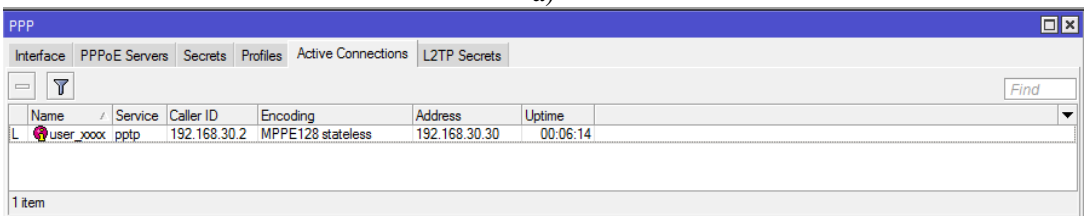


Slika 4.35. *Pokretanje Winbox aplikacije i b) početno sučelje WinBox aplikacije*

(35) Unutar izbornika *PPP* provjerite je li prikazana oznaka aktivne VPN konekcije.



a)



b)

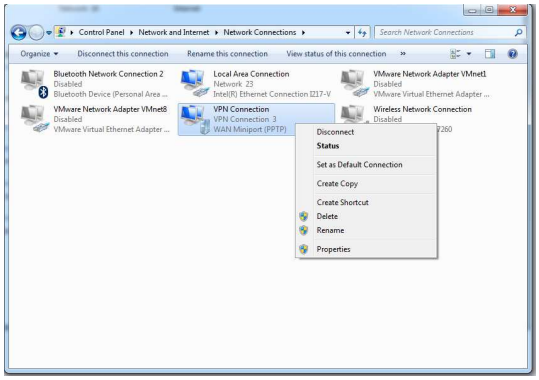
Slika 4.36. *a) Prikaz podataka o sučelju (Interface) kreiranih PPTP poslužitelja i b) prikaz sadržaja kartice s prikazom aktivnih konekcija (Active Connections) u izborniku PPP*

Zadatak 4. Provjerite:

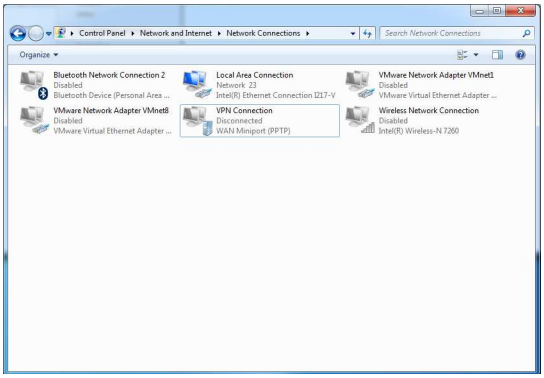
- IP adresu dodijeljenu klijentu: _____ /___
- IP adresu zadanog pristupnika (*default gateway*): _____
- postoji li konekcija između klijenta i sučelja *Ethernet1* usmjerivača (192.168.30.1): _____

(VIII) BRISANJE VPN POSTAVKI

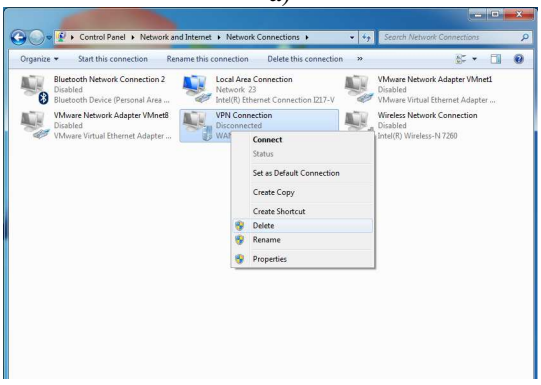
(36) Prema koracima prikazanim na slikama obrišite kreiranu VPN konekciju.



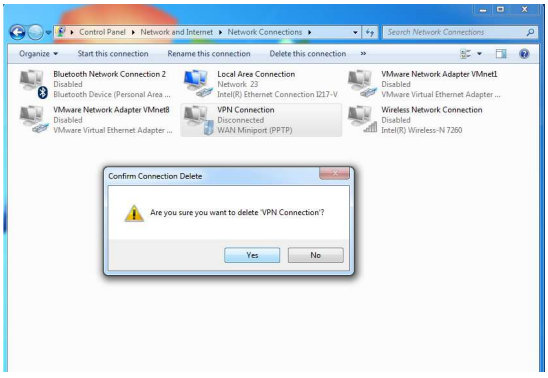
a)



b)



b)



d)

Slika 4.37. *a) Odabir opcije za raskid (Disconnect) VPN konekcije, b) prikaz ikone raskinute VPN konekcije, c) odabir opcije za brisanje (Delete) VPN konekcije i d) potvrđivanje brisanja VPN konekcije*

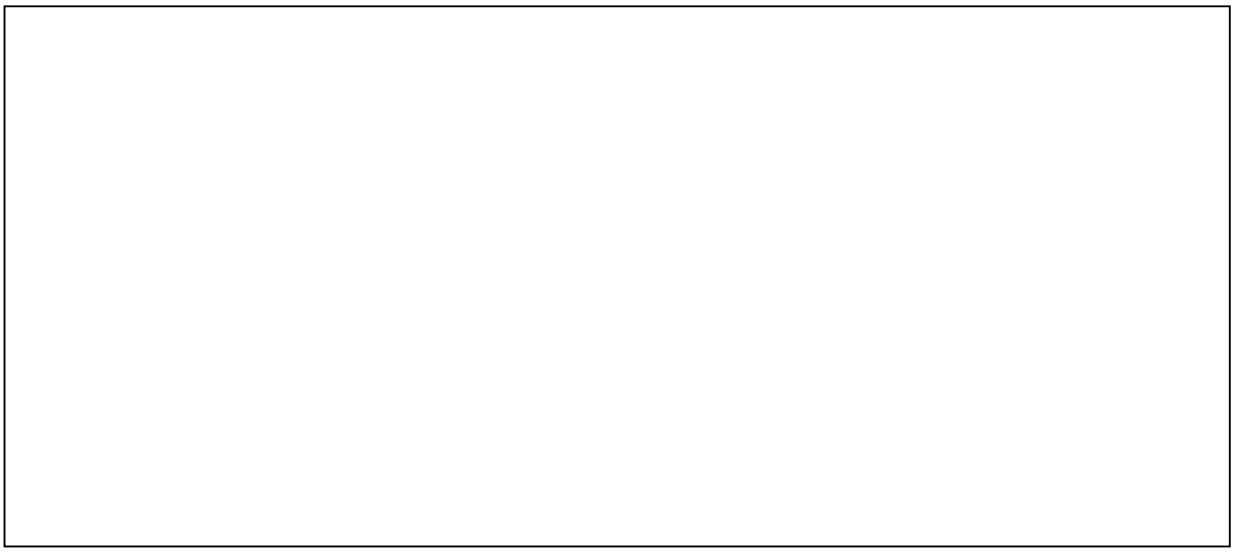
Vježba 5. - Simetrični kriptosustavi

Simetrični kriptosustavi se zasnivaju na činjenici da se isti ključ koristi i za kriptiranje i za dekriptiranje poruke. Ovakav oblik komunikacije kriptiranim porukama se odvija između dva sudionika, koji prethodno sigurno moraju razmijeniti ključ. Najveći problem simetričnog kriptiranja je upravo razmjena ključeva i kako je sigurno ostvariti.

Simetrični algoritmi se mogu podijeliti u dvije skupine. U jednu skupinu se ubrajaju algoritmi u kojima se kriptiraju blokovi podataka, a u drugu algoritmi u kojima se kriptira tok podataka. Kod kriptiranja blokova podataka algoritam uzima određeni blok podataka i prvo njega kriptira, zatim uzima slijedeći blok, pa kriptira i taj blok i tako cijelu poruku. Kod algoritama koji kriptiraju tok podataka kriptira se bit po bit teksta.

Zadatak 1. *DES (Data Encryption Standard)*

- U aplikaciji *CrypTool* realizirati sustav za šifriranje i dešifriranje pomoću DES kriptosustava.
- Šifrirati svoje ime i prezime (npr. „PETARPETROVIC“), uz proizvoljno izabrani ključ.
- Ucrtati kreirani sustav, zajedno sa pripadajućim ulazom i izlazom:



- Pomoću DES kriptosustava šifrirati sljedeće pojmove, uz proizvoljno izabrani ključ (ključ i šifrat upisati u heksadekadskom obliku):
    - SIGURNOSTRACUNALNIHSUSTAVA (ključ: _____)

      _____
    - KLASICNAKRIPTOGRAFIJA (ključ: _____)

      _____
    - ELEKTROTEHNICKIFAKULTET (ključ: _____)

      _____

- Dešifrirati sljedeće šifrate, ako se zna da su šifrirani pomoću DES kriptosustava, uz ključ 0x1234567890ABCDEF:
    - 8F 9A 68 A2 E8 E2 C3 7D 83 5A C7 E0 57 24 FC AE B0 F6 BC 5F 65 39 1C 3B:

      _____
    - 10 50 39 C6 0A 9A 10 33 BC CB B1 04 7E B7 71 0E:

      _____
    - F6 25 0B C0 6F 42 81 0A 90 C1 B1 A6 48 F9 27 8A:

      _____
    - E1 43 55 2A 91 F9 34 9E 48 7A B5 65 F7 7A D1 B1 BE 70 3F D6 97 D8 03 6E:

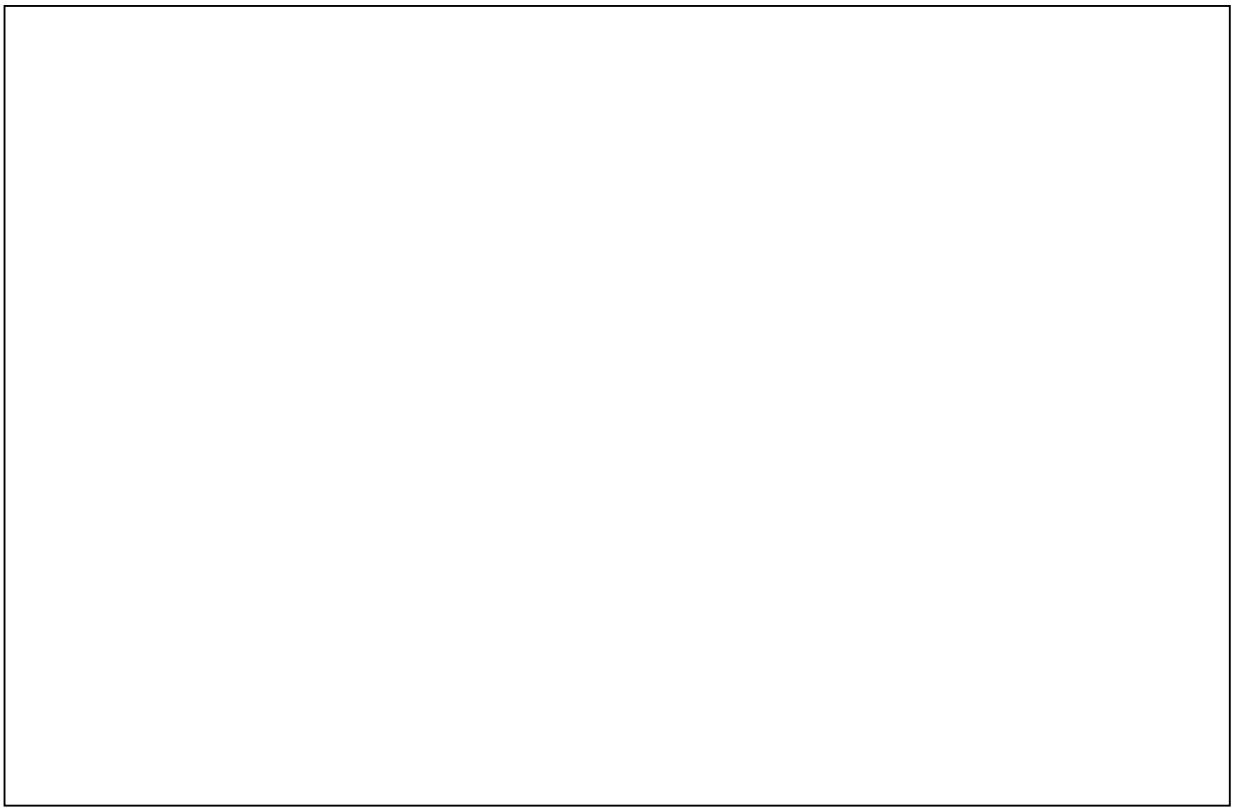
      _____

- Objasnite sličnosti i razlike u pojedinim modusima rada DES kriptosustava:

Zadatak 2. *AES (Advanced Encryption Standard)*

- U aplikaciji *CrypTool* realizirati sustav za šifriranje i dešifriranje pomoću AES-128 kriptosustava.
- Šifrirati svoje ime i prezime (npr. „PETARPETROVIC“), uz proizvoljno izabrani ključ.

- Ucrtati kreirani sustav, zajedno sa pripadajućim ulazom i izlazom:



- Pomoću AES-128 kriptosustava šifrirati sljedeće pojmove, uz proizvoljno izabrani ključ (ključ i šifrat upisati u heksadekadskom obliku):
  - NAPREDNOSIFRIRANJE (ključ: _____)

    _____
  - TEKSTZAENKRIPCIJU (ključ: _____)

    _____
  - SVEUCILISTEUOSIJEKU (ključ: _____)

    _____

- Dešifrirati sljedeće šifrate, ako se zna da su šifrirani pomoću AES-128 kriptosustava, uz ključ 0x11223344556677889900AABBCCDDEEFF:
  - 8D 19 3D 2F 35 1A C0 9E 5D E3 88 95 73 27 83 E2 01 34 42 06 47 34 AF 0B C4 6D 1E 58 42 1E 6E 89:

    _____

- 96 61 11 EA 62 3A B8 41 99 EE 20 76 EA B2 F1 2E 60 A6 10 F8 C1 9E 8A 7A D1 6F EC F6 21 F1 02 9C:

  _____

- D0 13 03 EB B4 69 F6 7E 8D 0F 50 ED 48 0B 81 37 91 2C 55 13 9E 84 48 BC 86 A0 B1 66 76 F5 77 5D:

  _____

- 7E C4 F1 A1 E7 65 E2 02 83 EC 1B 0D 5F E4 5B D0 FD 53 E4 34 6F 15 D2 2C 97 97 AC 84 36 4C C8 78:

  _____

- Objasnite sličnosti i razlike između DES i AES kriptosustava:

Vježba 6. - Simetrični kriptosustavi: DES (*Data Encryption Standard*) i trostruki DES (*Triple* DES)

UVOD

DES (*Data Encryption Standard*)

Jedan od najpoznatijih **standardnih algoritama** u području **simetrične kriptografije tajnog ključa**. Pri šifriranju (eng. *encryption*), DES algoritam koristi blokove otvorenog teksta duljine 64 bita, i ključ (eng. *key*) duljine 56 bita, a proizvodi blokove šifrata (eng. *ciphertext*) duljine 64 bita.

Pri dešifriranju (eng. *decryption*), DES algoritam koristi blokove šifrata duljine 64 bita, i ključ duljine 56 bita, a proizvodi blokove otvorenog teksta duljine 64 bita. Isti 56-bitni ključ koristi se i za šifriranje i za dešifriranje.

Postupak šifriranja sastoji se od **dvije permutacije** (P-blokovi) koje se nazivaju **inicijalna i finalna** permutacija te **šesnaest Feistel rundi**. Svaka runda koristi drugačiji 48-bitni ključ generiran na temelju kriptografskog ključa (eng. *cipher key*) prema predefiniranom algoritmu.

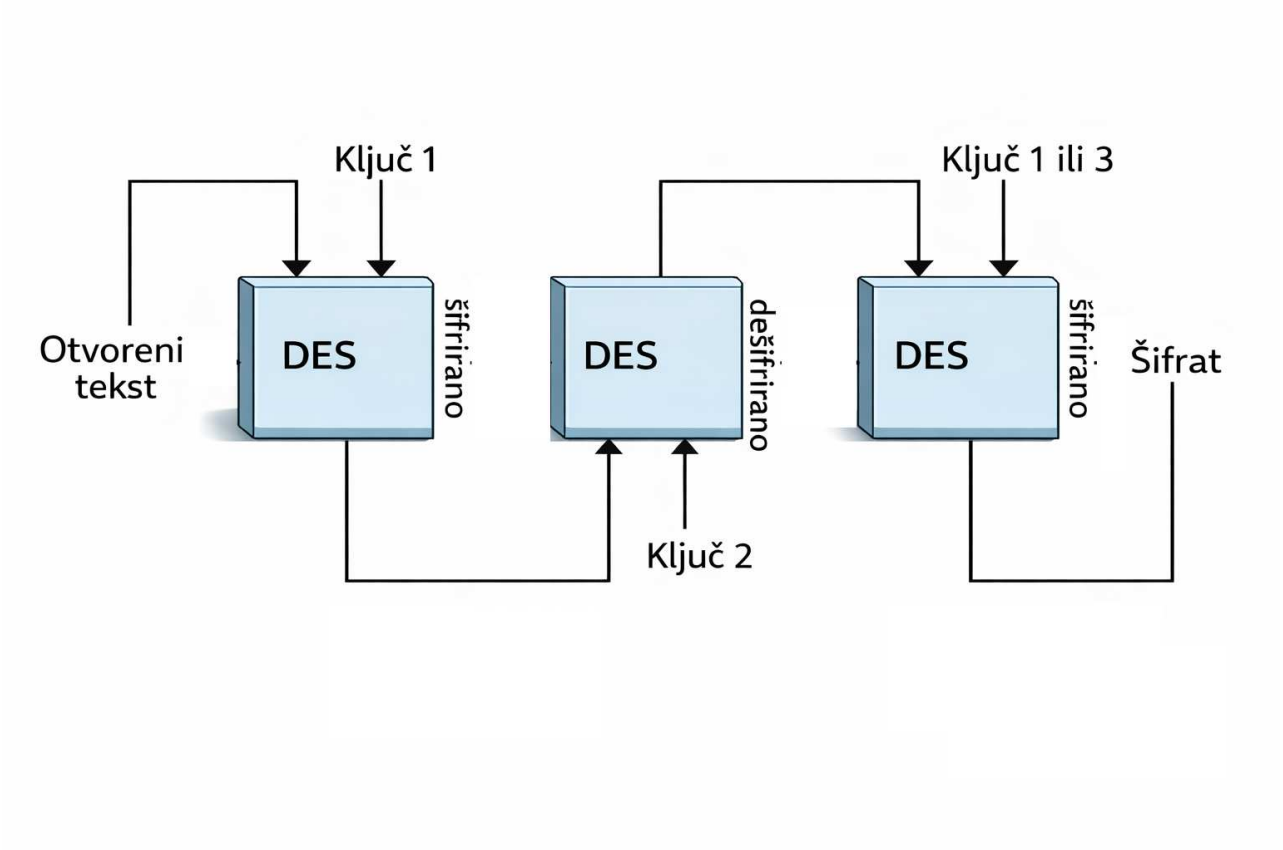
Algoritmi za šifriranje i dešifriranje:

- Pri postupku šifriranja lijevi odjeljak otvorenog teksta, L_0, šifrira se kao L_{16}.
- Pri postupku dešifriranja L_{16} se dešifrira kao L_0.
- Isto vrijedi i za R_0 i R_{16}.
- Ključeve runde (K_1 do K_{16}) potrebno je primijeniti obrnutim redoslijedom.
- Pri postupku šifriranja, runda 1 koristi K_1, a runda 16 koristi K_{16}
- Pri postupku dešifriranja, runda 1 koristu K_{16}, a runda 16 koristi K_1.

Trostruki DES (*Triple Data Encryption Standard*, 3DES)

DES algoritam je osjetljiv na napad grubom silom (eng. *brute force attack*), pa se većinom umjesto njega koriste snažnije kriptografske sheme. Budući da skup svih permutacija DES-a nije zatvoren, DES ne čini grupu.

Ovo svojstvo je važno, jer zahvaljujući tome vrijedi da se višestrukom uporabom DES-a može postići veća razina sigurnosti. Ako bi DES činio grupu, višestruki DES ne bi bio nimalo sigurniji od običnog DES-a.



Slika 6.1. *Postupak šifriranja otvorenog teksta pomoću Triple DES algoritma*

Uz DES je stoga u primjeni više inačica višestrukog DES algoritma – dvostruki DES i trostruki DES, i to inačice sa različitim brojem ključeva.

U slučaju napada grubom silom potrebo je voditi računa o sljedećem:

- dvostruki DES: nije puno bolji od jednostrukog DES-a
- trostruki DES sa 2 ključa: 2^{112} mogućih kombinacija
- trostruki DES sa 3 ključa: 2^{168} mogućih kombinacija.

Stoga je najčešća zamjena za obični DES trostruki DES s tri ključa. Njegova sigurnost je za današnje pojmove i više nego zadovoljavajuća.

Za navedenu inačicu karakteristično je sljedeće:

• ključ je duljine 168 bitova (56 x 3=168)

• koriste se tri različita ključa (K, L, M)

• podatkovni blok se najprije šifrira pomoću ključa K, potom se dobiveni blok dešifrira pomoću ključa L, i konačno se dobiveni blok šifrira ključem M

• prilikom dešifriranja postupak je obrnut - blok šifrata se dešifrira ključem M, potom šifrira ključem Li konačno dešifrira ključem K

Razlog zbog kojeg se primjenjuje postupak enkripcija-dekripcija-enkripcija je vezan uz očuvanje kompatibilnosti sa običnim DES-om (ukoliko se uzme da je L=M ili K=L 3DES se svodi na obični DES).

ZADACI

Uvodne upute:

U svrhu analize DES kriptografskih sustava u vježbi je potrebno koristiti aplikaciju *CrypTool*, alat namijenjen proučavanju različitih klasičnih, simetričnih, asimetričnih kriptografskih sustava i metoda njihove kriptoanalize.

DES *(Data Encryption Standard)*

Zadatak 1. Aplikacija *CrypTool* omogućuje analizu sljedećih načina rada DES blokovnih šifri: elektronička bilježnica (eng. *electronic codebook*, skr. ECB) i ulančavanje šifriranih blokova (eng. *cipher-block chaining*, skr. CBC). Grafički prikažite sheme koje opisuju postupak šifriranja za navedene načine rada.

DES (ECB):	DES (CBC):

Zadatak 2. Pomoću **DES (ECB)** i **DES (CBC)** algoritama potrebno je šifrirati vlastito ime i prezime (otvoreni tekst), uz zadani ključ: 0x1122334455667788. Dobivene kriptograme potrebno je upisati u heksadekadskom obliku.

Otvoreni tekst: _____

a) DES (ECB) - Dobiveni kriptogram:_____

b) DES (CBC) - Dobiveni kriptogram:_____

Zadatak 3. Pomoću **DES (ECB)** te **DES (CBC)** algoritama potrebno je šifrirati zadani pojam (otvoreni tekst), uz isti proizvoljni ključ. Odabrani ključ i dobivene kriptograme potrebno je upisati u heksadekadskom obliku.

Odabrani ključ: _____

Otvoreni tekst: SIGURNOSTINFORMACIJSKIHSUSTAVA

a) DES (ECB) - Dobiveni kriptogram:_____

b) DES (CBC) - Dobiveni kriptogram:_____

Zadatak 4. Objasnite sličnosti i razlike između ECB i CBC načina rada blokovnih šifri.

Zadatak 5. Uz primjenu DES (ECB) algoritma:

A) Šifrirajte navedeni otvoreni tekst ako je zadani ključ: 0x1234567890ABCDEF

Otvoreni tekst: SIFRIRANJEIDESIFRIRANJE

DES (ECB) - Dobiveni kriptogram:_____

B) Pokušajte dešifrirati tako dobiveni kriptogram primjenom opcije analiziranja (*Analysis*) uz unos djelomično poznatog ključa (pri čemu oznaka „*“ predstavlja nepoznatu vrijednost) te navedite koliko je vremena potrebno za dovršetak postupka dešifriranja u svakom pojedinom slučaju:

Ključ:	Potrebno vrijeme:
0x12345678********	_____
0x1234**********	_____
0x**********	_____

Zadatak 6. Uz primjenu DES (CBC) algoritma:

A) Šifrirajte navedeni otvoreni tekst ako je zadani ključ: 0x1234567890ABCDEF

Otvoreni tekst: SIFRIRANJEIDESIFRIRANJE

DES (CBC) - Dobiveni kriptogram:_____

B) Pokušajte dešifrirati tako dobiveni kriptogram primjenom opcije analiziranja (*Analysis*) uz unos djelomično poznatog ključa (pri čemu oznaka „*“ predstavlja nepoznatu vrijednost) te navedite koliko je vremena potrebno za dovršetak postupka dešifriranja u svakom pojedinom slučaju:

Ključ:	Potrebno vrijeme:
0x12345678********	_____
0x1234**********	_____
0x**********	_____

Zadatak 7. Usporedite potrebno vrijeme za dešifriranje kriptograma pri primjeni različitih DES načina rada – DES (ECB) te DES (CBC):

_____

_____

Triple DES *(Triple Data Encryption Standard)*

Zadatak 8. Uz primjenu Triple DES (ECB) algoritma:

A) Šifrirajte navedeni otvoreni tekst ako je zadani ključ: 0x1234567890ABCDEF0000000000000000

Otvoreni tekst: SIFRIRANJEIDESIFRIRANJE

Triple DES (ECB) - Dobiveni kriptogram:_____

B) Pokušajte dešifrirati tako dobiveni kriptogram primjenom opcije analiziranja (*Analysis*) uz unos djelomično poznatog ključa (pri čemu oznaka „*“ predstavlja nepoznatu vrijednost) te navedite koliko je vremena potrebno za dovršetak postupka dešifriranja u svakom pojedinom slučaju:

Ključ:	Potrebno vrijeme:
0x1234567890ABCDEF**********	_____
0x12345678**********	_____
0x**********	_____

Zadatak 9. Uz primjenu Triple DES (CBC) algoritma:

A) Šifrirajte navedeni otvoreni tekst ako je zadani ključ: 0x12345678000000000000000000000000

Otvoreni tekst: SIFRIRANJEIDESIFRIRANJE

Triple DES (CBC) - Dobiveni kriptogram:_____

B) Pokušajte dešifrirati tako dobiveni kriptogram primjenom opcije analiziranja (*Analysis*) uz unos djelomično poznatog ključa (pri čemu oznaka „*“ predstavlja nepoznatu vrijednost) te navedite koliko je vremena potrebno za dovršetak postupka dešifriranja u svakom pojedinom slučaju:

Ključ:	Potrebno vrijeme:
0x1234567890ABCDEF**********	_____
0x12345678**********	_____
0x**********	_____

Zadatak 10. Usporedite potrebno vrijeme za dešifriranje kriptograma pri primjeni različitih Triple DES načina rada – DES (ECB) te DES (CBC):

_____

_____

Zadatak 11. Usporedite potrebno vrijeme za dešifriranje kriptograma pomoću DES i Triple DES pri primjeni različitih načina rada:

a) pri primjeni ECB - _____

b) pri primjeni CBC -_____

Vježba 7. - Simetrični kriptosustavi: AES (*Advanced Encryption Standard*)

UVOD

Budući da je DES algoritam osjetljiv na napad grubom silom, umjesto njega koriste se druge kriptografske sheme, a jedna od njih je Triple DES algoritam.

Alternativni prstup predstavlja primjena AES algoritma. AES je potpuno drugačiji algoritam. Otporan je na kriptoanalizu i napad grubom silom.

AES parametri

AES podatkovni blok naziva se **stanjem** (eng. *state*). AES koristi blokove sljedećih duljina:

Tablica 7.1. *Prikaz i usporedba AES parametara*

Veličina ključa (riječi/bajtovi/bitovi)	**4 / 16 / 128**	**6 / 24 / 192**	**8 / 32 / 256**
Veličina bloka otvorenog teksta (riječi/bajtovi/bitovi)	4 / 16 / 128	4 / 16 / 128	4 / 16 / 128
Broj rundi	10	12	14
Veličina ključa po rundi (riječi/bajtovi/bitovi)	4 / 16 / 128	4 / 16 / 128	4 / 16 / 128
Proširena veličina ključa (riječi/bajtovi)	44 / 176	52 / 208	60 / 240

AES funkcije

Pri šifriranju AES koristi sljedeće četiri funkcije:

- zamjenu (supstituciju) bajtova - *SubBytes*
- pomak redova - *ShiftRows*
- miješanje stupaca - *MixColumns*
- dodavanje ključa runde - *AddRoundKey*.

- Samo stanje *Add Key* koristi ključ.
- Ostala tri stanja - *Shift Row*, *Mix Column* i *Nibble Substitution*, zasnivaju se na razmještanju i zamjeni (tj. na difuziji i konfuziji) bajtova te sami po sebi ne doprinose povećanju sigurnosti.
- Sve operacije koje se provode pri šifriranju su reverzibilne zbog dešifriranja.

Algoritmi za šifriranje i dešifriranje:

- Algoritmi za šifriranje i dešifriranje nisu identični
- Finalna runda ima samo tri operacije, pa je algoritam reverzibilan
- S-blok se često koristi pri postupcima šifriranja u simetričnim kriptosustavima. Kod AES-a je svih 16 S-blokova u svakoj rundi je potpuno identično.

Obilježja dizajna S-blokova:

  - male korelacije između ulaznih i izlaznih bitova
  - nije moguće opisati izlaz kao jednostavnu funkciju ulaza
  - nema fiksnih ili suprotnih točaka

- Izmiješani stupci i pomaknuti retci osiguravaju da svi izlazni bitovi ovise o svim ulaznima nakon nekoliko rundi.

ZADACI

Uvodne upute:

U svrhu analize AES kriptografskih sustava u vježbi je potrebno koristiti aplikaciju *CrypTool*, alat namijenjen proučavanju različitih klasičnih, simetričnih, asimetričnih kriptografskih sustava i metoda njihove kriptoanalize.

AES *(Advanced Encryption Standard)*

Zadatak 1. S-blokovi koji se koriste pri AES šifriranju implementiraju inverzne funkcije u Galois polju. Definirajte Galois polje s 4 elementa, GF(2^2), primjenom primitivne funkcije $f(x) = x^2+x+1$. Rješenja upišite u tablicu.

Tablica 6.2. *Aritmetika sumiranja u Galois polju GF(2^2) s 4 elementa*

Sumiranje:

+				

Tablica 6.3. *Aritmetika množenja u Galois polju GF(2^2) s 4 elementa*

Množenje:

×				

Zadatak 2. Pomoću **AES (CBC)** algoritma potrebno je šifrirati vlastito ime i prezime (otvoreni tekst), uz zadani ključ: 0x1234567890ABCDEF0000000000000000. Dobiveni kriptogram potrebno je upisati u heksadekadskom obliku.

Otvoreni tekst: _____

Dobiveni kriptogram:_____

Zadatak 3. Pomoću **AES (CBC)** algoritma potrebno je šifrirati zadani pojam (otvoreni tekst), uz proizvoljni ključ. Odabrani ključ i dobivene kriptograme potrebno je upisati u heksadekadskom obliku.

Odabrani ključ: _____

Otvoreni tekst: SIGURNOSTINFORMACIJSKIHSUSTAVA

Dobiveni kriptogram:_____

Zadatak 4. Uz primjenu AES (CBC) algoritma:

A) Šifrirajte navedeni otvoreni tekst ako je zadani ključ: 0x12345678000000000000000000000000

Otvoreni tekst: SIFRIRANJEIDESIFRIRANJE

AES (CBC) - Dobiveni kriptogram:_____

B) Pokušajte dešifrirati tako dobiveni kriptogram primjenom opcije *Analysis* uz unos djelomično poznatog ključa (pri čemu oznaka „*“ predstavlja nepoznatu vrijednost) te navedite koliko je vremena potrebno za dovršetak postupka dešifriranja u svakom pojedinom slučaju:

Ključ:	Potrebno vrijeme:
0x1234567890ABCDEF**********	_____
0x12345678**********	_____
0x**********	_____

Zadatak 5. Navedite osnovne prednosti primjene AES algoritma:

_____

_____

Zadatak 6. Navedite duljne blokova otvorenog teksta koje se koriste pri šifriranju pomoću sljedećih algoritama:

AES: _____

DES: _____

Triple DES: _____

Zadatak 7. Navedite duljne ključeva koje se koriste pri šifriranju pomoću sljedećih algoritama:

AES: _____

DES: _____

Triple DES: _____

Zadatak 8. Usporedite vrijeme dešifriranja kriptograma pomoću AES (CBC) i DES (CBC) algoritama:

_____

_____

Zadatak 9. Usporedite vrijeme dešifriranja kriptograma pomoću AES (CBC) i Triple DES (CBC) algoritama:

_____

_____

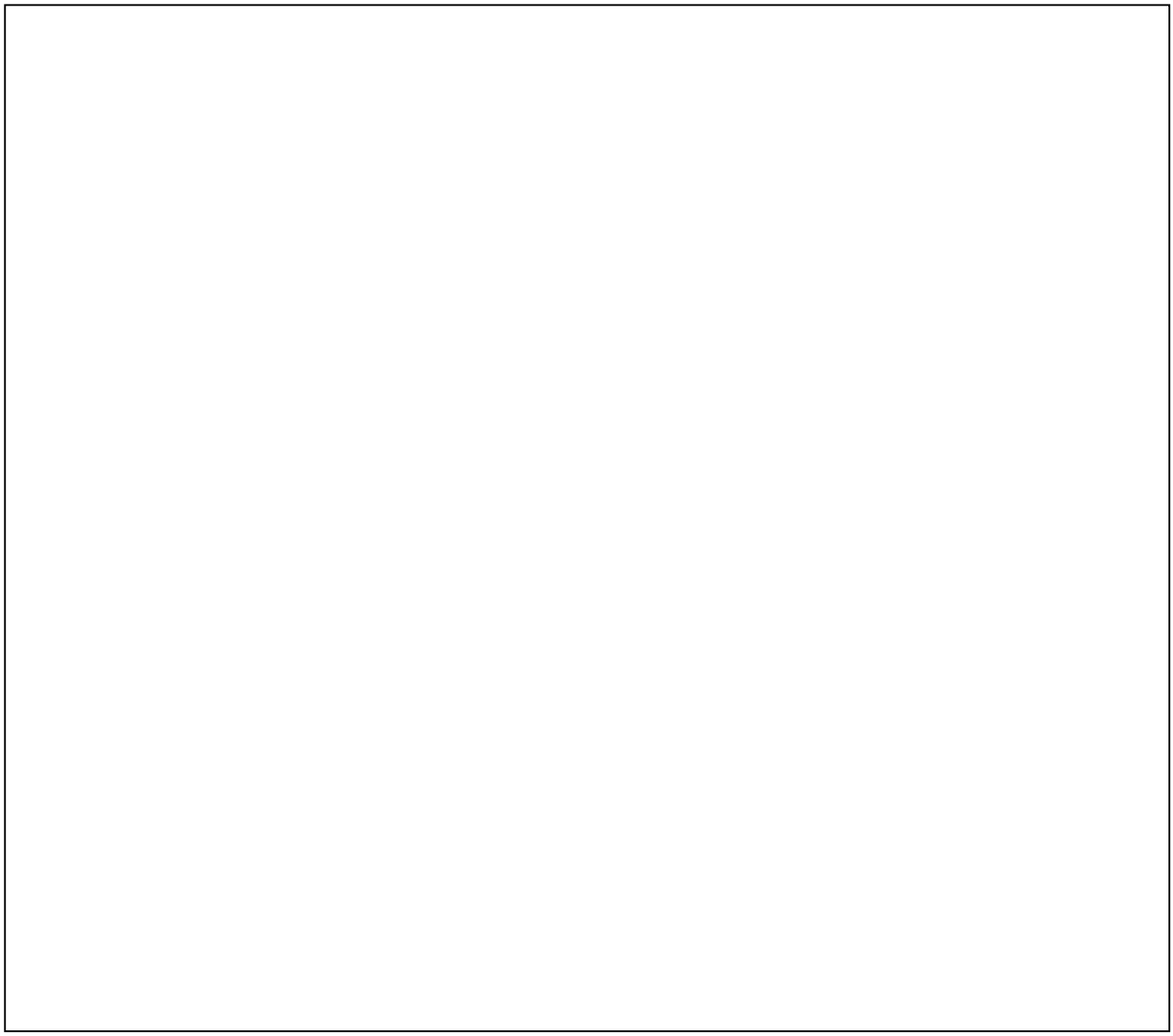
Vježba 8. - Asimetrični kriptosustavi

Asimetrični kriptosustavi (kriptosustavi s javnim ključem) koriste dva ključa: javni ključ i odgovarajući tajni ključ. Sa javnim ključem pošiljatelj može kriptirati poruku, a dekriptirati je može samo primatelj koji zna tajni ključ. Javni ključ ne treba biti tajna, on može biti dostupan svima, a njegova točnost garantira da jedino primatelj koji ima tajni ključ može čitati poruku.

Asimetrični kriptosustavi su sporiji nego simetrični. Zbog toga u pravilu asimetrični kriptosustavi služe za razmjenu ključeva koji se koriste u simetričnom kriptosustavu.

Zadatak 1. *RSA kriptosustav*

- U aplikaciji *CrypTool* realizirati sustav za šifriranje i dešifriranje pomoću RSA kriptosustava.
- Generirati ključ (privatni i javni) za RSA kriptosustav (objasnite kako se generiraju ključevi).



- Pomoću prethodno generiranog ključa prikazati i objasniti postupak RSA šifriranja na primjeru vlastitog imena i prezimena (npr. „PETAR PETROVIC“).

- Šifrirati sljedeće primjere otvorenog teksta, pri čemu je za svaki primjer potrebno generirati novi ključ (osim šifrata upisati i korištene ključeve), te za provjeru provesti i postupak dešifriranja.

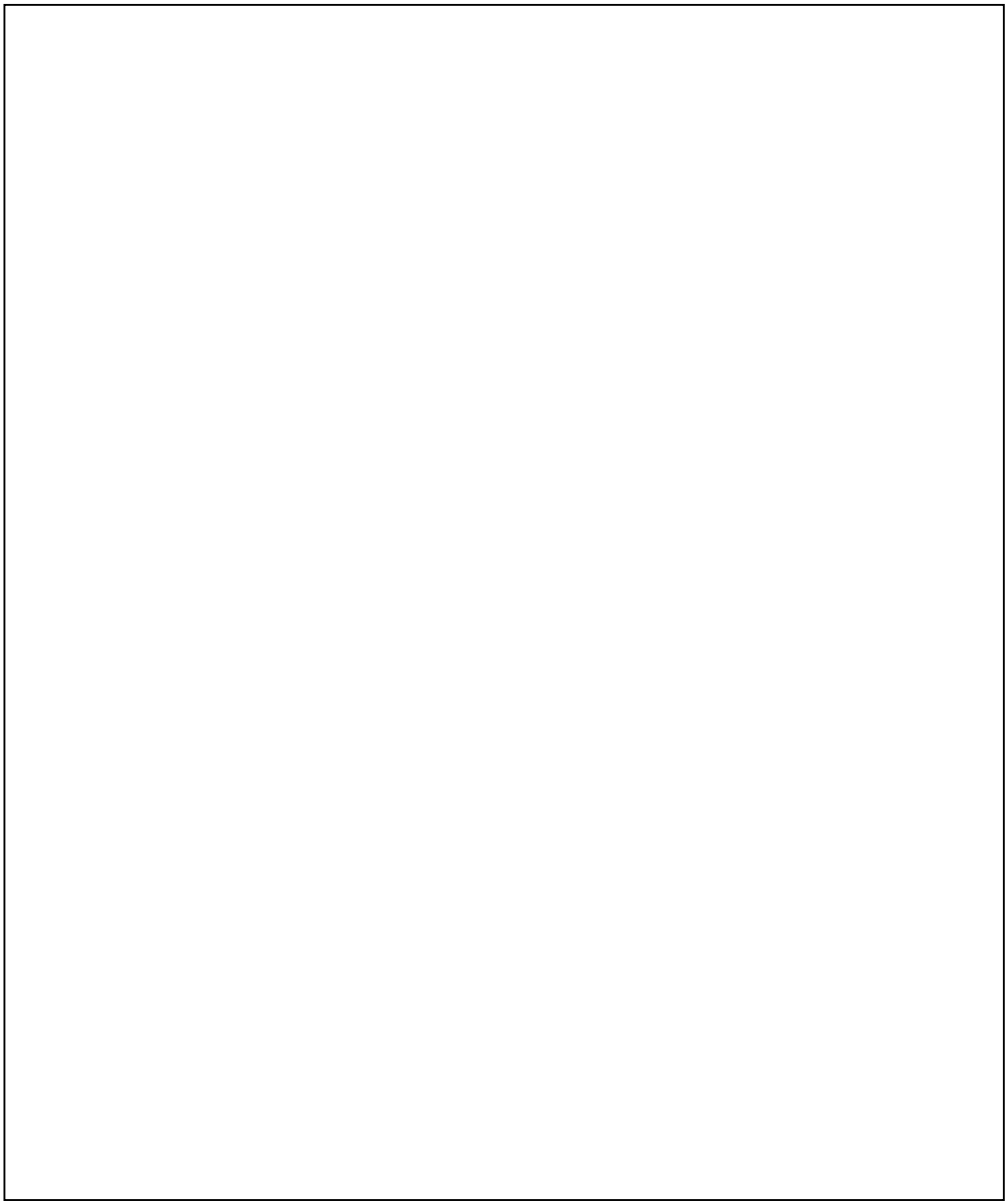
a) RON RIVEST

b) ADI SHAMIR

c) LEONARD ADLEMAN

Zadatak 2. *Protokol Diffie-Hellman za razmjenu ključeva*

- U aplikaciji *CrypTool* realizirati sustav za razmjenu ključeva između dvije strane Diffie-Hellmanovim postupkom (ucrtati i objasniti).



- Za pet različitih skupova (proizvoljno izabranih) početnih vrijednosti generirati dijeljene ključeve Diffie-Hellmanovim postupkom (pomoću prethodno realiziranog sustava), te upisati i objasniti potrebna izračunavanja:

Vježba 9. - Asimetrični kriptosustavi: RSA algoritam

UVOD

Kriptosustavi s javnim ključem, odnosno asimetrični kriptosustavi, za razliku od simetričnih kriptosustava, temelje se na primjeni konkretnih matematičkih funkcija, a ne na primjeni supstitucija i permutacija. Razvoj asimetrične kriptografije vezan je uz potrebu primjene metoda za sigurnu razmjenu ključeva.

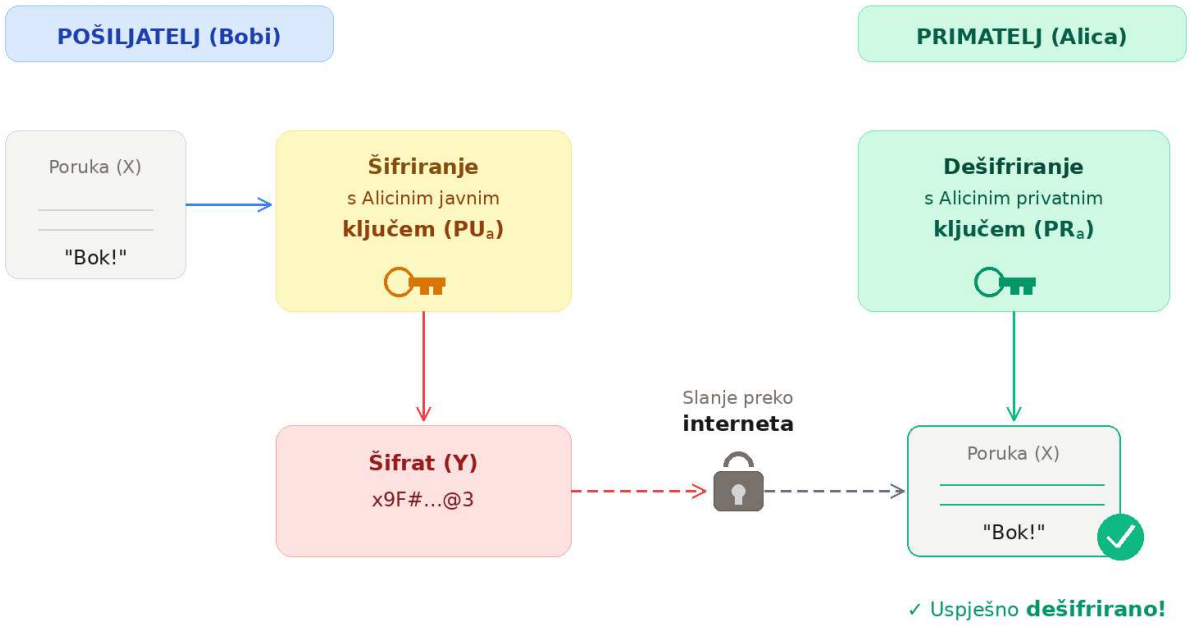
U pravilu se asimetrični kriptografski algoritmi oslanjaju na primjenu jednog ključa za šifriranje, ključa koji se naziva javnim (dostupan je svima), te drugog ključa za dešifriranje, ključa koji se obično naziva tajnim (privatnim). Iako su ovi ključevi međusobno povezani, iz ključa za šifriranje nemoguće je u ograničenom vremenu izračunati ključ za dešifriranje.

Postupci šifriranja i dešifriranja se odvijaju prema sljedećem:

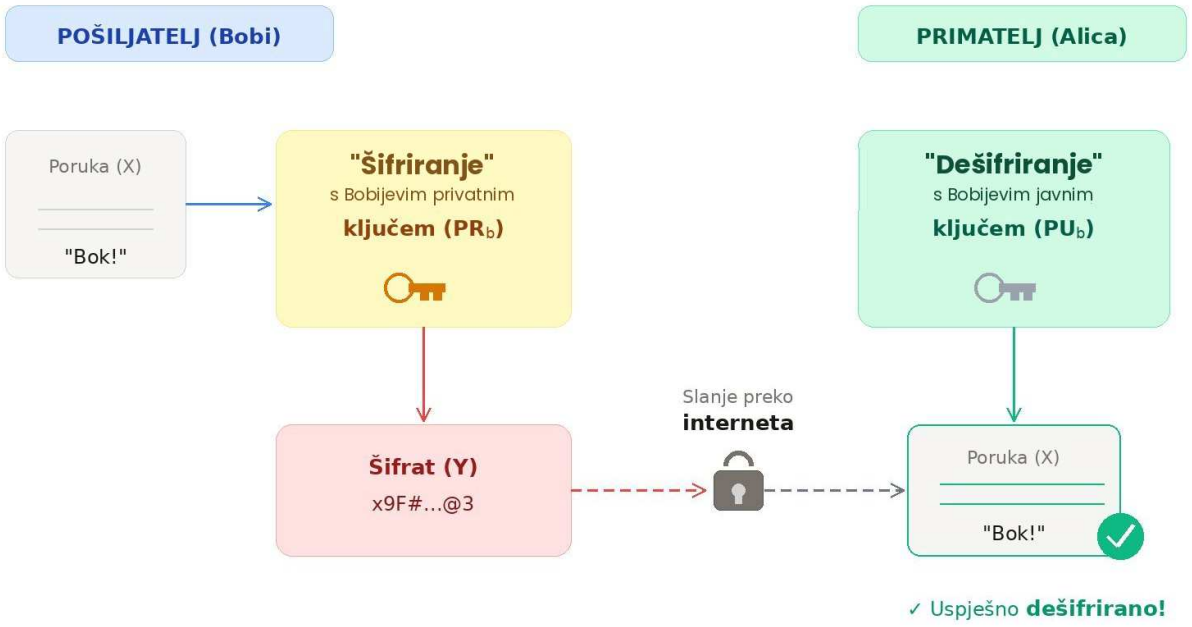
- Svaki korisnik generira par ključeva koji će se koristiti za šifriranje i dešifriranje poruka.
- Jedan od tih ključeva definira se kao javno dostupan, dok se drugi čuva u tajnosti.
- Kada korisnik A šalje tajnu poruku korisniku B, za šifriranje treba koristiti javni ključ korisnika B.
- Korisnik B će tada primljenu poruku dešifrirati svojim tajnim ključem. Nitko drugi ne može dešifrirati poruku budući da samo korisnik B zna svoj tajni ključ.

Pri definiranju pojedinih veličina najčešće se koriste sljedeće oznake:

- $X = [X_1, X_2, \ldots, X_M]$ – poruka namijenjena korisniku B koju generira korisnik A, a koja se sastoji od niza simbola iz neke konačne abecede
- PU – javni ključ koji generira korisnik
- PR – privatni ključ
- $Y = [Y_1, Y_2, \ldots, Y_N]$ – šifrat kreiran pomoću poruke X_i i javnog ključa.



Slika 9.1. *Postupak asimetričnog šifriranja poruke pomoću javnog ključa*



Slika 9.2. *Postupak asimetričnog šifriranja poruke pomoću tajnog ključa*

RSA algoritam

Prilikom konstrukcije asimetričnih kriptosustava obično se primjenjuju složeni matematički problemi poput faktorizacije velikih prirodnih brojeva, tj. na njihovom rastavljanju na faktore.

RSA (*Rivest, Shamir i Adleman*) kriptosustav kao jedan od najpoznatijih asimetričnih kriptosustava temelji se na problemu faktorizacije prirodnih brojeva s preko 250 znamenaka.

Kod RSA kriptosustava otvoreni tekst i šifrat prikazani su kao cijeli brojevi između 0 i *n-1*, pri čemu je vrijednost *n* najčešće 1024 bita, pa je $n<2^{1024}$.

Pri šifriranju se otvoreni tekst šifrira se u blokovima, pa svaki blok ima binarnu vrijednost manju od *n*. Zato veličina svakog bloka mora biti manja od ili jednaka: $log_2(n)+1$. Najčešće je veličina bloka *i* bitova, gdje je $2^i < n \leq 2^{i+1}$.

Procesi šifriranja i dešifriranja opisani su sljedećim izrazima:

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

pri čemu i korisnik koji šalje poruku, tj. pošiljatelj, i primatelj moraju znati vrijednost *n*. Vrijednost *e* zna pošiljatelj, dok vrijednost *d* zna samo primatelj.

Javni ključ označava se kao $PU=\{e, n\}$, a privatni ključ $PR=\{d, n\}$.

Za šifriranje javnim ključem, moraju vrijediti sljedeći uvjeti:

- za sve vrijednosti $M < n$ moguće je pronaći vrijednosti *e*, *d* i *n* takve da je:
$$M^{ed} \bmod n = M$$
- za sve vrijednosti $M < n$ moguće je izračunati:
$$M^e \bmod n \text{ i } C^d \bmod n$$
- nije moguće unutar određenog ograničenog vremenskog perioda odrediti vrijednost *d* ukoliko su poznate vrijednosti *e* i *n*.

Relacija:

$$M^{ed} \bmod n = M$$

bit će zadovoljena ukoliko su *e* i *d* multiplikativni inverzi modulo $\boldsymbol{\phi(n)}$, gdje je $\phi(n)$ Eulerova funkcija.

Eulerova funkcija predstavlja broj onih vrijednosti u nizu 1, 2, ..., *n* koje su relativno proste *n*.

Za $\phi(n)$ vrijedi sljedeće:

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$$

Pri tome se veza između *e* i *d* može definirati kao:

$$ed \ mod \ \phi(n) = 1$$

Navedeno je ekvivalentno izrazima:

$$ed \equiv 1 \ mod \ \phi(n)$$
$$d = e^{-1} \ mod \ \phi(n)$$

odosno, *e* i *d* su multiplikativni inverzi modulo $\phi(n)$.

Ukoliko se primjene pravila modularne aritmetike, navedeno je točno samo ako su *d* i *e* relativno prosti s $\phi(n)$, odnosno ako je najveći zajednički faktor od $\boldsymbol{\phi(n)}$ i *d* jednak 1, te ako je najveći zajednički faktor od $\boldsymbol{\phi(n)}$ i *e* jednak 1.

Navedeni izraz zadovoljava zahtjeve RSA algoritma.

RSA shema sastoji se od sljedećeg:

$\boldsymbol{p}$ i $\boldsymbol{q}$ (dva prosta broja)	- privatni (izabrani)
$\boldsymbol{n = pq}$	- javni (izračunat)
$\boldsymbol{e}$ (takav da je: $nzd(\phi(n),e) = 1$; $1 < e < \phi(n)$)	- javni (izabran)
$\boldsymbol{d} \equiv e^{-1}(mod \ \phi(n))$	- privatni (izračunat)

Privatni ključ sastoji se od para $\{d, n\}$, a javni ključ sastoji se od para $\{e, n\}$.

Ako korisnik A objavi svoj javni ključ, te korisnik B šalje poruku *M* korisniku A, tada korisnik *B* izračunava šifrat prema sljedećem:

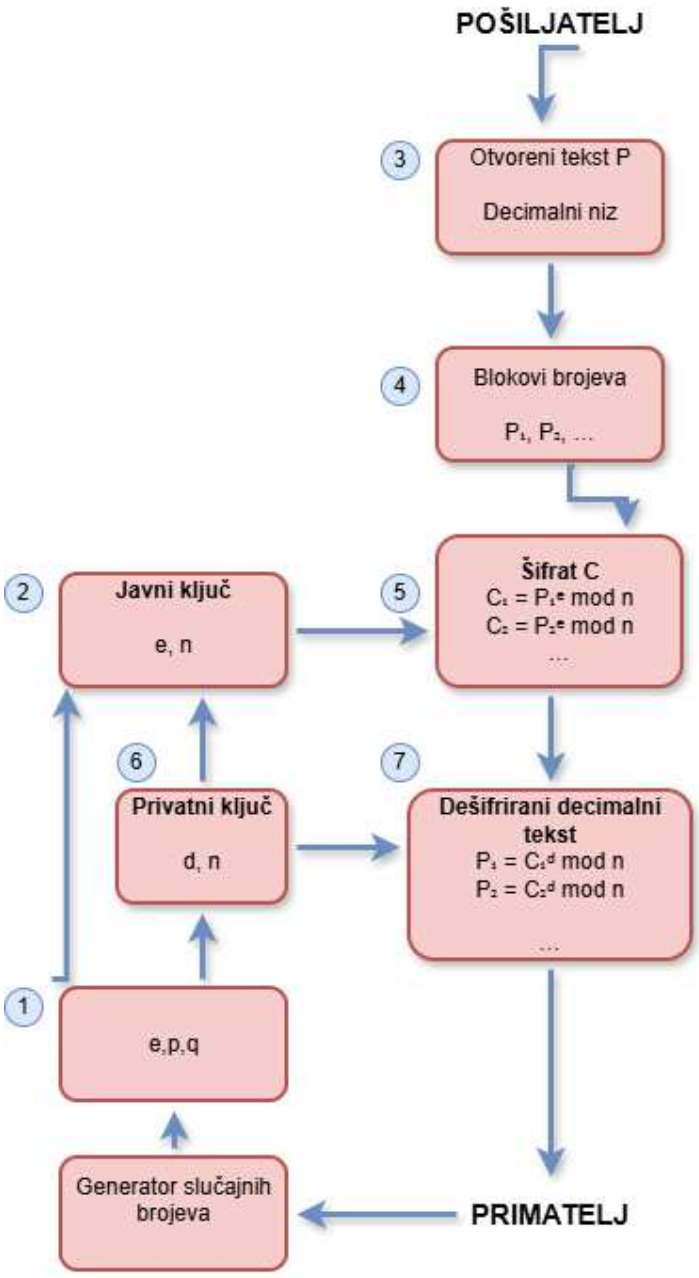
$$C = M^e \ mod \ n$$

i šalje ga korisniku A.

Korisnik A dešifrira poruku na sljedeći način:

$$M = C^d \ mod \ n.$$

Primjer procesiranja blokova pomoću RSA algoritma prikazan je na donjoj slici.



Slika 9.3. *Prikaz sheme šifriranja otvorenog teksta pomoću RSA algoritma*

ZADACI

Uvodne upute:

U svrhu analize RSA kriptografskih sustava u vježbi je potrebno koristiti aplikaciju *CrypTool*, alat namijenjen proučavanju različitih klasičnih, simetričnih, asimetričnih kriptografskih sustava i metoda njihove kriptoanalize.

RSA algoritam

Zadatak 1. U primjeru primjene RSA algoritma te za dva zadana prosta broja $p = 17$ i $q = 11$ potrebno je:

a) izračunati n: _____

b) izračunati $\phi(n)$: _____

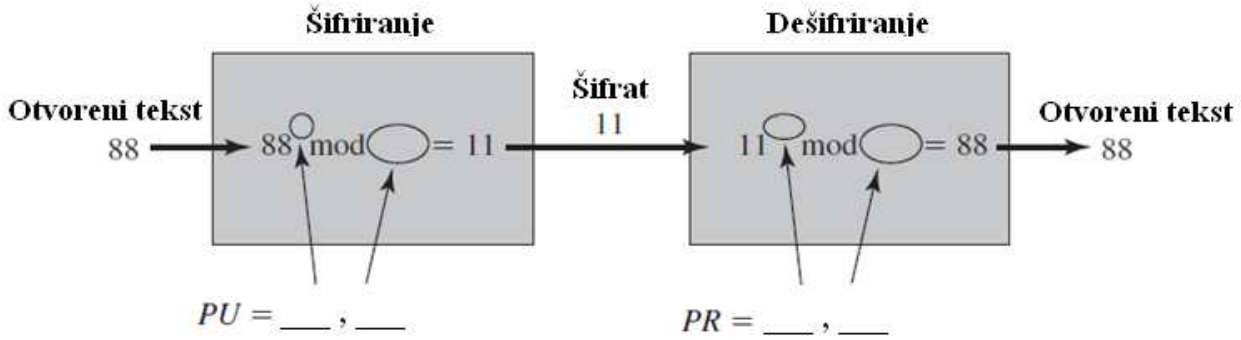
c) izabrati e (tako da je e relativno prost sa $\phi(n)$ te manji od $\phi(n)$): _____

d) izračunati d (takav da je $de \equiv 1\ (mod\ \phi(n))$ te $d < \phi(n)$): _____

e) navesti dobiveni javni ključ PU: { _____ , _____ }

f) navesti privatni ključ PR: { _____ , _____ }

Zadatak 2. Primjer na slici pokazuje postupak šifriranja i dešifriranja otvorenog teksta, tj. poruke, $M = 88$. Prema prethodnom zadatku sliku dopunite odgovarajućim vrijednostima:



Slika 9.4. *Komponente javnog i tajnog RSA ključa*

Zadatak 3. Aplikacija *CrypTool* omogućuje provedbu postupaka RSA šifriranja i dešifriranja.

a) Provedite postupak RSA šifriranja (*encryption*) proizvoljnog otvorenog teksta uz jedan od postojećih predefiniranih ključeva i upišite vrijeme potrebno za šifriranje:
   Vrijeme šifriranja: _____

b) Dobiveni šifrat iz primjera a) dešifrirajte uz primjenu istog ključa i navedite vrijeme potrebno za RSA dešifriranje (*decryption*).
   Vrijeme dešifriranja:_____

c) Usporedite dobivena vremena:_____

Napomena: *U sljedećim primjerima potrebno je koristiti inačicu 2.1 aplikacije CrypTool.*

Zadatak 4. Grafički prikažite shemu koja opisuju postupak RSA šifriranja (*RSA Encryption*).

Zadatak 5. U tablicu upišite oznake i objasnite uloge svakog od prikazanih blokova.

Tablica 9.1. *Oznake blokova na shemi koja prikazuje algoritam RSA šifriranja*

Oznaka (naziv) bloka:	Uloga navedenog bloka:

Zadatak 6. Provjerite ispravnost dobivenog rješenja iz Zadatka 2. nakon postupka RSA šifriranja pri unosu prethodno definiranih ulaznih vrijednosti.

Upišite vrijednost dobivenog rješenja: _____

Zadatak 7. Uz iste vrijednosti ulaznih parametara kao u prethodnom primjeru unesite drugu poruku. Upišite dobiveni rezultat postupka RSA šifriranja:

Dobiveni šifrat: _____

Ukratko komentirajte što se dogodilo: _____

Zadatak 8. Grafički prikažite shemu koja opisuju postupak RSA dešifriranja (*RSA Decryption*).

Zadatak 9. Objasnite uloge svakog od prikazanih blokova.

Tablica 9.2. *Oznake blokova na shemi koja prikazuje algoritam RSA dešifriranja*

Oznaka (naziv) bloka:	Uloga navedenog bloka:

Zadatak 10. Provjerite ispravnost dobivenog rješenja iz Zadatka 2. za postupak RSA dešifriranja (unesite prethodno definirane vrijednosti).

Upišite vrijednost dobivenog rješenja: _____

Vježba 10. - Asimetrični kriptosustavi: Digitalni potpis

UVOD

Način primjene asimetričnih kriptografskih sustava, tj. kriptografskih sustava temeljenih na javnom ključu uključuje sljedeća područja primjene:

- šifriranje / dešifriranje
- digitalni potpis
- razmjenu ključeva.

Digitalni potpis zasniva se na ideji da se pomoću izvorne poruke i tajnog ključa pošiljatelja može u digitalnom sustavu generirati pošiljateljev potpis koji je analogan potpisu na papiru. Primatelj poruke može verificirati autentičnost potpisa pošiljatelja ukoliko posjeduje izvornu poruku i javni ključ pošiljatelja.

Jedna od najvažnijih prednosti asimetričnih kriptosustava u usporedbi sa simetričnim kriptosustavima upravo je mogućnost njihove primjene za potrebe digitalnog potpisivanja poruke.

Dok su neki asimetrični kriptografski algoritmi prikladni za sva tri područja primjene, drugi su prikladni za manji broj primjena.

Tablica 10.1. *Područja primjene asimetričnih algoritama šifriranja*

Algoritam	Šifriranje / Dešifriranje	Digitalni potpis	Razmjena ključeva
RSA	Da	Da	Da
Eliptička krivulja	Da	Da	Da
Diffie–Hellman	Ne	Ne	Da
DSS	Ne	Da	Ne

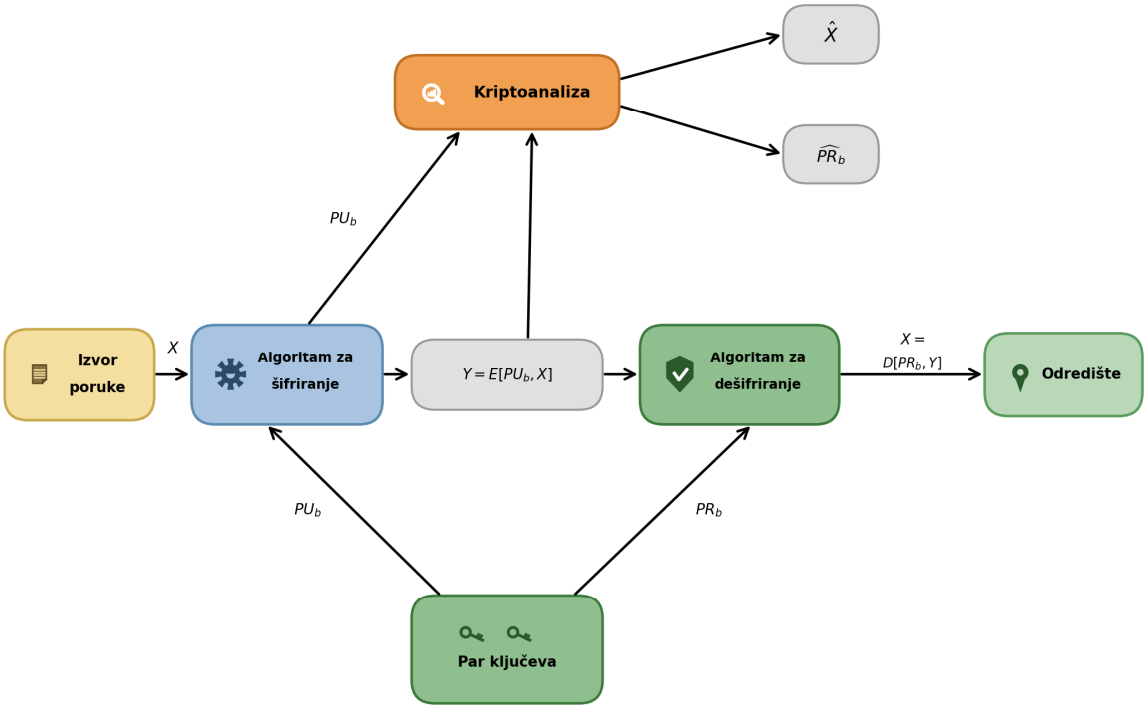
Digitalni potpis predstavlja asimetrični kriptosustav, tj. kriptosustav temeljen na javnom ključu. Takav potpis omogućuje:

a) autentifikaciju korisnika - primatelj može provjeriti je li primljenu poruku poslao određeni pošljatelj
b) nepobitnost poslane poruke - pošiljatelj ne može poreći slanje poruke ukoliko primatelj posjeduje poruku s njegovim potpisom.

Postupak digitalnog potpisivanja poruke uključuje sljedeće postupke:

- generiranje javnog i privatnog ključa za potpisivanje poruke
- generiranje potpisa, odnosno potpisivanje poruke
- provjeru potpisa.

Omogućavanje sigurnosti komunikacije



Slika 10.1. *Primjena asimetričnog kriptosustava za omogućavanje sigurne komunikacije*

Pošiljatelj (korisnik A) generira poruku $X = [X_1, X_2, \ldots, X_M]$ koja se sastoji od niza simbola iz neke konačne abecede namijenjenu prmatelju (korisniku B).

Korisnik B generira par ključeva - javni ključ PU_b te privatni ključ PR_b, poznat isključivo njemu.

Pomoću poruke X i javnog ključa PU_b, korisnik A kreira šifrat $Y = [Y_1, Y_2, \ldots, Y_N]$:

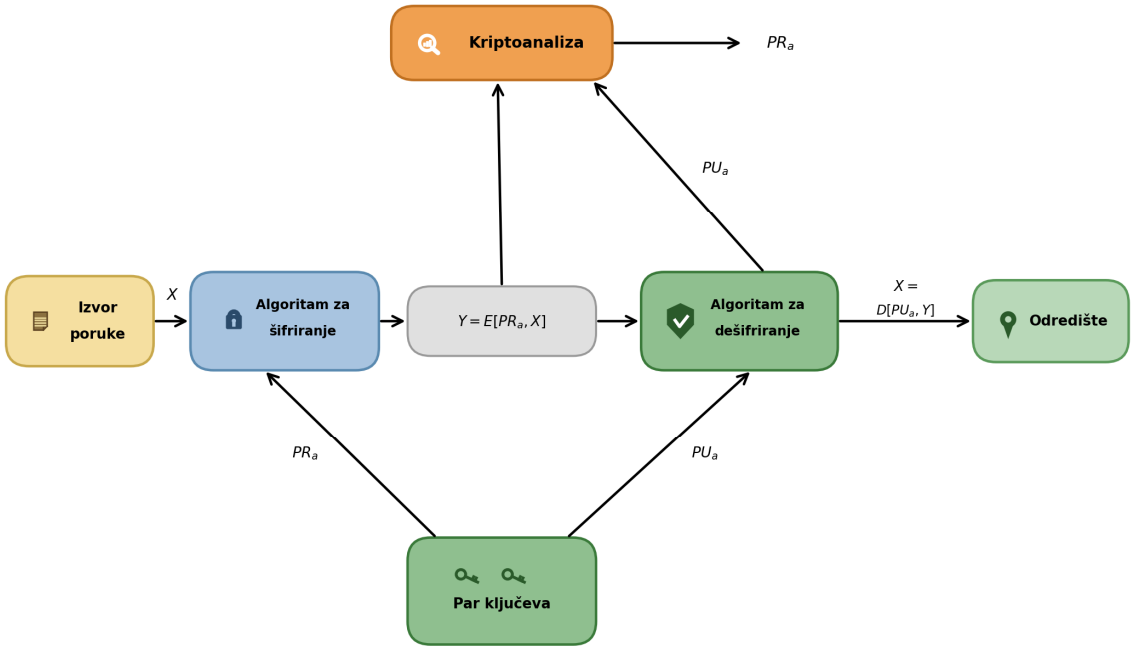
$$Y = E\ (PU_b, X)$$

Korisnik B provodi postupak dešifriranja:

$$X = D\ (PR_b, Y)$$

Cilj potencijalnog napada je promatranjem šifrata Y_i uz poznat javni ključ Pu_b otkriti sadržaj poruke (X) kao i privatni ključ PR_b.

Omogućavanje autentičnosti komunikacije



Slika 10.2. *Primjena asimetričnog kriptosustava za provjeru autentičnosti komunikacije*

Korisnik A poruku koja je namijenjena korisniku B prije slanja šifrira svojim privatnim ključem PR_a:

$$Y = E\ (PR_a, X)$$

Korisnik B može dešifrirati ovu poruku pomoću javnog ključa korisnika A:

$$X = D\ (PU_a, Y)$$

Kako je poruka šifrirana privatnim ključem korisnika A jedino korisnik A može biti pošiljatelj poruke, pa cijela šifrirana poruka predstavlja digitalni potpis.

Isto tako, budući da se sadržaj šifrirane poruke ne može izmijeniti bez poznavanja privatnog ključa korisnika A (PR_a), uz autentičnost pošiljatelja zajamčen je i integritet poruke.

Kako opisani način primjene asimetričnog kriptosustava za osiguranje autentičnosti i integriteta poruke ne osigurava i njezinu tajnost, ukoliko se istovremeno želi osigurati povjerljivost, autentičnost i integritet poruke, nužna je dvostruka primjena algoritma asimetrične enkripcije:

$$Z = EPU_b, EPR_a, X$$

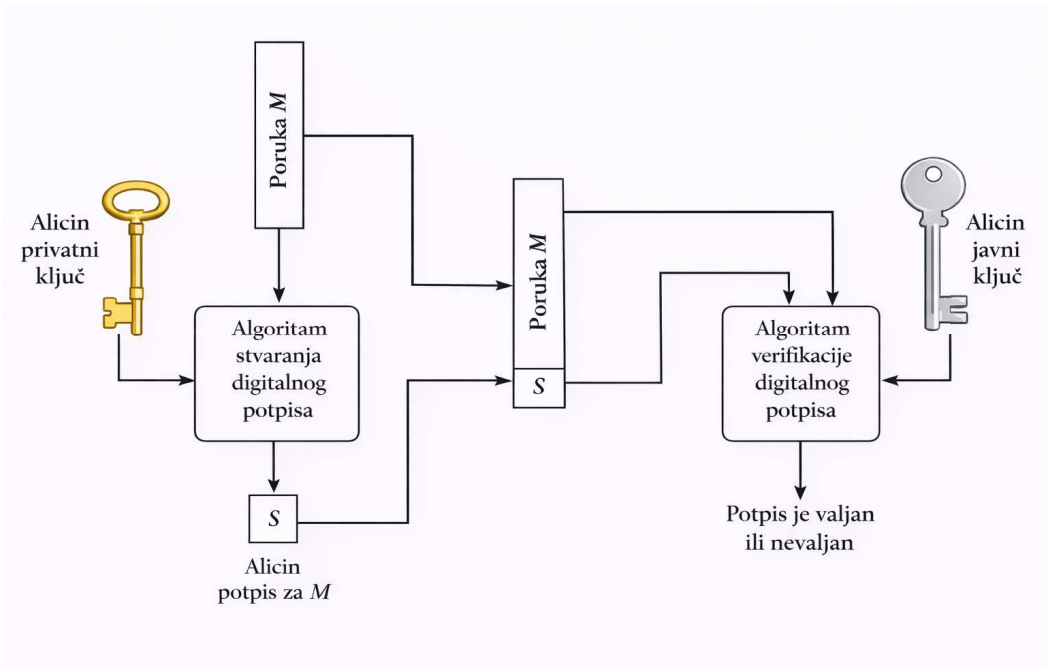
$$X = D\ (PU_a, D\ (PR_b, Z)$$

Osnovne pretpostavke koje algoritam temeljen na javnom ključu mora zadovoljiti:

- za primatelja treba biti jednostavno generirati odgovarajući par javnog i privatnog ključa (PU_b, PR_b)
- za pošiljatelja treba biti jednostavno generirati šifrat uz poznavanje primateljevog javnog ključa i poruke
- za primatelja treba biti jednostavno dešifrirati poruku pomoću privatnog ključa
- za napadača ne smije biti moguće u definiranom ograničenom vremenu odrediti privatni ključ PR_b iz javnog ključa PU_b
- za napadača ne smije biti moguće u definiranom ograničenom vremenu odrediti izvornu poruku uz poznanje šifrata i javnog ključa PU_b
- poželjno je da se dva ključa mogu primijeniti u bilo kojem redoslijedu:

$$M = D[PU_b, E(PR_b, M)] = D\ [PR_b, E(PU_b, M)]$$

Generički model procesa digitalnog potpisa



Slika 10.3. *Postupci generiranja i verifikacije digitalnog potpisa*

U praksi se za digitalni potpis najčešće koriste algoritmi koji su dizajnirani isključivo za funkcije digitalnog potpisa, a ne može ih se koristiti za enkripciju ili razmjenu ključeva iako se temelje na tehnici javnog ključa. Jedan od najpoznatijih primjera takvih algoritama za digitalni potpis je DSA *(Digital Signature Algorithm).*

Međutim, u situacijama kada se želi osigurati autentičnost izvora i integritet poruke potrebno je koristiti kriptosustave temeljene na primjeni javnog ključa.

Neki kriptosustavi s javnim ključem, poput RSA, mogu se izravno koristiti za potpisivanje poruke.

ZADACI

Uvodne upute:

U svrhu analize primjene digitalnih potpisa u vježbi je potrebno koristiti aplikaciju *CrypTool*, alat namijenjen proučavanju različitih klasičnih, simetričnih, asimetričnih kriptografskih sustava i metoda njihove kriptoanalize.

Digitalni potpis *(Digital Signature)*

Zadatak 1. Grafički prikažite shemu dvostruke primjene algoritma asimetrične enkripcije.

Zadatak 2. Objasnite zašto unatoč njhovim prednostima asimetrični kriptosustavi u praksi ne predstavljaju zamjenu za simetrične kriptosustave.

_____

_____

_____

Zadatak 3. Objasnite na koji način se postiže autentičnost izvora i integritet poruke kod RSA algorima.

_____

_____

_____

Zadatak 4. Aplikacija *CrypTool* omogućuje analizu RSA algoritma pri kreiranju digtalnog potpisa.

Nakon pokretanja aplikacije *CrypTool* 1.4 iz izbornika digitalnih potpisa (*Digital Signatures/PKI*) odaberite opciju *PKI* te zatim generiranje/uvoz ključeva (*Generate/Import Keys*...). Unesite sljedeće podatke:

Prezime *(Last name)*: _____

Ime *(First name)*: _____

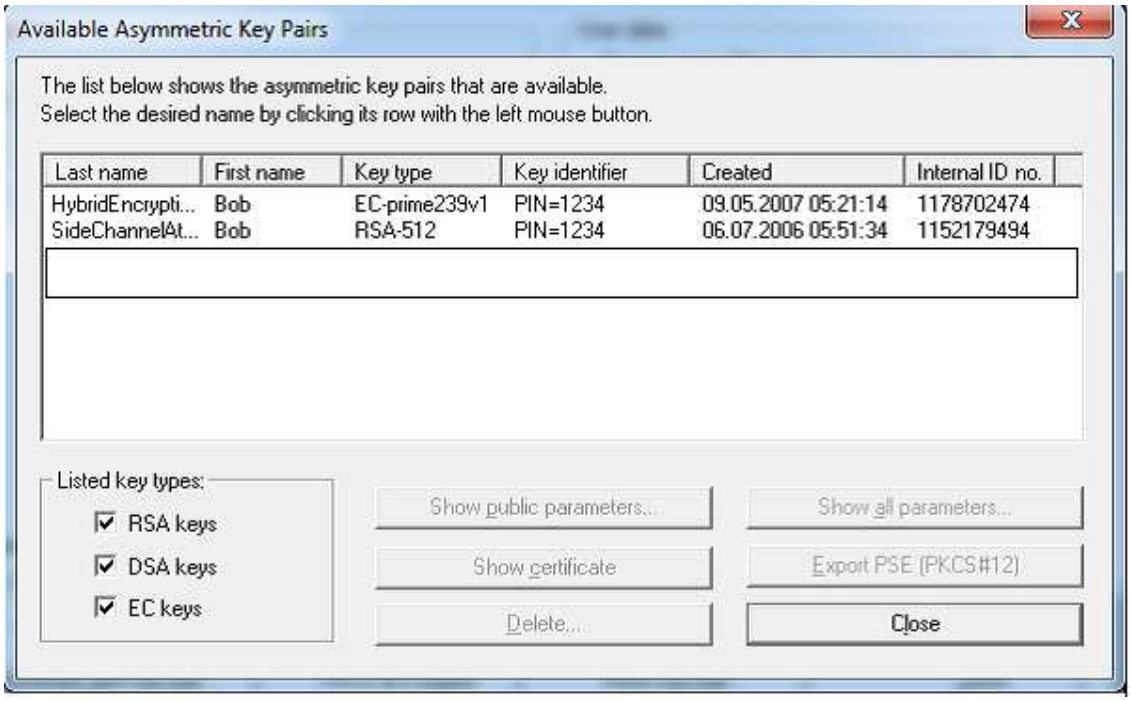
Identifikator ključa (*Key identifier*): _____

PIN kod (*PIN code*) (npr. *cryptool*): _____

PIN (*PIN*) (npr. *cryptool*): _____

Kliknite na opciju za generiranje novog para ključeva (*Generate new key pair*). U prozoru koji se pojavi odaberite opciju *OK*.

Zadatak 5. Kliknite na opciju za prikaz para ključeva (*Show Key Pair*) te u predviđeni prostor (u okvir) na donjoj slici upišite prikazanu kombinaciju oznaka.



Slika 10.4. *Podaci o generiranom digitalnom potpisu*

Zadatak 6. Prikažite certifikat klikom na prikaži certifikat (*Show certificate*). Navedite što se sve od podataka nalazi u prikazanom prozoru.

_____

_____

_____

Zatvorite oba prozora za certificiranje podataka (*Certificate Data*) i za dostupne asimetrične parove ključeva (*Available Asymmetric Key Pairs*).

Zadatak 7. Za potpisivanje početnog dokumenta *startingexample-en.txt*, iz izbornika digitalnog potpisivanja (*Digital Signatures/PKI*) odaberite opciju za potipisivanje poruke (*Sign Message*). Odaberite sljedeće postavke:

Odabir hash funkcije (*Choose hash function*): RIPEMD-160
Odabir algoritma za potpisivanje (*Choose signature algorithm*): RSA

U izbornik za odabir ključa koji će se koristiti pri potpisivanju (*Choose a key/PSE to be used when signing*) unesite isti unos koji ste prethodno upisali za identifikator ključa (*Key identifier*), a za PIN kod (*PIN code*) upišite prethodno odabrani. Kliknite na opciju potpisivanja (*Sign*).

Navedite koje je vrijeme porebno za generiranje digitanog potpisa:_____

Zadatak 8. Nakon potvrde (*OK*) zatvara se prozor i prikazuje potpisani dokument. Navedite na kojem se mjestu nalazi digitalni potpis u prikazanom dokumentu u odnosu na tekst samog dokumenta.

_____

_____

_____

Pregledniji prikaz na kojem se jasno vidi podjela između digitalnog potpisa i teksta dokumenta moguće je dobiti preko izbornika digitalnog potpisivanja (*Digital Signature/PKI*) te izborom opcije za izvod potpisa (*Extract Signature*).

Zadatak 9. Iz izbornika digitalnog potpisivanja (*Digital Signature/PKI*) odaberite opciju za verifikaciju potpisa (*Verify Signature*) kako biste provjerili da dokument nije izmijenjen. Potrebno je selektirati kreirani potpis s popisa i kliknuti na opciju verifikacije potpisa (*Verify signature button*). Navedite poruku koja je ispisana u prikazanom okviru:

_____

_____

Zadatak 10. Izmijenite sadržaj potpisanog dokumenta brisanjem prve riječi iz prikazanog teksta. Iz izbornika digitalnog potpisivanja (*Digital Signature/PKI*) odaberite opciju za verifikaciju potpisa (*Verify Signature*). Navedite poruku koja je ispisana u prikazanom okviru:

_____

_____

Vježba 11. - *Hash* funkcije: SHA, MD i RC *hash* funkcije

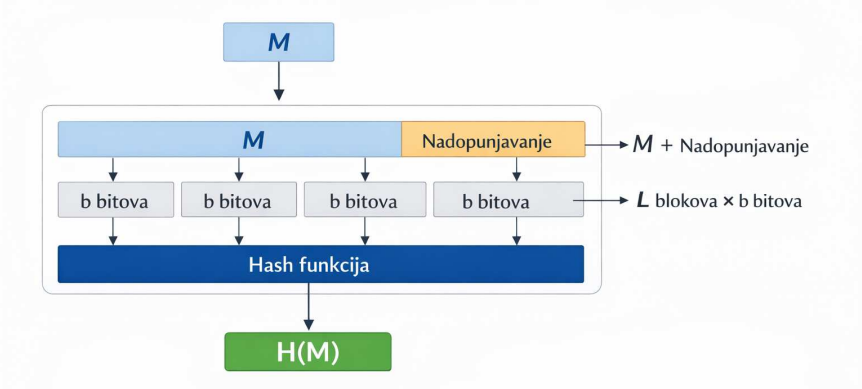
UVOD

Hash funkcija *H* je funkcija koja za podatkovni blok M varijabilne duljine izračunava „*hash*“ vrijednost unaprijed određene fiksne duljine:

$$h = H(M)$$

Čak i mala promjena podatkovnog bloka M (na jednom ili više bitova) rezultira promjenom pripadne *hash* vrijednosti. Na taj je način uz primjenu *hash* funkcije moguće zaštititi integritet podataka.

Duljina bloka *M* se modificira na *L* blokova od *b* bita. Ukoliko je potrebno, posljednji blok se dopunjuje (eng. *padding*) do duljine *b* bita.



Slika 11.1. *Izračun hash vrijednosti i njeno dodavanje izvornoj poruci*

Hash funkcije koje se koriste u kriptografiji moraju zadovoljiti sljedeća svojstva:

- *Hash* funkciju moguće je primijeniti na blokove proizvoljne duljine
- Za svaki blok *M* relativno je lako izračunati *H*(*M*)
- Za zadanu vrijednost *h* nije moguće naći *M* takav da je *H*(*M*) = *h*
- Za zadani *x* efektivno nije moguće naći *y* takav da je *H*(*x*)=*H*(*y*)
- Efektivno nije moguće naći par (*x*, *y*) tako da je *H*(*x*)=*H*(*y*)

Postoji više načina na koje se *hash* vrijednost *H* može koristiti uz poruku *M*:

- poruka se zajedno sa dodanim *hash* kodom šifrira pomoću simetrične šifre
- primjena simetrične enkripcije samo na *hash* kod
- koristi se *hash* funkcija za autentifikaciju, a ne koristi se enkripcija
- koristi se *hash* funkcija za autentifikaciju, a dodaje se i enkripcija, pa se osigurava tajnost poruke.

Među kriptografske *hash* funkcija ubrajaju se:

- **SHA: SHA-1, SHA-2, SHA-3 -** najraširenije *hash* funkcije (osim za enkripciju, koriste se i za provjeru očuvanja integriteta poruke)
- **MD: MD2, MD4 i MD5** (također se, osim za enkripciju, koriste i za provjeru očuvanja integriteta poruke)
- **RC: RC2 i RC4** (koriste se za enkripciju poruke).

SHA (*Secure Hash Algoritam*)

Uz posljednje vrijeme SHA (*Secure Hash Algorithm*) je najraširenija *hash* funkcija. SHA algoritam je standardiziran pod nazivom SHS (*Secure Hash Standard*). Kako se SHA-0 i SHA-1 inačice algoritma više ne smatraju dovoljno sigurnima, kroz vrijeme su se pojavile poboljšane varijante (SHA-2): SHA-256, SHA-384, SHA-512, i dr.

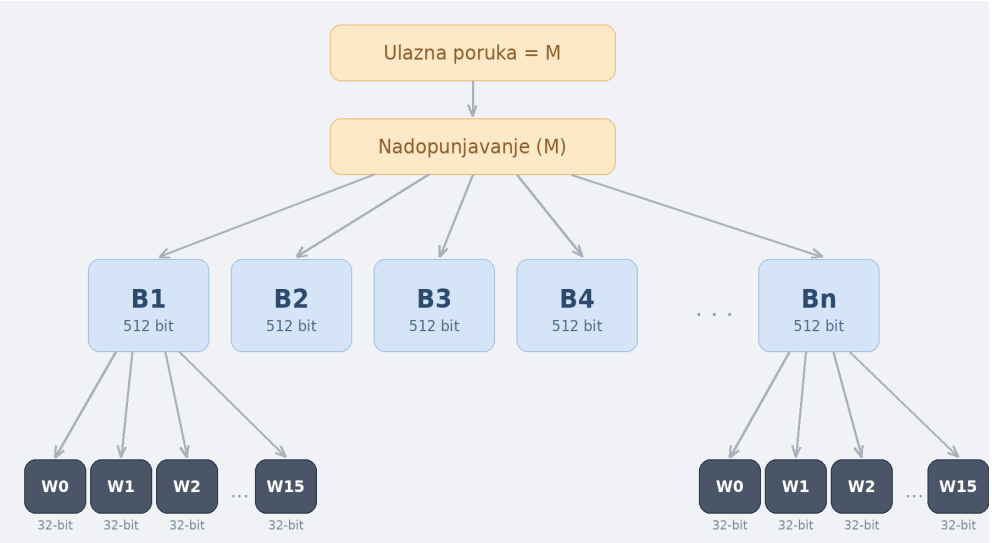
Tablica 11.1. *Prikaz i usporedba dostupnih inačica SHA algoritma*

Svojstvo	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Veličina sažetka poruke (bitovi)	160	224	256	384	512
Veličina poruke (bitovi)	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Veličina bloka (bitovi)	512	512	512	1024	1024
Veličina riječi (bitovi)	32	32	32	64	64
Broj koraka	80	64	64	80	80

SHA-1:

Algoritam kao ulaz uzima poruku definirane maksimalne duljine te kao izlaz daje sažetak poruke (eng. *message digest*) duljine 512 bita. Ulazna poruka procesira se u blokovima od po 512 bita. Postupak procesiranja sastoji se iz više koraka:

- korak 1: Dodavanje bitova za nadopunu, tj. nadopunjavanje;
  ukupna duljina dopunjene poruke je višekratnik vrijednosti 512.
- korak 2: Podjela nadopunjene poruke (eng. *dividing pad*);
  svaki B_i označava 512-bitni blok; svaki B_i se dijeli na 16 x 32-bitne riječi (W): W_0, W_1, …, W_{15}.



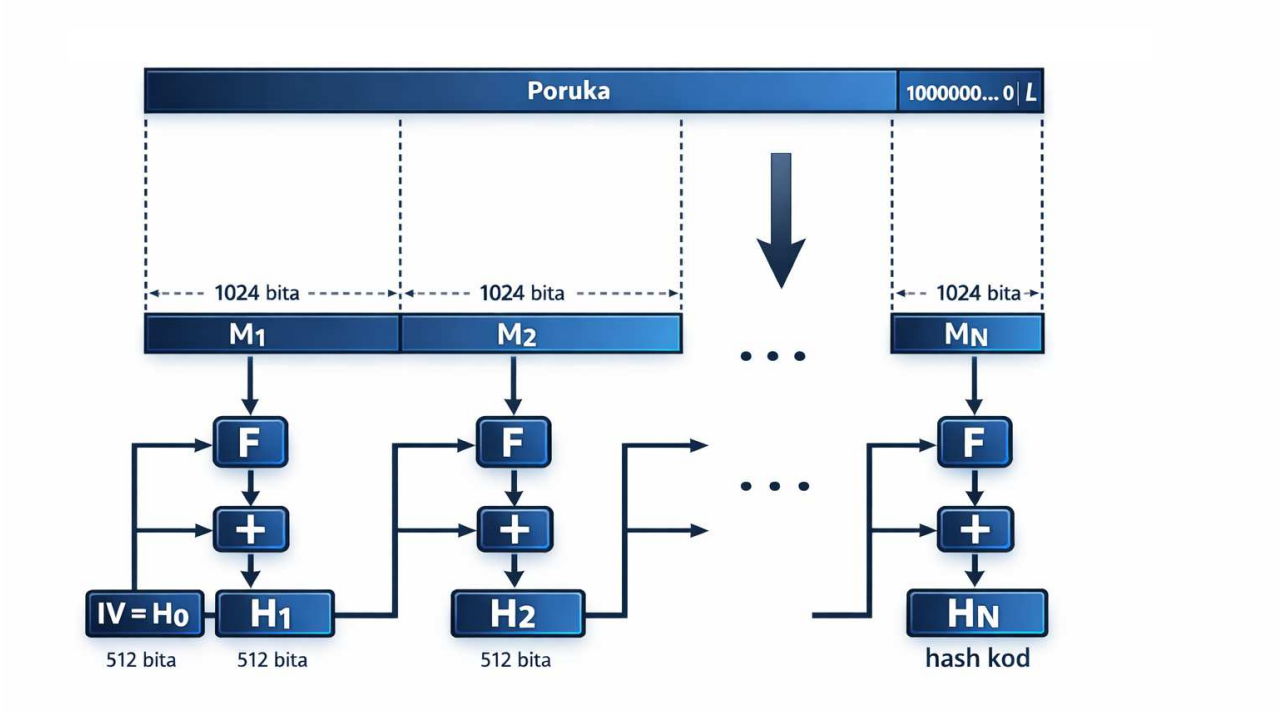
Slika 11.2. *Podjela nadopunjene poruke (pad(M)) na blokove (B) i riječi (W)*

- korak 3: Izračun $W_{16} - W_{79}$;
  proširivanje 16 riječi u 80 riječi.
- korak 4: Deklariranje inicijalizacijskih vrijednosti za 32-bitne riječi;
  određivanje konstantnih vrijednosti koje se primjenjuju u petlji.
- korak 5: Petlja

- korak 6: Završetak;
  nakon završetka svih koraka na svakom od 512-bitnih blokova (B_1, B_2, …, B_n) nadopunjene poruke definiran je 160-bitni sažetak poruke.

SHA-512:

Algoritam kao ulaz uzima poruku maksimalne duljine od 2128 bita, te kao izlaz daje sažetak poruke duljine 512 bita. Ulazna poruka procesira se u blokovima od po 1024 bita.



Slika 11.3. *Postupak izračuna sažetka (hash code) izvorne poruke duljine L bita*

Postupak procesiranja sastoji se iz više koraka:

- korak 1: Dodavanje bitova za nadopunu
  Duljina nadopune koja se dodaje poruci: $P \equiv 896 \ mod \ 1024$.
- korak 2: Dodavanje duljine poruke
  Poruci se dodaje blok od 128 bita u kojima je zapisana duljina originalne poruke (bez nadopune).
- korak 3: Inicijalizacija *hash* međuspremnika
  Za pohranjivanje međurezultata i krajnjih rezultata *hash* funkcije koristi se međuspremnik kojeg se može prikazati kao osam 64-bitnih registara (a, b, c, d, e, f, g, h).
- korak 4: Procesiranje poruke u 1024-bitnim blokovima
  Jezgru algoritma čini modul koji se sastoji od 80 rundi.
- korak 5: Izlaz
  Nakon što se procesira svih 1024-bitnih blokova, izlaz predstavlja 512-bitni sažetak poruke.

ZADACI

Uvodne upute:

U svrhu analize *hash* funkcija, u vježbi je potrebno koristiti aplikaciju *CrypTool*, alat namijenjen proučavanju različitih klasičnih, simetričnih, asimetričnih kriptografskih sustava i metoda njihove kriptoanalize.

Hash funkcije

Zadatak 1. U aplikaciji *CrypTool* 2.1 za proizvoljnu ulaznu poruku duljine oko 500 znakova izračunajte tražene SHA *hash* vrijednosti, te ih upišite u heksadecimalnom obliku.

a) SHA-1: _____

b) SHA-256: _____

c) SHA-384: _____

d) SHA-512: _____

Zadatak 2. Obrišite prvu riječ u originalnom tekstu poruke i izračunajte SHA-1 *hash* vrijednosti te ju upišite u heksadecimalnom obliku.

SHA-1: _____

Zadatak 3. Usporedte dobivene SHA-1 *hash* vrijednosti iz 1. i 2. primjera. Što zaključujete?

_____

_____

Zadatak 4. U aplikaciji *CrypTool* 1.4 za proizvoljnu ulaznu poruku duljine oko 500 znakova izračunajte tražene MD *hash* vrijednosti odabirom izbornika individualnih procedura (*Indiv. Procedures*), a zatim *hash* (*Hash*), te ih upišite u heksadecimalnom obliku.

a) MD2: _____

b) MD4: _____

c) MD5: _____

Zadatak 5. Obrišite prvu riječ u originalnom tekstu poruke i izračunajte MD *hash* vrijednosti te ih usporedite sa zapisima iz prethodnog primjera. Što zaključujete?

_____

_____

Zadatak 6. U aplikaciji *CrypTool* 1.4 za proizvoljnu ulaznu poruku duljine oko 500 znakova izračunajte traženu RC *hash* vrijednost prema sljedećem. Iz izbornika odaberite opciju za šifriranje/dešifriranje (*Encrypt/Decript*) i zatim opciju za simetrično šifriranje (*Symmetric (modern)*) uz zadanu duljnu ključa. Zatim provedite postupak napada grubom silom (*brute-force attack*) na šifrirani tekst tako što ćete iz izbornika za analiziranje (*Analysis*) odabrati opciju za simetrično šifriranje (*Symmetric (modern)*) uz primjenu ključa iste duljine kakav je korišten pri šifriranju. Navedite vrijeme potrebno za određivanje originalnog teksta.

a) RC2 (24-bitni ključ): _____

b) RC2 (32-bitni ključ): _____

c) RC4 (24-bitni ključ): _____

d) RC4 (32-bitni ključ): _____

Zadatak 7. Usporedite međusobno vremena potrebna za dešifriranje poruke šifrirane uz primjenu RC2 i RC4 *hash* funkcija, pri primjeni ključeva jednake duljine.

_____

_____

Zadatak 8. Grafički prikažite blok shemu za generiranje RC2 *hash* vrijednosti prikazanu u aplikaciji *CrypTool* 2.1.

Zadatak 9. Na temelju prikazane sheme objasnite princip rada kriptografske RC2 *hash* funkcije.

_____

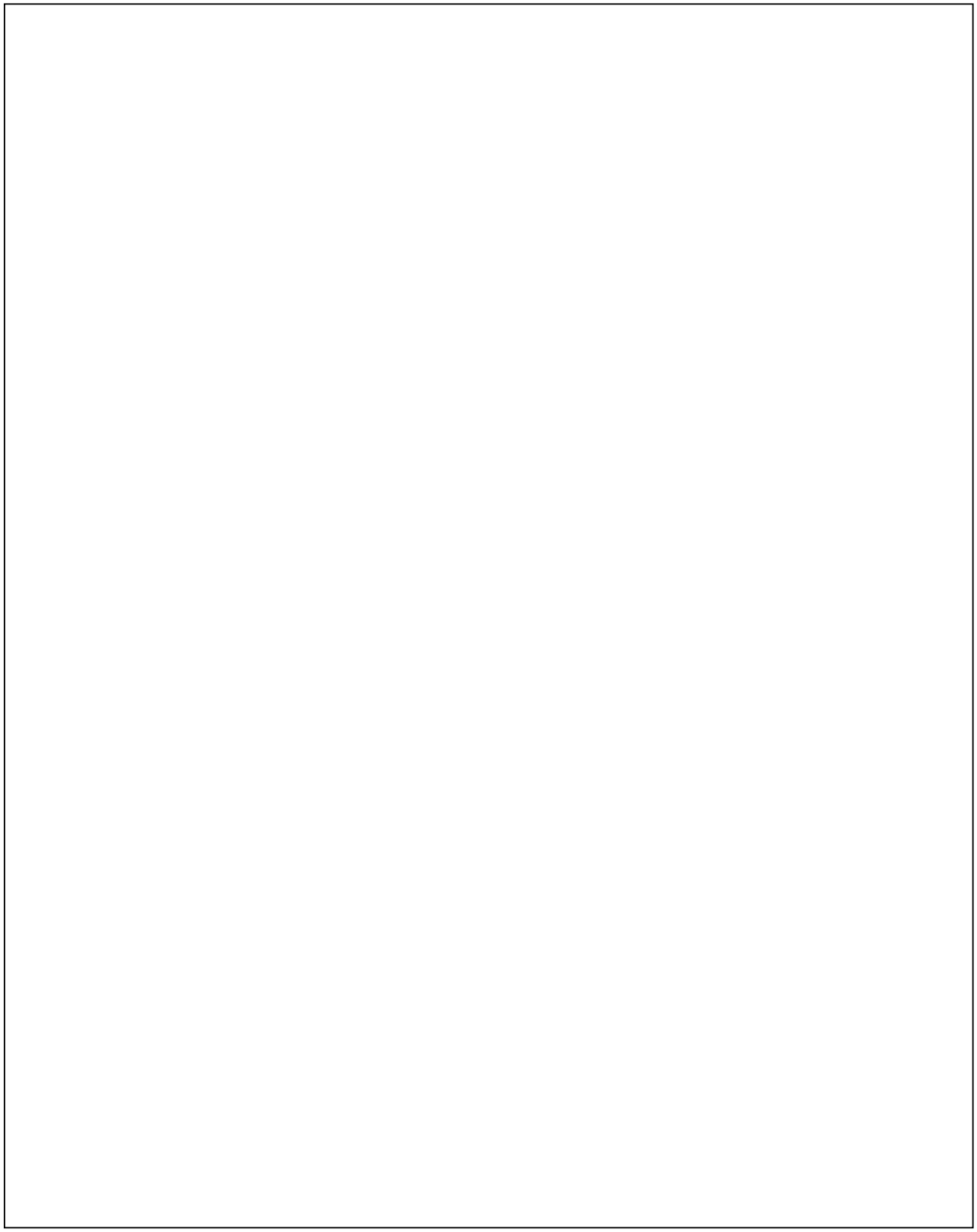
_____

_____

_____

_____

Zadatak 10. Grafički prikažite blok shemu za generiranje RC4 *hash* vrijednosti prikazanu u aplikaciji *CrypTool* 2.1.



Vježba 12. - Kriptosustavi s javnim ključem: DSA algoritam

UVOD

Iako se neki kriptosustavi s javnim ključem, poput RSA, mogu izravno koristiti za potpisivanje poruke, u praktičnoj primjeni se za digitalni potpis najčešće koriste algoritmi dizajnirani isključivo u tu svrhu. Njih se ne može koristiti za šifriranje ili razmjenu ključeva iako se temelje na tehnici javnog ključa.

Jedan od najpoznatijih algoritama koji se koristi isključivo za digitalni potpis je DSA (*Digital Signature Algorithm*). DSA pristup koristi *hash* funkciju, tj. SHA algoritam. *Hash* kod predstavlja ulaz u funkciju digitalnog potpisa, zajedno sa slučajnim brojem, *k*, generiranim samo za taj potpis.
Funkcija potpisa ovisi o:

- pošiljateljevom privatnom ključu (PR_a) i
- globalnom javnom ključu (PU_G).

Rezultat je digitalni potpis koji se sastoji od dva dijela, označena sa *s* i *r*.

Na prijemnoj strani generira se *hash* kod pristigle poruke. Ovaj kod zajedno sa potpisom ulazni je parametar funkcije za verifikaciju koja ovisi o:

- globalnom javnom ključu (PU_G) i
- pošiljateljevom javnom ključu (PU_a) koji je uparen sa pošiljateljevim privatnim ključem (PR_a)

Izlaz iz verifikacijske funkcije je vrijednost jednaka *r* komponenti potpisa (ukoliko je potpis valjan).

DSA algoritam

Algoritam se sastoji od tri koraka:

A) Stvaranje ključeva:

1. odabir 160-bitnog prostog broja q
2. odabir L-bitnog prostog broja p tako da vrijedi: $p = qz + 1$ za neki cijeli broj z,

   $512 \leq L \leq 1024$, L djeljivo s 64
3. odabir h takvog da vrijedi: $1 < h < p - 1$, $g = h^z \bmod p > 1$
4. stvaranje nasumičnog broja x, tako da vrijedi: $0 < x < q$
5. izračun $y = g^x \bmod p$
6. (p, q, g, y) je javni ključ, a x je privatni ključ.

B) Potpisivanja poruke:

1. stvaranje nasumičnog broja k, tako da vrijedi: $0 < k < q$
2. izračun $r = (g^k \bmod p) \bmod q$
3. izračun $s = (k^{-1}(\text{SHA-1}(m) + xr)) \bmod q$, gdje je SHA-1($m$) tzv. hash funkcija primijenjena na poruci m
4. ponoviti postupak ako je $r = 0$ ili $s = 0$
5. potpis je (r, s).

C) Provjera vjerodostojnosti potpisa:

1. ako $0 < r < q$ ili $0 < s < q$ nije zadovoljeno potpis se smatra neispravnim
2. izračun $w = s^{-1} \bmod q$
3. izračun $u_1 = (\text{SHA-1}(m)w) \bmod q$
4. izračun $u_2 = (rw) \bmod q$
5. izračun $v = ((g^{u1}y^{u2}) \bmod p) \bmod q$
6. potpis je valjan ako vrijedi $v = r$.

Dakle, postoje tri javna parametra (p, q, g) koji mogu biti zajednički za grupu korisnika. Bira se:

- prosti broj q (N-bitni)
- prosti broj p (duljine između 512 i 1024 bita, takav da dijeli (p-1))
- broj g (veći od 1, u obliku: $h(p-1)/q \bmod p$, gdje je h cijeli broj između 1 i (p-1)).

Svaki korisnik bira privatni ključ i generira javni ključ:

- privatni ključ x (treba biti broj između 1 i (q-1) i treba biti izabran slučajnim odabirom)
- javni ključ y (izračunava se iz privatnog kao: $y = g^x \bmod p$).

Iako je izračunavanje y uz poznati x je relativno jednostavno, u razumnom vremenu nije moguće izračunati x iz poznatog y.

Kako bi kreirao potpis, pošiljatelj izračunava vrijednosti r i s, kao funkcije javnih komponenti (p, q, g) i svojeg privatnog ključa (x). Pošiljatelj izračunava *hash* vrijednost poruke $H(M)$ i dodatno generira pseudoslučajni cijeli broj k (koji treba biti jedinstven za svako potpisivanje).

Primatelj izračunava v kao funkciju javnih varijabli (p, q, g), pošiljateljevog javnog ključa y i *hash* koda.

Potpis je valjan ukoliko se dobivena vrijednost podudara s r komponentom digitalnog potpisa.

ZADACI

Uvodne upute:

U svrhu analize DSA algoritma, u vježbi je potrebno koristiti aplikaciju *CrypTool*, alat namijenjen proučavanju različitih klasičnih, simetričnih, asimetričnih kriptografskih sustava i metoda njihove kriptoanalize.

DSA algoritam *(Digital Signature Algorithm)*

Zadatak 1. Za zadane parametre DSA algoritma $q = 199$, $h = 3$ i $z = 4$, izračunajte sve preostale potrebne parametre javnog ključa:

p: _____

g: _____

y: _____

Zadatak 2 Aplikacija *CrypTool* omogućuje analizu DSA algoritma pri kreiranju digtalnog potpisa. Nakon pokretanja aplikacije *CrypTool* 1.4 iz izbornika digitalnog potpisivanja (*Digital Signatures/PKI*) odaberite opciju infrastrukture javnih ključeva (*Public Key Infrastructure*, skr. *PKI*) te zatim opciju za generiranje/uvoz ključeva (*Generate/Import Keys*...). Nakon odabira DSA algoritma, unesite sljedeće podatke:

Prezime *(Last name)*: _____

Ime *(First name)*: _____

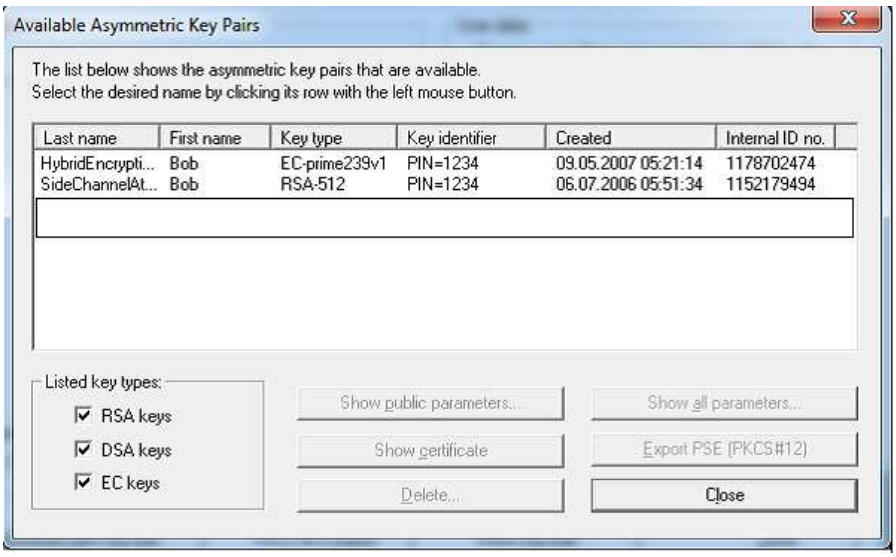
Identifikator ključa (*Key identifier*): _____

PIN kod (*PIN code*) (npr. *cryptool*): _____

PIN (*PIN*) (npr. *cryptool*): _____

Kliknite na opciju za generiranje novog para ključeva (*Generate new key pair*). U prozoru koji se pojavi odaberite opciju *OK*.

Zadatak 3. Kliknite na opciju za prikaz para ključeva (*Show Key Pair*) te u predviđeni prostor (u okvir) na donjoj slici upišite prikazanu kombinaciju oznaka.



Slika 12.2. *Prikaz podataka o generiranom digitalnom potpisu*

Zadatak 4. Odaberite opciju za prikaz certifikata (*Show certificate*). Navedite što se sve od podataka nalazi u prikazanom prozoru.

_____

_____

_____

Zatvorite oba prozora, za certificiranje podataka (*Certificate Data*) i za prikaz dostupnih asimetričnih parova ključeva (*Available Asymmetric Key Pairs*).

Zadatak 5. Za potpisivanje početnog dokumenta *startingexample-en.txt*, iz izbornika digitalnog potpisivanja (*Digital Signatures/PKI*) odaberite opciju za potpisivanje dokumenta (*Sign Document*). Odaberite sljedeće postavke:

Odabir *hash* funkcije (*Choose hash function*): SHA-1
Odabir algoritma za potpisivanje (*Choose signature algorithm*): DSA

U izbornik za izbor ključa za potpisivanje (*Choose a key/PSE to be used when signing*) unesite isti unos koji ste prethodno upisali za identifikator ključa (*Key identifier*), a za PIN kod (*PIN code*) upišite prethodno odabrani. Kliknite na opciju potpisivanja (*Sign*).

Nakon potvrde (*OK*) zatvara se prozor i prikazuje potpisani dokument. Navedite na kojem se mjestu nalazi digitalni potpis u prikazanom dokumentu u odnosu na tekst samog dokumenta.

_____

Zadatak 6. Navedite što se sve od informacija nalazi uz digitalni potpis.

_____

_____

Pregledniji prikaz na kojem se jasno vidi podjela između digitalnog potpisa i teksta dokumenta moguće je dobiti preko izbornika digitalnog potpisivanja (*Digital Signature/PKI*) te izborom opcije za izvod potpisa (*Extract Signature*).

Zadatak 7. Iz izbornika digitalnog potpisivanja (*Digital Signature/PKI*) odaberite opciju za verificiranje potpisa (*Verify Signature*) kako biste provjerili da dokument nije izmijenjen. Potrebno je selektirati kreirani potpis s popisa i kliknuti na opciju za verifikaciju potpisa (*Verify signature button*). Navedite poruku koja je ispisana u prikazanom okviru:

_____

_____

Zadatak 8. Izmijenite sadržaj potpisanog dokumenta brisanjem prve riječi iz prikazanog teksta. Iz izbornika digitalnog potpisivanja (*Digital Signature/PKI*) odaberite opciju za verificiranje potpisa (*Verify Signature*). Navedite poruku koja je ispisana u prikazanom okviru:

_____

_____

Vježba 13. - Autentifikacija poruka unutar sigurnosne arhitekture vozila: MAC i HMAC

UVOD

Sigurnosna arhitektura vozila

Napadi na vozila mogu se podijeliti na logičke i fizičke. Logički napad može izvesti ili eksterni napadač ili interni napadač koji ima pristup samo logičkim sučeljima i eksternoj komunikaciji. Fizički napad može izvesti samo interni napadač, budući da zahtijeva izravan fizički pristup.

Logički napadi su napadi putem raspoloživih logičkih sučelja i eksterne komunikacije, te uključuju pasivne i aktivne metode. U skupinu logičkih napada ubrajaju se: kriptografski napadi, softverski napadi i komunikacijski napadi.

- Kriptografski napad (kriptoanaliza) pokušava probiti sigurnosne mjere IT sustava kroz dva moguća pristupa: zlouporabom postojećeg propusta u kriptografskom algoritmu koji se primjenjuje te pokušajima otkrivanja ključa i sadržaja „grubom silom" *(brute force)* – pogađanjem (sistematskim pretraživanjem svih mogućih ključeva).
- Softverski napad podrazumijeva sve napade koji pokušavaju iskoristiti postojeća softverska sučelja i funkcionalnosti (na način za koji nisu izvorno namijenjeni).
- Komunikacijski napadi podrazumijevaju sve aktivne i pasivne napade (eksterne i interne) na sve dostupne komunikacijske kanale. Pasivni napad podrazumijeva „prisluškivanje" komunikacije bez ometanja komunikacijskog postupka. Aktivni napad podrazumijeva sustavno presretanjei manipulaciju podacima, te umetanjenovih poruka.

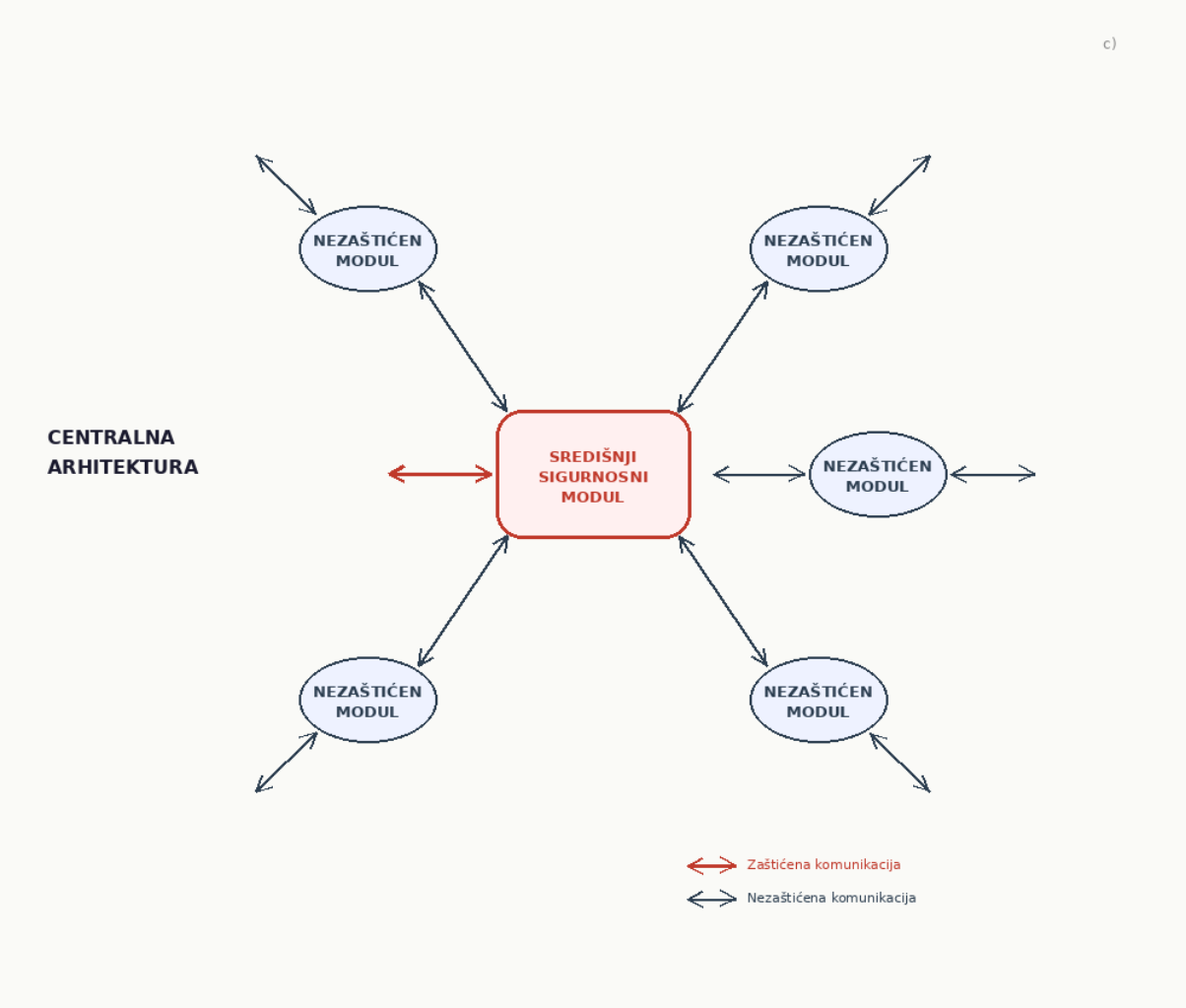
Fizički napadi podrazumijevaju izravan napad na hardver s ciljem pristupa internim (hardverski zaštićenim) podacima, onemogućavanje fizičkih sigurnosnih mjera kako bi se omogućili daljnji napadi te uvođenje fizičkih signala.

Sigurnosni moduli

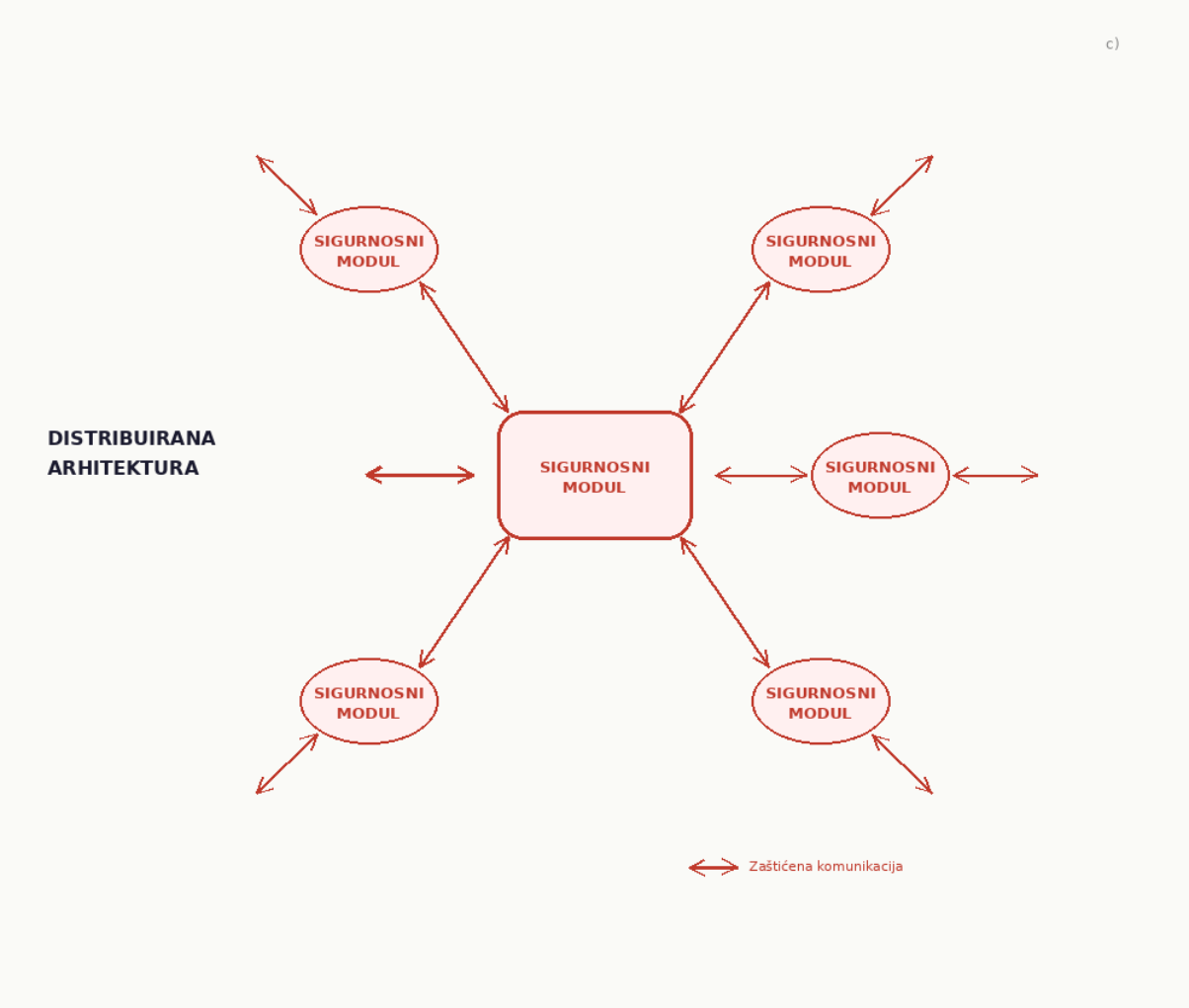
Sigurnosni modul može se postaviti na svaku sigurnosno-kritičnu komponentu u vozilu.

U vozilima se pojavljuju tri tipa sigurnosne arhitekture:
• centralna sigurnosna arhitektura (eng. *central security architecture*)
• distribuirana sigurnosna arhitektura (eng. *distributed security architecture*)
• djelomično distribuirana arhitektura (eng. *semi-central architecture*).

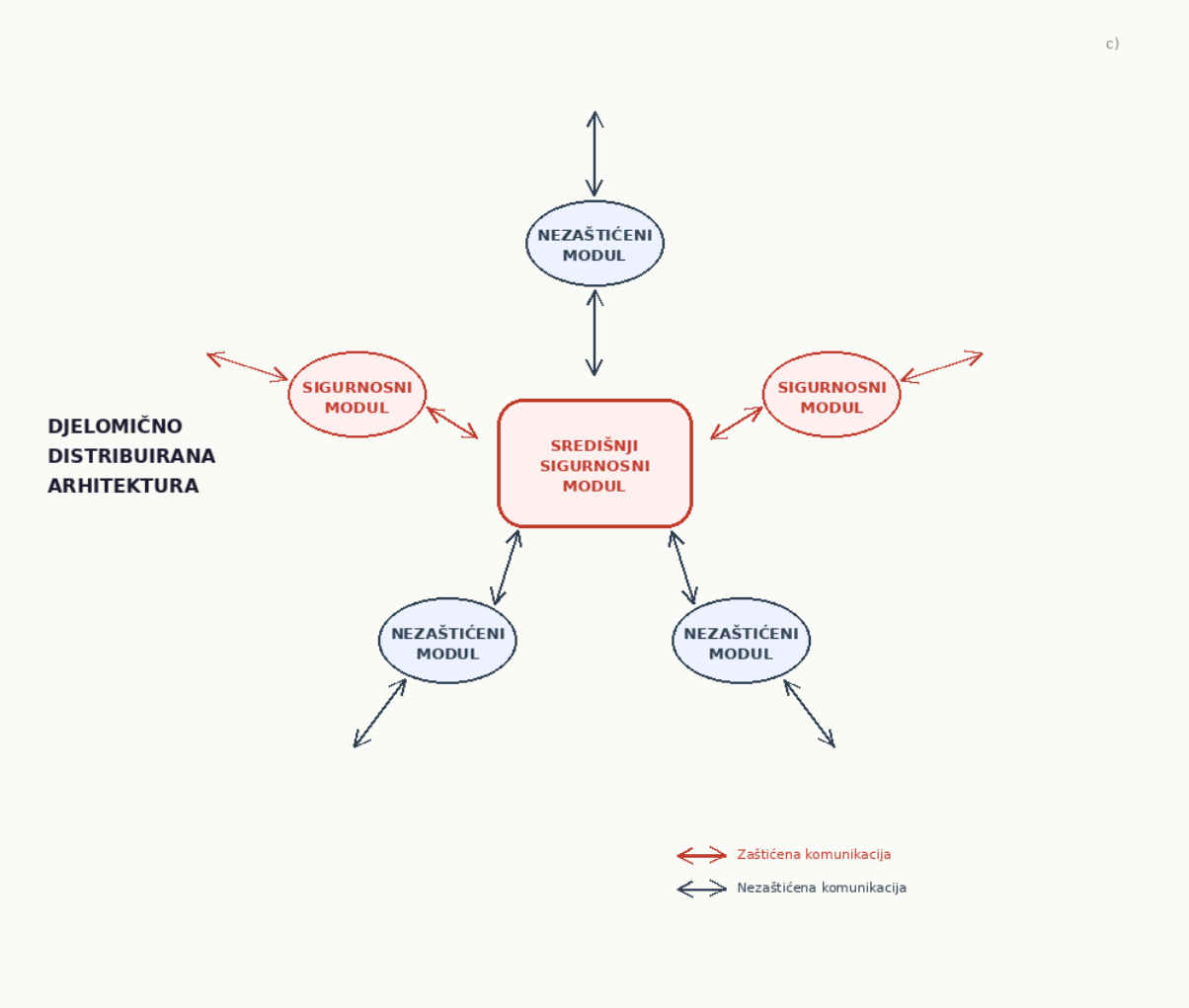
Kod centralne sigurnosne arhitekture jedan središnji sigurnosni modul pruža sigurnosne usluge za sve interne i eksterne kontrolere i uređaje u vozilu. Ovaj modul može biti implementiran odvojeno, ali u idealnom slučaju on predstavlja dio središnje upravljačke jedinice ili neke druge jedinice koja implementira aplikacije koje zahtijevaju zaštitu. Ostale jedinice također mogu koristiti usluge središnjeg sigurnosnog modula (npr. za potrebe uspostave i upravljanja ključevima, zaštićenu pohranu i međusobnu autentifikaciju).



a) *Centralna sigurnosna arhitektura u vozilu*



b) *Distribuirana sigurnosna arhitektura u vozilu*



c) *Djelomično distribuirana sigurnosna arhitektura u vozilu*

Slika 13.1. *Sigurnosne arhitekture u vozilu*

Kod distribuirane sigurnosne arhitekture svi uključeni uređaji i kontroleri implementiraju dio od ukupne sigurnosne funkcionalnosti. Moguća su dva pristupa:
• arhitektura koja se oslanja na nekoliko potpuno funkcionalnih i zaštićenih sigurnosnih modula
• arhitektura koja se temelji na obaveznoj kolaboraciji više uređaja kako bi se omogućila određena sigurnosna funkcionalnost.

Djelomično distribuirana sigurnosna arhitektura predstavlja kombinaciju centralne i distribuirane sigurnosne arhitekture. Ona se oslanja na središnji potpuno funkcionalni sigurnosni modul, ali dodatno koristi i nekoliko odvojenih modula sa nekim autonomnim sigurnosnim funkcijama (npr. za kritične senzore i aktuatore). Dodatni kontroleri implementiraju samo jedan dio sigurnosnih funkcionalnosti, dok se za preostale oslanjaju na središnji modul.

Sigurnosni modul predstavlja specijalizirani kriptografski mikrokontroler na siguran način povezan sa hardverom vozila kojeg treba štititi. Sigurnosni modul također je zaštićen mjerama fizičke sigurnosti. On na siguran način omogućava različite sigurnosno-kritične usluge: kriptografske operacije (šifriranje, dešifriranje, kreiranje *hash*-a), siguran tajmer, generiranje slučajnih brojeva, osiguranje komunikacije i pohrane.

Sigurnosni modul može se realizirati softverski ili korištenjem standardnog sigurnosnog kontrolera (eng. *Trusted Platform Module*, skr. TPM). Moguća su i druga rješenja temeljena na integriranom krugu specifičnom za primjenu (eng. *Application-Specific Integrated Circuit*, skr. ASIC) ili programabilnom logičkom nizu (eng. *Field-Programmable Gate Array*, skr. FPGA).

TPM modul (eng. *Trusted Platform Module*)

TPM modul je razvijen od strane konzorcija *Trusted Computing Group*, skr. TCG. Standardiziran je pod oznakom ISO/IEC 11889.

Pruža sljedeće usluge:

- hardverski generator slučajnih brojeva (eng. *Random Number Generator*, skr. RNG)
- kriptografski pogon (eng. *engine*) za šifriranje i potpisivanje: RSA
- kriptografske *hash* funkcije: SHA-1, HMAC
- memorija samo za čitanje (eng. *Read Only Memory*, skr. ROM) za programirani softver, tj. firmver (eng. *firmware*) i certifikate
- električno izbrisiva programabilna memorija samo za čitanje (eng. *Electrically Erasable Programmable Read-Only Memory*, skr. EEPROM) za interne ključeve.

Slika 13.2. *Prikaz usluga koje omogućuje TPM modul*

Ad Hoc mreža za vozila (eng. *Vehicular Ad hoc NETwork*, skr. **VANET**)

VANET mreža predstavlja posebnu vrstu bežične *ad hoc* mreže (*Mobile Ad hoc NETwork*, skr. MANET) u kojoj vozila predstavljaju pokretne čvorove. Zbog određenih specifičnosti VANET mreža klasični sigurnosni mehanizmi iz MANET mreža nisu izravno primjenjivi. U VANET mrežama susreću se dva tipa komunikacije:

- **komunikacija između vozila** (eng. *vehicle to vehicle*, **V2V**)
- **komunikacija vozila sa infrastrukturom** (eng. *vehicle to infrastructure,* **V2I**)

Jedinica koja ostvaruje komunikaciju na strani vozila (eng. *On Board Unit*, skr. OBU) koristi se za elektroničku naplatu cestarine i pametne prometne sustave, a jedinica na strani infrastrukture (eng. *Road Side Unit*, skr. RSU) koristi se za bežičnu razmjenu podataka između infrastrukture i vozila.

Sigurnosni ciljevi

• **Autentifikacija** (eng. *authenticity*):
podrazumijeva mogućnost provjere porijekla podataka (poruka, programa) i komponenti (hardver, firmver) u vozilu.
• **Povjerljivost** (eng. *confidentiality*):
podrazumijeva sprečavanje neautoriziranog pristupa zaštićenim i privatnim podacima
• **Integritet** (eng. *integrity*):
podrazumijeva sprečavanje neautorizirane modifikacije podataka
• **Dostupnost** (*eng. availability*):
podrazumijeva osiguranje da autorizirani korisnik uvijek ima pristup podacima i usluzi

Autentifikacija poruka

Autentifikacija poruke predstavlja proceduru koja omogućuje provjeru dolazi li primljena poruka doista od navedenog pošiljatelja, te je li poruka izmijenjena prilikom prijenosa. Mehanizmi autentifikacije poruke (i digitalnog potpisa) sastoje se od:
1. funkcije koja proizvodi autentifikator
2. protokola koji omogućuje verifikaciju autentifikatora na prijemniku.

Funkcije autentifikacije poruke

• ***Hash*** **funkcije:**
- funkcije koje mapiraju poruku proizvoljne duljine na jednu vrijednost (*hash*) koja je fiksne duljine i služi kao autentifikator;
• **Šifrati poruke:**
- šifrat cijele poruke služi kao njezin autentifikator;
• **Kodovi za autentifikaciju poruke (MAC kod):**
- MAC kod (*Message Authentication Code*) je funkcija poruke i tajnog ključa koja daje vrijednost fiksne duljine koja služi kao autentifikator.

MAC kodovi

• MAC kod se naziva i kriptografskom kontrolnom sumom (eng. *cryptographic checksum*).
• Sudionici u komunikaciji dijele zajednički tajni ključ.
• MAC kod izračunava se kao funkcija poruke i ključa:

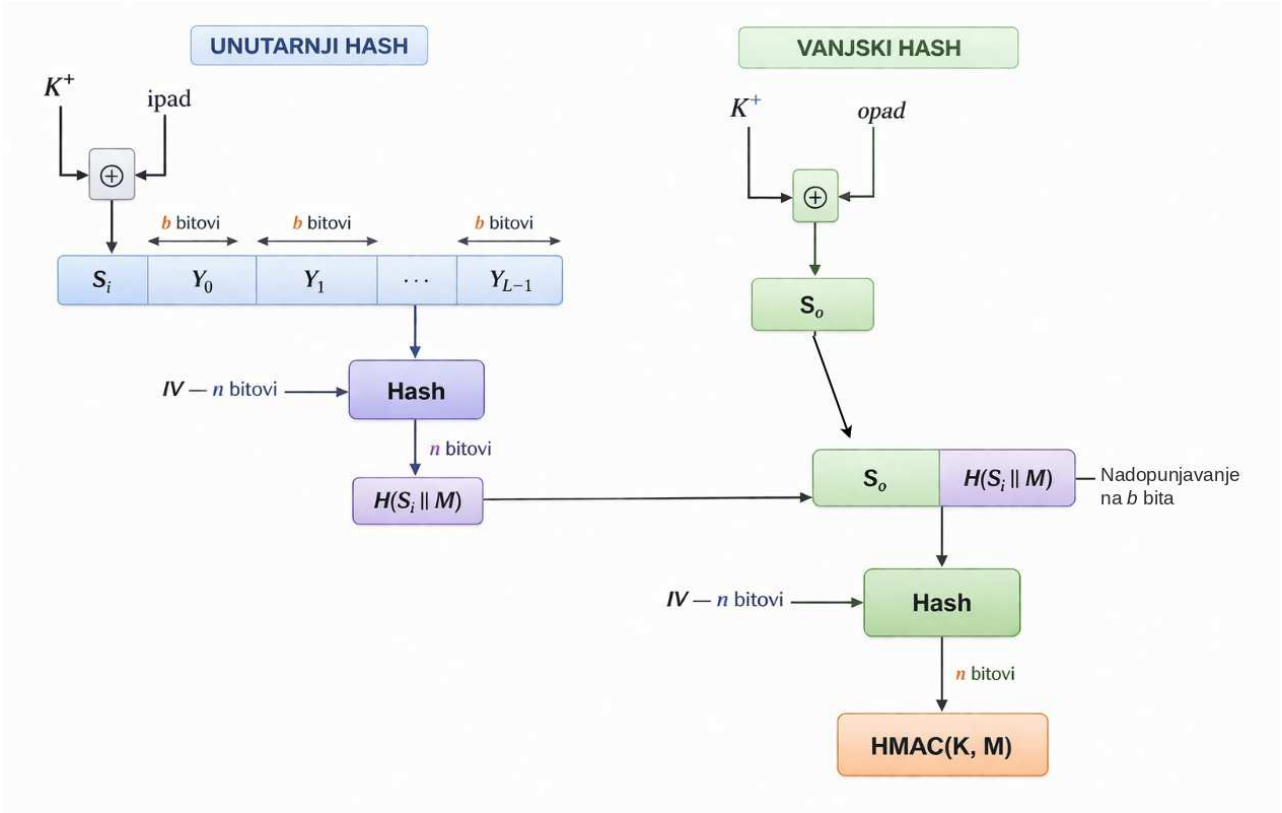
$$\boldsymbol{MAC}=\boldsymbol{C}(\boldsymbol{K},\boldsymbol{M})$$

gdje je: *M* - ulazna poruka
C - MAC funkcija
K - zajednički tajni ključ
MAC - kriptografska kontrolna suma

Poruka i MAC kod se šalju primatelju. Za primljenu poruku primatelj izračunava MAC kod (pomoću istog tajnog ključa), te uspoređuje izračunatu i primljenu vrijednost. Ukoliko se ove dvije vrijednosti razlikuju, primatelj zna da je poruka, ili sama hash vrijednost, pri prijenosu promijenjena.

HMAC

Jedna od najraširenijih MAC shema je HMAC (*Hash-based Message Authentication Code*), koja se temelji na proizvoljnoj *hash* funkciji.



Slika 13.3. *Prikaz rada HMAC algoritma*

HMAC je definiran sljedećim izrazom:

$$\text{HMAC}(K, M) = \text{H}[(K^+ \oplus \text{opad}) \parallel \text{H}[(K^+ \oplus \text{ipad}) \parallel M]]$$

Pri čemu je:

$$\text{ipad} = 00110110$$
$$\text{opad} = 01011100$$

ZADACI

Uvodne upute:

U svrhu analize HMAC sheme, u vježbi je potrebno koristiti aplikaciju *CrypTool*, alat namijenjen proučavanju različitih klasičnih, simetričnih, asimetričnih kriptografskih sustava i metoda njihove kriptoanalize.

HMAC *(Hash-based Message Authentication Code)*

Zadatak 1. Definirajte oznake navedene na shemi HMAC algoritma prikazanog na slici 13.4.

H: _____

IV: _____

M: _____

Y_i: _____

L: _____

b: _____

n: _____

K: _____

K^+: _____

Zadatak 2. Grafički prikažite blok shemu za generiranje HMAC-MD5 autentifikacijskog koda prikazanu u aplikaciji *CrypTool* 2.1.

Zadatak 3. Objasnite princip rada MD5 kriptografske *hash* funkcije i prikazanog sustava za generiranje HMAC-MD5 koda.

_____

_____

_____

_____

_____

_____

Zadatak 4. Uz proizvoljno izabrani ključ, generirajte HMAC-MD5 kod za ulaznu poruku koja se sastoji od osobnog imena i prezimena.

Ulazna poruka: _____

HMAC-MD5 (hex): _____

Ključ: _____

Zadatak 5. Kolika je duljina generiranog HMAC-MD5 koda?

_____

_____

Zadatak 6. Unutar kojeg sigurnosnog modula u VANET-u se koriste *hash* i HMAC sheme?

_____

_____

Vježba 14. - Kriptografske hash funkcije

Hash-funkcije su funkcije koje za ulaznu poruku daju šifriranu poruku uglavnom fiksne duljine. Preciznije rečeno, hash-funkcija pridružuje nizovima znakova proizvoljne konačne duljine nizove znakova fiksne duljine, od npr. *n* bita. Osnovna ideja hash-funkcija je da hash služi kao kompaktna reprezentativna slika (digitalni otisak) ulazne vrijednosti koji se ne može dobiti pomoću neke druge ulazne vrijednosti.

Na najvišoj razini, hash-funkcije se dijele u dvije klase: hash funkcije bez ključa koje za ulazni parameta imaju samo poruku i hash funkcije s ključem koje za ulaz imaju poruku i tajni ključ.

Zadatak 1. *CRC (Cyclic Redundancy Check)*

- U aplikaciji *CrypTool* realizirati sustav za generiranje koda za cikličku provjeru redundancije.
- Ucrtati i objasniti sustav za generiranje CRC vrijednosti.

- Pomoću prethodno kreiranog sustava za generiranje CRC-a za vlastito ime i prezime kao ulaznu poruku (npr. „PETAR PETROVIC“) generirati sljedeće CRC vrijednosti (dobivene vrijednosti upisati u heksadekadskom obliku, te za svaki primjer upisati generatorski polinom u standardnom i u heksadekadskom obliku):

  a) CRC-24/OPENPGP

  Generatorski polinom (heksadekadski): _____

  Polinom (standardni oblik):
  _____

  CRC vrijednost (heksadekadski):
  _____

  b) CRC-32

  Generatorski polinom (heksadekadski): _____

  Polinom (standardni oblik):
  _____

  CRC vrijednost (heksadekadski):
  _____

  c) CRC-40/GSM

  Generatorski polinom (heksadekadski): _____

  Polinom (standardni oblik):
  _____

  CRC vrijednost (heksadekadski):
  _____

  d) CRC-64

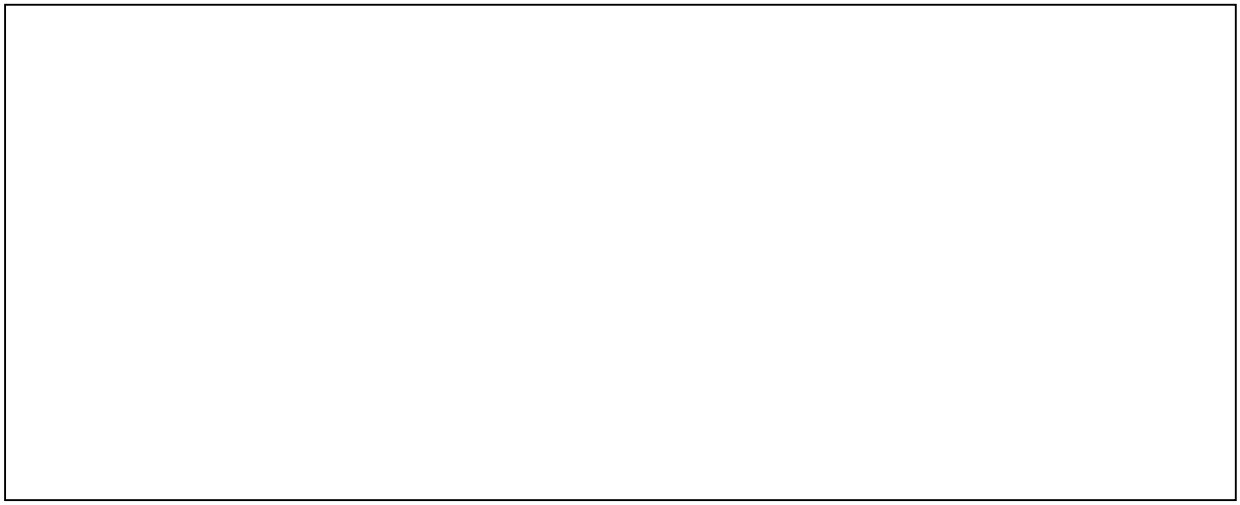
  Generatorski polinom (heksadekadski): _____

  Polinom (standardni oblik):
  _____

  CRC vrijednost (heksadekadski):
  _____

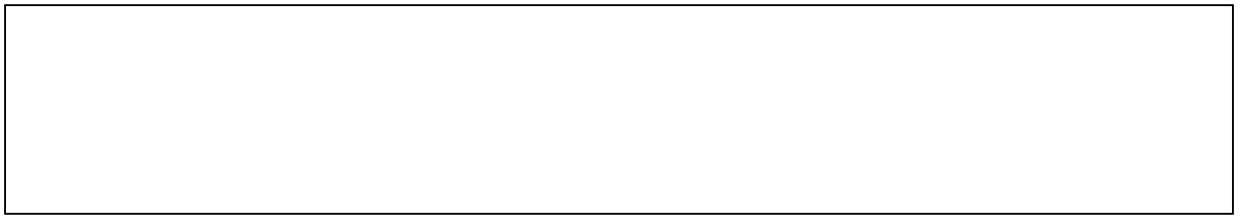
Zadatak 2. *Secure Hash*

- U aplikaciji *CrypTool* realizirati sustav za generiranje SHA kriptografske hash funkcije.
- Ucrtati i objasniti sustav za generiranje SHA hash vrijednosti.



- Za proizvoljnu ulaznu poruku (duljine 300-500 znakova) izračunati tražene hash vrijednosti, te ih upisati u heksadecimalnom obliku.

Ulazna poruka:



a) SHA-1:
_____

_____

b) SHA-256:
_____

_____

c) SHA-384:
_____

_____

d) SHA-512:
_____

_____

Zadatak 3. *HMAC*

- Istražiti i objasniti princip rada MD5 kriptografske hash funkcije.

- U aplikaciji *CrypTool* realizirati sustav za „ručno“ generiranje HMAC-MD5 autentifikacijskog koda.

- Ucrtati i objasniti sustav za generiranje HMAC-MD5 koda.

- Generirati HMAC-MD5 kod za vlastito ime i prezime kao ulaznu poruku, uz proizvoljno izabrani odgovarajući ključ.

  Ulazna poruka:

  _____

  HMAC-MD5 (hex):

  _____

  Ključ:

  _____

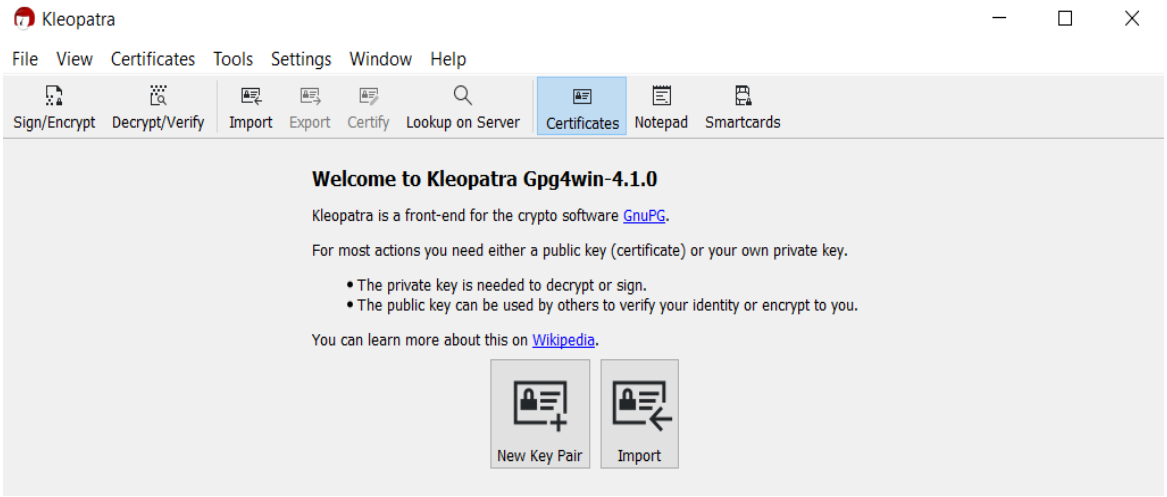
Vježba 15. - Upravljanje certifikatima i ključevima

UVOD

Za potrebe osiguranja komunikacije putem elektroničke pošte i enkripciju datoteka moguće je koristiti programski paket *Gpg4win* (*www.gpg4win.org*). Riječ je o besplatnom instalacijskom paketu za *MS Windows* platformu koji uključuje *GnuPG* enkripcijski softver, softver za upravljanje certifikatima, ekstenzije za *Windows Explorer* i *MS Outlook*, kao i prateću dokumentaciju. *GnuPG* je besplatan softver otvorenog koda, svakome dostupan za privatnu ili komercijalnu uporabu. Temeljen je na međunarodnom standardu *OpenPGP* (RFC 4880), koji je u potpunosti kompatibilan sa PGP (*Pretty Good Privacy*) te koriste istu infrastrukturu. Od verzije 2 *GnuPG* podržava i kriptografski standard S/MIME (IETF RFC 3851, ITU-T X.509 i ISIS-MTT/Common PKI).

Zadatak 1. *Kreiranje certifikata (ključeva)*

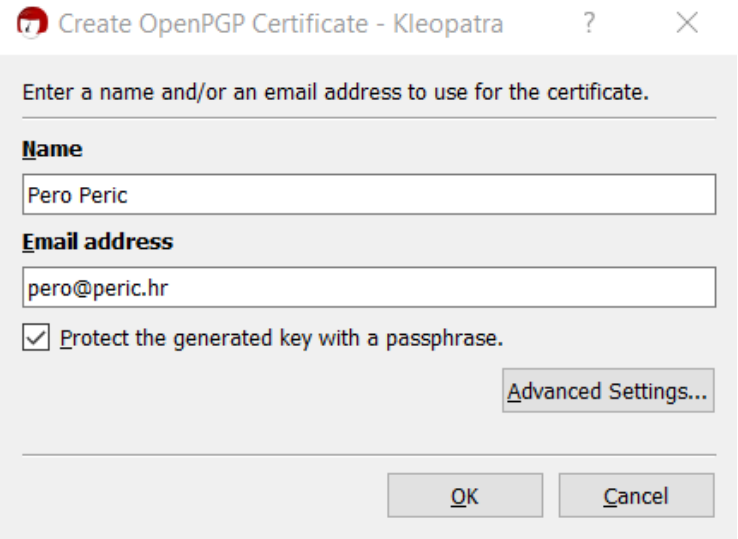
- Unutar paketa *Gpg4win* za upravljanje certifikatima i ključevima koristi se aplikacija *Kleopatra* prikazana na slici.



Slika 15.1. *Prikaz glavnog sučelja Kleopatra aplikacije*

- Iz izbornika *File* izabrati opciju *New OpenPGP Key Pair.…*

- U sljedećem dijaloškom okviru (slika 15.2.) unesite tražene podatke (ime i prezime, e-mail). Budući da su ovi podaci javno vidljivi, za potrebe vježbe **ne treba unositi stvarne podatke**, već neke izmišljene!

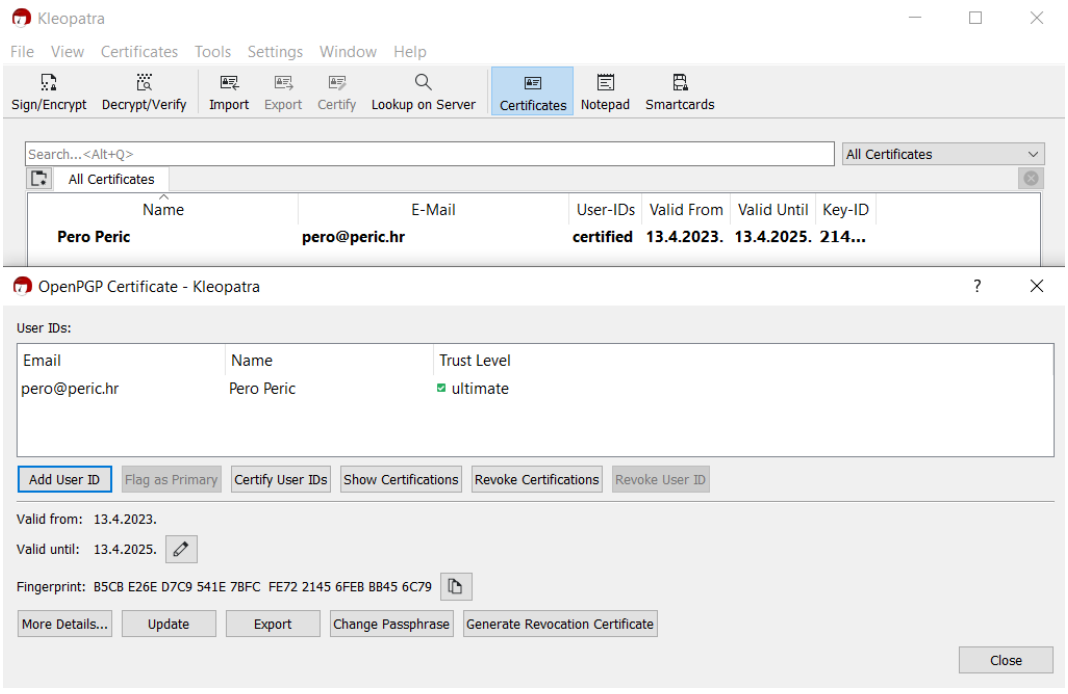


Slika 15.2. *Kreiranje OpenPGP certifikata*

- Ukoliko uključite opciju zaštite generiranog ključa uz primjenu lozinke (*Protect the generated key with a passphrase*) ključ ćete moći dodatno zaštititi proizvoljno izabranom lozinkom *(passphrase)*. Lozinku će biti potrebno potvrditi još jednim unosom.

- Ukoliko je par ključeva (privatni i javni ključ) uspješno kreiran, pojavit će se poruka o uspješnom kreiranju certifikata i bit će naveden njegov „otisak prsta“ *(fingerprint)*.

- Kreirani certifikat bit će sada vidljiv i u glavnom sučelju programa *Kleopatra* (unutar kartice *Certificates*).



Slika 15.3. *Prikaz kreiranog certifikata u glavnom sučelju Kleopatra aplikacije*

- Pogledati detalje o kreiranom certifikatu - dvostruko kliknuti na certifikat ili odabrati desni klik + opciju detalji (*Details*).

- Prepisati detalje o kreiranom certifikatu te ih prokomentirati:

Zadatak 2. *Razmjena javnog certifikata (javnog ključa)*

Javni certifikat (ključ) može se distribuirati na više načina: slanjem e-mailom, objavom na *OpenPGP* poslužitelju ili osobnim web stranicama, osobnom isporukom (npr. na USB memoriji)... Za potrebe testiranja koristit će se robot elektroničke pošte *Adele*, kojemu se šalje vlastiti javni certifikat. Koristeći vlastiti javni ključ *Adele* šalje enkriptiranu elektroničku poruku, zajedno sa javnim certifikatom.

- U programu *Kleopatra* potrebno je izabrati ranije kreirani certifikat i potom opciju za izvoz datoteke (*File → Export...*)

- Potrebno je spremiti javni certifikat pod proizvoljnim imenom, ali obavezno sa ekstenzijom *.asc* kako bi se certifikat spremio u tekstualnom obliku, te kako bi ga se kasnije moglo vidjeti pomoću tekst editora.

- Potrebno je pregledati spremljeni certifikat pomoću nekog tekst editora, te upisati vlastita zapažanja i komentare:

- Javni certifikat moguće je poslati kao tekst unutar tijela e-mail poruke (kopirati ga i zalijepiti) ili kao privitak elektroničke poruke.

- Potrebno je poslati vlastiti javni certifikat e-mail robotu *Adele* na: *adele-en@gnupp.de* ili *adele@gnupp.de*. Također, potrebno je razmijeniti vlastiti javni certifikat sa kolegom putem elektroničke pošte. Unijeti vlastita zapažanja i komentare:

Zadatak 3. *Pohrana i autentifikacija javnog certifikata*

- Primljeni javni certifikat potrebno je importirati u program *Kleopatra* izborom opcije uvoza datoteke (*File → Import...*) nakon čega treba izabrati datoteku *.asc* u koju je pohranjen certifikat. Ukoliko je certifikat primljen unutar tekstualnog dijela elektroničke poruke, potrebno ga je pomoću tekst editora te kopiranja i lijepljenja pohraniti kao *.asc* datoteku (prije importa).

- Po primitku certifikata potrebno je provesti njegovu autentifikaciju (pomoću *fingerprint* oznake), odabirom opcije za provjeru certifikata (*Certificates → Certify...*).

- Upisati vlastita zapažanja i komentare:

Zadatak 4. *Enkripcija i dekripcija datoteka*

- *Gpg4win* se osim za enkripciju i potpisivanje elektroničkih poruka može koristiti i za enkripciju i potpisivanje bilo koje datoteke. Potpisivanje datoteke pomoću privatnog certifikata (ključa) osigurava da datoteka neće biti neovlašteno modificirana. Enkripcija datoteke pomoću privatnog certifikata (ključa) osigurava njezinu tajnost (može joj pristupiti samo osoba koja posjeduje pripadajući privatni ključ).

- Potrebno je izabrati proizvoljnu datoteku, te joj zaštititi integritet digitalnim potpisivanjem (*File → Sign/Encrypt…*), izabrati samo potpisivanje (datoteka s potpisom će dobiti ekstenziju *.sig*). Potrebno je pogledati potpis nekim tekst editorom.

- Potrebno je provjeriti integritet potpisane datoteke (dvostruki klik ili opcija *Decrypt/Verify…*) - potpis i izvorna datoteka moraju biti u istoj mapi. Potrebno je namjerno napraviti promjenu na izvornoj datoteci, pa ponovno provjeriti potpis.

- Upisati vlastita zapažanja i komentare:

- Potrebno je izaberati proizvoljnu datoteku, te je enkriptirajti. Pogledati enkriptiranu datoteku pomoću tekst editora.

- Razmijeniti s kolegom putem elektroničke pošte (kao privitak) enkriptiranu datoteku.

- Upisati vlastita zapažanja i komentare:

Vježba 16. - Kriptoanaliza

Kriptoanaliza predstavlja proučavanje metoda za saznavanje šifriranih informacija, bez posjedovanja tajnih podataka koji su obično potrebni da bi se pristupilo tim informacijama. Ovo obično podrazumijeva pronalaženje tajnog ključa.

Kriptoanaliza se također koristi da označi svaki pokušaj zaobilaženja drugih tipova kriptografskih algoritama i protokola uopće. Međutim, kriptoanaliza obično ne razmatra metode napada čija primarna meta nisu slabosti promatranog kriptografskog sustava i češće dovode do rezultata nego tradicionalna kriptoanaliza.

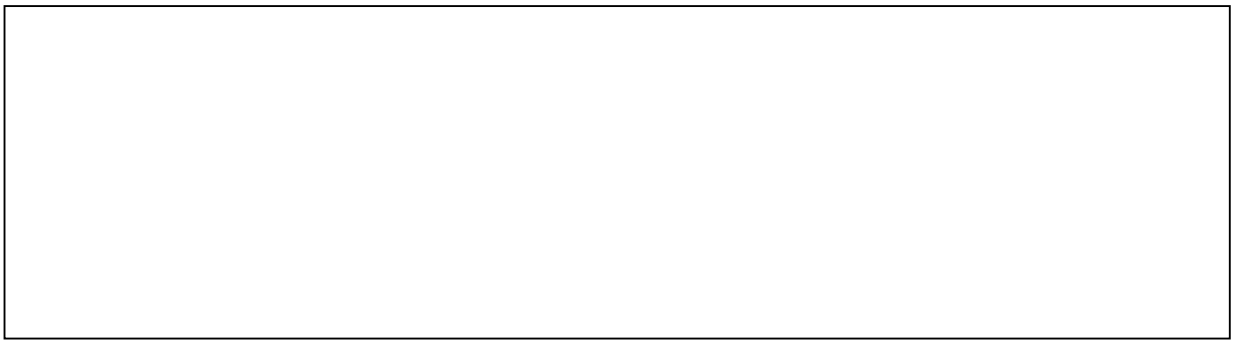
Zadatak 1. *Cezarova šifra*

- U aplikaciji *CrypTool* pomoću sustava za kriptoanalizu Cezarove šifre „grubom silom“ dekriptirati sljedeće šifrate:
  - UWRSJGNSKAXJS:
    _____
  - EGFGSTWUWVFSKMHKLALMUABS:
    _____
  - KVCVBFDLEZBRTZAV:
    _____
  - VASBEZNGVXN:
    _____

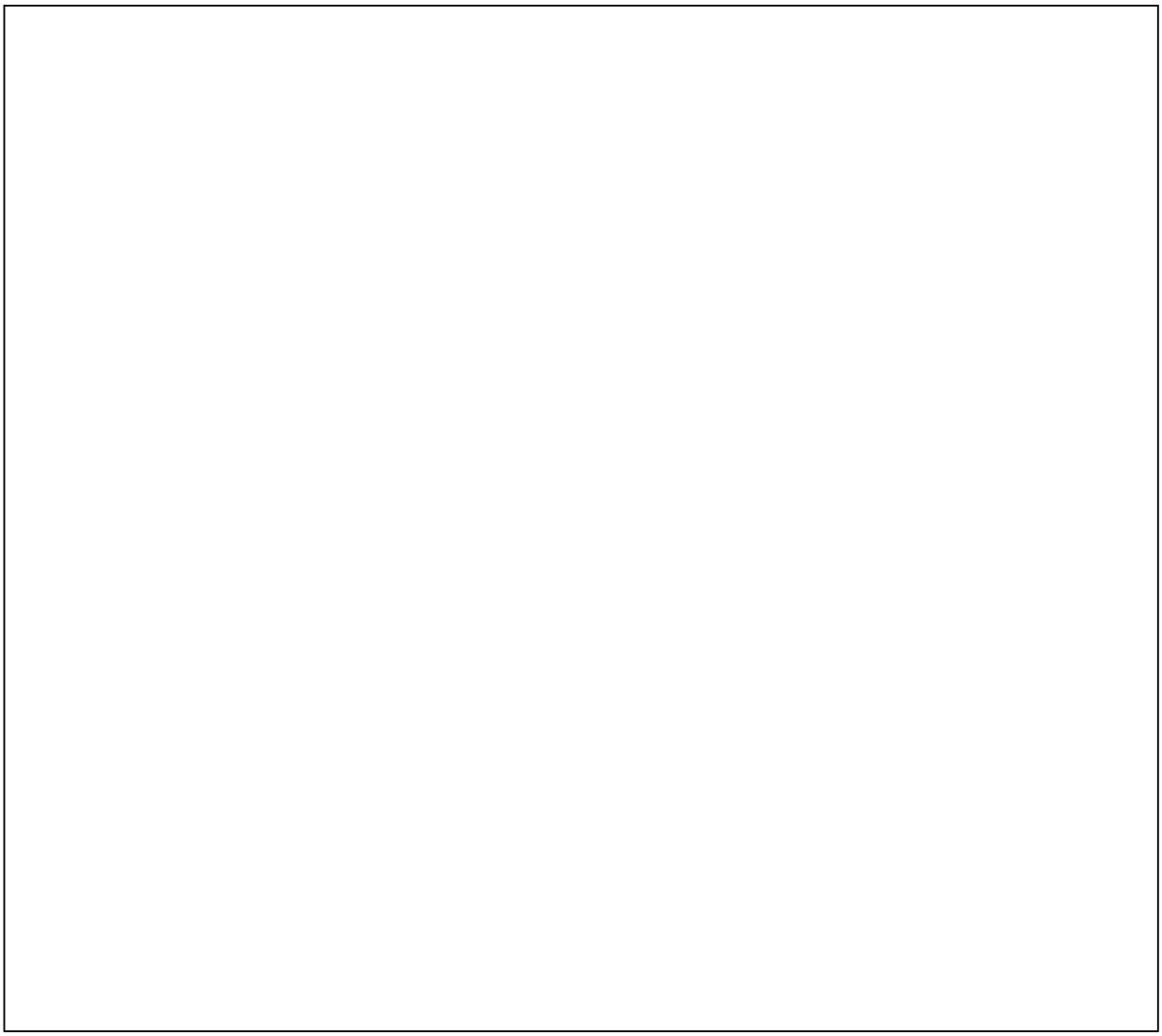
- Ucrtati i objasniti sustav za kriptoanalizu Cezarove šifre „grubom silom“:

- Pomoću sustava za kriptoanalizu Cezarove šifre „grubom silom“ dekriptirati sljedeći šifrat:

Aopz zhtwsl wlymvytz h iybal-mvyjl jpwolyalea-vusf haahjr vu aol Jhlzhy jpwoly. Aol ihzpj wypujpwsl pz aoha aol jpwolyalea pz kljyfwalk dpao hss wvzzpisl zopma chsblz huk mvy lhjo ylzbsapun wshpualea pa pz joljrlk pm pa jvuahpuz dvykz myvt h kpjapvuhyf. Pm zlclyhs dvykz hyl mvbuk pa jhu il hzzbtlk dpao opno wyvihipspaf aoha aopz pz aol jvyylja kljyfwapvu.



- Ucrtati i objasniti sustav za kriptoanalizu Cezarove šifre analizom frekvencija:



- Pomoću sustava za kriptoanalizu Cezarove šifre analizom frekvencija dekriptirati sljedeći šifrat:

Zxbpxo txp x mlifqfzfxk xka dbkboxi lc qeb ixqb Oljxk obmryifz, tel dobxqiv buqbkaba qeb Oljxk bjmfob ybclob pbfwfkd mltbo xka jxhfkd efjpbic afzqxqlo lc Oljb, mxsfkd qeb txv clo qeb fjmbofxi pvpqbj.

- U predviđeni prostor upisati vlastite zaključke, zapažanja i komentare:

Zadatak 2. *Vigenereova šifra*

- Dekriptirati sljedeći tekst, ako se zna da je šifriran Vigenereovom šifrom:

  Vpt mmiub llpc fwrbqvpbtk hvukgptkkwc vj r rwafecrppiikkk rptygz lhw wqzbbprvms ic Cgwc Iekvqhae Rnjtyxz czdbru 1467 cvs bwvf i blxrn kxwlvt lxzg kq alpxtj jtaavgv rptygz pstycjtaw. Rnjtyxz'u anzxvo wcsc jyqijlvf iawlrdmiz ewvmg zimgzps aftlh, hru uexagyga llvv kvspgrvms ic ntqiprx vpt sikvmg vj kjm rvvigaevrukvv hpgjiqlx zp bwl gzrptyxvzb. Ahxvt, qc 1508, Qsycvclw Ktqioidkch, pr yka lvvb Rwapkicxwpe, zpdtuxvf bwl xrdcah vvebp, h gikbxjec ewbwsegvi vj kjm Kpkvpèzt jmgjmg. Alv Vzxalvoqjz gzrpty, lfymklv, fptn wvfxqslh r rzdnvvuaxci, ikoxk eef xglhzebpipv ughaid hwg zazvkwprx dmidivp kxwlvt iawlrdmiz.

- U predviđeni prostor upisati vlastite zaključke, zapažanja i komentare (analizirati princip rada sustava za kriptoanalizu Vigenereove šifre):

Zadatak 3. *DES i AES*

- Šifrirati vlastito ime i prezime (npr. PETARPETROVIC) pomoću DES algoritma, uz zadani ključ: 0x1234567890ABCDEF:

  Šifrat (hex):

  _____

- Pomoću sustava za kriptoanalizu DES-a pokušati dekriptirati prethodno dobiveni šifrat, uz unos dijela ključa („*“ označava nepoznati dio ključa). U tablicu unijeti potrebno vrijeme dekriptiranja:

Ključ	Vrijeme
1234567890ABCDEF	
12345678********	
123456**********	
1234************	
****************	

- Šifrirati vlastito ime i prezime (npr. PETARPETROVIC) pomoću AES algoritma, uz zadani ključ: 0x11223344556677889900AABBCCDDEEFF:

  Šifrat (hex):

  _____

- Pomoću sustava za kriptoanalizu AES-a pokušati dekriptirati prethodno dobiveni šifrat, uz unos dijela ključa („*“ označava nepoznati dio ključa). U tablicu unijeti potrebno vrijeme dekriptiranja:

Ključ	Vrijeme
11223344556677889900AABBCCDDEEFF	
11223344556677889900AABB********	
1122334455667788990************	
112233445566778899**************	
11223344556677**************	
******************************	

- U predviđeni prostor upisati vlastite zaključke, zapažanja i komentare:

Vježba 17. - Skeniranje portova

Skeniranje porta proces je provjere svih priključaka na IP adresi kako bi se vidjelo jesu li oni otvoreni ili zatvoreni. Za potrebe skeniranja portova u vježbi će se koristiti alat *nmap* (*https://nmap.org*), odnosno njegovo grafičko sučelje *Zenmap*. Za aktivno praćenje mrežnog prometa koristit će se alat *Wireshark* (*https://www.wireshark.org*).

Zadatak 1.

- Saznati IP adresu svojeg i susjednog računala pomoću naredbe *ipconfig* iz naredbenog retka.
- Pomoću naredbe *ping* iz naredbenog retka provjeriti povezivost ova dva računala.
- Zabilježiti, te komentirati i objasniti najvažnije informacije dobivene ovim naredbama:

Zadatak 2.

- Pomoću aplikacije *Zenmap* napraviti skeniranje portova odredišnog (susjednog) računala, koristeći pri tome različite metode skeniranja (mogu se koristiti različiti unaprijed predefinirani profili). Pri svim skeniranjima aktivno pratiti mrežni promet pomoću aplikacije *Wireshark*.

- Zabilježiti, te komentirati i objasniti najvažnije informacije dobivene skeniranjem. Proučiti i objasniti različite metode i tehnike skeniranja (od koristi će biti i *nmap* dokumentacija na webu):

Zadatak 3.

- Pomoću aplikacije *nmap* iz naredbenog retka napraviti skeniranje susjednog računala izabranim metodama skeniranja. Aktivno pratiti mrežni promet pomoću aplikacije *Wireshark*.

- Komentirati i objasniti rezultat:

Zadatak 4.

- Pomoću aplikacije *Zenmap* napraviti skeniranje pet različitih destinacija (jedna zadana i četiri proizvoljne – u tablicu upisati odabrane). Aktivno pratiti mrežni promet pomoću *Wiresharka*.

Tablica 17.1. *Popis odabranih destinacija*

scanme.nmap.org

- Komentirati i objasniti dobivene rezultate, osvrnuti se i na korištene metode skeniranja:

Popis kratica:

AES (*Advanced Encryption Standard*) napredni standard šifriranja

AP (*Access Point*) pristupna točka

ARP (*Address Resolution Protocol*) protokol za mapiranje logičkih IP adresa uređaja s fizičkim MAC adresama

ASIC (*Application-Specific Integrated Circuit*) integrirani krug specifičan za primjenu

CBC (*Cipher Block Chaining*) načina rada blokovnih šifri za lančano povezivanje blokova šifri

CRC (*Cyclic Redundancy Check*) ciklička provjera zalihosti

DES (*Data Encryption Standard*) standard šifriranja podataka

DHCP (*Dynamic Host Configuration Protocol*) protokol za dinamičku konfiguraciju klijenta

DNS (*Domain Name System*) sustav dohvaćanja naziva domene

DSA (*Digital Signature Algorithm*) algoritama za digitalni potpis

ECB (*Electronic Codebook*) načina rada blokovnih šifri kao elektronički šifrarnik

FPGA (*Field-Programmable Gate Array*) programabilni logički niz

HMAC (*Hash-based Message Authentication Code*) kod za autentifikaciju poruka temeljen na *hash*-u

HMAC (*Hash-based Message Authentication Code*) MAC shema koja se temelji na proizvoljnoj *hash* funkciji

ICMP (*Internet Control Message Protocol*) Internetski protokol za upravljačke poruke

IP (*Internet Protocol*) Internet protokol

IPv4 (*Internet Protocol Version 4*) Internet protokol verzije 4

LAN (*Local Area Connection*) lokalna mrežna konekcija

MAC adress (*Media Access Control*) fizička adresa mrežnog sučelja

MAC kod (*Message Authentication Code*) autentifikator poruke fiksne duljine

NAT (*Network Address Translation*) prevođenje mrežnih adresa

OBU (*On Board Unit*) komunikaciju na strani vozila

PGP (*Pretty Good Privacy*) šifriranje i dešifriranje e-pošte i datoteka

PPP (*Point-to-Point*) protokol za povezivanje od točke do točke

PPTP (*Point-to-Point Tunneling Protocol*) protokol za tuneliranje podataka od točke do točke

PSK (*Pre-Shared Key*) unaprijed dijeljeni ključ

RSA algorithm (*Rivest, Shamir i Adleman*) algoritam kriptografije s javnim ključem

RSU (*Road Side Unit*) jedinica na strani infrastrukture

SHA (*Secure Hash Algorithm*) kriptografska hash funkcija koja računa *hash* vrijednosti, tj. sažetak

poruke

SSID (*Service Set Identifier*) naziv Wi-Fi mreže

TCP (*Transmission Control Protocol*) protokol za prijenos podataka s kontrolom toka

TPM (*Trusted Platform Module*) standardni sigurnosni kontroler

V2I (*vehicle to infrastructure*) komunikacija vozila sa infrastrukturom

V2V (*vehicle to vehicle*) komunikacija između vozila

VANET (*Vehicular Ad hoc NETwork*) *Ad hoc* mreža vozila

VPN (*Virtual Private Network*) virtualna privatna mreža

WLAN (*Wireless Local Area Network*) bežična lokalna mreža

WPA (*Wi-Fi Protected Access*) protokol zaštićenog pristupa Wi-Fi-ju

WPA (*Wi-Fi Protected Access*) zaštićeni Wi-Fi pristup

Literatura:

1.) A. Dujella, M. Maretić, Kriptografija, Element, Zagreb, 2007.

2.) W. Stallings, Cryptography and Network Security – Principles and Practice, Paerson, Boston, 2016.

3.) W. Stallings, Network Security Essentials – Applications and Standards, Prentice Hall, New Jersey, 2013.

4.) I. S. Pandžić i drugi, Uvod u teoriju informacije i kodiranje, Element, Zagreb, 2007.

5.) Ž. Ilić i drugi, Teorija informacije i kodiranje, Element, Zagreb, 2014.

6.) *MikroTik* dokumentacija, dostupno na: https://www.mikrotik.com/documentation

7.) *MikroTik* priručnik, dostupno na: https://wiki.mikrotik.com/wiki/Manual:TOC