

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 23.06.2026 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Младен Перишић под насловом „Пројектовање и анализа VPN решења за безбедно повезивање удаљених локалних мрежа". Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Младен Перишић је рођен 27.09.2001. године у Бору. Завршио је основну школу „3. октобар” у Бору са одличним успехом. Уписао је природно-математички смер у Гимназији „Бора Станковић” у Бору коју је 2020. године такође завршио са одличним успехом. Исте године је уписао Електротехнички факултет у Београду, студијски програм Електротехника и рачунарство. Основне академске студије завршио је на модулу Телекомуникације и информационе технологије – смер Информационо-комуникационе технологије, у септембру 2024. године, са просечном оценом 7,68 и оценом 10 на одбрани дипломског рада. Мастер студије на Електротехничком факултету у Београду уписао је 2024. године на модулу Електротехника и рачунарство – смер Информационо-комуникационе технологије. Од маја 2024. године био је ангажован као практикант у компанији CETIN, а од октобра исте године запошљен је на позицији инжењера специјалисте у радио приступној мрежи у компанији CETIN, Београд.

2. Извештај о студијском истраживачком раду

Студијски истраживачки рад обухватио је проучавање технологија за безбедно повезивање удаљених локалних мрежа преко заједничке транзитне IP инфраструктуре. Размотрени су намена и основне врсте виртуелних приватних мрежа, безбедносни захтеви при преносу података, архитектура IPsec протокола и улога IKEv1 протокола у договарању безбедносних асоцијација. Посебна пажња посвећена је разликама између статичког site-to-site IPsec повезивања и DMVPN архитектуре, као и улогама mGRE, NHRP и EIGRP механизма у динамичком успостављању путања између локација.

На основу прегледа литературе и техничке документације дефинисан је експериментални модел са централним седиштем и три филијале. За реализацију је изабрано окружење GNS3, док је за анализу снимљеног саобраћаја употребљен Wireshark. Утврђена је методологија која обухвата проверу основне IP повезивости, конфигурисање VPN механизма, испитивање комуникације између крајњих уређаја, анализу криптографске заштите и праћење понашања мреже при прекиду и поновном успостављању WAN везе централног седишта.

3. Опис мастер рада

Мастер рад обухвата 63 стране, са укупно 23 слике, 11 табела и 13 референци. Организован је у осам поглавља, након којих следе литература, списак скраћеница и спискови слика и табела.

У првом поглављу, представљени су предмет и циљ рада, мотиви за безбедно повезивање географски удаљених локалних мрежа и основни приступ поређењу два изабрана VPN решења.

Друго поглавље, обрађује појам, намену и поделу VPN решења. Размотрени су основни безбедносни захтеви који се постављају пред такве мреже, укључујући поверљивост, интегритет и аутентификацију. Треће поглавље, даје теоријску основу практичног дела. Описани су IPsec и ESP, поступак успостављања безбедносних асоцијација применом IKEv1 протокола, GRE и mGRE тунели, NHRP механизам, DMVPN архитектура и улога EIGRP протокола у размени рута.

У четвртном поглављу, дефинисани су захтеви, топологија и адресни план мреже. Приказано је лабораторијско окружење са рутерима централног седишта и три филијале, као и поступци провере и поређења реализација.

Пето поглавље, описује конфигурисање шест међулокацијских VPN односа. Представљени су IKEv1 и IPsec параметри, приступне листе, сгупто мар конфигурација и рутирање. Обухваћени су функционални тестови, анализа безбедносних асоцијација и снимљеног саобраћаја, као и испитивање утицаја прекида WAN везе централног седишта.

Шесто поглавље, приказује конфигурисање mGRE интерфејса, NHRP механизма, IPsec профила и EIGRP протокола. Анализирани су регистрација филијала, динамичко учење рута и формирање непосредне путање

између филијала. Посебно су обрађени отказ WAN везе hub рутера и поступак опоравка комуникације у коришћеном окружењу.

У седмом поглављу, решења су упоређена према сложености конфигурације, скалабилности, безбедносним механизмима, путањама корисничког саобраћаја и понашању при отказу.

Осмо поглавље, обједињује главне резултате, истиче предности и ограничења испитаних приступа и указује на правце даљег рада.

4. Анализа са кључним резултатима

У раду су на истој физичкој топологији и са истим основним адресним планом реализовани статички full-mesh IPsec и DMVPN треће фазе. Поређење је показало да се главна разлика односи на успостављање и одржавање међулокацијских односа. Статичка реализација за четири локације захтева шест унапред конфигурисаних VPN односа, чији број и сложеност одржавања расту са проширивањем мреже. DMVPN смањује потребу за појединачним конфигурисањем веза између филијала применом NHRP механизма и динамичке размене рута. Непосредна комуникација могућа је у оба решења: код статичког модела VPN односи су унапред дефинисани, док је у DMVPN моделу проверено динамичко формирање BR1–BR3 пречице.

Испитивање отказа HQ WAN везе показало је да је код статичког решења испитана комуникација између филијала настављена преко непосредне IPsec везе. У DMVPN моделу губитак EIGRP суседства са јединственим hub рутером и повлачење потребне руте довели су до прекида комуникације BR1–BR3. Тиме је показано да независност путање корисничког саобраћаја од централног седишта не подразумева и независност контролне равни.

При опоравку је забележено неусаглашено IPsec стање, уз поруке о неважећим SPI вредностима. Комуникација је обновљена након ручног уклањања криптографских сесија на рутерима филијала и њиховог поновног успостављања. Овај налаз ограничен је на посматрани тест и не представља доказ губитка конфигурације или опште особине DMVPN архитектуре.

Основни доприноси рада су:

- Пројектовање и реализација заједничког лабораторијског модела за испитивање два VPN приступа.
- Провера заштићене комуникације анализом тестова, безбедносних асоцијација и снимљеног саобраћаја.
- Поређење конфигурационе сложености, могућности проширивања и начина успостављања непосредних веза.
- Анализа зависности од централног уређаја кроз испитивање отказа и опоравка.

5. Закључак и предлог

У мастер раду успешно су пројектована, реализована и анализирана два VPN решења за безбедно повезивање удаљених локалних мрежа. Рад повезује теоријске основе VPN технологија са практичном конфигурацијом, провером рада протокола и тумачењем експерименталних резултата. Приказано поређење омогућава сагледавање предности и ограничења статичког IPsec и DMVPN приступа у оквиру испитаног модела.

Кандидат је показао способност систематичног приступа пројектовању мреже, примени одговарајућих алата и анализи уочених појава. Посебну вредност рада представља разматрање понашања мреже при отказу и разликовање конфигурације уређаја од динамичког стања протокола и безбедносних асоцијација. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да прихвати мастер рад кандидата Младена Перишића под насловом „Пројектовање и анализа VPN решења за безбедно повезивање удаљених локалних мрежа” и одобри његову јавну усмену одбрану.

Београд, 11.09.2026. године

Чланови комисије:

др Младен Копривица Доцент
сагласан, 11.09.2026.

др Зоран Чича Редовни професор
сагласан, 11.09.2026.