МИНИСТАРСТВО ОДБРАНЕ
УНИВЕРЗИТЕТ ОДБРАНЕ
ВОЈНА АКАДЕМИЈА

ЗАВРШНИ РАД

ПРИМЕНА ТЕХНОЛОГИЈЕ ВИРТУЕЛНИХ ПРИВАТНИХ МРЕЖА У ЗАШТИТИ ПАКЕТСКОГ ТЕЛЕФОНСКОГ САОБРАЋАЈА

студент:

Мићо Живановић

ментор:
пуковник
доц.др Иван Вулић, дипл. инж.

Београд, 2023.

1. Увод

Пренос информација путем рачунарске мреже (Интернета) је постао саставни део пословања компанија и банака, функционисања академске заједнице, комуницирања људи, рада управних органа и дистрибуције најразличитијих садржаја (подаци, Web, мултимедијални садржаји и слично).

У почетку развоја Интернета нису разматрани механизми заштите, већ су постепено додавани током развоја мреже.

Захтеви за безбедношћу преноса информација путем Интернета доживели су велике промене током последњих деценија. Безбедносне мере су потребне да би се подаци заштитили током преношења. Под тим мерама се подразумевају мере за одвраћање, спречавање, откривање и опоравак нарушавања безбедности, које се односи на преношење информација.

Архитектуре и механизми заштите преноса путем Интернета постали су императив у даљем развоју мреже. Они се односе на технике контроле права приступа, системе за откривање напада, системе криптозаштите и заштиту мреже (рутера, сервера и гејтвеја) од спољних и унутрашњих напада.

У пракси заштите преноса информација постављени су кључни циљеви и то: поверљивост, интегритет, аутентичност, непорецивост и расположивост.

Да би се остварили наведени циљеви развијени су безбедносни механизми, као процеси пројектовани за откривање, спречавање или опоравак од безбедносног напада.

Унапређење безбедносног система се постиже безбедносним сервисима за обраду или комуникацију, којима се унапређује безбедност система за обраду података и пренос информација једне организације. Безбедносни сервиси користе један или више безбедносних механизама.

Безбедносни сервиси су: аутентификација, контрола приступа, поверљивост података, интегритет података, непорецивост и сервис расположивости.

Примена различитих безбедносних сервиса је условљена врстом преношеног садржаја (говор, подаци, IP TV, Web, мултимедија, видео конференција и др.), за које је развијен низ протокола и стандарда заштите.

Један од најчешће коришћених садржаја је пренос телефоније, која је прошла кроз транзицију од аналогне, преко телефоније у дигиталним мрежама интегрисаних сервиса (ISDN), до данас актуелног пакетског преноса телефонског сигнала (VoIP).

За пакетски пренос телефоније развијени су протоколи намењени за успоставу, одржавање и раскид преноса телефоније путем рачунарске мреже (RTP, RTCP, SIP и H.323). Протоколи о којима је реч омогућавају пренос садржаја у реалном времену, за који је потребно обезбедити сигуран пренос у складу са напред наведеним захтевима и циљевима.

Тајност преноса је циљ који омогућава пренос, тако да је преношени садржај неразумљив непозваним корисницима. Механизам тајности се постиже употребом различитих кроптографских алгоритама (симетричних и асиметричних).

Један од најчешће употребљаваних механизама за заштиту тајности путем шифровања је технологија виртуелних приватних мрежа (Virtual Private Networks – VPN).

За успоставу виртуелних приватних мрежа развијен је низ протокола (IPSec, AH, ESP, ISAKMP, IKE и други).

Предмет рада биће заштита пакетског телефонског саобраћаја употребом технологије виртуелних приватних мрежа.

У првом поглављу биће приказани најважнији механизми и сервиси заштите кроз поделу мреже на управљачку, контролну и раван података. У равни података посебна пажња биће посвећена технологији виртуелних приватних мрежа употребом IPSec протокола.

Предмет другог поглавља су принципи преноса пакетског телефонског саобраћаја (VoIP) и најважнији протоколи развијени за пренос истог (SIP, H.323 и RTP).

Тежиште у раду биће на једној реализацији заштите пакетског телефонског саобраћаја, употребом технологије виртуелних приватних мрежа, на реалној мрежној опреми.

Цео процес мерења и анализе мрежног саобраћаја је обрађен у четвртом поглављу, кроз анализу незаштићеног и заштићеног саобраћаја у преносу.

Главни проблем који ће бити разматран у раду је методологија заштите пакетског телефонског (VoIP) саобраћаја употребом виртуелних приватних мрежа, од конфигурисања мрежних уређаја за успоставу мреже за пренос података, а потом VoIP саобраћаја, преко конфигурисања уређаја за услугу успостављања заштите виртуелном приватном мрежом (VPN), преко успоставе, најпре, VoIP саобраћаја, потом успоставе VPN тунела, да би се у финалном делу извршило снимање (мерење) мрежног саобраћаја, употребом софтверског алата Wireshark. На крају ће бити анализиран мрежни саобраћај, са акцентом на кључним процесима у мрежи, како оних који се односе на пренос сервиса у реалном времену, тако и оних који се односе на успоставу и одржавање VPN тунела.

Основно питање које се поставља у раду је место и улога одређених мрежних протокола, као и редослед њиховог појављивања у процесу успоставе пакетског телефонског саобраћаја, успоставе VPN тунела и каснији пренос садржаја у реалном времену.

Циљ рада је приказ и објашњење улоге комуникационих протокола у једном приступу реализацији заштите пакетског телефонског саобраћаја, употребом технологије виртуелних приватних мрежа.

Из наведеног циља проистичу задаци: приказ развијености техника заштите преноса у односу на раван примене (управљачка, контролна и раван података), теоријски осврт на достигнути ниво развијености мрежних протокола (специфично за пренос и заштиту пакетског телефонског саобраћаја), конфигурисање мрежних уређаја за остварење наведеног сервиса и његову заштиту, успостава VoIP саобраћаја у незаштићеном и заштићеном преносу, снимање мрежног саобраћаја софтверским алатом, и на крају, анализа мрежног саобраћаја.

Методолошки, рад ће се базирати на следећим основним и општенаучним методама:

Метод дефиниције ће бити коришћен у поступку одређивања основних појмова који се односе на све аспекте мрежне комуникације, релевантне за обрађивану тему.

Метод моделовања ће тежишно бити примењиван приликом једног приступа реализацији заштите пакетског телефонског саобраћаја употребом технологије виртуелних приватних мрежа, уз реализацију једног функционалног модела.

Аналитичка и синтетичка метода ће бити тежишно примењена у четвртом поглављу рада, када ће, након анализе мрежног саобраћаја, бити извршена синтеза закључака о свим процесима у мрежи у току реализације функционалног модела.

У доступној литератури је акценат дат на структури и намени мрежних протокола, са тежиштем на приказу формата у којима се дати протоколи остварују (заглавља порука, адресирање, информациони садржај који се преноси, заштитна заглавља, нумерација оквира – пакета и слично).

Настанак и развој одређених протокола, са свим променама током развоја истих, је доступан на Web презентацији међународне организације IETF (Internet Engineering Task Force), кроз RFC (Requests for Comments) документе (техничке прописе, стандарде и информативне документе).

Најпосле, произвођачи мрежне опреме (Cisco) су учинили доступним јавности све аспекте конфигурисања и рада мрежне опреме.

Може се закључити да је у току развоја глобалне мреже – Интернета, развијен читав низ протокола прилагођен захтевима корисника (према врстама сервиса), као и степену развијености мрежног хардвера и софтвера.

Протоколи су прилагођени седмослојној структури OSI модела Интернета и представљају јединствен протокол стек, који обједињује све функције и рад сваког слоја понаособ.

2. Технологије заштите података у рачунарским мрежама

У умрежавању, раван је апстрактна концепција о томе где се одвијају одређени процеси. Термин се користи у значењу „раван постојања“. Две равни које се најчешће помињу у умрежавању су: контролна раван и раван података (такође позната као раван за прослеђивање).

У литератури је заступљена подела рачунарске мреже према механизмима и протоколима који се користе у процесу заштите преноса података на:

1) Управљачку раван (Management Plane),

2) Контролну раван (Control Plane) и

3) Раван података (Data Plane).

Већина саобраћаја у мрежи који се одвија кроз рутер, одвија се преко равни података. Осим наведеног, процесор рутера усмерава одређене пакете, као што су пакети ажурирања табела рутирања и пакети за одржавање и управљање мрежом. Овај саобраћај се често назива саобраћај у контролној и управљачкој равни. Управљачка раван се, међутим, сматра одвојеном из функционалне перспективе, како би се дефинисали различити механизми заштите за управљање саобраћајем [1][2].

2.1. Заштита података у управљачкој равни

Протоколи и информациони садржај намењени за надзор и управљање мрежних компонената, од стране радне станице администратора мреже, представљају управљачку раван. За наведене потребе развијени су бројни протоколи, међу којима су најпознатији: TELNET, NTP (Network Time Protocol), SSH (Secure Shell), SNMP (Simple Network Management Protocol), SSL/TLS, Protected syslog, Parser views и други, што представља основу заштите целокупне мреже [2].

Управљање мрежом има за циљ ефикасно и рационално коришћење мрежних ресурса. Наведено се остварује кроз следеће ситуације:

- Откривање грешке на интерфејсу рачунара или рутера,
- Надгледање рачунара и других уређаја у мрежи,
- Праћење саобраћаја у циљу помоћи приликом распоређивања ресурса,
- Откривање брзих промена у табелама рутирања,
- Праћење SLA (Service Level Agreement) споразума и
- Откривање упада.

Према Међународној организацији за стандардизацију (ISO), модел за управљање мрежама обухвата управљање перформансама, управљање грешкама, управљање конфигурацијом, управљање обрачунавањем (евидентирање и контрола приступа корисника мрежним ресурсима, наплаћивање коришћења, додељивање привилегија) и управљање безбедношћу [1].

Из наведеног се може извести закључак о функцијама управљачке равни у рачунарској мрежи.

Поред хардверских мрежних компоненти, развијени су софтвери (протоколи) који омогућавају управљање и испитивање статуса управљаног уређаја. Развијен је низ протокола који омогућавају приступ мрежним уређајима, конфигурисање истих, надзор над мрежним уређајима и временска синхронизација мрежних уређаја.

Ради разумевања функција управљачке равни, размотрићемо протоколе који се користе у управљачкој равни мреже и то: 1) NTP (Network Time Protocol) протокол, 2) SNMP (Simple Network Management Protocol) протокол, 3) SSH (Secure Shell) протокол и 4) TELNET протокол.

2.1.1. NTP (Network Time Protocol) протокол

Пренос података кроз рачунарску мрежу подразумена кретање пакета кроз исту, различитим путањама и пренос садржаја, код којих је битан елемент време када је кренула трансмисија пакета (како би се исти на пријемној страни поставио у редослед који омогућава реконструкцију садржаја – поруке са предајне стране, извршила синхронизација порука у случају преноса мултимедијалног садржаја и како би се отклониле слабости

мреже у току преноса, тзв. „џитер“, односно отклонио негативан утицај кашњења порука кроз мрежу).

Да би се отклонили различити проблеми у току преноса информационог садржаја кроз мрежу, важно је да мрежа буде синхронизована.

Карактеристично је, да је временска синхронизација посебно значајна за пренос сервиса у реалном времену. С тим у вези, развијен је протокол за синхронизацију времена (NTP).

NTP је мрежни протокол за синхронизацију времена између мрежних уређаја у мрежама са комутацијом пакета. NTP има за циљ да синхронизује времена рада рачунара и других мрежних уређаја у односу на универзално време (UTC).

Протокол обично функционише по клијент – сервер моделу, али се може користити и у комуникацији два равноправна ентитета, где оба равноправна уређаја могу бити извор времена синхронизације. Рутер у мрежи се конфигурише као NTP сервер, док истовремено може бити конфигурисан и као клијент, ради пријема синхронизације времена у односу на неки „виши“ сервер у мрежи.

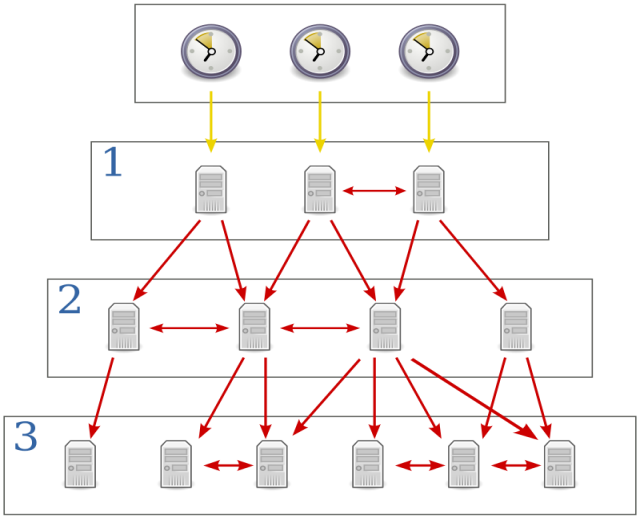
NTP протокол омогућава синхронизацију временских база мрежних уређаја, коришћењем протокола UDP (User Datagram Protocol) на порту број 123.

Протокол ћемо анализирати кроз две последње верзије и то: верзија NTPv3, наведена у документу RFC 1305 и верзија 4 (NTPv4), што је документовано у препоруци RFC 5905.

Поред наведених, развијена је верзија протокола NTS (Network Time Security), што је безбедна верзија NTP протокола. Наведени стандард је документован у препоруци RFC 8915.

На слици 1. је представљена структура мреже са применом NTP протокола са три примарна референтна извора, који раде као примарни сервери времена. Сврха NTP протокола је да пренесе информације о мерењу времена, са ових сервера на друге сервере времена путем Интернета, као и унакрсна провера сатова и смањивање грешака услед кварова опреме или услова пропагације сигнала. Одређени број хостова или мрежних пролаза, који делују као секундарни сервери времена, покрећу NTP са једног или више

примарних сервера. Да би смањили оптерећење протокола, секундарни сервери дистрибуирају време преко NTP протокола преосталим хостовима у локалној мрежи.



Слика 1. Структура мреже са применом NTP протокола

Подмрежа за синхронизацију је повезана мрежа примарних и секундарних временских сервера, клијената и међусобно повезаних спојних путева. Примарни сервер времена је директно синхронизован са примарним референтним извором, обично радио сатом. Секундарни сервер времена изводи синхронизацију, преко других секундарних сервера, од примарног сервера преко мрежних путања, које се могу делити са другим сервисима. Најчешће, подмрежа за синхронизацију примарног и секундарног сервера подразумева хијерархијску (master/slave) конфигурацију.

Као резултат овог дизајна, подмрежа се аутоматски реконфигурише да би произвела најтачније и најпоузданије време, чак и када један или више примарних или секундарних сервера или мрежне путање између њих то не успеју. Ово укључује случај када се сви нормални примарни сервери на евентуално подељеној подмрежи покваре, где ће један или више резервних примарних сервера наставити рад [3].

За разлику од претходних верзија NTP протокола, NTPv3 омогућава аутентификацију мрежних уређаја, што представља вид заштите у случају компромитације мреже и лажног оглашавања мрежних уређаја.

У реалним условима постоји могућност да нападач на мрежу поремети операције мерења времена између хостова, суптилним модификацијама података NTP поруке, као што је измена поља заглавља или одређене временске ознаке. У случајевима када је потребна заштита, чак и од ових врста напада, неопходан је посебно дизајниран механизам аутентификације порука заснован на криптографским техникама. Типични механизми укључују употребу криптографских сертификата, алгоритама и кључева, заједно са безбедним базама података и протоколима за управљање кључевима.

Према наведеном, свакој асоцијацији се додељују параметри које идентификују ауторитет за издавање сертификата, алгоритам за шифровање, криптографски кључ и евентуално друге податке.

За аутентификацију се користи DES алгоритам у 64 – битним блоковима, којима се дефинише крипто контролна сума у послатим порукама, док се у примљеним порукама врши контрола суме. Осим DES алгоритма, могу се користити и други криптографски алгоритми, уз претходни договор.

Формат аутентификатора се састоји од 96 бита, укључујући 32 – битни идентификатор кључа и 64 – битни крипто – контролни збир [3].

Верзија протокола NTPv4 је описана у документу RFC 5905, а наведена верзија протокола је компатибилна са претходном верзијом протокола.

У наведеној верзији протокола направљене су одређене мање промене у неким пољима заглавља протокола, које не утичу на интероперабилност између NTPv4 и претходних верзија NTP и SNTP.

NTPv4 дизајн превазилази значајне недостатке у NTPv3 дизајну, исправља одређене грешке и укључује нове функције. Конкретно, повећана је резолуција времена у којој се врши корекција сата, тј. у краћим временским интервалима се врши корекција времена синхронизације.

Модел NTPv4 подмреже укључује велики број широко доступних сервера примарног времена, синхронизованих путем различитих спојних путева. Сврха NTPv4 протокола је да пренесе информације о мерењу времена са ових примарних сервера на секундарне сервере времена и клијенте, путем приватних мрежа или јавног Интернета. Прецизно подешени

алгоритми ублажавају грешке које могу бити резултат прекида мреже, кварова сервера и могућих непријатељских радњи. Сервери и клијенти су конфигурисани тако да вредности теку ка клијентима са примарних сервера, преко разгранатих секундарних сервера.

Поуздана временска синхронизација захтева криптографске кључеве, који су важећи само у одређеном временском интервалу. Временски интервали се могу применити само када су сервери и клијенти, који учествују, поуздано синхронизовани са универзалним временом (UTC).

NTPv4 клијент може тврдити да има аутентично време за апликације, само ако су сви сервери на путу до примарних сервера аутентификовани. У NTPv4, сваки сервер аутентификује следеће сервере нижег слоја и проверава аутентичност сервера најнижег слоја (примарне). Важно је напоменути, да аутентификација у контексту NTP – а, не значи нужно да је време тачно. NTP клијент мобилише бројне истовремене асоцијације са различитим серверима и користи направљени алгоритам, да раздвоји истините од лажних временских ознака.

NTPv4 спецификација претпоставља да је циљ нападача да убаци лажне временске вредности, поремети протокол или блокира рад мреже, сервере или клијенте, лажним пакетима који исцрпљују ресурсе и ускраћују услугу легитимним апликацијама. Постоји велики број одбрамбених механизама који су већ уграђени у NTPv4 архитектуру, протокол и алгоритме, а који омогућавају заштиту од наведених непријатељских активности [4].

2.1.2. SNMP (Simple Network Management Protocol) протокол

Развојем Интернет протокол стека, осим протокола који омогућавају услуге на нивоу мреже на апликативном нивоу, указала се потреба за развојем протокола који ће омогућити администратору мреже да открива узроке проблема рада мреже, као и да исте отклања. Развојем Интернета и хетерогеношћу протокола и уређаја којима се управља, указала се потреба за развојем протокола, који ће омогућити управљање у тако хетерогеном окружењу. Један од протокола који наведено омогућава је SNMP (Simple Network Management Protocol) протокол.

Актуелна верзија протокола је SNMPv3, која је описана у документима RFC 2271 до 2275.

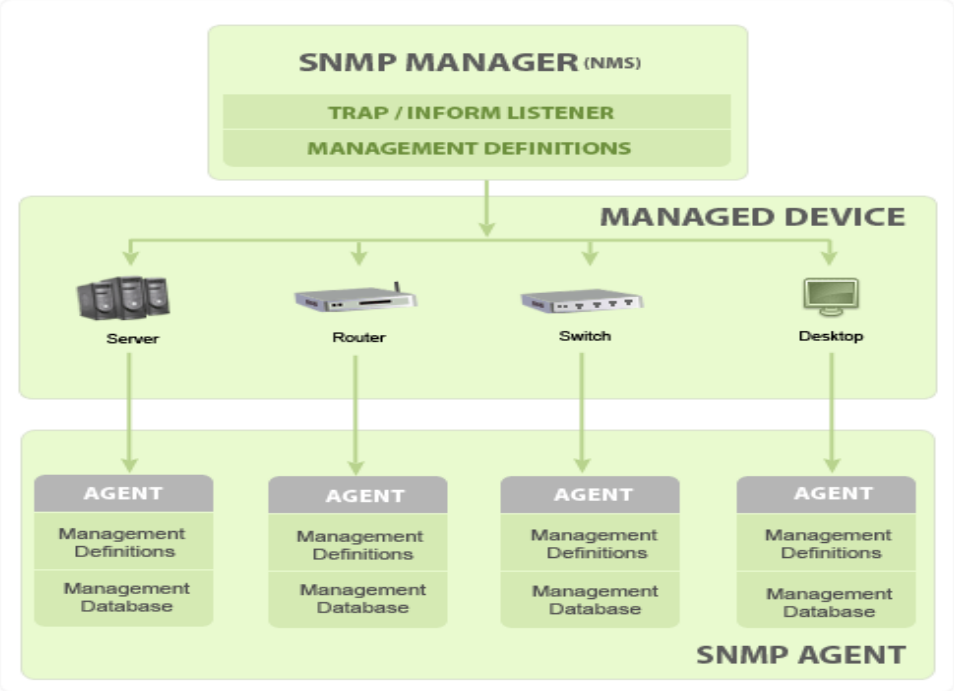
Укратко ћемо представити актуелну верзију протокола SNMPv3.

SNMP је протокол намењен за прикупљање и организовање информација о управљаним уређајима на IP мрежама и за модификацију тих информација ради промене понашања уређаја. SNMP излаже управљачке податке у облику варијабли на управљаним системима, организованим у бази информација за управљање, које описују статус и конфигурацију система. Ове варијабле се затим могу даљински испитивати (у неким околностима имењати) управљачким апликацијама. SNMP је саставни део Интернет протокол стека. С обзиром да је у свом раду ослоњен на TCP/IP конекцију и користи неки од протокола транспортног слоја (нпр. UDP протокол), може се рећи да SNMP протокол припада апликативном слоју OSI модела. У стандардној употреби SNMP – а, један или више администраторских рачунара имају задатак да надгледају или управљају групом хостова или уређаја у рачунарској мрежи. Сваки управљани систем извршава софтверску компоненту звану агент, који администратору доставља информације преко SNMP – а.

Мрежа којом се управља помоћу SNMP – а, састоји се од три кључне компоненте: управљани уређај, агент управљаних уређаја – софтвер, који ради на управљаним уређајима и станица за управљање мрежом (NMS – Network Management Station).

SNMP ентитети, који извршавају команде и апликације примаоца обавештења, надгледају и контролишу управљане елементе, су станице за управљање мрежом. Управљани елементи су уређаји као што су хостови, рутери, терминалски сервери итд., који се надгледају и контролишу путем приступа њиховим информацијама за управљање. Софтвер који ради на администраторском рачунару и управљани уређај је мрежни чвор, који имплементира SNMP протокол, који омогућава једносмерни (само читање) или двосмерни (читање и писање) приступ информацијама специфичним за чвор. Агент је софтверски модул за управљање мрежом, који се налази на управљаном уређају. Агент садржи локалне управљачке информације и преводи те информације у, или из, формата специфичан за управљачку станицу (NMS) [5].

Стандардна SNMP структура је приказана на слици 2.



Слика 2. Структура мреже са применом SNMP протокола [6].

Као у случају других протокола, и SNMP протокол је изложен различитим безбедносним претњама, према којима су развијени различити безбедносни механизми заштите. У наведене претње се убрајају: модификација информација, модификација тока порука, лажно представљање, прислушкивање или мониторинг саобраћаја и друге.

У циљу заштите од наведених претњи, за потребе безбедног функционисања протокола развијена су прилагођења SNMP протокола, са другим апликацијама и криптогрфским алгоритмима, описана у RFC документима (AES, SSH, TLS, HMAC SHA – 2 и други).

SNMPv3 дефинише формат и значење порука које размењују клијенти и сервери, као и облик имена и адреса. Протокол одређује податке којима се управља. Због сложености и различитости података којима се управља (које су дефинисане у базама података управљања, MIB – Management Information Base), које зависе од уређаја којима се управља, SNMPv3 је избегао могућ велики број команди којима се управља са базама података којима се управља, на начин да су све операције прилагођене моделу „читај – пиши“. Наведени модел је обезбедио стабилност SNMPv3, јер му дефиниција остаје непромењена без обзира на додавање нових варијабли у MIB.

Дефиниције су одређене скупом могућих SNMP операција, који је дат у табели 1.

Табела 1: Скуп могућих SNMP операција

Команда	**Значење**
Get-request	Прочитати вредност одрђене променљиве
Get-next-request	Прочитати следећу вредност без навођења имена променљиве
Get-bulk-request	Прочитати већу количину података (нпр. табелу)
Response	Одговор на претходне захтеве
Set-request	Уписати вредност у одређену променљиву
Inform-request	Референца на податке других (нпр. на прокси)
Snmpv2-trap	Одговор активиран неким догађајем
Report	Тренутно није дефинисано

Захтев за општошћу и флексибилношћу SNMPv3 протокола је омогућио више видова безбедности, који могу независно да се конфигуришу. SNMPv3 протокол подржава проверу аутентичности поруке, да би се обезбедило да поруке стижу од овлашћеног администратора, приватност којом се омогућава да поруке не могу да прочитају непозвана лица и овлашћења и контрола приступа заснована на приказу, да би само овлашћени администратори приступали одређеним ставкама. На крају, SNMPv3 омогућава даљинско конфигурисање, тако да администратор може да управља уређајем, а да се не налази на месту управљаног уређаја [7].

2.1.3. SSH (Secure Shell) протокол

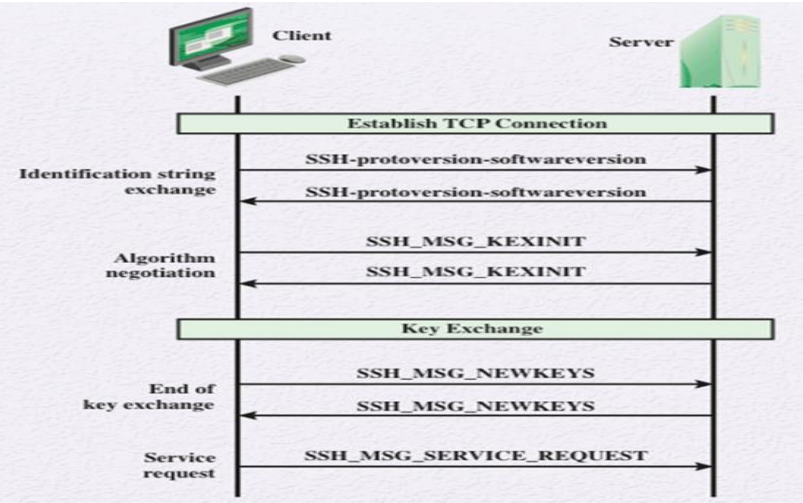
SSH протокол је један од протокола за приступ мрежном уређају, ради контроле и конфигурисања истог. За свој рад SSH протокол користи заштићене начине рада (употреба шифарских алгоритама), тако да онемогућава нападачу на мрежу, да у току рада администратора мреже, дође до креденцијала који се преносе од рачунара администратора до управљаног мрежног уређаја.

SSH протокол је одређен документима RFC 4250 до 4256. Првобитно је био намењен за заштићен удаљени притуп мрежном уређају, док се касније почео користити за друге потребе заштићеног преноса (пренос фајлова и електронске поште).

Процес успоставе SSH конекције се састоји од:

- Успоставе TCP конекције,
- Размена идентификационих стрингова,
- Дефинисање параметара за заштићени рад (преговарање о алгоритму и размена кључева),
- Захтев за услугом (захтев за аутентификацијом корисника, или за протокол конекције),
- Размена корисног садржаја SSH Transport layer пакета (заштићени шифровањем).

Претходно наведено је приказано на слици 3.



Слика 3. Размена пакета SSH протокола транспортног слоја [8]

SSH протокол се састоји од три главне компоненте:

– Протокол транспортног слоја (SSH TRANS). Транспортни протокол обезбеђује поверљиву комуникацију преко незаштићене мреже. Он врши аутентификацију хоста серверу, размену кључева, шифровање и заштиту интегритета. Такође, изводи јединствени број сесије који користе протоколи вишег нивоа,

– Протокола за аутентификацију корисника (SSH-USERAUTH). Протокол за аутентификацију обезбеђује скуп механизама, који се могу користити за аутентификацију корисника серверу. Појединачни механизми наведени у протоколу за аутентификацију користе број сесије, који обезбеђује транспортни протокол и/или зависе од гаранција безбедности и интегритета транспортног протокола,

– Протокол везе (SSH-CONNECT). Протокол везе специфицира механизам за мултиплексирање (канала) података преко поверљивог и аутентификованог транспорта. Такође, специфицира канале за приступ интерактивној комуникацији, за прослеђивање различитих екстерних протокола преко безбедног транспорта (укључујући произвољне TCP/IP протоколе) и за приступ безбедним подсистемима на хосту сервера.

Клијент шаље захтев за услугу, када се успостави безбедна веза транспортног слоја. Други захтев за услугу се шаље након што је аутентификација корисника завршена. Ово омогућава да се дефинишу нови протоколи и да коегзистирају са горе наведеним протоколима. Протокол везе обезбеђује канале који се могу користити за широк спектар намена.

Примарни циљ SSH протокола је побољшање безбедности на Интернету, на начин који је лак за имплементацију:

– Алгоритми који се користе за шифровање, интегритет и јавни кључ су познати,

– Алгоритми се користе са значајним величинама кључева, за које се верује да пружају заштиту на дужи период,

– Алгоритми се договарају у току успоставе сесије, у случају да је неки алгоритам неисправан, лако се прелази на неки други алгоритам, без модификације основног протокола. У ту сврху састављен је списак алгоритама који су на располагању приликом успостављања SSH конекције [9].

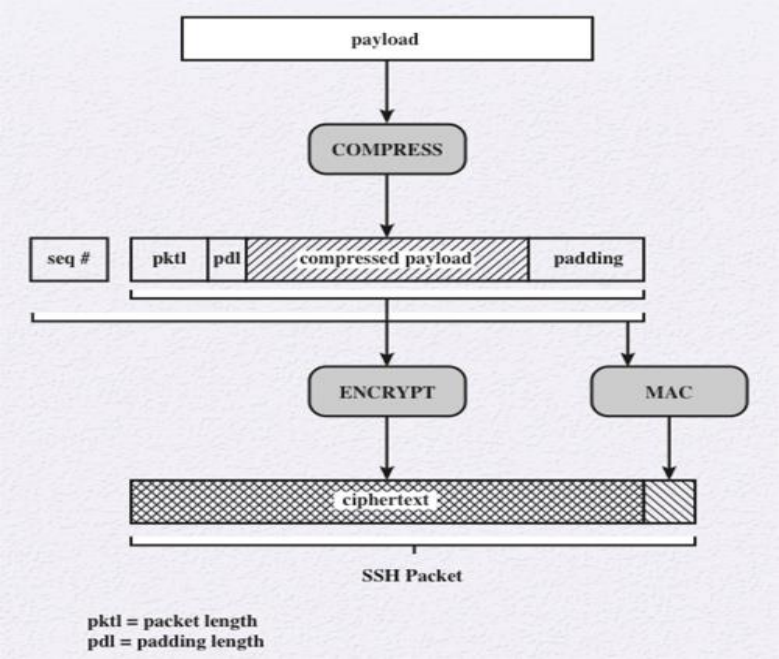
Слика 4. приказује формат поруке (пакета) који се преносе након успоставе TCP конекције и договарања алгоритма.

Садржај поруке (payload) се добија најпре компримовањем корисног садржаја, коме се додаје допуна (padding), која се додаје након што је договорен алгоритам шифровања.

Пре додавања броја MAC (Message authentication code), врши се шифровање (encrypt) над пакетом, без редног броја пакета, а пре израчунавања броја MAC.

На крају се додаје MAC, чија се вредност израчунава над целим пакетом и редним бројем пакета, и на крају се додаје шифрату.

Након размене пакета SSH протокола транспортног слоја и формирања пакета за SSH Transport Layer Protocol, врши се размена порука у SSH Connection Protocol.



Слика 4. Размена пакета SSH протокола транспортног кола [8]

2.1.4. TELNET протокол

TELNET је мрежни протокол стек Интернет протокола. Намена овог протокола је успостављање двосмерног осмобитног комуникационог саобраћаја између два умрежена рачунара. Најчешће се користи да осигура кориснику једног рачунара сесију за коришћење командне линије на другом рачунару. Назив протокола потиче од енглеских речи „телефонска мрежа“ (engl. **TEL**ephone **NET**work).

TELNET омогућава успостављање конекције са удаљеним системом на начин да се локални терминал понаша као да је терминал тог удаљеног система (терминал је: монитор + тастатура).

TELNET протокол је протокол апликативног нивоа OSI (Open System Interconnection) модела.

Сврха TELNET протокола је да обезбеди општу, двосмерну, осмобитно оријентисану комуникацију. Његов примарни циљ је да омогући комуникацију по моделу клијент – сервер. Предвиђено је да се протокол може користити и за комуникацију терминал–терминал, као и комуникацију процес–процес (дистрибуирано рачунање).

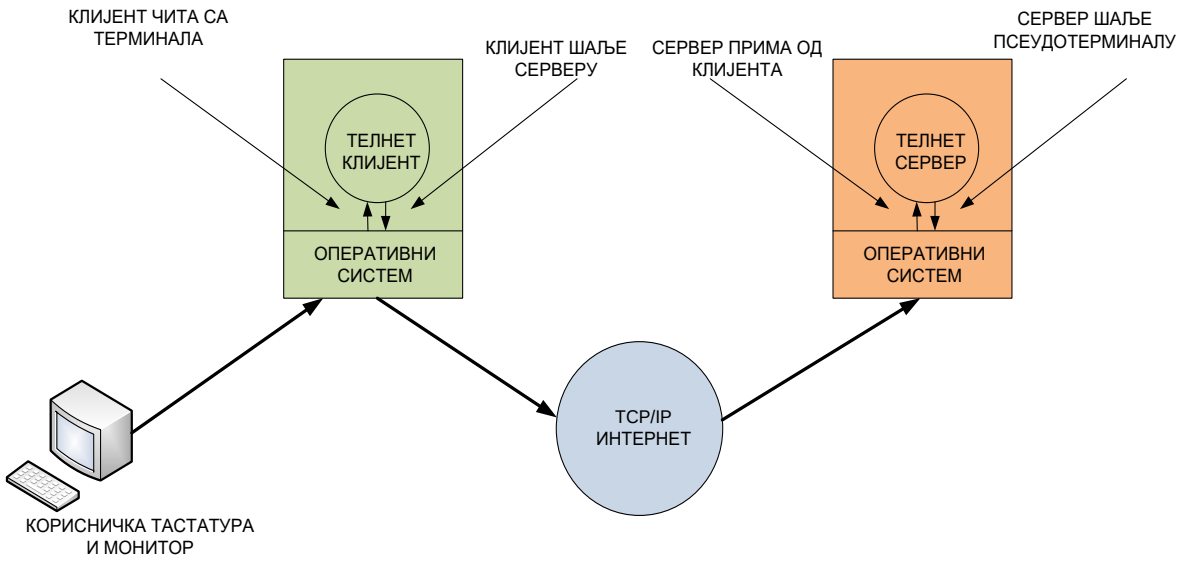
Избор удаљеног сервера се омогућава по доменском имену (DNS) или по IP адреси.

TELNET протокол нуди три основна сервиса:

1. мрежни виртуелни терминал,
2. механизам преговарања о опцијама и
3. симетричан поглед на терминале и процесе.

TELNET веза се успоставља након успоставе TCP/IP конекције.

Принцип успоставе TELNET везе приказан је на слици 5.

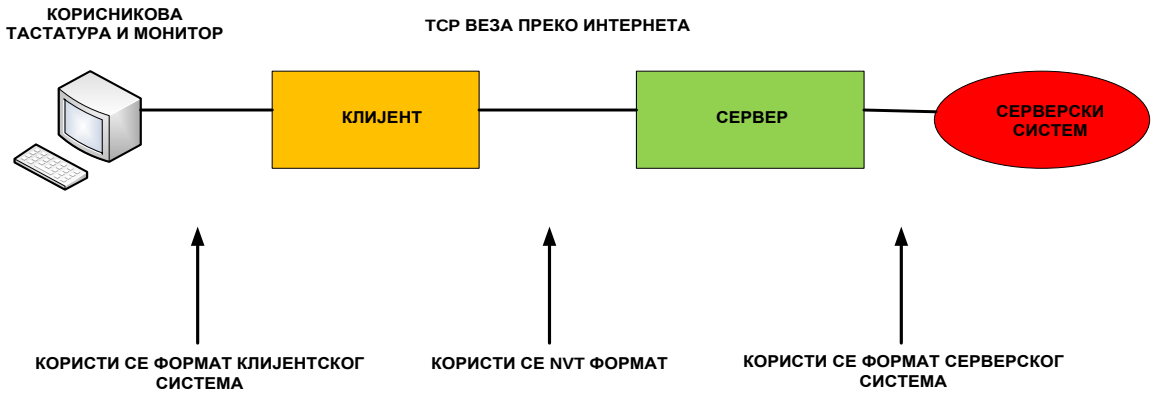


Слика 5. Путања података који у сесији тернимала ТЕЛНЕТ-а путују од корисникове тастатуре до удаљеног оперативног система [7]

Према слици, корисник позива TELNET апликативни програм, који постаје тада клијент, који потом успоставља TCP везу. По успостави везе, клијент преноси знакове које шаље корисник у правцу сервера. Омогућена је и веза у супротном смеру, на начин да се послати знакови према серверу враћају кориснику и приказују на монитору корисника. Најчешће се не ради само о једној вези, коју опслужује сервер, већ се остварује више једновремених веза. Када се TELNET веза први пут успостави, претпоставља се да сваки крај почиње и завршава се на „мрежном виртуелном терминалу“ (Network Virtual Terminal).

С обзиром да се TELNET комуникација остварује са више различитих рачунара и оперативних система, неопхподно је прилагођавање за сваки конкретни случај. Оно се остварује помоћу мрежних виртуелних теминала (NVT), који дефинише начин на који се подаци и команде преносе преко Интернета. Дефиниција NVT формата се састоји од 7 – битних USASCII знакова и један бит за командне низове знакова (што представља 8 – битне комбинације знакова). У пракси то значи да се за командне знакове одређује специјална секвенца (IAC – interpret as command), која указује да иза ње следи командни знак.

Наведени пренос и прилагођавање преноса је приказано на слици 6.



Слика 6. Путања података који у сесији тернимала ТЕЛНЕТ-а путују од корисникове тастатуре до удаљеног оперативног система [7]

TELNET протокол је конструисан тако да преговара о опцијама у току преноса, на начин да свака страна може да постави захтев [7].

Основна стратегија за подешавање коришћења опција је да било која страна (или обе), иницирају захтев да нека од опција ступи на снагу. Друга страна тада може или прихватити или одбити захтев. Ако се захтев прихвати, опција одмах ступа на снагу; ако је одбијен, повезани аспект везе остаје као што је наведено за NVT [10].

TELNET, као протокол, у почетном развоју није имао развијене механизме безбедне размене информација. Касније допуне протокола увеле су безбедносне механизме (препоруке RFC 2941 – 2946).

Без договорених безбедносних опција, он само прослеђује поруке између NVT – ова, које представљају два TELNET процеса.

У својој најчешћој употреби, као протокол за приступ удаљеном терминалу (TCP порт 23), TELNET се повезује са сервером који захтева аутентификацију на нивоу корисника преко корисничког имена и лозинке у незаштићеном облику, док се сервер не аутентификује кориснику.

Опција TELNET аутентификације омогућава аутентификацију корисника и аутентификацију сервера. Провера аутентичности сервера се обично врши заједно са аутентификацијом корисника. Да би подржали ове безбедносне услуге, два TELNET

ентитета морају прво да преговарају о својој спремности да подрже опцију TELNET аутентификације. Након што се сложе да подрже ову опцију, стране су тада у могућности да изврше преговоре о подопцији (о протоколу за аутентификацију који ће се користити), а могуће и о удаљеном корисничком имену које ће се користити за проверу ауторизације [11].

Кроз RFC документе су дефинисани типови аутентификације (NULL, KERBEROS_V4,KERBEROS_V5, SRP, SSL, KEA_SJ, KEA_SJ_INTEG, DSS, NTLM и други). Један од недостатака TELNET протокола је то што корисници морају да унесу своје лозинке, да би се пријавили на удаљене системе, које се у отвореном тексту прослеђују кроз мрежу, тако да постоји могућност да ће лозинке бити компромитоване од стране нападача на мрежу.

Сврха аутентификације је да обезбеди оквир за пролазак информација о аутентификацији кроз TELNET сесију и механизам за омогућавање шифровања тока података као нуспојава успешне аутентификације или путем накнадне употребе опције TELNETENCRYPT. То значи да:

1) корисничка лозинка неће бити послата у отвореном облику кроз мрежу,

2) ако наведени TELNET процес има одговарајуће информације за аутентификацију, он може аутоматски да пошаље информације и корисник неће морати да уписује никакве лозинке,

3) када је аутентификација успешна, ток података може бити шифрован да би се обезбедила заштита од активних и пасивних напада [12].

Један од докумената наводи, да се за аутентификасцију може користити криптоалгоритам KERBEROS_V5, са TELNET протоколом. Овај механизам се такође може користити за обезбеђивање кључева за пружање услуга поверљивости података у комбинацији са опцијом TELNET шифровања [13].

Могућност преговарања о заједничком механизму аутентификације између клијента и сервера је карактеристика опције аутентификације, коју треба користити опрезно. Када је преговарање обављено, аутентификација још није извршена. Стога, сваки систем нема начина да зна да ли разговара или не са системом с којим намерава. Нападач на мрежу би

могао да покуша да преговара о коришћењу система за аутентификацију који је или слаб, или га је већ компромитовао [14].

Допунама стандарда, дефинисана је опцијаTELNET шифровања, као метод пружања услуга поверљивости података за TELNET ток података. Посебним документима се дефинише сваки шифарски алгоритам, који се користи за заштиту TELNET саобраћаја.

Да би се омогићила опција шифровања потребно је да се испреговара опција ENCRYPT између клијента и сервера, која пружа заштиту од пасивних напада, али не и од активних напада.

Спецификација дефинише метод за обезбеђивање поверљивости података TELNET току података. Нажалост, сви механизми шифровања који су обезбеђени у оквиру ове опције не обезбеђују интегритет података. Проблем би могао бити решен приступом који би користио Diffie – Hellman режим TLS – а, праћен TELNET опцијом AUTHENTICATION, где би механизам аутентификације укључивао поруке клијента и сервера које су израчунате током TLS преговора [15].

2.2. Заштита података у контролној равни

Контролна раван је део мреже, који контролише прослеђивање пакета података између мрежних уређаја. Карактеристичан пример је процес креирања табела рутирања, који се сматра делом контролне равни. Рутери користе различите протоколе за идентификацију мрежних путања и чувају те путање у табелама рутирања. Контролна раван мрежног уређаја обрађује саобраћај који је најважнији за одржавање функционалности мрежне инфраструктуре. Контролна раван се састоји од апликација и протокола између мрежних уређаја, што укључује Border Gateway Protocol (BGP), Interior Gateway Protocols (IGP), као што су Enxanced Interior Gateway Routing Protocol (EIGRP) и Open Shortest Path First (OSPF). Наведени протоколи подразумевају коришћење аутентификације, чиме се спречава измена рутинг табела, лажним рутинг информацијама.

Осим наведених протокола, у контролној равни примењују се правила (полисе) приступа мрежним уређајима (CoPP – Control Plane Policing) и заштита контролне равни (CPPr – Control Plane Protection).

2.2.1. Полисе приступа мрежним уређајима (CoPP – Control Plane Policing)

Перформансе мрежних уређаја су ограничене оним што се може обрадити интегрисаним колима и оним што се може обрадити на централној процесорској јединици (CPU – Central Processor Unit) уређаја помоћу софтвера. Када се превише саобраћаја преусмери према контролној равни уређаја, централна процесорска јединица може бити преоптерећена, што резултира немогућношћу контролне равни да изврши све потребне задатке. Ово стање може утицати не само на овај појединачни уређај, већ и на друге уређаје у мрежи. Да би се минимизирали ефекти на перформансе контролне равни, комбинација полиса приступа мрежним уређајима, хардверских лимитатора брзине и листа контроле приступа (ACL – Access control lists), може се користити за смањење протока контролне равни, чиме се спречава компромитовање перформанси контролне равни [16].

Преоптерећење пакетима у контролној равни мрежног уређаја може успорити процесе рутирања и, као резултат, смањити нивое мрежних услуга и продуктивност корисника. Један од разлога за преоптерећену контролну раван уређаја је неефикасно коришћење додељених ресурса меморије и централног процесора. Исти резултат се може десити ако се напади извиђања или ускраћивања услуге (Distributed Denial of Service) појаве на контролној равни, или ако се протокол рутирања лоше понаша.

Полисе приступа мрежним уређајима (CoPP – Control Plane Policing) пружају начин за администраторе да заштите управљачки процесор на комутатору (свичу и рутеру) од преоптерећења саобраћајем (генерисаног од злонамерних или незлонамерних извора), које би могло да омета његову способност да одржава проток саобраћаја у равни података. На пример, напад ускраћивања услуге може довести до претераног саобраћаја који би успорио процесор за управљање и негативно утицао на пропусну моћ комутатора.

Политика полиса приступа мрежним уређајима се састоји од једне или више класа. Свака класа дефинише један или више циљних протокола и како се управља њиховим саобраћајем.

Радње које се могу применити на све пакете који одговарају једној класи су:

- Одбацивање пакета који не одговарају одређеној класи,

- Постављање приоритета обраде,
- Подешавање максималне брзине преноса података према управљачком процесору уређаја,
- Подешавање максималне величине дотока података у пакетима, која се шаље управљачком процесору.

Могу се дефинисати до 32 политике полиса приступа мрежним уређајима, али само једна може бити активна на уређају истовремено. Политика полиса приступа мрежним уређајима мора увек бити активна на мрежном уређају и поставља се глобално за дати уређај.

Сваки мрежни уређај има подразумевану политику полиса приступа мрежном уређају, која се аутоматски примењује при првом покретању [17].

Функција контроле контролне равни је да повећава сигурност на мрежном уређају, тако што штити процесор од непотребног или DDoS (Distributed Denial of Service) саобраћаја.

Већином саобраћаја којим управља процесор уређаја, управља се путем контролне и управљачке равни.

Политика полиса приступа мрежним уређајима може се користити у заштити нивоа контроле и управљања и обезбедити стабилност рутирања, доступност и испоруку пакета. Политика полиса приступа мрежним уређајима користи наменску конфигурацију контролне равни, да обезбеди могућности филтрирања и ограничавања брзине за пакете контролне равни [18].

На пример, ако се контролној равни представи велика количина лажних пакета, које генерише вирус или црв, комутатор ће потрошити превише времена на обраду и одбацивање непотребног саобраћаја. Ово на крају може преплавити процесор руте, који је одговоран за руковање функцијама контролне равни уређаја, и може зауставити процесе мрежног уређаја.

Кључне предности које пружа политика полиса приступа мрежним уређајима су следеће:

– Заштита од напада непотребног или DDoS (Distributed Denial of service) саобраћаја на инфраструктурне рутере и комутаторе,
– Контролу пакета који су намењени контролној равни рутера или комутатора,
– Лакоћу конфигурације,
– Већу поузданост и доступност платформе,
– Проширује заштиту од напада непотребним саобраћајем (DDoS – Distributed Denial of Service) на инфраструктурним свичевима, обезбеђујући механизам за финију контролу саобраћаја на контролној равни, који омогућава да се ограничи брзина за сваки тип појединачно,
– Обезбеђује механизам за рано одбијање пакета који су усмерени на затворене или неактивне портове,
– Пружа могућност ограничавања употребе низа протокола, тако да ниједна поплава једног протокола не може преплавити улазни интерфејс [19].

Дефинисање контролне класе саобраћаја у контролној равни, политике полиса приступа мрежним уређајима, почиње са класификацијом саобраћаја у контролној равни. У том циљу, потребно је прво идентификовати саобраћај у контролној равни и раздвојити га у различите мапе класа.

Примена политика контроле контролне равни, пошто иста филтрира саобраћај, од кључне је важности да се стекне адекватан ниво разумевања о легитимном саобраћају, који је намењен процесору, пре примене.

Политика полиса приступа мрежним уређајима се састоји од следећих корака, који представљају методологију која олакшава процес дизајнирања и примене исте:

Корак 1: Одредити класификациону шему за мрежу и идентификовати познате протоколе који приступају процесору и поделити их у категорије водећи рачуна о специфичности мреже,

Корак 2: Дефинисати листе приступа,

Корак 3: Прегледати идентификовани саобраћај и прилагодити класификацију (у идеалном случају, класификација обављена у кораку 1, идентификовала је сав потребан саобраћај намењен рутеру),

Корак 4: Ограничити опсег изворних адреса,

Корак 5: Сузити број врста листа приступа на овлашћене изворне адресе. На пример, само познатим станицама за управљање мрежом требало би да буде дозвољен приступ SNMP портовима на рутеру.

Корак 6: Прецизирати политике полиса приступа мрежним уређајима имплементацијом ограничења брзине. Анализирати број пакета и информације о брзини и сходно томе развијати политику ограничавања брзине [20].

2.2.2. Заштита контролне равни (CPPr – Control Plane Protection)

Заштита контролне равни се односи на механизме који се примењују с циљем вршења класификације саобраћаја којим се оптерећује рутер (комутатор).

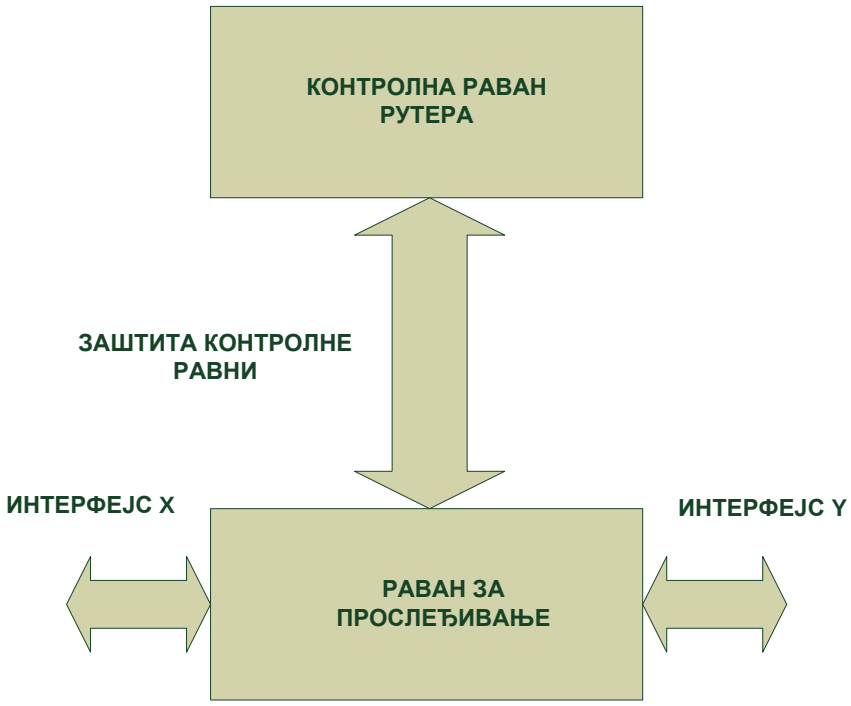
Обзиром да рутери представљају основну компененту рачунарских мрежа и да се помоћу истих врши рутурање мрежног саобраћаја, које је одређено рутинг табелама, неопходно је размотрити архитектуру рутера и рањивост истог на безбедносне претње, у овом случају конкретно у контролној равни, и примени заштите контролне равни.

Архитектура рутера може се приказати као раздвајање хардвера и софтвера на: раван за прослеђивање и контролну раван рутера.

Контролна раван рутера подржава функције рутирања и управљања. Генерално се састоји од хардверских и софтверских компоненти за руковање пакетима намењених самом уређају, као и прављење и слање пакета који се формирају локално на уређају.

Раван прослеђивања се обично састоји од хардверских и софтверских компоненти, одговорних за примање пакета на долазном интерфејсу, обављање претраге да би се идентификовала IP адреса пакета на следећем скоку и одредио најбољи одлазни интерфејс према одредишту и прослеђивање пакета преко одговарајућег излазног интерфејса.

Наведене две равни и њихова функционалност се могу приказати схемом на слици 7.



Слика 7. Заштита контролне равни рутера

Хардвер контролне равни рутера обично није оптимизован за рад са саобраћајем велике брзине. С обзиром на наведено, хардвер контролне равни рутера је подложнији нападима ускраћивања услуге (DDoS), него хардвер равни за прослеђивање, који је пројектован за саобраћај већих брзина. Имајући у виду значај размене података о рутирању у мрежи, императив је да контролна раван рутера остане стабилна, без обзира на саобраћајно оптерећење.

Контролна раван рутера обрађује саобраћај намењен рутеру, а због ширег опсега функционалности је подложнија безбедносним рањивостима и вероватнија мета за DDoS напад од равни за прослеђивање.

Заштита контролне равни рутера је концепт филтрирања или ограничавања брзине нежељеног саобраћаја, који би био преусмерен из равни података до контролне равни рутера.

Препоручљиво је заштитити контролну раван рутера имплементацијом механизама за потпуно филтрирање или ограничење брзине саобраћаја, који није потребан на нивоу контролне равни (тј. нежељени саобраћај). Заштита контролне равни рутера је концепт

филтрирања или ограничавања брзине нежељеног саобраћаја, који би био преусмерен са равни за прослеђивање до контролне равни рутера. Што су филтери и ограничавачи брзине ближе равни за прослеђивање и хардверу за линијску брзину, то је заштита ефикаснија и отпорнији је систем на DDoS нападе.

Метода описана на слици 1., илуструје како заштитити контролну раван рутера од нежељеног саобраћаја. Имајући у виду да ће се сценарији примене разликовати, одређена примена није генерално применљива у свим ситуацијама. Категоризација легитимног саобраћаја у контролној равни рутера је критично важна за успешну имплементацију.

Неки од примера филтрирања саобраћаја могу обухватати следеће врсте саобраћаја:

– Дозвола за ICMP и ICMPv6 саобраћај из било ког извора, ограничено на брзину од 500 kb/s, за сваку категорију,
– Дозвола за OSPF саобраћај са рутера унутар одређене и дефинисане подмреже и OSPFv3 саобраћаја са IPv6 *unicast* адреса,
– Дозвола за интерни BGP (iBGP) саобраћај са рутера унутар одређених подмрежа,
– Дозвола за NTP саобраћај са NTP сервера унутар дефинисане подмреже,
– Дозвола за саобраћај протокола за управљање мрежом (SNMP) са станица за управљање мрежом унутар дефинисане подмреже,
– Дозвола за SSH саобраћај са станица за управљање мрежом унутар дефинисане подмреже,
– Дозвола за DNS саобраћај са DNS сервера унутар одређене и претходно дефинисане подмреже,
– Дозвола за други IPv4 и IPv6 саобраћај, који није у вези са класама саобраћаја који су претходно наведени, уз брзину ограничену на 500 kb/s и одбијање саобраћаја изнад те брзине за сваку категорију.

У равни за прослеђивање је инсталиран филтер. Овај филтер прати саобраћај који је наведен у претходном делу, у коме су описане врсте саобраћаја као пример фитрирања. Пошто је филтер наметнут у равни за прослеђивање, он спречава нежељени саобраћај да заузима пропусни опсег на интерфејсу, који повезује раван за прослеђивање са контролном равни рутера. Бројачи који се налазе у филтеру су важан форензички алат за анализу

потенцијалних напада и као непроцењива помоћ за отклањање грешака и решавање проблема.

Поред филтера, лимитатори брзине за одређене класе саобраћаја су такође инсталирани у равни прослеђивања. Ови лимитатори брзине помажу да се додатно контролише саобраћај, који ће стићи до контролне равни рутера за сваку филтрирану класу, као и сав саобраћај који се не подудара са прецизно дефинисаном класом.

Приликом дизајнирања метода заштите контролне равни, постоје два независна дела која треба узети у обзир: класификацију саобраћаја (тј. које врсте саобраћаја одговарају филтерима) и акције политике предузете у вези са класификованим саобраћајем (тј. одбијање, дозвола, ограничење брзине итд.) [21].

2.2.3. Аутентификација рутинг протокола

Аутентификација рутинг протокола се примењује како би се спречила измена рутинг табела од стране нападача на мрежу. Размена порука између рутинг протокола подлеже утврђивању веродостојности порекла – аутентификацији. За аутентификацију се користе различити алгоритми, који могу бити различити и у односу на различите IP подмреже. [25]

Навешћемо најчешће методе аутентификације следећих рутинг протокола: OSPFv2 (Open shortest Path First), RIPv2 (Routing Information Protocol) и BGPv4 (Border Gateway Protocol).

Технике које се примењују за аутентфикацију OSPFv2 протокола могу бити:

- аутентификација лозинком и
- провера аутентичности са сажетком порука (MD –5).

Једноставна аутентификација лозинком (отвореним текстом), омогућава да се лозинка (кључ) конфигурише у једном домену. Рутери у истој области који желе да учествују у домену рутирања мораће да буду конфигурисани са истим кључем. Недостатак ове методе је, што је подложан пасивним нападима. Нападач пасивним нападом на мрежу, може лако доћи до податка о лозинки и тиме обесмислити аутентификацију лозинком, и у даљем вршити снимање целокупног саобраћаја и потенцијалну измену пакета и података за рутирање.

Аутентификација лозинком се једноставно конфигурише следећим командама:

ip ospf authentication−key „садржај кључа“ (за наведено се одређује посебан интерфејс)

area „ознака области“ **authentication** (одређује се за конкретан OSPF процес рутера)

Потврда аутентичности са сажетком порука (message digest), или коришћењем дигиталног потписа, је криптографска аутентификација употребом тзв. једносмерних „хеш“ функција. Кључ (лозинка) и идентификациони број кључа су конфигурисани на сваком рутеру посебно. Рутер користи алгоритам који је део OSPF пакета (MD5), кључ и идентификациони број кључа, да генерише „сажетак поруке“, који се додаје пакету. За разлику од једноставне аутентификације, кључ се не размењује преко комуникационе линије. Саставни део OSPF пакета је редни број, који се прогресивно увећава како би се спречио напад понављањем пакета.

Аутентифкација сажетком порука (дигиталним потписом) се једноставно конфигурише следећим командама:

ip ospf message−digest−key key id md5 „садржај кључа“ (за наведено се одређује посебан интерфејс).

area „ознака области“ **authentication message−digest** (одређује се за конкретан OSPF процес рутера) [22].

Када је у питању избор једносмерне „хеш“ функције за аутентификацију, у последње време се поред MD5, користи SHA – 2 алгоритам.

Када је у питању RIPv2 протокол, најчешће се не користи аутентификација лозинком, већ се користи аутнтификација дигиталним потписом, коришћењем једносмерних „хеш“ функција. У употреби су MD5, SHA – 2 и HMAC SHA-1, SHA-256, SHA-384, and SHA-512 алгоритми.

BGPv4 протокол рутирања користи напред наведне технике аутентификације, које се разликују по питању имплементације у односу на произвођача мрежне опреме (Cisco, Juniper).

2.3. Заштита равни података

Рачунарске мреже, поред других намена (заједничко коришћење мрежних ресурса, управљање процесима и друго), користе се за пренос информационог садржаја или остваривање корисничких сервиса. У току преноса, информациони садржај је изложен различитим врстама напада, што пред пројектанте и мрежне инжењере поставља захтеве за применом различитих техника у циљу заштите наведеног саобраћаја.

Технике заштите се мрежног саобраћаја у равни података се могу поделити према слоју мреже у којој се примењују. Примери техника заштите у мрежном, транспортном и апликативном слоју су: примена приступних листи, фајервол, системи за превенцију упада – Intrusion prevention systems (IPS), пресретање TCP сегмената (TCP intercept) и други.

Технике заштите у слоју података су: заштита портова (Port Security), DHCP извиђање, динамичка ARP инспекција (DARP inspection) и друге.

Посебан механизам заштите информационог садржаја који се преноси путем Интернета су виртуелне приватне мреже (VPN – Virtual Private Networks).

За реализацију виртуелних приватних мрежа користе се различите технологије и протоколи, и то: IPSec, GRE (Generic Routing Encapsulation), Draft Martini, L2TPv3, IEEE 802.1Q, MPLS LSP, PPTP (Point-to-Point Tunneling Protocol), SSL (Secure Sockets Layer) и друге.

Виртуалне приватне мреже се користе за заштиту саобраћаја у ширем смислу, и могу се успоставити на L1, L2 и L3 мрежном слоју OSI модела.

Да би се остварила заштита виртуелним приватним мрежама, потребно је уградити уређаје које омогућавају потребне функционалности.

У наредном поглављу ћемо размотрити најчешћу технологију успоставе виртуелних приватних мрежа употребом IPSec протокола.

2.4. Заштита података применом технологије виртуелних приватних мрежа

Једна од технологија која омогућава заштиту преноса података у равни података је технологија виртуелних приватних мрежа (VPN – Virtual Private Networks). Наведена технологија пружа следеће могућности умрежавања:

– Интранет, умрежавање географски дислоцираних објеката;

– Удаљени приступ мобилних корисника (рад од куће);

– Екстранет, ограничени приступ некој мрежи из других мрежа (приступ пословних партнера корпоративном WAN-у) [8].

За реализацију виртуелне приватне мреже могу се користити периферни кориснички уређаји (хост, рутер или свич), на локацији корисника (CE – Customer Edge) и периферни мрежни уређаји провајдера (PE – Provider Edge).

Виртуелну приватну мрежу чини више удаљених мрежа које су повезане преко Интернета. Због коришћења заједничких ресурса на Интернету, комуникација међу корисницима виртуелне приватне мреже се мора заштитити. Заштита виртуелне приватне мреже се остварује помоћу баријера, које имплементирају IPSec протокол у тунел моду [23].

VPN тунел је веза између два PE рутера или два CE уређаја, који представљају крајње тачке тунела [24].

Према IETF, IP VPN се могу класификовати у зависности од одговорности у погледу управљања на:

– VPN којима управља корисник (Customer Provisioned VPN, CP VPN);

– VPN којима управља провајдер сервиса (Provider Provisioned VPN, PP VPN) [25].

Према локацији VPN опреме, PP VNP се могу поделити на:

– CE – базиране, код којих су крајње тачке VPN лоциране код корисника;

– PE – базиране, код којих су крајње тачке VPN тунела лоциране код провајдера, на PE рутеру.

У зависности од понуђеног сервиса, PE – базиране VPN се деле на:

– PE – базиране L2 VPN (које пружају сервисе OSI слоја 2);
– PE – базиране L3 VPN (које пружају сервисе OSI слоја 3);
– CE – базиране VPN (пружају само сервисе OSI слоја 3).

За пренос информационог садржаја преко Интернета неопходно је обезбедити заштиту у преносу. Чест је случај да компаније користе Интернет као окосницу за повезивање својих филијала или клијената како би остварили пренос података за своје потребе. Из наведеног разлога намеће се потреба за заштитом преношеног саобраћаја. У ту сврху користе се различите технологије, од којих је једна – технологија виртуелних приватних мрежа. За реализацију вритуелних приватних мрежа на раполагању је више технологија, зависно од тога да ли се VPN реализује као „област – област“ (site–to–site) или као „удаљени приступ“ (remote access). У оба наведена случаја најчешће се користи IPSec (IP Security) протокол. IPSec протокол штити пакете између два уређаја у мрежи [23].

Уређаји којима се реализује IPSec су: сервер, рутери, кориснички рачунари или специјализовани хардвер. IPsec протокол пружа две врсте заштите: аутентификацију и поверљивост.

Механизам аутентификације осигурава, да је примљени пакет заиста послао онај ко је у заглављу пакета наведен као извор и да се пакет није променио током преноса, док механизам поверљивости омогућава ентитетима у комуникацији да шифрују поруке како би спречили непозвана лица да дођу до садржаја порука [8]. За шифровање података користе се симетрични алгоритми (DES, 3DES, AES), што захтева поуздану размену кључева страна у комуникацији, и за ту сврху се користе протоколи за аутентификацију (неки од протокола из IETF (IKE - Internet Key Exchange) стандарда) [23].

Развој безбедности у архитектури Интернета се одвијао постепено, у чему је значајно место имала Радна група за инжењеринг Интернета (IETF – Internet Engineering Task Force). Само увођење стандарда је ишло постепено. Први у низу стандард IETF који се односио на безбедност у архитектури Интернета био је стандард RFC 1636 (Request for Comments). Стандард се односио на основе безбедности Интернета (употреба firewall – a, сервис аутентификације, приватности и др.) [26].

Да би се адекватно разумео начин формирања VPN сесије, и на прави начин представио приликом едукације, биће размотрено неколико најважнијих докумената IETF, којима су дефинисани модови рада VPN, механизам аутентификације, размена криптографских кључева и заштита поверљивости.

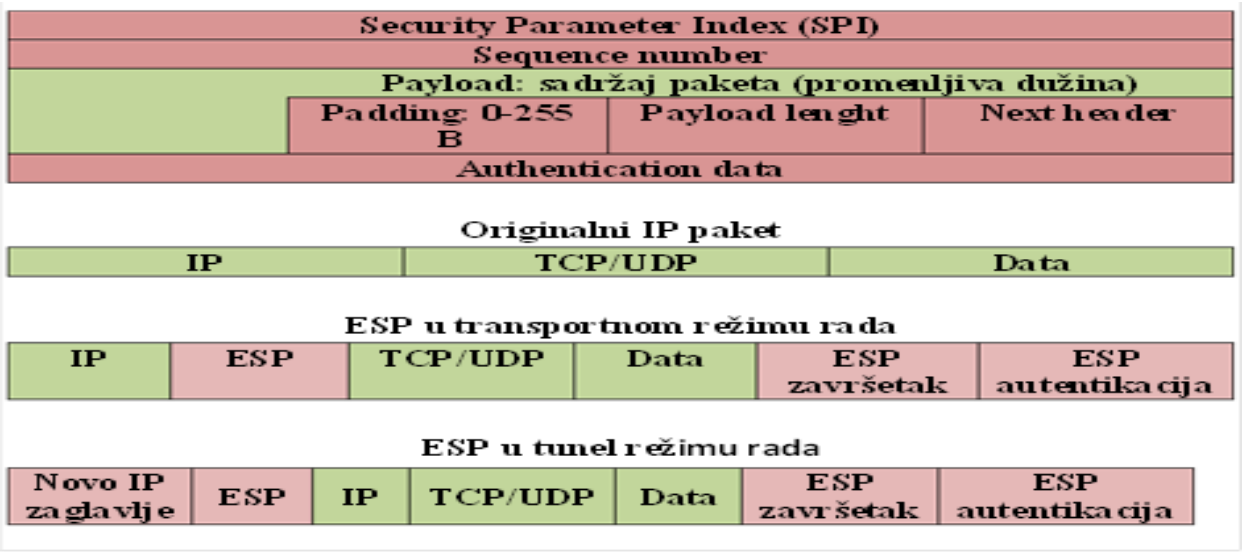
IPSec користи два протокола за безбедност: AH (Authentication Header) i ESP (Encapsulating Security Payload). Заглавље аутентификације (AH) је дефинисано спецификацијом RFC 4302 (IP Authentication Header), док је ESP енкапсулирајуће безбедно паковање (Encapsulating Security Payload) дефинисано спецификацијом RFC 4303. AH и ESP подржавају два режима рада: транспортни режим и тунеловање.

У транспортном режиму AH аутентификује IP користан садржај и одабране делове IP заглавља, док ESP шифрује и опционо аутентификује IP користан садржај. Тунеловање врши заштиту целог IP пакета. Наведено се постиже након додавања AH i ESP поља и третирања целог пакета као корисног садржаја новог спољног IP пакета, са новим IP заглављем.

У режиму тунеловања, ESP шифрује и опционо аутентификује цео унутрашњи IP пакет, укључујући унутрашње IP заглавље, док AH у режиму тунеловања аутентификује цео унутрашњи IP пакет и одабране делове спољног IP заглавља [8].

Редослед поступака са пакетима за рад ESP у транспортном и тунел режиму је следећи:

– У транспортном режиму, блок података који се састоји од сегмента транспортног слоја, са додатим ESP завршним блоком, се шифрује, са додатим заглављем за аутентификацију (опционо);
– У режиму тунеловања, ESP се користи за шифровање целог IP paketa, ESP заглавље иде испред пакета и шифрује се пакет заједно са ESP завршним блоком.



Слика 8. Опсег ESP шифровања у транспортном и тунел моду [27]

Слика 8., приказује формат једног ESP пакета. Индекс безбедносних параметара (SPI) дефинише једну безбедносну асоцијацију, којом се одређује алгоритам шифровања и аутентификације, кључеви, иницијализационе вредности, животни век кључева и везани параметри, који се користе уз ESP. Број секвенце је вредност бројача пакета, којом се спречава понављање пакета. Садржај пакета је променљиве дужине и представља сегмент транспортног слоја (transport mod) или IP пакет (tunel mod). У тунел моду, целом пакету се додаје ново IP заглавље које има довољно информација за рутирање, али не и за анализу саобраћаја [27].

Важан део IPSec, који се односи на управљање кључевима, обухвата одређивање и дистрибуцију кључева. Документом RFC 4301 дефинисане су две врсте управљања кључевима:

– Ручно (администратор дефинише систем сопственим кључевима и кључевима других система са којима комуницира);

– Аутоматизовано (омогућава генерисање кључева за безбедносну асоцијацију на захтев који је погодан за велике системе са растућом конфигурацијом) [28].

Протокол који се користи за аутоматизовано управљање кључевима за IPSec је ISAKMP (Internet SecurityAssociation and key Management Protocol) и дефинисан је документом IETF RFC 2408. ISAKMP дефинише процедуре за креирање и управљање безбедносним

асоцијацијама, технике генерисања кључева, ублажавање претњи (нпр. од DDoS напада)[24].

ISAKMP не налаже конкретан алгоритам за размену кључева, већ се састоји од једног скупа типова порука, које омогућавају употребу разноврсних алгоритама за размену кључева.

Карактеристике IKE одређивања кључева су:

- Осујећење DDoS напада;
- Омогућава размену кључева за преговарање око групе кључева;
- Обезбеђује од напада понављањем, коришћењем једнократних бројева;
- Омогућава размену јавних кључева;
- Онемогућава напад типа "човек у средини".

IKE потпротокол обезбеђује договарање протокола, алгоритама и кључева између учесника у комуникацији, проверава аутентичност учесника који учествују у поступку договарања, омогућава размену података на основу којх ће се генерисати кључеви и управљати разменом кључева. IKE подпротокол одвија се у две фазе [29].

У првој фази два учесника успостављају безбедни комуникациони канал, којим ће се обавити договарање безбедносних параметара и размена кључева. Договарање параметара и размена кључева, односно успостава безбедносне асоцијације обавља се у другој фази. За спровођење поступка користе се три начина размене информација, два за прву фазу и један за другу фазу IKE потпротокола:

- Основни начин;
- Агресивни начин;
- Брзи начин.

Основни начин размене информација (engl. Main mode), користи се у првој фази IKE потпротокола и служи да се успостави безбедан комуникациони канал којим ће се обавити размена података потребних за каснију комуникацију AH или ESP потпротоколима.

Агресивни начин размене, слично као и основни, користи се у првој фази IKE потпротокола и служи за успостављање сигурног комуникационог канала за договор учесника и не обавља се кроз безбедни канал. Агресивни начин користи само три поруке у

размени и нешто је једноставнији и бржи од основног начина, али се доказивање идентитета не врши кроз безбедан канал.

Након успоставе безбедног канала применом основног или агресивног начина размене, започиње друга фаза IKE потпротокола. Друга фаза користи се брзим начином размене кључева, која служи за договарање безбедносних параметара комуникације AH или ESP потпротоколом и за размену тајних симетричних кључева.

3. Принципи преноса телефонског саобраћаја употребом пакетске комутације и Интернет протокола

Развој Интернета има за последицу да се, упоредо са тим, поставио захтев за пренос различитих сервиса (Web, mail, IP телефонија и телевизија и друго).

Пренос телефонског саобраћаја је прошао еволуцију од аналогног преноса, преко дигиталног преноса у мрежама интегрисаних сервиса (ISDN), до пакетског преноса телефоније – VoIP.

Основна подела преноса телефонског саобраћаја је према начину комутације, на пренос комутацијом кола и пренос комутацијом пакета. Пакетска комутација користи две технике: виртуелно коло и датаграм.

Пакетски пренос подразумева комутацију коришћењем IP протокола, а у новије време коришћење протокола развијених за пренос садржаја у реалном времену (RTP, SIP и H.323).

Протоколи преноса треба да испуне одређене стандарде, као што су могућност детекције и корекције грешака, потврђивање пријема пакета, ретрансмисију пакета и слично.

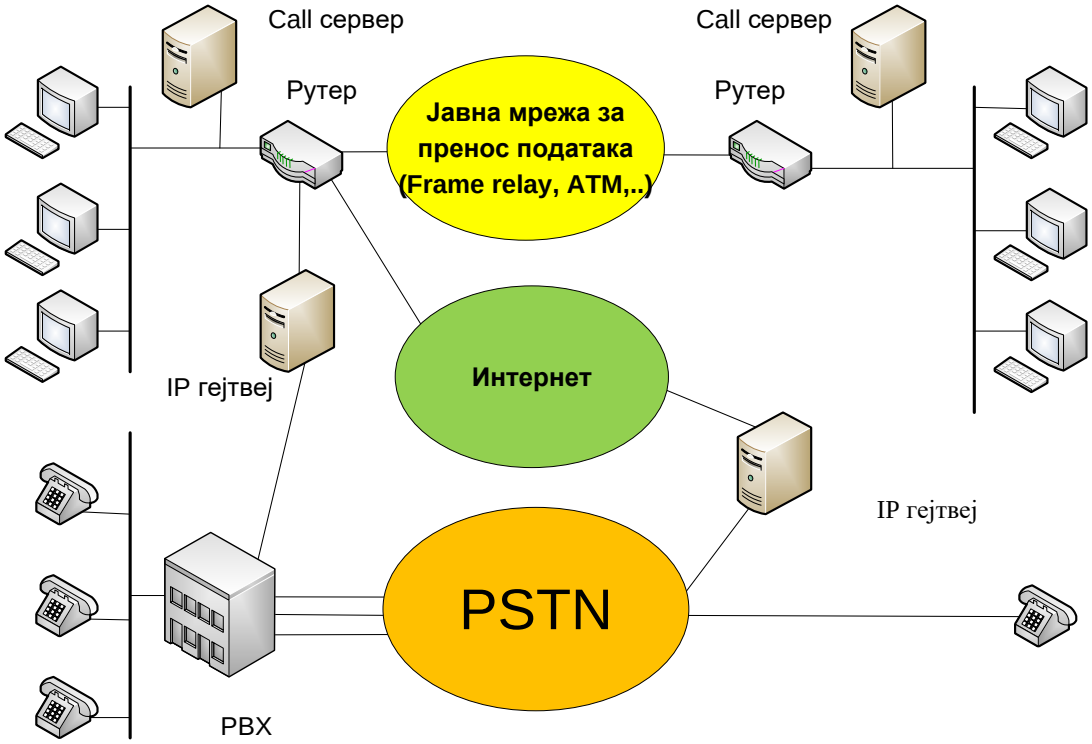
За пренос садржаја у реалном времену ретрансмисија пакета није неопходна, јер поновно слање пакета који је претходно изгубљен, не би имао пуно смисла.

Наведена транзиција преноса телефоније има за последицу да се IP телефонија уводила и уводи постепено, уз интегрисање са ранијим системима преноса (PSTN, ISDN).

Интегрисање са наведеним системима преноса телефоније је узроковало развијање посебне архитектуре. Развијени су следећи елементи за повезивање: Gateway уређаји за повезивање са PSTN и ISDN системима преноса, различите врсте адаптера, IP телефони, апликације или VoIP софтвери који омогућавају да се рачунар користи као телефон, VoIP картице, сервери и друго.

Пренос говора преко IP мрежа захтева прихватање говорног сигнала и његову конверзију у IP пакете. Наведено омогућавају IP телефони, као и посебни софтвери који омогућавају пренос IP телефоније употребом персоналних рачунара.

Имајући све наведено у виду, једна уопштена мрежа за пренос IP телефоније може се приказати схемом на слици 9.



Слика 9. Топологија VoIP система

У поређењу са другим системима преноса, пакетски пренос телефоније има одређене предности које се огледају у следећем:

- Могућност истовременог преноса са другим сервисима (Web, Mail, мултимедија,...),
- Нижа цена и трошкови коришћења опреме,
- Могућност интеграције преноса говора и података,
- Потенцијално захтевају мањи пропусни опсег,
- Распрострањеност IP мрежа,
- Могућност грађења мрежа опремом различитих произвођача,
- Лака проширивост и флексибилност IP мрежа [30].

Све наведено има за последицу убрзано увођење IP телефоније и развијање протокол стека за пренос сервиса у реалном времену. У наредним поглављима биће представљени најважнији протоколи који се користе за пренос IP телефонског саобраћаја.

3.1. Преглед најважнијих протокола који се користе за пакетски пренос телефонског саобраћаја

Поред најважнијих протокола TCP/IP протокол стека на транспортном нивоу (TCP и UDP), развијени су протоколи који су специфично развијени за пренос садржаја у реалном времену (мултимедијалних саржаја, IP телефоније...).

Наведени протоколи треба да омогуће решавање проблема пристизања пакета и редоследу како су послати, обезбеђење података о изгубљеним пакетима, обезбеђење квалитета преноса, успостављање и раскидање телефонске комуникације, повезивање са другим мрежама (PSTN, ISDN, PABx, LAN), конверзију сигнала из једне у другу мрежу и слично.

Најчешће коришћени протоколи који обезбеђују наведене функционалности у преносу IP телефоније су: RTP (Real-Time Transport Protocol), RTCP (RTP Control Protocol), H.323 протокол и SIP (Session Initiation Protocol).

Осим наведених протокола, постоје цели протокол стекови који су саставни део H.323 и SIP протокола.

3.2. RTP (Real-Time Transfer Protocol) протокол

RTP протокол је намењен за пренос садржаја у реалном времену (телефонија, мултимедија). Одређен је документима RFC 3550 и 3551. Потреба за преносом сервиса у реалном времену је захтевала примену једноставнијих протокола, без успостављања везе (UDP), али се временом појавио проблем губитка пакета и пристизања пакета у редоследу како су послати.

Како UDP протокол није обезбеђивао наведене функције, развијен је RTP протокол, који су свом формату има податке о времену слања пакета (сегмента). Поред наведених проблема који су решени помоћу RTP протокола, развијен је RTCP протокол, којим се обезбеђује квалитет преноса, подаци о изгубљеним пакетима и о џитеру (промена у времену кашњења пакета кроз мрежу).

RTCP протокол не преноси информациони садржај, већ наведене податке, који се преносе кроз посебну сесију, опционо када се активира RTCP протокол.

RTP протокол омогућава пренос симултаних сесија говора и слике, где се на пријему врши синхронизација два сигнала у времену. Осим наведеног, RTP протокол омогућава пренос у комуникацији више учесника (конференција), пренос различитих брзина сигнала, комбиновање више токова који долазе из различитих извора у један RTP ток, као и пренос у случају када две стране користе различите технике кодовања [30].

Формат RTP заглавља приказан је на слици 10.

Слика 10. Формат RTP заглавља [30]

За потребе објашњења наведених функција протокола значајни су следећи делови RTP заглавља:

– Број CSRC – број идентификатора контрибутора извора. Користи се код успоставе конференције, као број значајан за рад миксера, који формира један сигнал од више учесника у конференцији (број је увек мањи за један од броја учесника, јер се не рачуна пријемна страна).

– Број секвенце – намењен је за обезбеђење информација за слагање пакета у редослед слања и за детектовање губитка пакета.

– Временска ознака (timestamp) – намењена за синхронизовано представљање података и израчунавање џитера.

– Идентификатор извора синхронизације (SSRC) – идентификује извор синхронизације, односно извор RTP тока. У општем случају то је предајна страна RTP пакета.

– Идентификатор првобитних извора (CSRC) – користи се за идентификацију извора медија који учествују у сесији (код преноса конференције преко миксера) [30].

RTCP протокол има четири функције:

– Обезбеђење повратних информација које се односе на квалитет дистрибуције података,

– Обезбеђење информације о идентификатору RTP извора на транспортном нивоу – CNAME – Canonical Name (разликује се од SSRC идентификатора, јер је исти за једног учесника сесије, док се SSRC може мењати услед проблема и прекида, или је различит за пренос говора и слике код мултимедијалног преноса, док је CNAME увек исти за једног учесника сесије),

– Слање RTCP пакета од стране свих учесника,

– Преноси минимално контролисане информације (специфично код слабо контролисаних сесија, где учесници приступају сесији без контроле приступа и размене параметара) [30].

3.3. H.323 протокол

H.323 протокол је дефинисан препорукама ITU – T (ITU Telecommunication Standardization Sector), а намењен је за дефинисање протокола задужених за мултимедијалне комуникације, преко мрежа са комутацијом пакета.

Комуникација преко H.323 може се остварити у било којој пакетској мрежи, независно од топологије мреже.

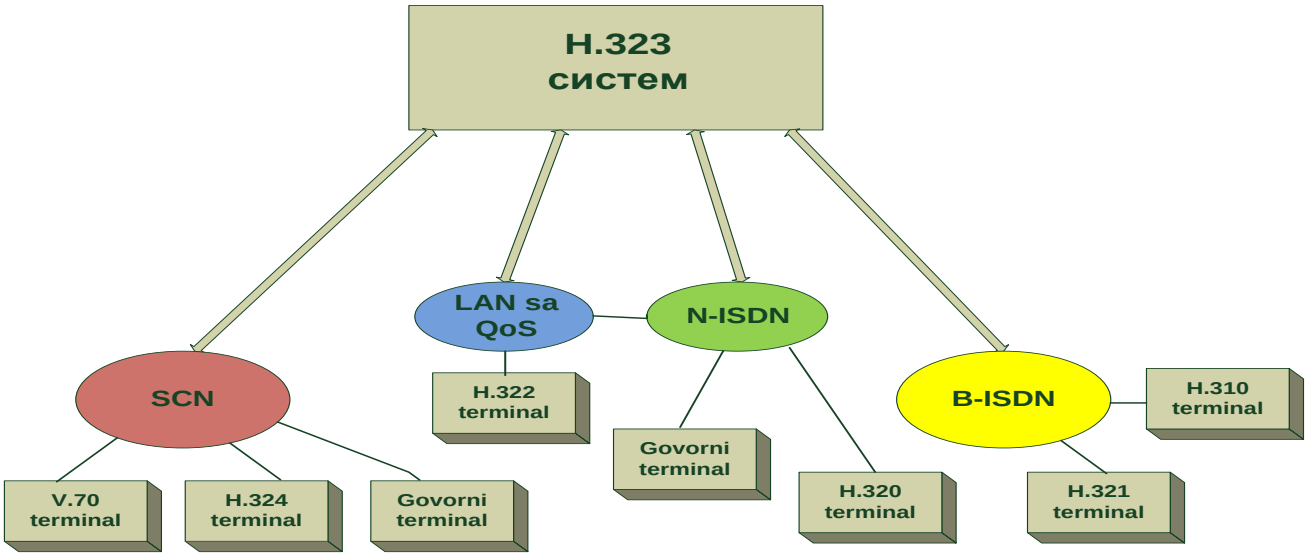
Слика 11. приказује H.323 терминале који као основу користе пакетску мрежу.

Слика 11. Коришћење пакетске мреже од стране H.323 терминала [30]

H.323 се користи као сигнализациони и контролни протокол у VoIP мрежама и за IP видео конференције. Због наведеног, H.323 протокол је у себе абсорбовао RTP протокол.

H.323 протокол омогућава комуникацију са другим типовима мрежа и то: ускопојавсне ISDN (H.320), широкопојасне ISDN (H.321 и H.310), локалне рачунарске мреже (H.322) и мреже на бази комутације кола (SCN – Switched Circuit Networks, H.324).

Слика 12. приказује интероперабилност H.323 и других H.32x мрежа.



Слика 12. Коришћење пакетске мреже од стране H.323 терминала [30]

Приказана интероперабилност је омогућена увођењем гејтвеја, који врши превођење формата или сигнализације.

Унутрашња структура H.323 система се састоји од:

- Терминала
- Гејтвеја (Gateway)
- Гејткипера (Gatekeeper) и
- MCU (Multipoint Control Unit)

Терминал се користи за двосмерну мултимедијалну комуникацију у реалном времену (нпр. IP телефон).

Гејтвеј омогућава повезивање две мреже засноване на различитим системима преноса. Омогућава повезивање H.323 мреже са мрежама које нису засноване на H.323 стандарду.

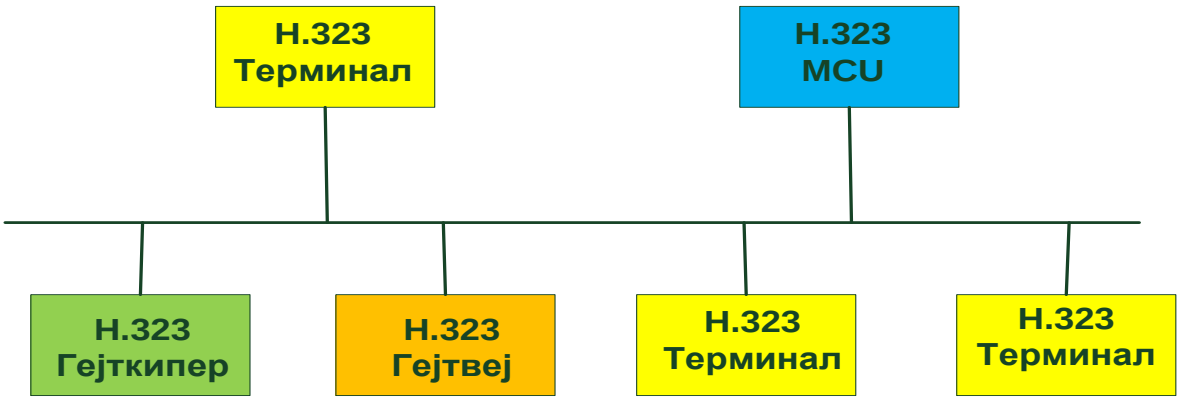
Гејткипер контролише све остале H.323 компоненте (терминале, гејтвеје и MCU) и одређује се опционо. Једним гејткипером је одређена једна зона, у којој гејтипер врши ауторизацију, транслацију адресе, управљање пропусним опсегом, усмеравање позива, утврђивање идентитета терминала и друго.

Multipoint Control Unit подржава конференцијску везу три и више терминала, усклађује кодере/декодере који се користе у конференцији и управља конференцијским ресурсима.

Поред зона, у H.323 систему, постоји и административни домен који подразумева више зона којима се управља из једног центра.

H.323 стандард представља скуп протокола који обављају различите функције и односе се на: аудио/видео кодере и декодере, регистрацију, приступ, статус, сигнализирање позива, контролу позива, протокол преноса у реалном времену (RTP), протокол контроле преноса у реалном времену (RTCP) и остало [30].

Структура H.323 архитектуре је приказана на слици 13.



Слика 13. Компоненте H.323 система [30]

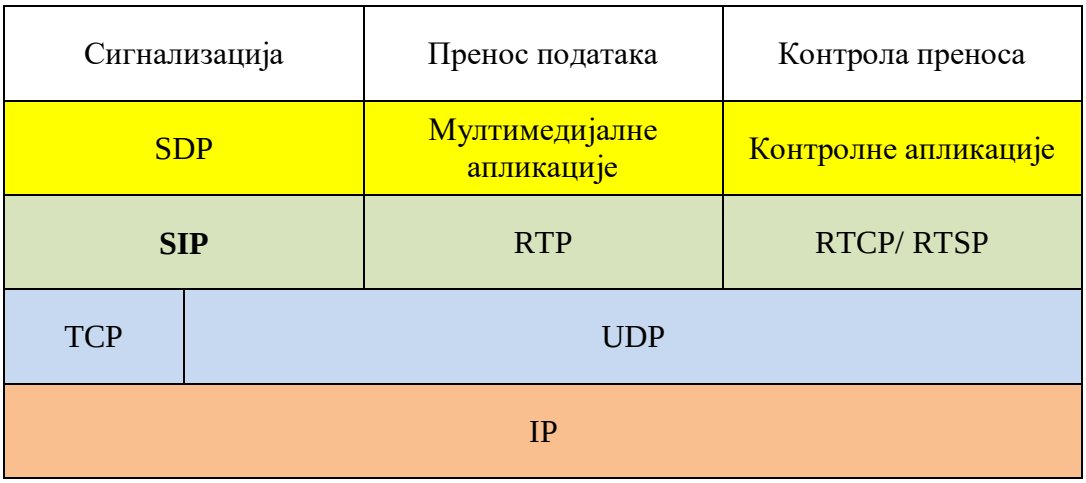
3.4. SIP (Session Initiation Protocol) протокол

SIP протокол је намењен за успостављање разноврсних сесија (unicast, multicast), интерактивних комуникација (Интернет мултимедијалне конференције, Интернет телефонски позиви, мултимедијална дистрибуција). Базиран је на HTTP протоколу (текстуално кодовање порука), као и на моделу комуникације клијент – сервер.

Поред успоставе везе, обезбеђује и опис карактеристика сесије корисницима. Припада групи *peer – to – peer* протокола.

Поруке SIP протокола се могу преносити преко UDP и TCP протокола. Поруке SIP протокола се могу преносити преко IP, ATM и Frame Relay мрежа (најчешће се користе IP мреже).

Место SIP протокола у VoIP протокол стеку је приказано на слици број 14.



Слика 14. Место SIP протокола у VoIP протокол стеку [30]

Пренос мултимедијалних садржаја (као и VoIP) се врши RTP протоколом, а исто се контролише RTCP протоколом. SDP (Session Description Protocol) протокол је намењен за размену конфигурационих података RTP и RTCP протокола, података о броју UDP порта и података о захтеваном пропусном опсегу.

Елементи SIP мреже су:

- Кориснички агент (UA – User Agent),
- Прокси сервер,
- Редирекциони сервер,
- Регистрар сервер.

Кориснички агент може бити клијент или сервер, зависно од тога да ли иницира успоставу везе или ослушкује долазеће позиве. Може бити хардверски или софтверски реализован.

Прокси сервер прослеђује сигнализацију од корисника према мрежи и обрнуто.

Редирекциони сервер прима SIP захтев, мапира одредишну адресу или више адреса и враћа их пошиљаоцу захтева, и тиме помаже у рутирању.

Рад SIP протокола се заснива на регистрацији корисника, како би могли да иницирају и примају позиве. Регистрација омогућава мобилност корисника, тако што се подаци о кориснику достављају регистрар серверу (SIP адреса, тренутна контакт адреса регистрар серверу). Осим наведени елемената, SIP архитектура има и *Location* сервер (базу података о корисницима). *Location* сервер је функционална компонента која може бити интегрисана са неким од осталих сервера.

Адресе у SIP протоколу имају формат облика:

user@host, параметри

Може се закључити да су адресе SIP протокола сличне e-mail адресама, као и да нису везане за кориснички уређај, већ идентификују учесника. Сигнализационе процедуре обично стартују SIP адресама, да би се касније преводиле у адресе у којима фигурише име конкретног хоста где је учесник улогован.

SIP поруке се деле на:

- Захтеве (requests), које клијенти шаљу серверима,
- Одговоре (responses), које сервери враћају клијентима.

Постоје основни SIP захтеви (INVITE, ACK, OPTIONS, BYE, CANCEL, REGISTER) и додатни SIP захтеви (INFO, UPDATE, REFER, SUBSCRIBE, MESSAGE, PRACK).

SIP одговори су подељени у класе и то:

- 1xx – информативни одговори,
- 2xx – позитивни одговори,
- 3xx – преусмеравање,
- 4xx – грешка у захтеву,
- 5xx – грешка сервера,
- 6xx – глобална грешка.

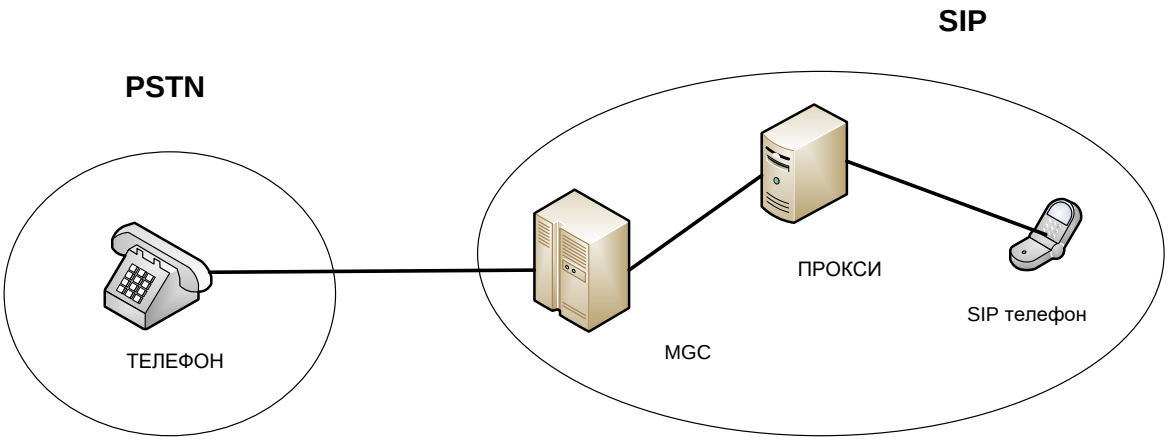
Прва цифра у одговору дефинише класу одговора, док остале две конкретан одговор из класе.

Основне сигнализационе процедуре SIP протокола су: регистрација, регистрација са аутентификацијом, позивање, раскидање сесије, редирекциони сервери и прокси сервери.

SIP је сигнализациони протокол који не служи за управљање мрежним ресурсима, али може да се повеже са механизмима који служе у те сврхе и обезбедити квалитет сервиса.

SIP протокол омогућава и повезивање са PSTN мрежама, помоћу гејтвеја који извршава конверзију сигнализације и сигнализационих процедура, као и самог тока који преноси информације.

Слика 15. показује успоставу везе SIP телефона и телефона у PSTN мрежи.



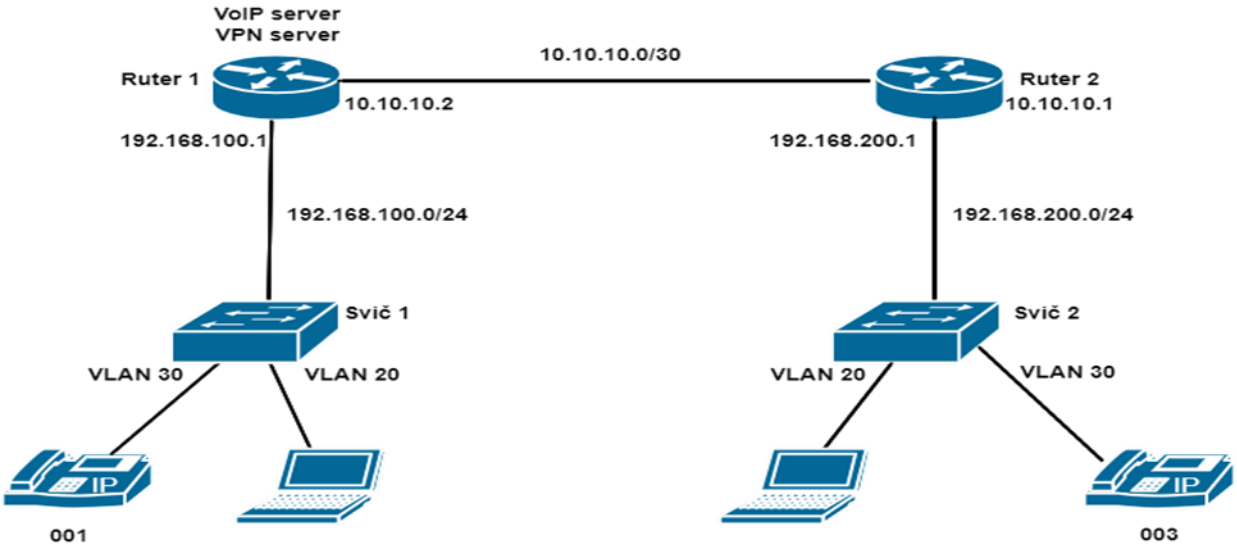
Слика 15. Успостава везе SIP телефона и телефона у PSTN мрежи [30]

У приказаној шеми, MGC (Media Gateway Controller) врши конверзију сигнализације.

4. Један приступ реализацији заштите пакетског телефонског саобраћаја употребом технологије виртуелних приватних мрежа

4.1. Опис задатка и спецификација коришћене опреме

Један приступ реализацији заштите пакетског телефонског саобраћаја употребом технологије виртуелних приватних мрежа представљена је схемом на слици број 16.



Слика 16. Топологија мреже једног приступа реализацији заштите пакетског телефонског саобраћаја употребом технологије виртуелних приватних мрежа

Приказана топологија мреже има за циљ успоставу VoIP саобраћаја у незаштићеном и заштићеном преносу.

Заштићен пренос је омогућен успоставом remote access (удаљени приступ) VPN сесије, у тунел моду, користећи IPSec протокол.

Најпре је извршено успостављање мрежне конективности, конфигурацијом уређаја помоћу стандардних команди из опсега CISCO командне линије (CLI – Command Line Interface).

Потом је извршено конфигурисање VPN сервера на рутеру 1, VoIP сервера (централе), успостава VoIP саобраћаја у незаштићеном и заштићеном моду, респективно.

Успостава и одржавање VoIP саобраћаја (незаштићеног и заштићеног) је на крају анализирано употребом софтверског алата Wireshark.

Наведено приказивање и анализа саобраћаја омогућена је употребом софтверског IP телефона Zoiper, који су инсталирани на рачунарима у мрежи.

Успостава VPN сесије је вршена коришћењем апликације VPN Client.

Приликом реализације приказане мрежне топологије, коришћена је следећа мрежна опрема:

- Рутери CISCO 2900…….....2 ком.

CISCO 2900 серија рутера нуди значајне перформансе и скалабилност за средње велике мреже. Ови уређаји подржавају различите брзине, укључујући подршку за Гигабит Етернет и опционо WAN везу високог капацитета.

CISCO 2900 рутери су дизајнирани за интеграцију различитих сервиса и функционалности, као што су firewall, VPN, IP телефонија, видео конференције и друге комуникационе сервисе. Наведено омогућава организацијама да користе један уређај за различите потребе уместо више одвојених уређаја.

CISCO 2900 рутери обично долазе са модуларним слотовима, који омогућавају додавање додатних модула за проширење капацитета и функционалности.

CISCO 2900 серија рутера пружа напредне могућности за заштиту мреже и података.То укључује интегрисане firewall опције, VPN подршку за сигуран приступ и комуникацију преко јавних мрежа, IDS/IPS (Intrusion Detection/Prevention System) функционалност за откривање и спречавање неовлашћеног приступа и друге безбедносне механизме.

CISCO 2900 рутери омогућавају централизовано управљање мрежом, путем разних управљачких и мониторинг алата, што олакшава одржавање, дијагностику и праћење перформанси мреже.

CISCO 2900 рутери подржавају широк спектар мрежних протокола и технологија, укључујући IPv4, IPv6, MPLS (Multiprotocol Label Switching), QoS (Quality of Service) и друге.

Поред основних функционалности рутера, CISCO 2900 серија омогућава имплементацију различитих напредних сервиса и апликација, као што су видео конференција, IP телефонија, виртуализација мреже и сервиса, оптимизација мреже и многе друге.

CISCO 2900 серија рутера долази са различитим моделима који могу имати различите комбинације интерфејса.

Интерфејси који се налазе на CISCO 2900 серији рутера:

Етернет интерфејси су Фаст Етернет (10/100/1000 Mb/s) портови и користе се за повезивање са локалним мрежама (LAN) или другим уређајима.

WAN интерфејси:

CISCO 2900 серија рутера обично има интерфејсе који подржавају различите типове WAN конекција, као што су T1/E1, T3/E3, ADSL, VDSL, SHDSL и друге технологије које омогућавају повезивање са спољним мрежама.

USB интерфејси:

Неке верзије CISCO 2900 рутера такође садрже USB интерфејсе који се могу користити за повезивање додатних уређаја, као што су USB меморијски уређаји или USB модеми.

Модуларни интерфејси:

Ови интерфејси омогућавају додавање различитих модула за проширење функционалности рутера. Ови модули могу обухватати додатне Етернет портове, подршку за VoIP, подршку за безбедносне функционалности и друге.

Конзолни и управљачки интерфејси:

Ови интерфејси омогућавају администраторима да се повежу са уређајем за конфигурацију, управљање и дијагностику. То укључује конзолни порт, TELNET и SSH (Secure Shell) за даљинску администрацију [31].

Техничке карактеристике CISCO 2900 рутера дате су у табели 2.

Табела 2: Техничке карактеристике рутера Cisco 2900 [31]

	Cisco 2901	**Cisco 2911**	**Cisco 2921**	**Cisco 2951**
Услуге и број слотова				
Уграђена хардверска криптографија	да	да	да	да
Укупан број WAN 10/100/1000 портова	2	3	3	3
RJ-45-портова	2	3	3	3
Број слотова за сервисне модуле	0	1	1	2
Величина меморије DDR2 ECC DRAM	512 MB	512 MB	512 MB	512 MB

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Величина меморије (DDR2 ECC DRAM) - максимално	2 GB	2 GB	2 GB	2 GB
Број екстерних USB 2.0 Flash Memory слотова (Тип A)	2	2	2	2
USB конзолних портова (Тип B) (до 115.2 kb/s)	1	1	1	1
Број серијских конзолних портова	1	1	1	1
Број Auxiliary портова	1	1	1	1

Слика 17. Изглед рутера Cisco 2900

– Свичеви Cisco CATALYST 3650.....2 ком.

Cisco CATALYST 3650 је серија мрежних свичева која се често користи у пословним и корпоративним мрежама. Пружају низ напредних функционалности и могућности за управљање и оптимизацију мрежног саобраћаја.

Основне карактеристике Cisco CATALYST 3650 свичева су:

Стекинг (спајање у “Stack”):

Cisco CATALYST 3650 свичеви подржавају могућност спајања више уређаја у стек, како би се постигла већа скалабилност и управљање. То омогућава администраторима да управљају са више уређаја као са једним логичким ентитетом, олакшавајући конфигурацију и управљање мрежом.

Unified Access (јединствени приступ):

Ови свичеви су део Cisco Unified Access архитектуре, која омогућава интегрисано управљање мрежама са кабловским и бежичним уређајима, што олакшава конзистентно пружање услуга и политика на свим уређајима у мрежи.

Power over Ethernet (PoE):

Многe верзије Cisco CATALYST 3650 свичева подржавају Power over Ethernet технологију, што омогућава напајање бежичних приступних тачака, IP телефона и других уређаја преко Етернет кабла, без потребе за додатним напајањем.

Advanced Security (напредна сигурност):

Cisco CATALYST 3650 свичеви пружају напредне могућности сигурности, укључујући функционалности као што су Access Control Lists (ACLs), 802.1X аутентификација, Port Security, IP Source Guard и други механизми за заштиту мреже од неовлашћеног приступа.

Quality of Service (QoS):

Cisco CATALYST 3650 свичеви подржавају QoS функционалности, које омогућавају приоритетни третман одређеног саобраћаја, као што је VoIP, видео и други саобраћај, како би се осигурала оптимална изведба мреже.

Advanced Layer 3 Routing (напредно усмеравање на слоју 3):

Cisco CATALYST 3650 свичеви пружају могућност рутирања на 3 слоју ISO OSI мреже, што значи да могу преусмеравати IP саобраћај између различитих подсистема мреже, што их чини одговарајућим за различите топологије мреже.

Cisco TrustSec (сигурносни механизми):

TrustSec технологија омогућава имплементацију сигурносних политика базираних на улогама и идентитетима корисника, што доприноси бољој заштити мреже од претњи.

Wireless Controller (бежични контролер):

Неки модели Cisco CATALYST 3650 свичева садрже интегрисане бежичне контролере, што олакшава управљање бежичном мрежом и приступним тачкама.

Network Automation (аутоматизација мреже):

Cisco CATALYST 3650 подржава Cisco DNA Center, централизовано управљање и аутоматизацију мреже, олакшавајући конфигурацију, праћење и дијагностику.

Smart Operations (интелигентне операције):

Cisco CATALYST 3650 свичеви нуде интелигентне операције као што су аутоматско откривање и конфигурација уређаја, идентификација и упозорења о проблемима у мрежи, као и могућности за анализу мрежног саобраћаја.

Cisco CATALYST 3650 серија мрежних прекидача (свичева) долази у различитим моделима са различитим комбинацијама интерфејса, а ови модели су често означени бројевима као што су 3650-24T, 3650-48ПС, 3650-48ФД и слично.

Врсте интерфејса на Cisco CATALYST 3650 свичевима су:

Етернет интерфејси:

Ови интерфејси су најчешће Фаст Етернет (10/100/1000 Mb/s) или 10 Гигабит Етернет портови. Користе се за повезивање уређаја унутар локалне мреже (LAN) или за линкове према другим свичевима или мрежним уређајима.

Uplink интерфејси:

Uplink интерфејси су обично бржи портови (нпр. 10 Гигабит Етернет), који се користе за повезивање са осталим свичевима или уређајима на вишем нивоу у мрежној хијерархији.

Stacking интерфејси:

Cisco CATALYST 3650 свичеви подржавају Stacking (спајање у стек), како би се постигла већа скалабилност и управљање. Stacking интерфејси омогућавају физичко повезивање више свичева, како би се управљали као један уређај.

Конзолни и управљачки интерфејси:

Ови интерфејси омогућавају администраторима да се повежу са свичем за конфигурацију, дијагностику и управљање.То укључује конзолни порт, TELNET и SSH (Secure Shell) за даљинску администрацију.

USB интерфејси:

Неки модели Cisco CATALYST 3650 свичева имају USB портове који се могу користити за додатне уређаје и функционалности.

PoE интерфејси:

Многе верзије Cisco CATALYST 3650 свичева подржавају Power over Ethernet технологију, која омогућава напајање бежичних приступних тачака, IP телефона и других уређаја преко Етернет кабла.

Бежични интерфејси:

Неки модели Cisco CATALYST 3650 свичева имају интегрисане бежичне контролере и могу подржавати бежичне приступне тачке [32].

Слика 15 приказује изглед Cisco CATALYST 3650 свича.

Слика 18. Изглед Cisco CATALYST 3650 свича

– Рачунар са ETH мрежним интерфејсом.....2 ком.

Слика 19. Изглед рачунара са ETH мрежним интерфејсом

– IP телефони.....2 ком.

Слика 20. Изглед VoIP телефона

4.2. Конфигурација рутера и свичева за успоставу рачунарске мреже

Команде за конфигурацију мрежног уређаја и успостављање мрежне конективности су приказане: за рутер R1, у прилогу број 1.

Наведеним командама извршено је подешавање интерфејса Гигабит Етернет 0/0, постављена је мрежна адреса и субнет маска, извршено аутоматско подешавање дуплексног режима рада интерфејса, постављено је аутоматско подешавање брзине интерфејса, повезан криптографски "map1" са овим интерфејсом за евентуално шифровање саобраћаја.

Потом су извршена подешавања за интерфејс ГигабитЕтернет 0/1, као и субинтерфејсе 0/1.1 и 0/1.2. За наведене интерфејсе је постављено таговање 802.1Q VLAN са идентификаторима 20 и 30, респективно, као и постављање IP адреса за наведене субинтерфејсе.

Потом је извршено конфигурисање за OSPF рутирање, постављање интерфејса ГигабитЕтернет 0/1, као пасивног за рутирање мрежа 10.10.10.0, 20.20.20.0 и 30.30.30.0.

На крају је одређен опсег IP адреса за VPN клијенте.

Команде за подешавање рутера R1 приказана у прилогу број 2.

Значење наведених подешавања су аналогна подешавањима рутера R1.

Команде за подешавање свича S1 су приказане у прилогу број 3.

Наведеним командама одређени су портови за VLAN 20 и 30, респективно, као и транк порт ка рутеру R1 за пренос саобраћаја из VLAN – ова, ка рутеру R1.

Дефинисане су IP адресе и мрежне маске за VLAN 20 и 30.

Команде за конфигурацију свича S2 идентичне су командама за дефинисање VLAN портова и транк порта, постављеним на свичу S1.

Командама су дефинисане IP адресе за успостављање IP саобраћаја у VLAN 20 и 30 [33][34].

4.3. Конфигурација рутера за успоставу VPN сервера

Команде за конфигурацију рутера R1, као VPN сервера дате су у прилогу број 4.

Командом: license udi pid CISCO2921/K9 sn FCZ161520KM, одређује се идентификатор рутера користећи његов серијски број у сврху лиценцирања.

Командом: license boot module c2900 technology-package uck9, одређује се лиценцни пакет технологије која ће се користити при покретању, у овом случају, то је "uck9" пакет, који омогућава безбедносне функционалности на рутеру.

Потом се редом креира кориснички налог са именом "admin" и лозинком "admin1", затим crypto isakmp policy 10, којом се започиње конфигурација Internet Security Association and Key Management Protocol (ISAKMP) политике, са бројем секвенце 10.

Команда encr 3des, специфицира алгоритам енкрипције, који ће се користити за ISAKMP преговоре.

Команда: hash md5, специфицира алгоритам хеширања за ISAKMP преговоре, користи се MD5.

Команда: authentication pre-share, поставља метод аутентификације за ISAKMP преговоре као дељених претходно дефинисаних кључева (pre-shared keys).

Команда: group 2, специфицира Diffie-Hellman групу која ће се користити за ISAKMP преговоре.

Команда: crypto isakmp client configuration group cisco, дефинише конфигурациону групу ISAKMP клијента под називом "cisco" за VPN клијенте.

Команда: key cisco123, одређује претходно дефинисан кључ за конфигурациону групу ISAKMP клијента.

Команда: crypto ipsec transform-set set1 esp-3des esp-md5-hmac, дефинише IPsec трансформациони сет под називом "set1", са специфицираним алгоритмима енкрипције (3DES) и заштите интегритета (MD5).

Команда: mode tunnel, поставља тунел IPsec мод.

Команда: crypto dynamic-map map1 10, дефинише динамички криптографску мапу под називом "map1", са бројем секвенце 10.

Команда: set transform-set set1, повезује претходно дефинисан трансформациони сет "set1" са динамичком криптографском мапом.

Команда: reverse-route, конфигурише динамички криптографску мапу, да креира повратне руте за удаљенеVPN клијенте.

Команда: crypto map map1 client authentication list abc1, повезује листу аутентификације "abc1" са криптографском мапом, ради аутентификације долазних клијената.

Команда: crypto map map1 isakmp authorization list abc2, повезује листу ауторизације "abc2" са криптографском мапом ради ауторизације долазних ISAKMP сесија.

Команда: crypto map map1 client configuration address respond, конфигурише криптографску мапу, да користи адресу на коју VPN клијент одговара за конфигурацију клијента.

Команда: crypto map map1 10 ipsec-isakmp dynamic map1, означава да ће унос криптографске мапе са бројем секвенце 10 користити динамичку криптографску мапу под називом "map1" [35].

Команде за конфигурацију рутера R2, као удаљене стране, су дате у прилогу број 5.

Наведене команде омогућавају прихватање корисничких услова за лиценцирање Cisco уређаја, покретање и активацију лиценце за FoundationSuiteK9 пакет, покретање и активацију лиценце за AdvUCSuiteK9 пакет, који се обично користи за напредне услуге и функционалности, конфигурацију интерфејса и субинтерфејса и постављање тагова за VLAN – ове [35].

4.4. Конфигурација VoIP сервера

Успостављање VoIP сервера (VoIP централе) је извршено на рутеру R1.

Конфигурација рутера R1, као VoIP сервера, дата је у прилогу број 6.

Наведеним командама је одређено активирање телефонске картице на уређају, за подршку VoIP комуникацији на уређају, као и глобално конфигурисање за VoIP услуге.

Команда: allow-connections sip to sip, дозвољава успостављање SIP (Session Initiation Protocol) везе између два SIP уређаја (нпр. између два IP телефона).

Команда: sip, конфигурише SIP протокол, који се користи за успостављање и управљање VoIP комуникацијом.

Команда: registrar server expires max 600 min 60, конфигурише регистрациони сервер за SIP уређаје. Дефинише се максимално време трајања регистрације од 600 секунди и минимално 60 секунди.

Команда: voice register global, конфигурише глобалне параметре регистрације VoIP уређаја.

Команда: mode cme, поставља мод регистрације VoIP уређаја. У овом случају, "cme" означава Cisco Call Manager Express (CME), што је Cisco – ева имплементација IP телефоније.

Команда: source-address 30.30.30.1 port 5060, поставља изворишну адресу и порт за SIP сигнализацију.

Команда: max-dn 35, дефинише максималан број корисничких DN (Directory Numbers) који се могу регистровати.

Команда: max-pool 10, дифинише максималан број регистрационих пулова.

Команда: authenticate register, поставља захтев за аутентификацију регистрације VoIP уређаја.

Команда: authenticate realm local, одређује да се аутентификација врши локално, на уређају.

Команда: voice register dn <broj>, дефинише информације за кориснички број (DN) VoIP уређаја.

Команда: number <broj>, одређује кориснички број телефона.

Команда: name <ime>, одређује име за кориснички број.

Команда: label <etiketa>, поставља етикету за кориснички број.

Команда: voice register pool <broj>, дефинише регистрациони pool за VoIP уређаје.

Команда: id mac <MAC adresa>, идентификује уређај по MAC адреси.

Команда: number <broj> dn <broj>, повезује кориснички број са DN.

Команда: username <korisničko ime> password <šifra>, поставља корисничко име и шифру за аутентификацију уређаја.

Команда: codec g711ulaw, поставља аудио кодек за комуникацију.

4.5. Успостава remote access VPN заштићене комуникације

Успостава remote access (удаљени приступ) VPN заштићене комуникације, вршено је помоћу софтверског телефона и корисничког софтвера за успоставу VPN сесије. За потребе формирања софтверског IP телефона кориштен је софтверски алат ZOIPER (слика 21.).

Успостава VPN тунела је вршена помоћу алата VPN Client.

Мерење мрежног саобраћаја је вршено помоћу софтверског алата Wireshark.

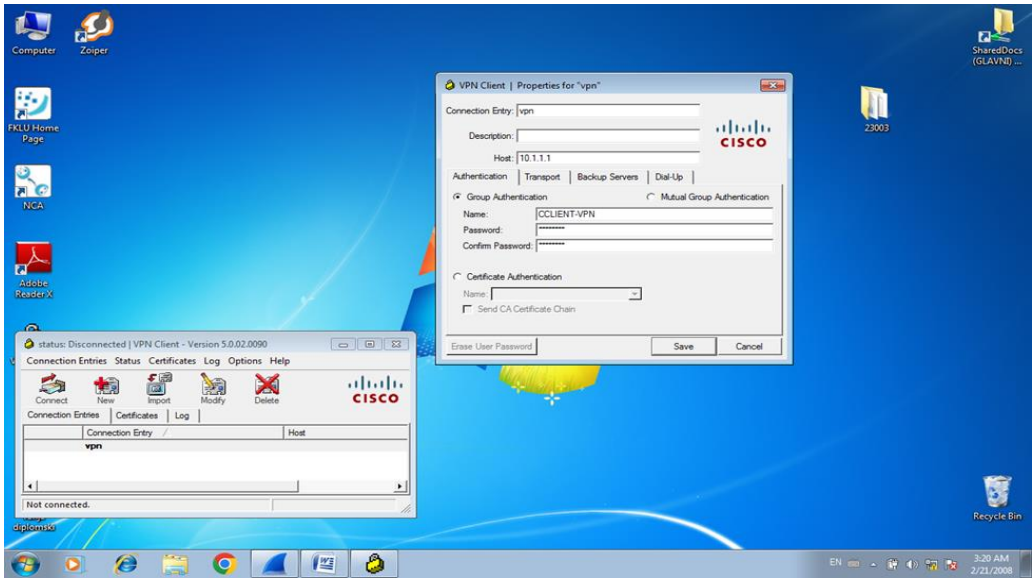
Пре успостављања VoIP комуникације, активира се рад софтверског алата Wireshark.

Након успоставе мрежне конективности, најпре телефон корисничког броја 001, позива учесника позивног броја 003 (слика 16.).

Слика 21. Изглед корисничког интерфејса софтверског алата ZOIPER

Мерење мрежног саобраћаја се врши у незаштићеном преносу, а добијени резултати мерења су приказани у табели број 3.

Након мерења саобраћаја у незаштићеном преносу, исти поступак је поновљен у заштићеном преносу. Након успоставе VPN конекције, употребом софтверског алата VPN Client (слика 22.), успостављена је VoIP конекција и пренос садржаја у реалном времену. Мерење наведених процеса приказано је у табели број 4.



Слика 22. Изглед корисничког интерфејса корисничког алата VPN Clien

5. Мерење и анализа мрежног саобраћаја

5.1. Анализа незаштићеног саобраћаја у преносу

Табела 3: Позив учесника 001 ка учеснику 003 без VPN заштите

R.br.	Vreme [s]	Izvorišna adresa	Odredišna adresa	Protokol	Veličina [B]
1.	0,00	Cisco_e1:aa:81	Spanning_tree	STP	60
2.	1,99	Cisco_e1:aa:81	Spanning_tree	STP	60
3.	2,73	ASUSTEkC_9d:86:8a	Cisco_00:e3:e1	ARP	42
4.	2,74	Cisco_00:e3:e1	ASUSTEkC_9d:86:8a	ARP	60
5.	3,433	40.40.40.3	192.168.100.1	DNS	75
6.	3,434	40.40.40.1	40.40.40.3	ICMP	70
7.	4,00	Cisco_e1:aa:81	Spanning_tree	STP	60
8.	5,32	40.40.40.1	224.0.0.5	OSPF	90
9.	5,99	Cisco_e1:aa:81	Spanning_tree	STP	60
10.	6,56	40.40.40.3	192.168.100.1	DNS	75
11.	6,561	40.40.40.1	40.40.40.3	ICMP	70
12.	7,16	40.40.40.3	30.30.30.1	TCP	590
13.	7,16	30.30.30.1	40.40.40.3	TCP	60
14.	7,16	40.40.40.3	30.30.30.1	TCP	386
15.	7,36	40.40.40.3	30.30.30.1	TCP	54
16.	7,99	Cisco_e1:aa:81	Spanning_tree	STP	60
17.	8,30	40.40.40.3	30.30.30.1	TCP	58
18.	6,83	40.40.40.3	30.30.30.1	SIP	590
19.	8,37	30.30.30.1	40.40.40.3	SIP	124
20.	11,98	40.40.40.3	10.10.10.2	SIP	459
21.	9,99	Cisco_e1:aa:81	Spanning_tree	STP	60
22.	11,97	10.10.10.2	40.40.40.3	RTP	214
23.	11,97	30.30.30.1	40.40.40.3	TCP	590
24.	11,97	30.30.30.1	40.40.40.3	SIP/SDP	424
25.	11,97	40.40.40.3	30.30.30.1	TCP	54
26.	11,98	40.40.40.3	10.10.10.2	RTP	55
27.	11,98	40.40.40.3	10.10.10.2	TCP	66
28.	11,98	10.10.10.2	40.40.40.3	TCP	60
29.	11,98	40.40.40.3	10.10.10.2	TCP	54
30.	11,98	10.10.10.2	40.40.40.3	TCP	60
31.	11,99	10.10.10.2	40.40.40.3	RTP	214
32.	12,01	10.10.10.2	40.40.40.3	RTP	214
33.	12,03	10.10.10.2	40.40.40.3	RTP	214
34.	12,25	40.40.40.3	10.10.10.2	RTP	214

Најважнији процеси преноса VoIP саобраћаја су приказани у табели 3.

У приказаним „догађајима“ у мрежи, могу се уочити најважнији процеси, који су осенчени различитим бојама.

Приликом успоставе незаштићеног преноса VoIP телефоније, најпре се успоставља TCP конекција, методом тзв. „троструког руковања“.

Следећи значајан процес је успостава SIP конекције између VoIP учесника, кроз поступак позивања, потврдног одговора позваног учесника и на крају, потврде успоставе SIP конекције од стране позиваоца.

Након наведених процеса, успоставља се пренос саобраћаја у реалном времену, помоћу RTP протокола.

Осим наведених најважнијих процеса, у табели се могу уочити и други значајни процеси за успоставу конективности у рачунарској мрежи, који су приказани кроз ARP, ICMP, OSPF, STP и DNS протоколе.

5.2. Анализа заштићеног саобраћаја у преносу

Табела 4: Позив учесника 001 ка учеснику 003 са VPN заштитом

R.br.	Vreme [s]	Izvorišna adresa	Odredišna adresa	Protokol	Veličina [B]
1.	0,03	Cisco_e1:aa:81	Spanning_tree	STP	60
2.	0,73	40.40.40.3	10.10.10.2	ISAKMP	126
3.	0,73	10.10.10.2	40.40.40.3	ISAKMP	126
4.	2,03	Cisco_e1:aa:81	Spanning_tree	STP	60
5.	4,03	Cisco_e1:aa:81	Spanning_tree	STP	60
6.	6,03	Cisco_e1:aa:81	Spanning_tree	STP	60
7.	6,88	Fe80:e010:c683:5106:f3e8	Ff02::1:2	DHCPv6	149
8.	8,03	Cisco_e1:aa:81	Spanning_tree	STP	60
9.	10,03	Cisco_e1:aa:81	Spanning_tree	STP	60
10.	10,88	Fe80:e010:c683:5106:f3e8	Ff02::1:2	DHCPv6	154
11.	12,03	Cisco_e1:aa:81	Spanning_tree	STP	60
12.	14,03	Cisco_e1:aa:81	Spanning_tree	STP	60
13.	16,03	Cisco_e1:aa:81	Spanning_tree	STP	60
14.	18,03	Cisco_e1:aa:81	Spanning_tree	STP	60
15.	19,32	Cisco_e1:aa:81	ASUSTEkC_9d:86:8a	ARP	60
16.	19,32	ASUSTEkC_9d:86:8a	Cisco_e1:aa:81	ARP	42
17.	20,03	Cisco_e1:aa:81	Spanning_tree	STP	60
18.	20,51	40.40.40.3	30.30.30.1	TCP	66
19.	22,03	30.30.30.1	40.40.40.3	TCP	60
20.	23,51	40.40.40.3	30.30.30.1	TCP	66
21.	24,03	Cisco_e1:aa:81	Spanning_tree	STP	60
22.	25,22	ASUSTEkC_9d:86:8a	Cisco_00:e3:e1	ARP	42
23.	25,23	Cisco_00:e3:e1	ASUSTEkC_9d:86:8a	ARP	60
24.	26,03	Cisco_e1:aa:81	Spanning_tree	STP	60
25.	27,50	40.40.40.3	10.10.10.2	SIP	1095
26.	27,50	10.10.10.2	40.40.40.3	SIP	284
27.	28,30	40.40.40.3	10.10.10.2	SIP	831
28.	30,25	10.10.10.2	40.40.40.3	RTP	214
29.	31,25	40.40.40.3	10.10.10.2	RTP	214
30.	30,50	10.10.10.2	40.40.40.3	RTP	214
31.	31,50	40.40.40.3	10.10.10.2	RTP	214
32.	31,75	10.10.10.2	40.40.40.3	RTP	214

Процеси наведени у току незаштићеног преноса су идентични са процесима у заштићеном преносу, с том разликом што свим наведеним процесима претходи успостава VPN тунела, која се огледа у размени порука ISAKMP протокола и успостави безбедносне асоцијације [8].

6. Могућност примене технологије виртуелних приватних мрежа у војсци

Примена технологије виртулених приватних мрежа у војсци представља један од могућих система заштите преноса информација. Могућа је реализација VPN комуникације преко различитих спојних путева (кабловски, оптички, радио релејни), што за војне потребе представља погодност, с обзиром да се услови успоставе комуникација могу мењати у складу са доступношћу одговарајуће инфраструктуре, условима које постављају теренски услови експлоатације телекомуникационих уређаја, као и динамика извођења војних операција.

За потребе телекомуникационо – информационог обезбеђења (ТкИОб) војске, може се користити инфраструтурна мрежа, за успоставу VPN тунела, као и дислокација јединица у складу са захтевима извођења војних операција.

С обзиром на опремање јединица за ТкИОб средствима телекомуникација, које омогућавају интеграцију различитих спојних путева, могуће су различите комбинације успоставе VPN комуникација.

Из наведеног се може закључити да технологија виртуелних приватних мрежа омогућава прилагођавање условима успоставе комуникација (у односу на расположиве спојне путеве), као и промену локација јединица у простору у складу са потребама извођења војних операција.

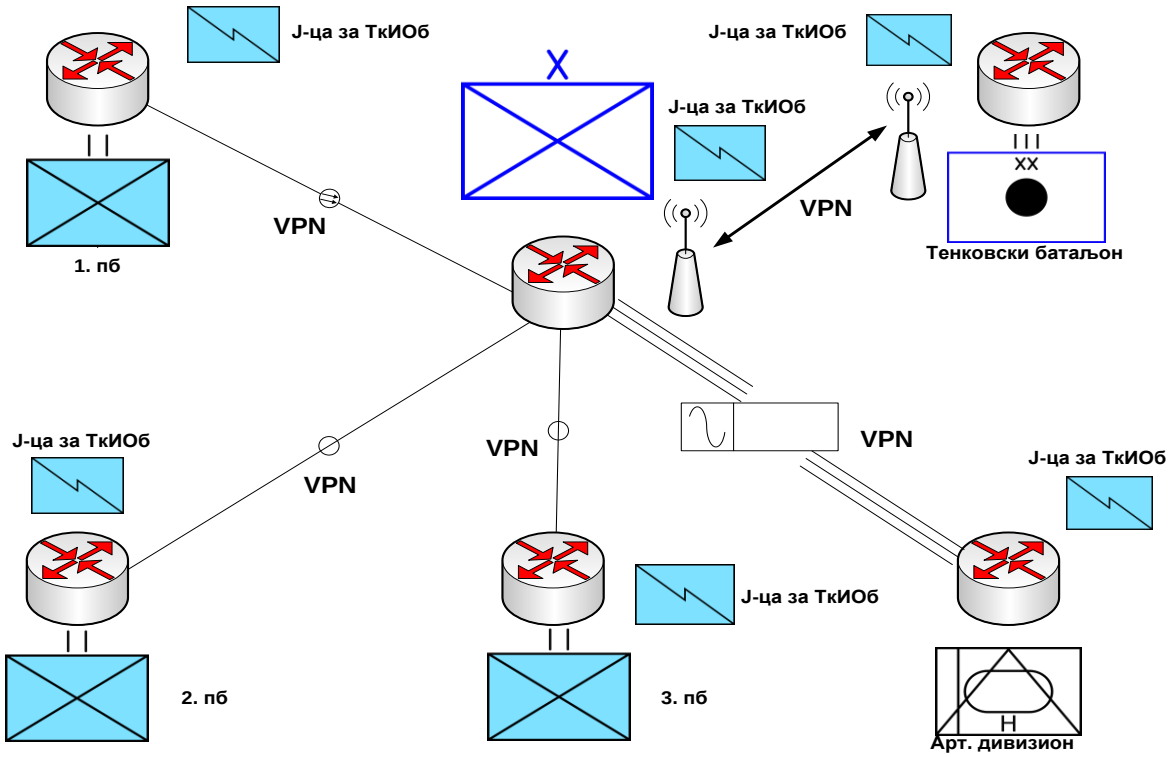
Примена технологије виртуелних приватних мрежа омогућава заштиту преноса свих врста телекомуникационих сервиса, што је захтев који поставља савремено командовање војним операцијама.

Заштита применом технологије виртуелних приватних мрежа омогућава висок степен тајности преноса информација, у складу са примењеним алгоритмима и примењеним криптографским кључевима, као и обезбеђење других безбедносних сервиса (аутентификација, интегритет).

Примена технологије виртуелних приватних мрежа омогућава пренос информација, како у уникаст, тако и у мултикаст мрежној реализацији, што такође представља један од захтева командовања (пренос информација само једном учеснику, или вишеструки пренос информација за више учесника).

На слици 23., приказана је могућност реализације комуникације применом технологије виртуелних приватних мрежа у јединици бригадног нивоа. Може се уочити да спојни пут између командних места јединица батаљонског нивоа, са командом бригаде, може бити различит (кабловски, оптички, радио – релејни).

Осим наведеног, технологија виртуелних приватних мрежа може имати значај за, како на тактичком, тако и на оперативном и стратегијском нивоу, повезивање организацијских целина Генералштаба, Министарства одбране, као и остваривање телекомуникација садејства и сарадње, са другим субјектима одбране и безбедности.



Слика 23. Могућности успоставе VPN комуникације у јединици бригадног нивоа

7. ЗАКЉУЧАК

Развој преноса телекомуникационих сервиса путем рачунарских мрежа је условио и развијање бројних безбедносних механизама за заштиту преноса истих.

Заштита у рачунарским мрежама се, у литератури, посматра кроз три равни (управљачку, контролну и раван података). У раду су приказане најважније и најчешће коришћене технологије заштите у контролној и управљачкој равни. Кроз један приступ реализацији заштите пакетског телефонског саобраћаја, приказана је заштита у равни података употребом IPSec протокола.

Посебан проблем, кроз еволуцију развоја рачунарских мрежа, представљао је пренос садржаја у реалном времену (телефонија, телевизија, мултимедија).

Пренос садржаја у реалном времену захтевао је развој посебних протокола, како за комутацију између учесника (SIP, H.323), тако и за пренос садржаја кроз успоставу посебних сесија за пренос (RTP, RTCP). Упоредо са обезбеђењем преноса и комутације сервиса у реалном времену, развијани су протоколи који су омогућавали криптозаштиту (IPSec протокол, VPN технологија и други).

Са практичног аспекта, омогућено је измештање и дислокација учесника и рачунарским мрежама, што је у пословној сфери омогућило рад са удаљених локација, уз коришћење постојеће мрежне инфраструктуре. Употреба VPN технологије у савременим условима организације војске (које карактеришу брзе промене услова извођења војних операција и промене локација јединица), има велики значај, јер омогућава успоставу безбедне комуникације и пренос сервиса у реалном времену, значајних за командовање јединицама, са различитих локација. Примена технологије виртуелних приватних мрежа има значај због обезбеђења захтева сигурног преноса информација (поверљивости, интегритета, аутентичности, непорецивости и расположивости), употребом савремених крипто – алгоритама.

Успостава и одржавање виртуелних приватних мрежа захтева од припадника органа телекомуникационо – информатичког обезбеђења јединица Војске Србије, стручност у

погледу познавања ТкИ система, мрежних технологија, система криптозаштите, као и употребу различитих софтверских алата.

Главни закључак приказаног је, да примена технологије виртуелних приватних мрежа у заштити пакетског телефонског саобраћаја, има значајне сличности са преносом других врста сервиса (Web, Mail), али и специфичности, које се огледају у примени протокола посебно развијених за пренос садржаја у реалном времену и комутацију између учесника (SIP, RTP).

Примена технологије виртуелних приватних мрежа има и посебне захтеве у поседовању опреме која је лиценцирана за успоставу наведених врста сервиса (VPN).

Приказан је један приступ реализацији успоставе заштите пакетског телефонског саобраћаја, погодан за едукацију, јер приказује процесе у мрежи у специфичним захтевима, погодним за развијање синтетичког схватања свих процеса у мрежи, у датом окружењу.

На основно питање које је постављено у раду, које је место и улога одређених мрежних протокола, као и редослед њиховог појављивања у процесу успоставе пакетског телефонског саобраћаја, успоставе VPN тунела и каснији пренос садржаја у реалном времену, дат је одговор кроз мерење и анализу мрежног саобраћаја. Приказани су протоколи који се појављују у датом једном приступу реализацији заштите пакетског телефонског саобраћаја употребом технологије виртулених приватних мрежа, као и редослед њиховог појављивања. Редослед појављивања протокола је условљен начином преноса саобраћаја (заштићен или незаштићен мод), као и начином конфигурисања мрежних уређаја и одређивање протокола за успоставу комуникације и пренос сигнализације (SIP протокол, ISAKMP, IPSec).

Будуће теме и задаци за истраживање примене технологије виртуелних приватних мрежа се могу односити на истраживање различитих технологија и протокола виртуелних приватних мрежа (у раду се приказана технологија употребом IPSec протокола) и то: GRE (Generic Routing Encapsulation), Draft Martini, L2TPv3, IEEE 802.1Q, MPLS LSP, PPTP (Point-to-Point Tunneling Protocol), SSL (Secure Sockets Layer) и друге.

8. ПРЕГЛЕД ТАБЕЛА

9. ПРЕГЛЕД ГРАФИЧКИХ ПРИКАЗА

10. ПРИЛОЗИ

Прилог број 1: Конфигурација рутера R1

```
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.252
duplex auto
speed auto
crypto map map1
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
interface GigabitEthernet0/1.1
description racunari vlan
encapsulation dot1Q 20
ip address 20.20.20.1 255.255.255.0
ip virtual-reassembly in
interface GigabitEthernet0/1.2
description Voice vlan
encapsulation dot1Q 30
ip address 30.30.30.1 255.255.255.0
router ospf 1
passive-interface GigabitEthernet0/1
network 10.10.10.0 0.0.0.3 area 0
network 20.20.20.0 0.0.0.255 area 0
network 30.30.30.0 0.0.0.255 area 0
ip local pool VPNPOOL 192.168.100.2 192.168.100.10
```

Прилог број 2: Конфигурација рутера R2

```
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/0.1
description racunari vlan
encapsulation dot1Q 20
ip address 60.60.60.2 255.255.255.0
ip virtual-reassembly in
interface GigabitEthernet0/0.2
description Voice vlan
encapsulation dot1Q 30
ip address 70.70.70.2 255.255.255.0
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
interface GigabitEthernet0/1.1
description racunari vlan
encapsulation dot1Q 20
ip address 40.40.40.1 255.255.255.0
ip virtual-reassembly in
interface GigabitEthernet0/1.2
description Voice vlan
```

encapsulation dot1Q 30

ip address 50.50.50.1 255.255.255.0

ip virtual-reassembly in

router ospf 1

passive-interface GigabitEthernet0/1

network 10.10.10.0 0.0.0.3 area 0

network 40.40.40.0 0.0.0.255 area 0

network 50.50.50.0 0.0.0.255 area 0

Прилог број 3: Конфигурација свича S1:

```
interface GigabitEthernet1/0/1
switchport access vlan 30
interface GigabitEthernet1/0/2
switchport access vlan 30
interface GigabitEthernet1/0/3
switchport access vlan 30
interface GigabitEthernet1/0/4
switchport access vlan 30
interface GigabitEthernet1/0/5
switchport access vlan 30
interface GigabitEthernet1/0/6
switchport access vlan 30
interface GigabitEthernet1/0/7
switchport access vlan 30
interface GigabitEthernet1/0/8
switchport access vlan 30
interface GigabitEthernet1/0/9
switchport access vlan 30
interface GigabitEthernet1/0/10
switchport access vlan 30
interface GigabitEthernet1/0/11
switchport access vlan 30
interface GigabitEthernet1/0/12
switchport access vlan 30
```

interface GigabitEthernet1/0/13

switchport access vlan 20

interface GigabitEthernet1/0/14

switchport access vlan 20

interface GigabitEthernet1/0/15

switchport access vlan 20

interface GigabitEthernet1/0/16

switchport access vlan 20

interface GigabitEthernet1/0/17

switchport access vlan 20

interface GigabitEthernet1/0/18

switchport access vlan 20

interface GigabitEthernet1/0/19

switchport access vlan 20

interface GigabitEthernet1/0/20

switchport access vlan 20

interface GigabitEthernet1/0/21

switchport access vlan 20

interface GigabitEthernet1/0/22

switchport access vlan 20

interface GigabitEthernet1/0/23

switchport access vlan 20

interface GigabitEthernet1/0/24

description Trunk-to-Router

switchportmode trunk

interface GigabitEthernet1/1/1

interface GigabitEthernet1/1/2

interface GigabitEthernet1/1/3

interface GigabitEthernet1/1/4

interface Vlan1

no ip address

shutdown

interface Vlan20

description Racunari Vlan

ip address 20.20.20.2 255.255.255.0

interface Vlan30

description Voice Vlan

ip address 30.30.30.2 255.255.255.0

Прилог број 4: Конфигурација рутера R1, као VPN сервера:

```
license udi pid CISCO2921/K9 sn FCZ161520KM
license boot module c2900 technology-package uck9
username admin password 0 admin1
redundancy
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp client configuration group cisco
key cisco123
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
mode tunnel
crypto dynamic-map map1 10
set transform-set set1
reverse-route
crypto map map1 client authentication list abc1
crypto map map1 isakmp authorization list abc2
crypto map map1 client configuration address respond
crypto map map1 10 ipsec-isakmp dynamic map1
```

Прилог број 5: Команде за кофигурацију рутера R2:

```
license udi pid CISCO2921/K9 sn FCZ161570F6
license accept end user agreement
license boot suite FoundationSuiteK9
license boot suite AdvUCSuiteK9
redundancy
interface GigabitEthernet0/0
ip address 10.10.10.1 255.255.255.252
duplex auto
speed auto
interface GigabitEthernet0/0.1
description racunari vlan
encapsulation dot1Q 20
ip address 60.60.60.2 255.255.255.0
ip virtual-reassembly in
interface GigabitEthernet0/0.2
description Voice vlan
encapsulation dot1Q 30
ip address 70.70.70.2 255.255.255.0
interface GigabitEthernet0/1.1
description racunari vlan
encapsulation dot1Q 20
ip address 40.40.40.1 255.255.255.0
ip virtual-reassembly in
```

```
interface GigabitEthernet0/1.2
description Voice vlan
encapsulation dot1Q 30
ip address 50.50.50.1 255.255.255.0
```

Прилог број 6: Конфигурација рутера R1, као VoIP сервера:

```
voice-card 0
voice service voip
allow-connections sip to sip
sip
registrar server expires max 600 min 60
voice register global
mode  cme
source-address 30.30.30.1 port 5060
max-dn 35
max-pool 10
authenticate register
authenticate realm local
voice register dn  1
number 001
name 001
label 001
voice register dn  2
number 002
name 002
label 002
voice register dn  3
number 003
name 003
label 003
```

```
voice register pool  1
id mac 0008.5D50.5FCF
number 1 dn 1
username 001 password 001
codec g711ulaw
voice register pool  2
id mac 0008.5D50.651A
number 1 dn 2
username 002 password 002
codec g711ulaw
voice register pool  3
id mac 5448.10CE.DDD2
number 1 dn 3
username 003 password 003
codec g711ulaw
```

11. ЛИТЕРАТУРА

[1] J.F. Kurose и K.W. Ross, „Умрежавање рачунара – од врха ка дну“, Рачунарски факултет, Београд, 2009.

[2] C. Paquet, “Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide“, Second Edition, Cisco Press, Indianapolis, 2013.

[3] Network Time Protocol (Version 3): Specification, Implementation and Analysis, RFC 1305, March 1992., https://www.rfc-editor.org/info/rfc1305.

[4] Network Time Protocol (Version 4): Protocol and Algorithms Specification, RFC 5905, June 2010., http://www.rfc-editor.org/info/rfc5905.

[5] An Architecture for DescribingSimple Network Management Protocol (SNMP) Management Frameworks,RFC 3411, December 2002., https://www.rfc-editor.org/rfc/rfc3411.html.

[6] https://www.manageengine.com/network-monitoring/what-is-snmp.html. (прегледано 08.04.2023. године).

[7] Douglas E. Comer, TCP/IP – принципи, протоколи и архитектуре, CET, Београд, 2001.

[8] W. Stallings, „Основе безбедности мрежа“, Рачунарски факултет Београд, 2014.

[9] The Secure Shell (SSH) Protocol Architecture, RFC 4251, January 2006., https://www.rfc-editor.org/info/rfc4251.

[10] TELNET Protocol Specification, RFC 854, May 1983., https://www.rfc-editor.org/info/rfc854.

[11] TELNET Authentication Using DSA, RFC 2943, September 2000, https://www.rfc-editor.org/rfc/rfc2943.html.

[12] TELNET Authentication Option, RFC 2941, September 2000, https://www.rfc-editor.org/rfc/rfc2941.html.

[13] TELNET Authentication: Kerberos Version 5, RFC 2942, September 2000, https://www.rfc-editor.org/rfc/rfc2942.html.

[14] TELNET Authentication: SRP, RFC 2944, September 2000, https://www.rfc-editor.org/rfc/rfc2944.html.
[15] TELNET Data Encryption Option, RFC 2946, September 2000,https://www.rfc-editor.org/rfc/rfc2946.html.
[16] Cisco Control Plane Policing Feature Guide| © 2014-2015 Cisco and/or its affiliates. Al, https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/cisco-copp-feature-guide.pdf. (прегледано: 12.04.2023. године).
[17] AOS-CX 10.06 CoPP Guide 6200, 6300, 6400 Switch Series, 2020 Hewlett Packard Enterprise Development LP, https://www.arubanetworks.com/techdocs/AOS-CX/10.06/PDF/6200/CoPP%206200%206300%206400.pdf. (прегледано: 18.04.2023. године).
[18] Supervisor Engine 6T Software Configuration Guide, Release 15.3SY, https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/153SY/config_guide/sup6T/15_3_sy_swcg_6T/introduction.pdf. (прегледано: 25.04.2023. године).
[19] Cisco Control Plane Policing Feature Guide| © 2014-2015 Cisco and/or its affiliates. Al, https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/cisco-copp-feature-guide.pdf, (прегледано: 08.07.2023. године)
[20] Control Plane Policing - Pearsoncmg.com, https://ptgmedia.pearsoncmg.com › downloads, https://ptgmedia.pearsoncmg.com/images/9781587143694/downloads/i9781587143694_app02.pdf. (прегледано: 25.04.2023. године).
[21] Protecting the Router Control Plane, RFC 6192, march 2011, https://www.rfc-editor.org/rfc/pdfrfc/rfc6192.txt.pdf.
[22] Cisco − OSPF Design Guide, http://ftp.unpad.ac.id/orari/library/library-ref-eng/ref-eng-2/network/routing/ospf-design-guide.pdf, (прегледано: 14.07.2023. године).
[23] А. Смиљанић, Основе и примена Интернета, ЕлектротехничкифакултетУниверзитета у Београду, Београд, 2015.
[24] Internet Security Association and key Management Protocol, RFC: 2408, novembar 1998, https://datatracker.ietf.org/doc/html/rfc2408.
[25] М. Стојановић, В. Аћимовић - Распоповић, Савремене IP мреже: Архитектуре, технологије и протоколи, Академска мисао, Београд, 2012.
[26] Security in the Internet Architecture, RFC: 1636, jun 1994, https://datatracker.ietf.org/doc/html/rfc1636.

[27] IP Encapsulating Security Payload, RFC: 4303, decembar 2005, https://datatracker.ietf.org/doc/html/rfc4303.
[28] Security Architecture for the Internet protocol, RFC: 4301, decembar 2005, https://datatracker.ietf.org/doc/html/rfc4301.
[29] Internet Key Exchange Protocol Version 2 (IKEv2), RFC: 5996, septembar 2010, https://datatracker.ietf.org/doc/html/rfc5996.
[30] Д. Немец, Д. Вукобратовић, В. Црнојевић, Ч. Стефановић, Технологија VoIP система, Факултет техничких наука Универзитета у Новом Саду, Нови Сад, 2007.
[31] https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html (прегледано: 24.07.2023. године).
[32] https://www.cisco.com/c/en/us/support/switches/catalyst-3650-series-switches/series.html, (прегледано: 03.08.2023. године).
[33] С. Гајин, Принципи конфигурисања рачунарских мрежа, Академска мисао, Београд, 2018.
[34] T. Lammle, CCNA Cisco Certified Network Associate, Компјутер библиотека, Београд, 2006.
[35] J. Frahim, O. Santos, Cisco ASA All – in – one Firewall, IPS, Anti – X, and VPN Adaptive Security Appliance, Second Edition, Cisco press, Indianapolis, 2010.
[36] K. Wallace, Implementing CiscoUnified CommunicationsVoice over IP and QoS(CVOICE) FoundationLearning Guide, Cisco press, Indianapolis, 2011.