thesis

МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ

МЭДЭЭЛЭЛ ХОЛБОО ТЕХНОЛОГИЙН СУРГУУЛЬ

Ууганбаяр Өнөбат

Voice encryption

Мэргэжил : Компьютерийн Системийн Хамгаалал

Компьютерийн ухааны бакалаврын төсөл

Улаанбаатар хот

2017 он

Бүлэг 1

Ерөнхий агуулга

1.1 Удиртгал

Өнөөдөр хүн бүр өөрийн гэсэн компютер болон эцсийн төхөөрөмжүүдээр утастай болон утасгүй сүлжээгээр дамжуулан интернетэд холбогдох боломжтой болсон. Монгол орон л гэхэд хүн амын 70 хувь нь интернет ашигладаг гэсэн судалгаа гарсан байдаг. Үүнийгээ дагаад интернет орчиндох мэдээллийн сан өдөр бүр өргөжиж мөн бизнесийн үйл ажиллагаа маш эрчимтэйгээр явагдах болсон юм. Өдөр бүр хэрэглээ нь өсөн нэмэгдэж буй интернэт хэрэглээг хянах ачааллыг болон хандалтын удирдлагыг зохицуулах нь хамгийн төвөгтэй асуудлуудын нэг болсон ба үүнийг зохицуулах олон арга байгаагын нэг нь Radius Server юм.

1.2 Зорилго

Энэхүү төсөлийн ажлын зорилго нь Voice encryption-ийг судлах ба OpenWRT, EAP -г судалж эдгээрийг ашиглан сүлжээг зохион байгуулах, замчлах, баталгаажуулалт хийх эрхийг судлаж туршиж үзэх юм. Radius server нь хэрэглэгчийг баталгаажуулах эрх олгох зориулалттай үйлчилгээ бөгөөд тохируулж туршиж үзнэ.OpenWRT нь нээлттэй эх бүхий үйлдлийн систем бөгөөд Access point дээр хөгжүүлэлт хийж тохиргоо хйин туршиж үзэх болно.

Бүлэг 2

Онол, арга зүйн бүлэг

2.1 Дуу авиа гэж юу вэ?

Ямар нэгэн биет хэлбэлзэх үедээ орчин тойрныхоо агаарыг хэлбэлзүүлдэг.Бидний сонсож буй дуу авиа агаарын хэлбэлзлээр дамждаг.Чичирхийлэн хөдөлж байгаа бие дуу авиаг үүсгэдэг. Нэг ёсондоо дуу авиа нь шахагдсан долгион бөгөөд тасралтгүй үргэлжилдэг.Дуу авиа нь ойно,хугарна, тархана. Агаар байхгүй бол дуу тарахгүй. Хүний чих 20-20000Гц давтамжтай дууны долгионыг мэдэрдэг.Хүн амьтан бие биетэйгээ харилцах мөн ойлголцохын тулд дуу авиаг ашигладаг.Дуу авиа улам хөгжин өргөжиж харилцаа холбоо хэмээх том салбар гарч ирсэн.Өдөр бүр л хүн болгон утас болон интернетээр дамжуулж өөр хоорондоо харилцаж мэдээлэл солилцож байна.

2.2 Харилцаа холбооны хөгжлийн үе шат

Утасгүй харилцаа холбооы технологи 1940-өөд оны дунд үед үүсч бий болсон боловч 1980-аад оноос нийтийн хэрэгцээнд нэвтэрч эхэлсэн байна.Зарим мэргэжилтнүүд утасгүй холбооны технологийн хөгжлийн эхний шатыг 0G хэмээн нэрлэдэг. Гар утасны технологийн хөгжлийн тухай Сүүлийн жилүүдэд дэлхийн улс орнууд гар утас буюу утасгүй харилцаа холбооны хөгжлийн 4-р (4G) үед шилжиж эхэлж байгаа билээ. Мөн манайд хэдэн жилийн өмнө хөдөлгөөнт интернетийн 4G Mobile Wimax утасгүй систем байгуулагдсан боловч гар утасны технологид хараахан нэвтэрч эхлээгүй байна. Энэ удаад гар утасны хөгжлийн үе шатуудын тухай товч танилцая.

0G Утасгүй харилцаа холбооны технологи 1940-өөд оны дунд үед үүсч бий болсон боловч 1980-аад оноос нийтийн хэрэгцээнд нэвтэрч эхэлсэн байна. Зарим мэргэжилтнүүд утасгүй холбооны технологийн хөгжлийн эхний шатыг 0G хэмээн нэрлэдэг. Энэ үеийн гар утаснууд радио долгионы зарчимаар ажилладаг бөгөөд овор, жин ихтэй байсан учир ихэвчлэн

автомашинд суурилуулан ашигладаг байжээ. Мөн одоогийн Иридиум системтэй төстэй сансарын холбооны технологи бүхий гар утаснууд усан онгоцны холбооны зориулалтаар ашиглагдаж байсан байна.

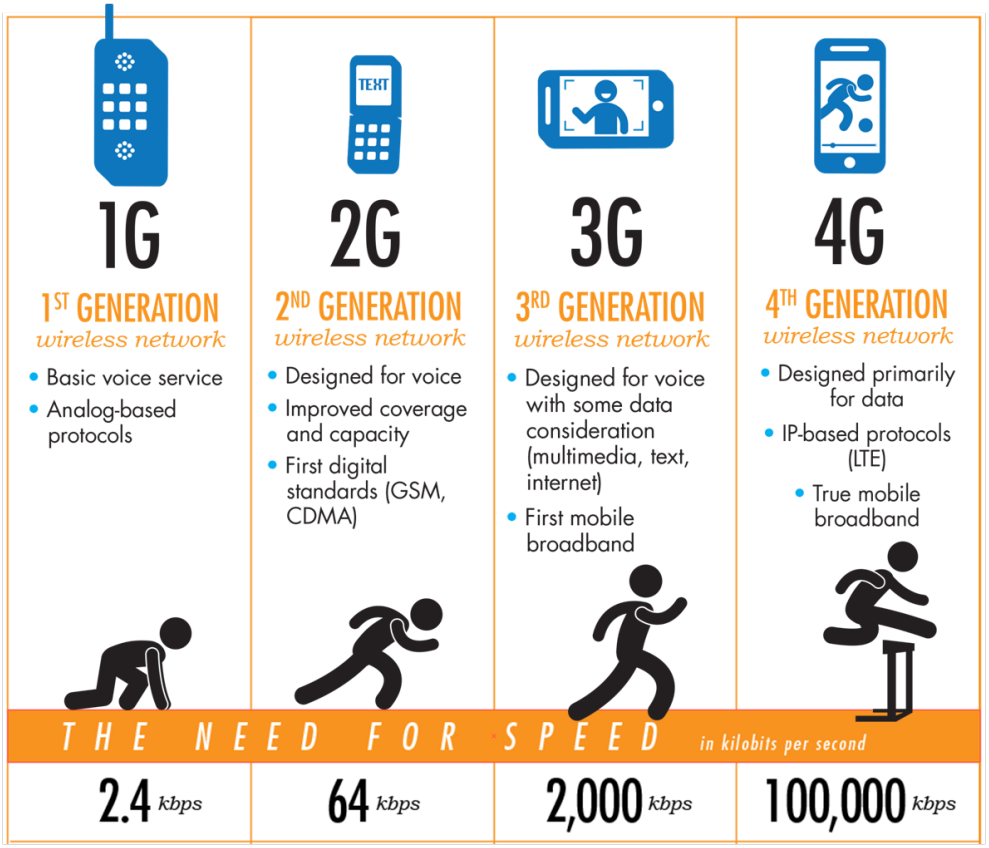
1G 1982 оноос эхний шатны гар утаснууд бүтээгдэж хүний дуу хоолойг аналоги долгион хэлбэрээр дамжуулж дууны өнгөнөөс хамаарах тасралтгүй дохиоллыг ашигладаг болов. Дохиоллын зурвасын хүрээ өргөн боловч, харьцангуй том хэмжээний батерей шаардагддаг, хөндлөнгийн элдэв дохиоллын нөлөөлөлд өртөмтгий, хамгаалалтын систем муу буюу зарим онцлог төхөөрөмж бүхий хүн бусдын яриаг хөндлөнгөөс сонсох боломжтой байжээ. Хамгийн сул тал нь бусдын утасны дугаарыг хуулж аваад өөрийн дураар ашиглах боломжтой байв.

2G 1991 оноос 2G стандарт боловсруулагдаж PDC, GSM мэтийн дижитал системүүд ашиглагдах болов. Энэ технолиги нь дуу хоолойг 1 буюу 0-оор илэрхийлэгдэх тоон дохиолд хувирган дамжуулдаг учир дээр дурдсан дутагдалуудыг бүрэн арилгасан илүү найдвартай систем болсон байна. Мөн дохиоллыг кодлон хувиргаж хамгаалалтын шаардлагийг бүрэн хангасан учир дохиоллын илүү нарийн зурвасыг хамарч, харьцангуй бага энерги зарцуулдаг учир батерейн хэмжээг жижигрүүлэх боломжтой болов. Мөн үнийн хувьд харьцангуй хямд болсон байна. Өөр нэг онцлог нь энэ үеийн технологиос эхлэн гар утсаараа SMS буюу богино хэмжээний текст илгээх, хүлээн авах боломжтой болсон байна. Адил урттай радио долгионы хүрээнд их хэмжээний харилцан ярианы долгионыг шахах боломжтой болсон учир гар утасны оператор компаниуд олноор байгуулагдаж, дэлхий даяар түгэн дэлгэрч эхэлсэн юм.

3G Олон улсын Телефон Харилцаа Холбооны байгууллагаас IMT-2000 хэмээх хөдөлгөөнт утасны стандартыг тодорхойлсон бөгөөд анхны 3G системийг 2001 онд япон улсын NTT Dokomo компани нэвтрүүлсэн байна. Энэ шатанд W-CDMA, CDMA2000 зэрэг өндөр хурдны дижитал системүүд голлож байна. 3G системийн гар утсаар дуу, дүрс болон өгөгдлийг өндөр үр ашигтайгаар дамжуулдагаас гадна интернетээр аялж мэдээлэл татаж авах, youtube видео үзэх, фото зураг агуулсан текст мэдээлэл илгээх боломжтой болсон байна. Мөн 3.5 G хэмээх завсрын ангиллыг гаргаж ирсэн бөгөөд интернетээс мэдээлэл унших хурдаар ялгаагдаж байна. 3G системээр интернетэд ойролцоогоор 200-700 кб/с хурдаар холбогддог бол 3.5 G системд 3.6 - 7.2 Мб/с хүртэлх хурдтай холбогдох боломжтой юм. Өөрөөр хэлбэл broadband буюу өргөн зурвасын интернетийг утсагүй технологиор хүлээн авах боломжтой болжээ. Харин 2009-2010 онд гарсан хамгийн сүүлийн үеийн зарим системүүд 15-24 мб/с хурдыг санал болгож байна.

4G Гар утасны TeliaSonera компани хамгийн анхны 4G сүлжээг Норвег болон Шведийн Осло, Стокольм хотуудад байгуулж 2009 оны 12 сард ашиглалтад оруулсан байна. Мөн 2010 оноос америк япон зэрэг улсуудад 4G системд шилжиж гар утас болон бусад хөдөлгөөнт төхөөрөмжүүд IP-д суурилсан хөдөлгөөнт өргөн зурвасын сүлжээнд 50 Бб/с-ээс

100 Мб/с хүртэлх хурдаар холбогдон интернет, өндөр чанар бүхий телевизийн нэвтрүүлэг, видео, онлайн тоглоом тоглох зэргээр орчин үеийн интернетэд суурилсан бүх төрлийн үйлчилгээг хүртэх боломжтой болж байна. Холболтын хурдаар өмнөх үеэс 10 дахин илүү бөгөөд цаашид 1Гб/с-д хүргэх боломжтой. 4G үеийн голлох 2 систем нь LTE-Advanced болон WiMax2 стандартууд бөгөөд аль аль нь хүчин чадал сайтай боловч өндөр өртөг шаардагдсан технологиуд юм. АНУ-д Sprint Nextel, Comcast компаниуд Mobile WiMAX сүлжээг байгуулж , 2010 оны 6 сараас анхны 4G гар утас HTC EVO-г худалдаалж эхэлсэн байна. Гар утасны дэлхийн хамгийн том оператор компани болох China Mobile ирэх жилээс 4G системд шилжихээ мэдэгдсэн билээ. Япон улсын хувьд Мобиком компаний хөрөнгө оруулагчдын нэг болох KDDI компани анхлан 4G системд шилжиж байна. Гэхдээ өөрийн сүлжээ байгуулаагүй бөгөөд Uq Wimax компаний сүлжээг ашиглаж байна. Сүүлийн жилүүдэд дэлхийн улс орнууд гар утас буюу утасгүй харилцаа холбооны хөгжлийн 4-р түвшинд шилжиж байна.



Зураг 2.1: Харилцаа холбооны хөгжлийн үе шат

2.2.1 4G түвшний давуу талууд

• Илүү хурдтай

• 4G Интернэт протокол IP ашигладаг учир маш олон зүйл дамжуулж чадна

• Илүү хол зайд дамжуулдаг.4G саад багатай орчинд 50км (WiMAX).

• Сүлжээ хоорондын шилжилт тасалдалгүйгээр хийдэг.

• Маш их хэмжээний хэрэглэгчтэй ажиллах чадвартай

• Маш хурдтай ажилладаг алгоритмуудтай.

• Алдаа засалтын код хамт дамжуулдаг

•Бүх IP сүлжээ дэмжинэ. (Tunnel болон Firewall, authentication буюу нэвтрэлтийн нууцлал хамгаалал, ip -р байршил тогтоох)

•Нууцлал хамгаалалт (Encryption protocol ашигладаг)

•IPv6 дэмждэг

2.3 AAA

AAA хэрэглэгч аюулгүйгаар хандах (зөвшөөрөл) юу хийж чадах вэ (адилтган танилт), болон хэрэглэгчийн бүртгэгдсэн төлбөр тооцоо (accounting) –г тодорхойлж аюулгүй байдлыг хангах боломжийг олгодог. AAA –г ашигласнаар ACL -ууд ашиглалгүйгээр хэрэглэгчийн хандах эрх, хяналтын нэмэгдүүлдэг түвшин байдаг. Жишээ нь, ISP сүлжээнд та бүх гадны хэрэглэгчидийг сервер дээрээ танилт хийж Telnet-ээр хандах боломжийг үүсгэж болно/authentication-ы жишээ/. Та зөвхөн сервер рүү хандах хэрэглэгчийн эрхийг тодорхойлоод зогсохгүй ямар хэрэглэгч ямар эрхтэйгээр хандах, ямар IP хаягтай хэрэглэгч хандаж болохгүй зэргийг тодорхойлж өгч болно. Хэрэглэгчийг гарцын төхөөрөмж дээр тодорхойлж өгөлгүйгээр AAA сервер дээрээ энэхүү үйлчилгээг тодорхойлж өгөөд сервэрээр дамжин тухайн хэрэглэгчийг адилтган танилт хийх болно. Энэ нь илүү найдвартай бөгөөд илүү том сүлжээнд тохируулахад шаардлагатай үйлчилгээ байх болно. Та гарцын төхөөрөмж дээрээ зөвхөн юу хийж болох , юу хийсэн зэргийг бүртгэх тохиргоог хийж өгөх болно. /Telnet-ээр хандахдаа мөн адил танилт хийж аюулгүй байдлыг хангадаг/. Тухайн байгууллага AAA серверийг тохируулснаар админ, хэрэглэгчдийн хандах эрхийг тодорхойлж өгөхдөө хэзээ яаж хандах зэргийг тодорхойлж өгнө. Ингэснээр сервэрлүү эрх бүхий хэрэглэгч үргэлж эхэнд нэвтэрдэг байхыг шаардана.

2.3.1 Authentication

1. Authentication нь интернэтэд санал болгодог үйлчилгээнүүдийг олж авахын тулд хийгдэж буй анхны үйлдэл юм. Энэ Алисийн тохиолдол карт хүчинтэй эсэхийг батлах үйлдэл юм. Картыг шалгах хамгийн түгээмэл арга нь хэрэглэгчийн нэр болон нууц үг юм. Өөрөөр нэг удаагийн тэмдэглэгээ, сертификат, Пин дугаар мөн биометрээр хайх зэрэг аргуудыг ашиглаж болно.

   Үйлилгээг хүссэн хэрэглэгчийг үйлчилгээ авах хүчинтэй эсэхийг баталгаажуулдаг.

   Бүртгэлтэй мэдээллээр дамжуулагдан хийдэг Жишээ нь нууц үг, тоон сертификат, утасны дугаар г.м

   Authentication амжилттай болсны дараа сессион эхэлдэг. Энэ нь сүлжээний холболт дуусах хүртэл үргэлжилдэг.

2.3.2 Authorization

1. Хэрэглэгчдийн authentication дээр үндэслэн хэрэглэгчдийн үйлчлэх үйлчилгээний төрлийг заана. Authorization ын жишээ нь: Исак нөөцийн хэрэглээг шалгах арга хэрэгсэл юм. Алисс нууц үгээр

Authentication хийсний дараа Исак тодорхой хязгаарыг оноож эсвэл илүү эрх олгож болно. Исак нь холбогдсон session-ы дугаарыг хязгаарлах, IP хаяг оноож өгөх, зарим урсгалын зөвшөөрөх, QoS-г хэрэгжүүлэх боломжтой. Authorization нь логик аргыг хэрэглэдэг. Жишээ нь Алис оюутан бол ажлын цагуудад интернэтэд орохыг хаах. Илүү зурвасын өргөн ашиглаж байвал энэхүү асуудлыг шийдэж хязгаарлах. Эх үүсвэр лүү хандах үед Authorization NAS дээр үндэслэн хийгддэг.

Жишээ нь: Цаг өдрөөр хязгаарлах, хаана байгаагаар нь хязгаарлах, олон удаа login хийхийг хязгаарлах

Үйлчилгээний жишээ нь: IP хаягаар шүүх, Хаяг оноох, замыг оноох, шифрлэлт, QoS /өөр үйлчилгээ, зурсын хяналт/, урсгалыг хяналт гэх мэт

2.3.3 Accounting

1. Хэрэглэгчийн сүлжээний нөөцийн хэрэглээг хянах. Ерөнхийдөө Хэрэглэгчийн үйлчилгээг эхэлсэн ба дууссан цаг, авсан үйлчилгээний төрөл, хэрэглэгчийн шинж чанар зэргийг цуглуулсан мэдээлэл. Хэрэглэсэн Удирдлага, төлөвлөгөө, төлбөр тооцоо байж болно Accounting нь нөөцийн хэрэглээг хэмжих арга юм. Accounting нь хэрэглээг тасралтгүй хэмжих процесс юм.

2.4 Баталгаажуулалт хийх протоколууд

Ерөнхийдөө баталгаажуулалт хийх 3 төрлийн арга байдаг.

1. PAP нь холболт тогтоох хамгийн энгийн арга бөгөөд 2 way handshake ашигладаг. Зөвхөн пассворд оор баталгаажуулалт хийдэг ба мөн энэ пассворд оо ямарч нууцлалгүй текст хэлбэрээр нь явуулдаг ингэснээр халдагад өртөхөд маш амархан болж байгаа юм.

2. CHAP нь handshake маягаар явагддаг бөгөөд хариу мессежийн хаш утга таарсан тохиолдолд холболтыг зөвшөөрдөг гэж хэлж болно PAP ыг бодвол илүү аюулгүй байж чаддаг учир нь холболтын хаяг, өгөгдөл, хэрэглэгчийн нэр нууц үгийг нийлүүлэн MD5 аар оруулж хаш утга гаргаж аван үүгээрээ баталгаажуулалт буюу танилт хийгддэг

3. EAP Extensible Authentication Protocol буюу EAP нь утасгүй сүлжээнд нэг цэгээс нөгөөд холбогдох холболтод ихэвчлэн хэрэглэддэг баталгаажуулалтын бүтэц хэсэг юм. Энэ нь RFC 3748 буюу хөгжүүлэгдэж RFC 5247 болсон стандартад агуулагдаж байдаг.

EAP нь мэдээлэл дамжуулахад шаардлагатай түлхүүрийн параметрүүдийг дамжуулах боломжоор хангадаг. EAP нь мессежний форматыг тодорхойлж өгдөг бөгөөд EAP ашигладаг протоколууд EAP мессеж агуулж байдаг. Энэ нь өргөн ашиглагддаг протокол юм.Энэхүү протокол нь мөн AAA түлхүүр солилцох аргыг тодорхойлж өгсөн байдаг нь RFC 4962 юм.

2.4.1 Радиус сервер нь гурван төрлийн хариу явуулдаг

RADIUS сервер нь NAS-руу гурван төрлийн хариуг явуулдаг.

(a) Access-reject Энэ нь тухайн хэрэглэгчийг тухайн сүлжээнд орохыг хориглосон мессэж юм. Үүнийг илгээж болох шалтгаан нь тухайн хэрэглэгчийн бүртгэл идэвхгүй эсвэл ямар нэгэн алдаа буюу нэвтрэх эрх буруу байх зэрэг байж болно.

(b) Access-Challenge Энэхүү мессэж нь тухайн хэрэглэгчээс нэмэлт мэдээлэл авах шаардлагатай бол илгээх бөгөөд энэ нь хоёр дахь нууц үг эсвэл pin код, картны дугаар зэрэг байж болно. Access-challenge нь зарим тохиолдолд илүү нууцлалтай байлгах үүднээс ашиглах боломжтой бөгөөд энэ нь хэрэглэгч болон RADIUS сервэр хоёрын хооронд нууцлалтай тунель үүсгэх бөгөөд ингэснээр NAS -д тэдгээр мэдээллийг харах боломжгүй.

(c) Access-accept Энэхүү мессэж нь тухайн хэрэглэгчийн сүлжээнд орохыг зөвшөөрч буйг илтгэх юм. Хэрэв тухайн хэрэглэгч сүлжээнд нэвтрэхийг зөвшөөрөгдсөн бол RADIUS сервер тодорхой давтамжтай тухайн хэрэглэгчийг дахин дахин шалгана. Сүлжээнд нэвтрэх эрх авсан хэрэглэгч тухайн компанийн сүлжээнд холбогдох боломжтой болно. Мөн тухайн хэрэглэгчийн холболтын мэдээлэл RADIUS серверийн дотоод санах ойд эсвэл LDAP, active directory зэрэгт хадгалагдаж байдаг.

Эдгээр гурван мессэжийн аль нь ч байсан тодорхой тайлбартай хамт явах бөгөөд энэ нь яагаад татгалзсан тухай эсвэл тавтай морил гэсэн мессэж байна.

2.5 Radius ын үзүүлэлт

2.5.1 Packet Format

Client болон серверийн хоорондох дамжуулалтыг хийхэд UDP багцыг ашигладаг. Протокол нь 1812 дугаар портоор холбогддог. Хэд хэдэн төрлийн packet -ын бүтэцтэй:

1. Access request

   Хандах хүсэлт

2. Access respond

   хандалтын хариу

3. Access reject

   хандалтыг цуцлах

4. Accounting request

   Бүртгэл шалгах хүсэлт

5. Accounting respond

   Бүртгэлийн хариу

6. Access challenge

   хандалтыг сорилт

7. Status Server

8. Status Client

9. Reserved

2.5.2 Радиус RFC2865 протокол

Радиус нь UDP хэрэглэдэг бөгөөд 1842 дугаар портыг ашиглаж холбогддог.

Код: Өгөгдлийн төрлийн таних тэмдэг

Access-request, Access-Accept

ID: Хүсэлтийн хариуг таруулахад ашиглагдах дугаар

Урт: өгөгдлийн урт

Баталгаажуулагч: санамсаргүй утга боловруулагдан нэг хүсэлт болон хариунд

агуулагдаж байх ёстой

Шинж чанар: Дамжуулагдаж буй өгөгдөл онцгой агуулагдаж байгаа мэдээллүүдийг агуулна

2.5.3 Authenticate хийгдэх үе шат

1. **Initialization**: Шинэ хэрэглэгч илэрхэд, баталгаажуулагч дээрх портууд баталгаажуулаагүй төлөвт буюу 802.1X трафик зөвшөөрөгдөж бусад трафик хаягдана.

2. **Initiation**: Баталгаажуулагч буюу AP нь EAP-request 2-р түвшиний хаяг дээр frame дамжуулах бөгөөд Хэрэглэгч өөр дээрээ энэ хаяг дээр чагнаад байж байх бөгөөд EAP-request Хүлээж авсан бол өөрийн мэдээлэл буюу USER ID агуулсан EAP-response frame буцааж дамжуулна. AP энэ Frame-ыг access request болгон серверлүү дамжуулна. Хэрэглэгч дахин нэвтрэх бол EAPOL-start frame дамжуулна харин хариуд нь AP дахиад EAP-request frame явуулна.

3. **Negotiation**: Сервер access challenge пакетыг AP -руу дамжуулна. Энэ нь EAP-request байх бөгөөд EAP method зааж өгсөн байна. AP энэ Frame-ыг хэрэглэгч рүү дамжуулах бөгөөд хэрэглэгч ирсэн EAP method ашиглан холбогдож болох бөгөөд эсвэл NAK буюу Negative ack хийж өөрийн холбогдохыг хүссэн EAP method-г дамжуулна.

4. **Authentication**: Хэрэглэгч ,сервер хоёр EAP method тохиролцоод EAP-success мессеж ирвэл AP портуудаа баталгаажсан төлөвт буюу Authorized төлөвт аваачин энгийн трафик дамжуулна. Хэрэв Unsuccessful байвал AP -н портууд Unauthorized хэвээрээ байна. Хэрэв хэрэглэгч холболтоо тасалвал EAPOL-logoff мессеж AP-руу дамжуулах бөгөөд үүний хариуд AP портоо unauthorized төлөвт оруулан EAP ээс бусад трафик хорино.

2.6 OpenWRT

OpenWrt Линуксийн кернел дээр суурилсан үйлдлийн систем бөгөөд энэ нь голдуу эмбэддэд төхөөрөмжүүд дээр сүлжээний урсгалыг замчлах үүргээр хэрэглэгддэг. OpenWRT нь багцын удирдлагатай бүрэн бичигдэхүйц файл системээр хангадаг мөн хамгийн бага үнэ бүхий техник хангамж болон өндөр чадамжийг санал болгодог. линукс кернел дээр суурилсаны давуу тал нь линуксын бусад кернел дээр болох бүх боломжууд хэрэгжих боломжтой болж байгаа юм.

2.7 EAP

Extensible Authentication Protocol буюу EAP нь утасгүй сүлжээнд нэг цэгээс нөгөөд холбогдох холболтод ихэвчлэн хэрэглэддэг баталгаажуулалтын бүтэц хэсэг юм. Энэ нь RFC 3748 буюу хөгжүүлэгдэж RFC 5247 болсон стандартад агуулагдаж байдаг.

EAP нь мэдээлэл дамжуулахад шаардлагатай түлхүүрийн параметрүүдийг дамжуулах боломжоор хангадаг. EAP нь мессежний форматыг тодорхойлж өгдөг бөгөөд EAP ашигладаг протоколууд EAP мессеж агуулж байдаг. Энэ нь өргөн ашиглагддаг протокол юм. Үүнийг 802.11 буюу WPA, WPA2 мөн 802.1X болгож хөгжүүлсэн байдаг. EAP нь олон төрөлтэй байдаг.

EAP-н утасгүй сүлжээнд ажилладаг төрөл нь EAP-TLS, EAP-SIM, EAP-AKA, LEAP болон EAP-TTLS зэрэг байна. Энэхүү протокол нь мөн AAA түлхүүр солилцох аргыг тодорхойлж өгсөн байдаг нь RFC 4962 юм.

2.8 802.1X болон EAPOL зарчим

Энэ нь портод суурилсан сүлжээнд нэвтрэх байдлын хянадаг бөгөөд, сүлжээнд нэвтрэх үед authentication шат нэмэгддэг. Энэ нь Extensible Authentication Protocol гэгдэх бөгөөд Lan Сүлжээнд хэрэглэн EAPOL гэгдэх болсон. Энэ нь authenticate хийхэд 3 төхөөрөмж шаардлагатай бөгөөд Хэрэглэгч, баталгаажуулагч болон баталгаажуулах сервер зэрэг орно. Сервер нь radius эсвэл EAP протокол дэмжиж ажилладаг байна. Баталгаажуулагч нь серверээс баталгаажуулсан мэдээлэл ирэх хүртэл Хэрэглэгчийг сүлжээнд холбохгүй бөгөөд Хэрэглэгч Username password эсвэл Certificate ашиглан холбогдоно. EAPOL нь Network шатанд ажиллана. 802.1X -2001 нь 2 логик порттой бөгөөд эдгээр нь Controlled port болон Uncontrolled port юм. Controlled port -руу зөвшөөрөлгүй төхөөрөмжүүд холбогдох боломжгүй байдаг бөгөөд харин Uncontrolled port нь EAPOL Frame дамжуулах үүрэгтэй байдаг. 802.1X -2004 нь Mutual authentication буюу хэрэглэгч буруу сүлжээнд холбогдож мэдээлэл алдахаас сэргийлдэг бөгөөд үүнийг ашиглаж байгаа хэрэглэгч өндөр түвши-

ний протоколыг серверээс баталгаажуулалт иртэл дамжуулахгүй бөгөөд ингэж мэдээлэл алдахаас сэргийлнэ.

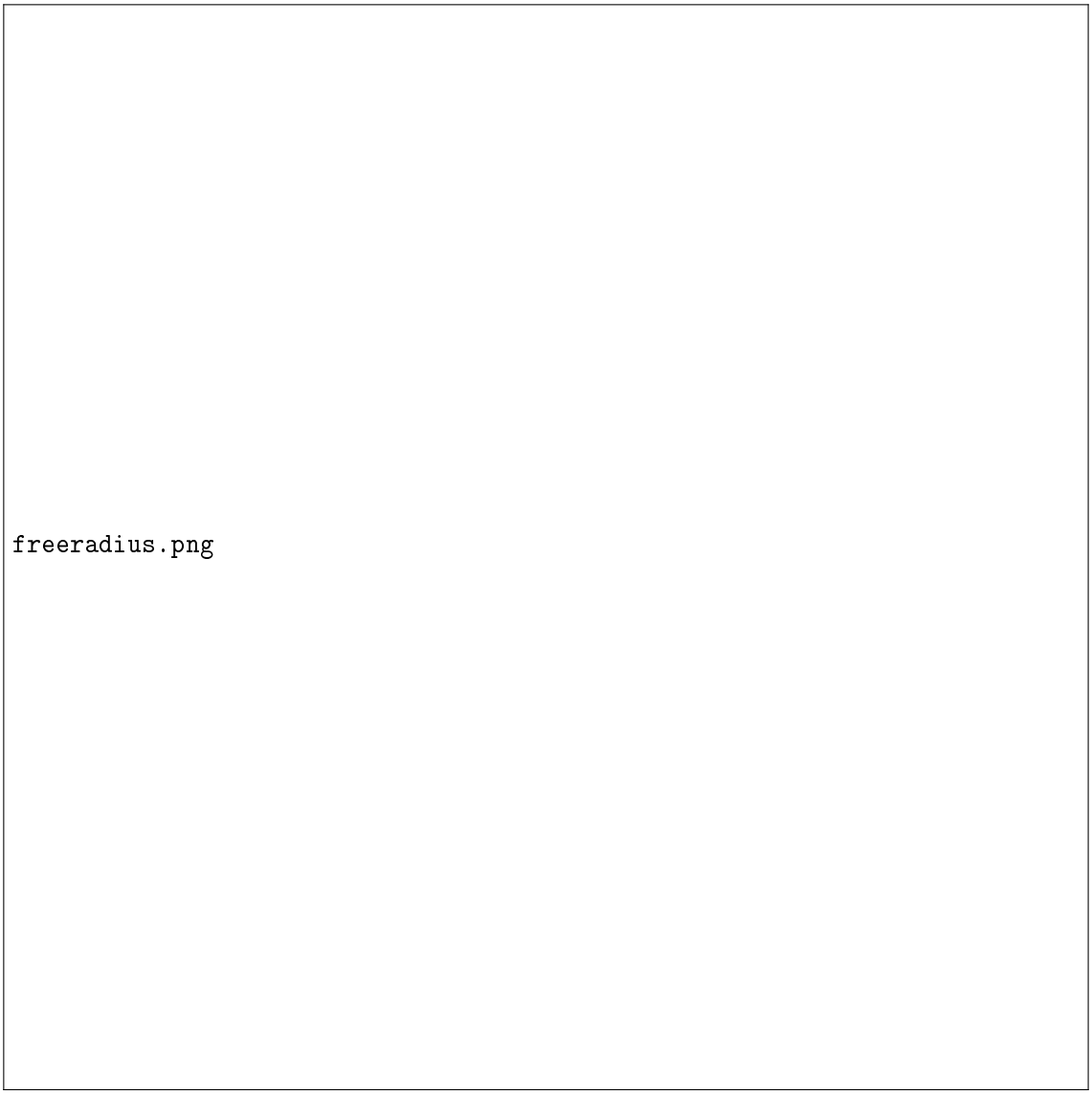
Authenticate хийх үе шат:

1. **Initialization**: Шинэ хэрэглэгч илэрхэд, баталгаажуулагч дээрх портууд баталгаажуулаагүй төлөвт буюу 802.1X трафик зөвшөөрөгдөж бусад трафик хаягдана.

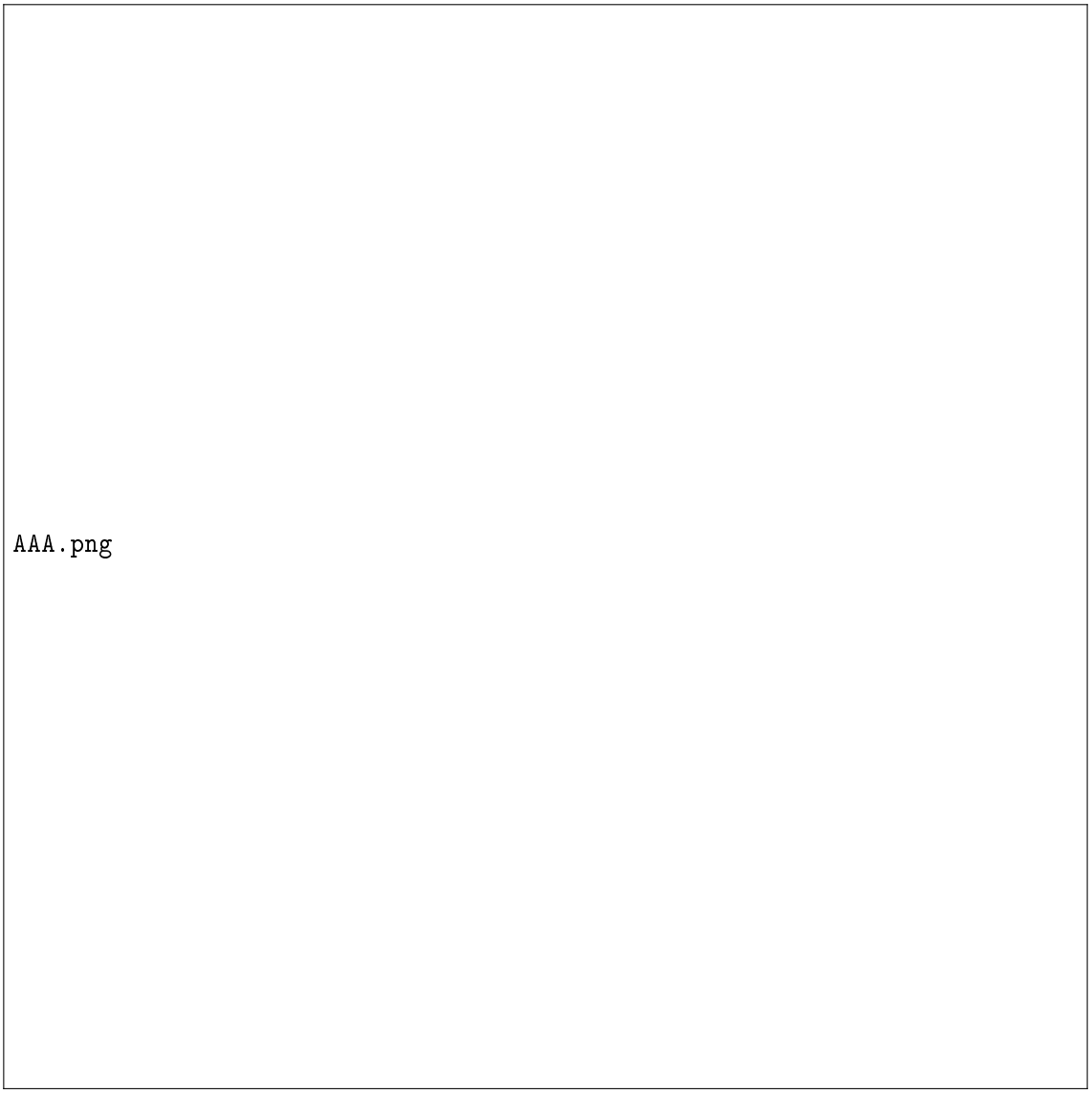
2. **Initiation**: Баталгаажуулагч буюу AP нь EAP-request 2-р түвшиний хаяг дээр frame дамжуулах бөгөөд Хэрэглэгч өөр дээрээ энэ хаяг дээр чагнаад байж байх бөгөөд EAP-request Хүлээж авсан бол өөрийн мэдээлэл буюу USER ID агуулсан EAP-response frame буцааж дамжуулна. AP энэ Frame-ыг access request болгон серверлүү дамжуулна. Хэрэглэгч дахин нэвтрэх бол EAPOL-start frame дамжуулна харин хариуд нь AP дахиад EAP-request frame явуулна.

3. **Negotiation**: Сервер access challenge пакетыг AP -руу дамжуулна. Энэ нь EAP-request байх бөгөөд EAP method зааж өгсөн байна. AP энэ Frame-ыг хэрэглэгч рүү дамжуулах бөгөөд хэрэглэгч ирсэн EAP method ашиглан холбогдож болох бөгөөд эсвэл NAK буюу Negative ack хийж өөрийн холбогдохыг хүссэн EAP method-г дамжуулна.

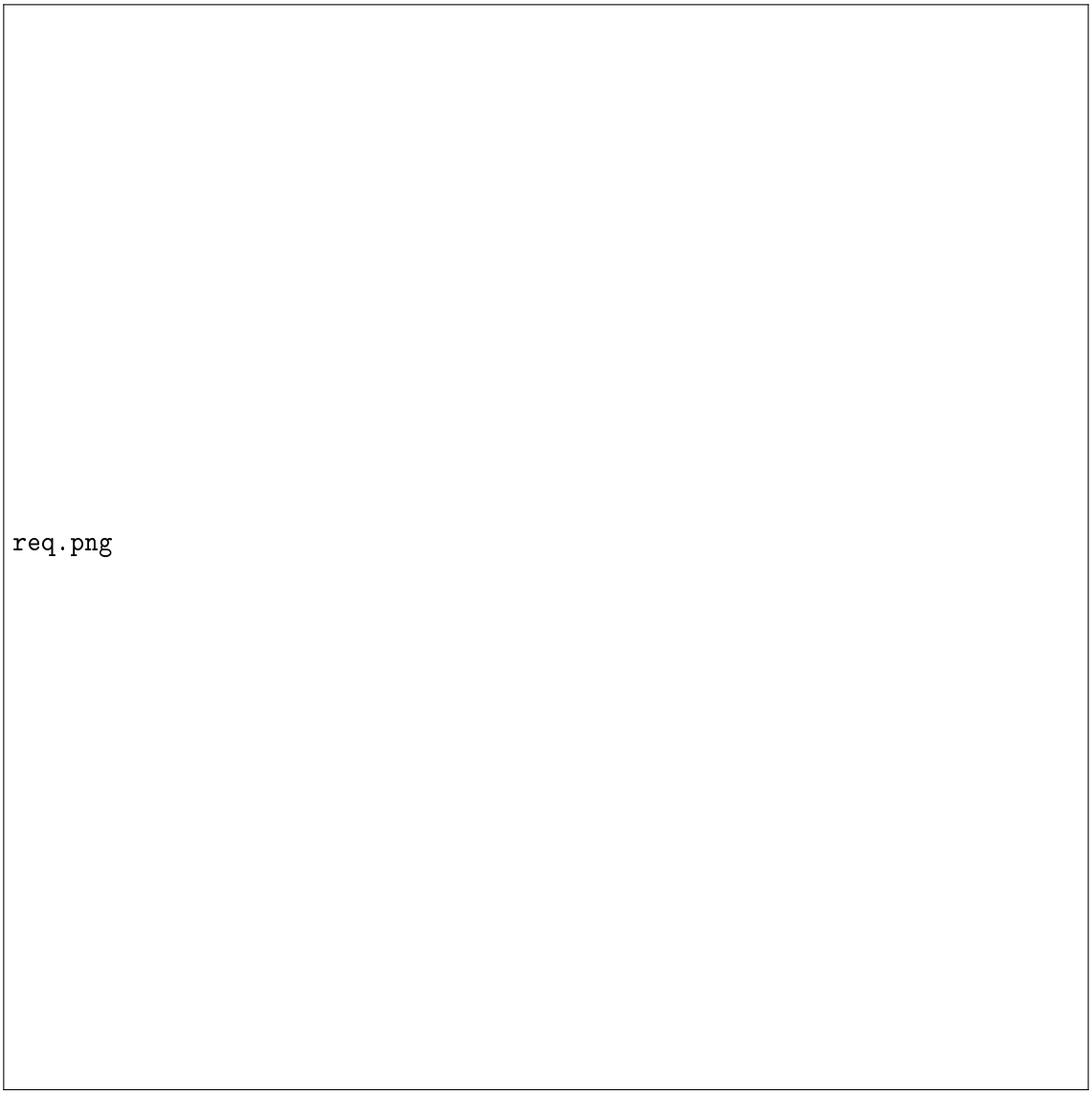
4. **Authentication**: Хэрэглэгч ,сервер хоёр EAP method тохиролцоод EAP-success мессеж ирвэл AP портуудаа баталгаажсан төлөвт буюу Authorized төлөвт аваачин энгийн трафик дамжуулна. Хэрэв Unsuccessful байвал AP -н портууd Unauthorized хэвээрээ байна. Хэрэв хэрэглэгч холболтоо тасалвал EAPOL-logoff мессеж AP-руу дамжуулах бөгөөд үүний хариуд AP портоо unauthorized төлөвт оруулан EAP ээс бусад трафик хорино.



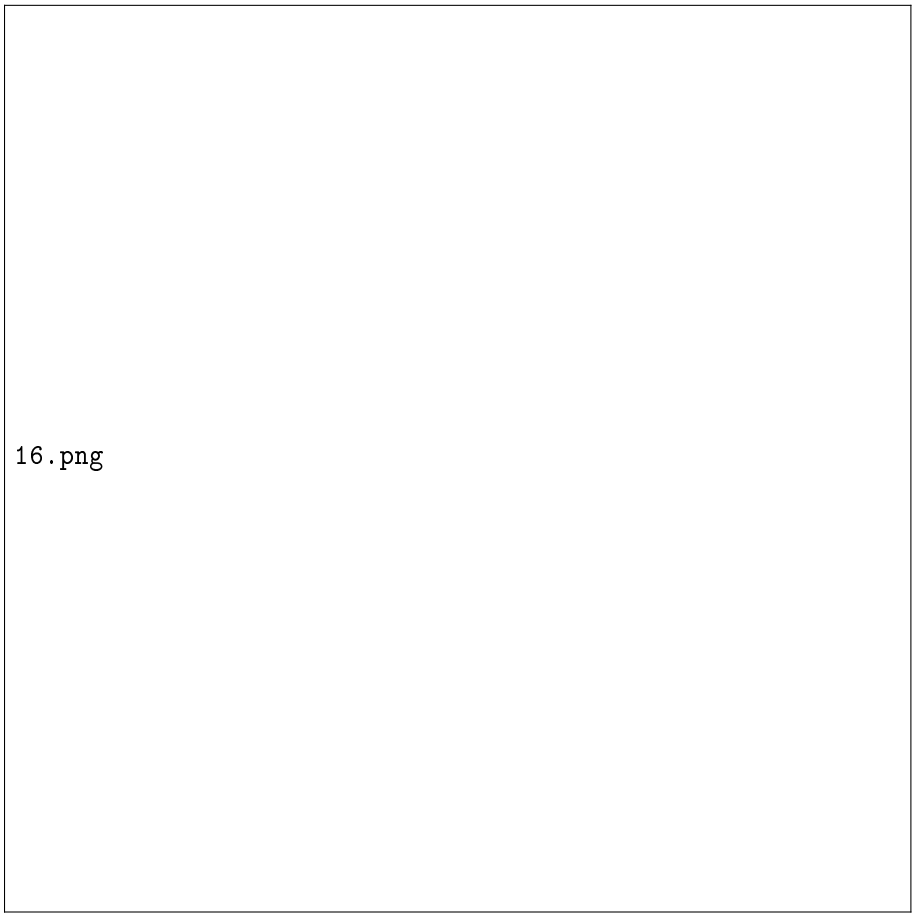
Зураг 2.2: Радиус сервер



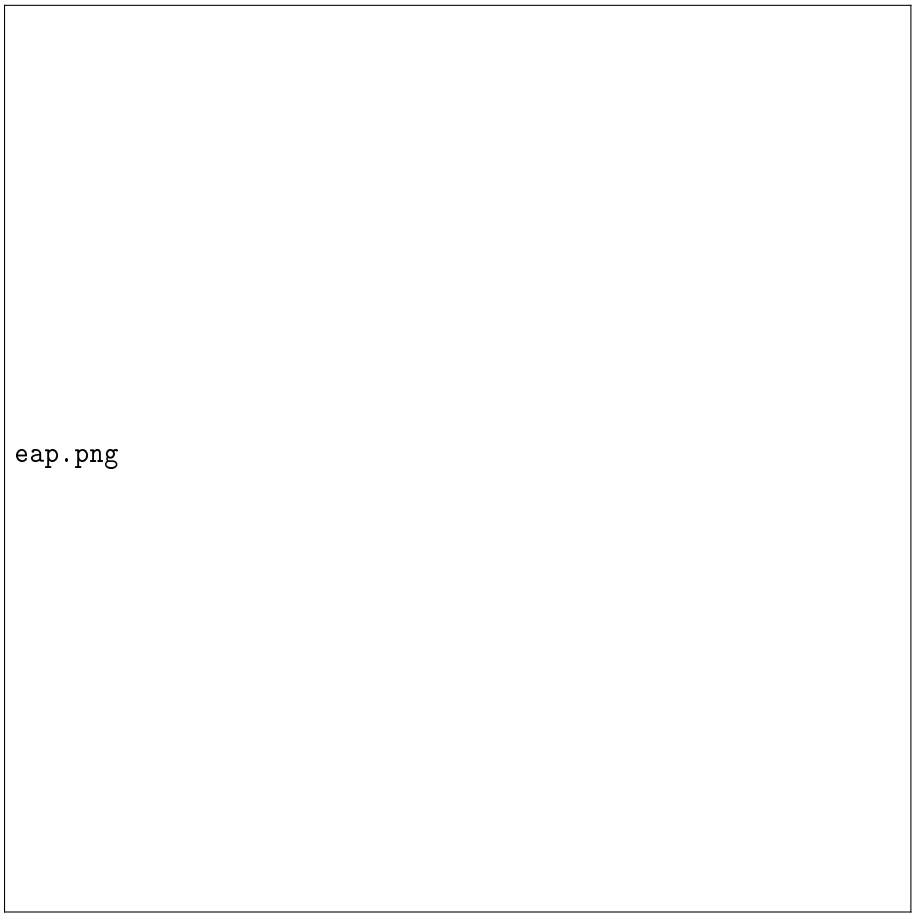
Зураг 2.3: HAC/PAC нь зөвшөөрлийг Радиус серверээс аван нэвтрүүлэх эсэхийг шийднэ.



Зураг 2.4: Баталгаажуулалт



Зураг 2.5: пакет задаргаа



Зураг 2.6: eap үйлдэл

Бүлэг 3

Судалгаа, шинжилгээний бүлэг

3.1 Радиус сервер

3.1.1 Бусад Радиус сервер

- BSDRadius BSDRadius-ийн python хэл дээр бичигдсэн нээлттэй эх бөгөөд VoIP хэрэглээнд зориулагдсан байдаг. Түгээмэл хэрэглэгддэг VoIP протоколууд (SIP and H.323) нь (CHAP digest) гэх мэт authentication-ий цөөн тооны аргуудыг хэрэглэдэг ба энэ нь overhead үйл ажиллагаа ба BSDRadius дахь хэмжээг багасгадаг.

- GNU Radius нь GPL-linecsed(Cistron variant) Radius -ын гүйцэтгэл бөгөөд маш өргөн хүрээний authentication-ы төлөвлөгөөнүүдийг дэмжиж байдаг. Үүнд:system database, SQL database болон PAM authentication багтдаг. Тэдгээрийн ихэнх кодууд нь Lex and Yacc зэргийг өргөн хэрэглэж дахин бичигдсэн байдаг. Дахин бичигдэх тохиргооны файл *incredibly* нь чухал хэрэгцээтэй.

- Jradius нь Java сервертэй ярилцдаг ба RADIUS -ын гарын авлагыг Java хэлдээр бичих боломжийг олгодог.

- OpenRadius нь GPL-licensed Radius протоколын гүйцэтгэл бөгөөд хуваагдсан нууцлалууд authentication мэдээлэл бодлого хэрэглэгчийн profile ууд болон өөр бусад боломжит эх сурвалжийг олж авах боломжыг олгодог. Unix password databases (including NIS/NIS+), livingston-style ASCII files and LDAP зэргийг дэмждэг.

Radiusd хэд хэдэн тохиргооны файлыг хэрэглэдэг. Тохиргооны файлууд нь ихэвчлэн /etc/raddb директорт хадгалагддаг. Файл бүр өөрийн man

хуудсандаа файлынхаа форматыг тодорхойлсон байна. Эдгээр файлууд нь:

- Radiusd.conf Администраторын тохируулсан зүйлүүд байдаг үндсэн тохиргооны файл. Энд сервер аль порт, ямар хаяг дээр, аль интерфэйсээрээ, ямар төрлийн пакетыг сонсох гэх мэт үндсэн тохиргоог хийж өгдөг.

- Dictionary Энэ файл нь ихэвчлэн статик байдаг. Энэ нь бусад тохиргооны файлд хэрэглэгддэг боломжит бүх RADIUS attribute-уудыг тодорхойлдог. Үүнийг өөрчлөх хэрэггүй. Энэ нь тухайн директор дахь бусад dictionary файлуудыг агуулдаг.

- Clients.conf Серверт холбогдохыг хүсч байгаа клинт бүрийн IP хаяг болон нууц түлхүүрийг агуулдаг. RADIUS клинтийг тохируулах 2 арга байдаг. IP subnet-ээр нь NAS-г групплэх боломжтой эсвэл hostname болон IP хаягаар нь NAS-г тодорхойлох боломжтой.

- Hints Хандалтын серверээр илгээсэн хэрэглэгчийн нэвтрэх нэр болон бусад параметрүүд дээр үндэслэн RADIUS серверлүү тодорхой санууулгуудыг (hints) тодорхойлдог. Энэ нь мөн хэрэглэгчийн нэрийг хөрвүүлдэг (Pusername /- username гэх мэт).

- Huntgroups Huntgroups-үүдийг тодорхойлдог ба тодорхой хэрэглэгчидийн тодорхой huntgroup-үүдэд хандах хандалтыг хязгаарладаг.

- Users Энд хэрэглэгчдийг тодорхойлдог. Энэ файл нь хэрэглэгч бүрийн аюулгүй байдлын болон тохиргооны мэдээллийг агуулдаг. Эхний талбар нь хэрэглэгчийн нэр, араас нь хэрэглэгчид баталгаажуулалтын шаардлагуудыг жагсаадаг. Эдгээр нь пассворд, хэрэглэгчийн нэр болон хэрэглэгчийн пассвордын дуусах хугацаа зэргийг агуулдаг. Тухайн нэгжээс баталгаажуулалтын хүсэлт хүлээн авагдсан үед, эдгээр утгууд шалгагддаг. Users файлд агуулагдаагүй хэрэглэгчдэд юу хийхийг тодорхойлоход “DEFAULT” нэрээр хэрэглэгч үүсдэг. “UNIX” гэсэн пассворд нь хэрэглэгчдэд UNIX password-н (/etc/password) баталгааг хэрэглэхийг баталгаажуулалтын серверт хэлж өгдөг. Tab тэмдэгт авсны дараах эхний мөр нь хэрэглэгчийн session эхлэхийг зөвшөөрөхөд тухайн нэгжрүү буцаах тохиргооны утгыг заадаг.

- Jump up - NAS нь сүлжээнд RADIUS серверийн клинт байдлаар ажиллах ба хэрэглэгчээс ирсэн мэдээллийг RADIUS серверлүү дамжуулдаг. Рүтэр, файрвол, свич зэрэг төхөөрөмж байна.

3.2 Freeradius танилцуулга

3.3 OpenWRT

OpenWrt Линуксийн кернел дээр суурилсан үйлдлийн систем бөгөөд энэ нь голдуу эмбэддэд төхөөрөмжүүд дээр сүлжээний урсгалыг замчлах үүргээр хэрэглэгддэг. OpenWRT нь багцын удирдлагатай бүрэн бичигдэхүйц файл системээр хангадаг мөн хамгийн бага үнэ бүхий техник хангамж болон өндөр чадамжийг санал болгодог. линукс кернел дээр суурилсаны давуу тал нь линуксын бусад кернел дээр болох бүх боломжууд хэрэгжих боломжтой болж байгаа юм.

3.3.1 Яагаад OpenWRT

-Нээлттэй систем учираас хүссэнээрээ удирдах боломжтой
-Линуксын Package Management тэй ажилладаг
-3400 гаруй санг агуулсан том хэмжээний багцуудтай
-Одоо ч гэсэн хөгжүүлэлтийн ажил хийгдэж байгаа
-Хамгийн бага зардлаар төхөөрөмж дээр хөгжүүлэлт хийх боломжтой

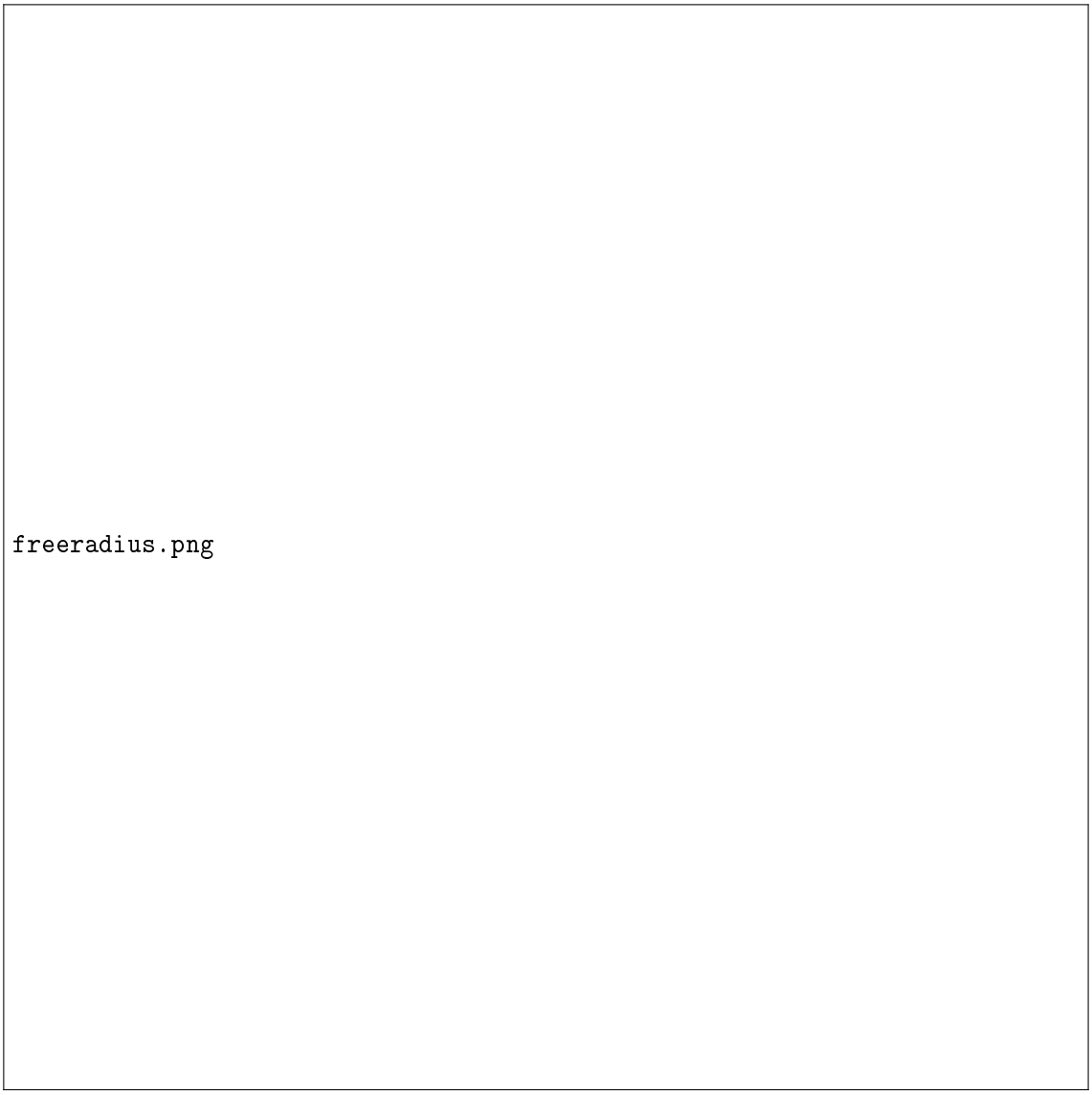
3.3.2 Интерфейс

- UCI гэдэг нь Unified Configuration Interface гэсэн үгний товчлол бөгөөд OpenWrt-н тохиргоог нэг цогц болгох зорилготой юм.Тохиргоо нь их хялбар, шууд тохируулж болохоор байвал бүх зүйлсийг хялбар болгох бөгөөд энэ нь UCI-н гол зорилго юм.UCI нь ихэнх системийн тохиргооны хамгийн чухал хэсэг маягаар ажиллана.Энэхүү чухал хэсгүүд нь тухайн төхөөрөмжийг ажиллуулахад байх шаардлагатай хамгийн гол хэсгүүд байх бөгөөд жишээдбэл вэб интефейс байх бөгөөд эдгээр байхгүй бол төхөөрөмж ажиллахад хүндрэлтэй болох юм. Удирлагатай системийн тохиргоонд хамгийн чухал хэсгүүд нь байхлах бөгөөд жишээлбэл гол сүлжээний интерфейсийн тохиргоо, утасгүй сүлжээний тохиргоо, лог бичиж авах тохиргоо мөн алсаас хандах боломж түүний тохиргоо гэх мэт.
  - коммандаар интерфейсд тохиргоо хийх боломжтой
  - скрипт бичих тохируулах боломжтой
  - тохиргоогоо хадгалж авах боломжтой
  - бусад програмд тохиргоо хийх боломжтой
- LuCI нь 2008 онд анх FFLuCI гэсэн нэрээр гарж байсан бөгөөд энэ нь Freifunk-Firmware болон OpenWrt-н White Russian болон Kamekaze зэрэг хувилбаруудад зориулагдан гарж байсан юм.

Үүний гол зорилго нь энгийн хялбар, үнэгүй Web интерфейсийг суурилуулагдсан төхөөмжүүдэд зориулан гаргаж ирэх байсан юм.Бусад тохиргооны интерфейсүүд Shell-script хэл ашигладаг байхад LuCI-н Lua програмчлалын хэл ашиглан интерфейс, модел, логик харагдац, болон обьект хэлбэртэй удирдах боломжтой болсон юм. Мөн энэ нь хэмжээг жижигхэн болгож өгсөн бөгөөд, жижиг хэмжээтэй ч хүчин чадал илүү ихэссэн байна. Хурдан ажиллах болон энгийн тохиргоо гэсэн давуу талтай.

- OpenWRT зориулагдсан вэб интерфейс
- Тохиргоо,админ эрх, статур, мониторинг
- тохиргоо хийхэд UCI г бодвол илүү хялбар үр дүнтэй

• Дараагын алхам хүртэлх хамгаалалтын төлөв. hop-by-hop
• Байнгын шинчлэл.
• Цэгээс цэгт холболтын PAP, CHAP -г дэмждэг
• MD5 шифрлэлт
• AAA загварыг дэмжин ажилладаг.
• Хэрэглэгч удаан хүлээх боломжгүй тийм учираас TCP протоколын дахин
дамжуулалт болон ACK -уудад нь шаардлаггүй болж байгаа юм.
•Олон хэрэглэгчдийг үйлчилгээгээр хангах мөн серверийн олон thread ашиглалт нь маш амархан.
•Offline хэрэглэгч байхгүй учираас.
•Stateless protocol



Зураг 3.1: Радиус сервер