RADIUS PROTOKOL

Jurić, Darko

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Elektronike

Darko Jurić

Z A V R Š N I R A D

RADIUS PROTOKOL

Split, rujan 2019.

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Elektronike

Predmet: Širokopojasne mreže

Z A V R Š N I R A D

Kandidat: Darko Jurić

Naslov rada: RADIUS protokol

Mentor: Toni Jončić

Split, rujan 2019.

SADRŽAJ

SAŽETAK

RADIUS protokol je kreiran na samim početcima 1990-ih godina. Kada se protokol pojavio, namjena mu je bila pružanje usluge autentikacije na distribuiranim *dial in* poslužiteljima. Danas se više koristi za autenticirani pristup VPN mrežama. Mnoge usluge na aplikacijskom sloju koriste RADIUS za centraliziranu autentikaciju, a također se događaju i stalne nadogradnje istog čime ga još uvijek čine nezamjenjivim autentikacijskim protokolom. RADIUS je standardiziran protokol implementiran u mrežnu opremu. Koristi se za autentikaciju, autorizaciju te administraciju. Transportno sredstvo RADIUS – a je UDP mrežni protokol niže razine. Kao i svaki protokol, RADIUS također sadrži sigurnosne propuste. Postoji nekoliko vrsta napada na tajni ključ, razne enkripcije i sl. TACACS, TACACS + , te Diameter su alternativni protokoli, no još uvijek nisu u potpunosti prepoznati.

Ključne riječi : RADIUS, autentifikacija, protokol

SUMMARY

The RADIUS protocol was created in the early 1990s. When the protocol appeared, its purpose was to provide authentication service on distributed dial in servers. Today, it is more used for authenticated access to VPN networks. Many application layer services use RADIUS for centralized authentication, and there are ongoing updates to the application layer, which still make it an irreplaceable authentication protocol. RADIUS is a standardized protocol implemented in network equipment. It is used for authentication, authorization and administration. RADIUS is a lower level UDP network protocol. Like any protocol, RADIUS also contains security vulnerabilities. There are several types of secret key attacks, various encrypts, etc. TACACS, TACACS +, and Diameter are alternate protocols, but not yet fully recognized.

Keywords : RADIUS, authentification, protocol

1. UVOD

RADIUS je danas često korišten protokol za autentikaciju, autorizaciju i administraciju korisnika. Najčešća primjena samog protokola je kod različitih vrsta usmjerivača, preklopnika i sličnih uređaja. RADIUS protokol baziran je na klijent – poslužitelj modelu . Takav model za transportno sredstvo koristi UDP mrežni protokol. S klijentske strane koristi se *Network Access Server* (NAS) programski paket, koji obavlja različite funkcije potrebne za prosljeđivanje određenih korisničkih parametara, te kod obrađivanja primljenih odgovora. Na drugoj strani poslužitelj je zaslužan za provjeru primljenih korisničkih parametara, te vraćanja konfiguracijskih parametara u svrhu kvalitetnije usluge korisniku. Komunikacija između klijenta i poslužitelja temelji se na tajnom ključu kojeg koriste i klijent i poslužitelj. Vrlo je važno napomenuti da se slanje tajnog ključa, iz sigurnosnih razloga, ne smije vršiti računalnom mrežom.

RADIUS protokol se koristi iz nekoliko razloga:

- Mrežni uređaji ne posjeduju mogućnost pohrane velikog broja podataka autentikacijskih parametara različitih korisnika zbog ograničenih resursa koje posjeduju.
- RADIUS protokol olakšava i centralizira administraciju korisnika. Mnogi davatelji internetskih usluga imaju na stotine tisuća korisnika koji se svakodnevno dodaju i brišu, a njihove informacije o autentikaciji se konstantno mijenjaju. RADIUS protokol pruža određenu razinu zaštite od različitih opasnosti koje se pojavljuju u mreži. Ostali protokoli za provjeru autentičnosti pružaju ili povremenu zaštitu, neadekvatnu zaštitu ili nepostojeću zaštitu. RADIUS u takvu svrhu koristi TACACS+ ili LDAP protokole za provjeru autentičnosti.
- Postoji velika podrška od različitih proizvođača mrežne opreme. Obzirom da se RADIUS protokol najčešće provodi u sklopu ugrađenih mrežnih uređaja, u takvim je okolnostima mogućnost za nadogradnju protokola slaba ili nikakva. Zbog velike prisutnosti RADIUS-a, promjene koje bi se mogle dogoditi u budućnosti bi morale biti kompatibilne s već standardiziranim rješenjima.

Zbog gore spomenutih razloga, RADIUS protokol se danas praktički smatra standardom za daljinsku autentikaciju korisnika i kao takav se provodi i kod novijih i kod starijih mrežnih elemenata.

1.1 Povijest i razvoj RADIUS protokola

Merit Network Inc. je neprofitna organizacija osnovana 1966. godine u svrhu povezivanja računala na 3 sveučilišta u Michiganu. Korištenjem ARPAnet protokola razvijaju vlastitu mrežu. Samo korištenje mreže se u početcima odvijalo između centralnih računala Univerity of Michigana-a, Michigan State University i Wayne State Universtiy-a. Na ranim početcima 1990 –ih godina spomenuta mreža je naveliko povezivala veleučilišta i sveučilišta te podržavala *dial in* pristup. Primjerice, student nekog od sveučilišta se mogao prijaviti na sustav s računala koje se nalazilo u mreži njegovog sveučilišta.

Potreba za distribuiranim *dial in* pristupom je bila velika u odnosu na broj poduzeća koji je mogao ponuditi nekakva rješenja. Organizacija Livingstone 1991. godine na jednom od Meritovih natječaja prijavljuje svoj model i njegove mogućnosti pod nazivom RADIUS protokol. Takav je model zadovoljio sve postavljene zahtjeve i odmah je prihvaćen. Nakon što ga je Merit kupio i implementirao, krenuli su u daljnje razvijanje kako bi protokol imao dodatne mogućnosti npr. *proxy za* distribuiranu autentikaciju i podršku za *dial in* usluge. U jesen 1992. godine IETF (*Internet Engineering Task Force*) osniva radnu grupu NASREQ (*Network Access Server Requirement*). Organizacija Livingstone 1994. godine predaje skicu RADIUS protokola NASREQ-u i traži da kod (*code*) poslužitelja bude dostupan svim korisnicima.

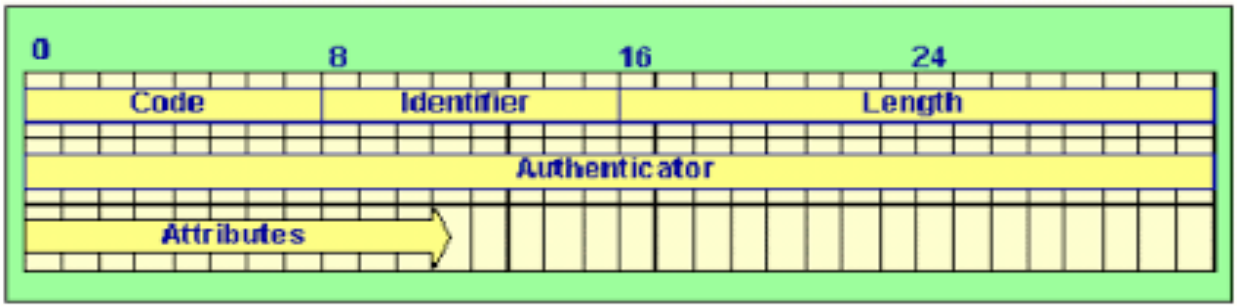
Postojale su velike rasprave oko toga da li bi RADIUS uopće trebao postati standard zbog njegove upitne sigurnosti. Unatoč svemu, svi NAS (Network Access Server) dobavljači su ga počeli koristiti na svojim proizvodima, gdje nakon nekog vremena RADIUS ipak postaje standard. Prvi RADIUS RFC dokument (2058) je izdan 1997. godine. Današnji standard RADIUS RFC (2865) izdan je sredinom 2000. godine. Također su napravljena i dva informativna dokumenta. RADIUS RFC (2866) ima mogućnost praćenja aktivnosti korisnika, a RADIUS *extensions* RFC (2869) pokriva dodatne mogućnosti i nadogradnje na službeni standard.

Broj dokumenta	Naslov dokumenta	Datum	Zamijenjen dokumentom
RFC 2058	*Remote Authentication Dial In User Service (RADIUS)*	Siječanj, 1997.	RFC 2138
RFC 2059	*RADIUS Accounting*	Siječanj, 1997.	RFC 2139
RFC 2138	*Remote Authentication Dial In User Service (RADIUS)*	Travanj, 1997.	RFC 2865
RFC 2139	*RADIUS Accounting*	Travanj, 1997.	RFC 2866
RFC 2548	*Microsoft Vendor-specific RADIUS Attributes*	Ožujak, 1999.	
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*	Lipanj, 2000.	Nadopunjavaju ga RFC 2868, 3575 i 5080
RFC 2866	*RADIUS Accounting*	Lipanj, 2000.	Nadopunjava ga RFC 2867
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*	Lipanj, 2000.	Nadopunjava RFC 2866

Tablica 1 Kronološki redoslijed izdavanja RFC dokumenata o RADIUS protokolu [3]

2.ANALIZA RADIUS PROTOKOLA

Klijent i poslužitelj međusobno izmjenjuju podatke koji se prenose putem RADIUS podatkovnih paketa. Kao što je već spomenuto u uvodnom poglavlju, protokol za transportno sredstvo koristi UDP mrežni protokol niže razine, odnosno paketi su enkapsulirani unutar njega. Također, protokol koristi *challenge - response* uzorak, odnosno upit - odgovor, u kojoj klijent šalje upit poslužitelj, a poslužitelj na temelju toga vraća odgovore klijentu. Na slici u nastavku će se prikazati format jednog RADIUS paketa.



Slika 1. RADIUS poruka[3]

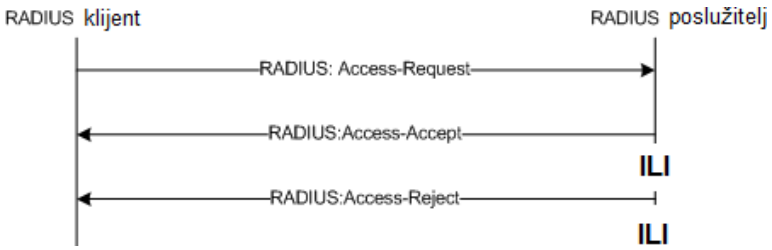
Obrazloženje pojedinačnih polja [2]:

- ***Code*** **-** polje veličine jednog bajta koje definira tip RADIUS podatkovnog paketa. Vrijednosti koje su moguće za ovo polje će se prikazati na sljedećoj tablici.
- ***Identifier*** **(ID) –** polje veličine jednog bajta koje klijentu omogućava jednoznačnu identifikaciju parova upit – odgovor.
- ***Length*** **-** 2 bajta koja predstavljaju veličinu paketa.
- ***Authenticator*** **–** vrijednost koju RADIUS poslužitelj koristi za provjeru ispravnosti odgovora, a također se koristi i kao algoritam za prikrivanje, odnosno zaštite korisničke lozinke.
- ***Attributes*** **–** sekcija u kojoj se nalaze proizvoljni atributi koji pripadaju samoj sesiji (upitu ili odgovoru). Jedini atributi koji su obvezni su *User – Name* i *User – Password* atributi, a ostali atributi su proizvoljni.

VRIJEDNOST	OPIS
1	Zahtjev za pristupom - (*Access – Request*)
2	Odobren pristup – (*Access – Accept*)
3	Odbijen pristup – (*Access – Reject*)
4	*Accounting* zahtjev – (*Accounting – Request*)
5	*Accounting* odgovor – (*Accounting – Response*)
11	Osporavanje pristupa – (*Access – Challenge*)
12	Status poslužitelja - *Status – Server (experimental)*
13	Status klijenta - *Status – Client (experimental)*
255	Rezervirano – (*Reserved*)

Tablica 2 Moguće vrijednosti RADIUS poruke [2]

U narednim poglavljima će se prikazati jedan tipičan postupak RADIUS autentikacije, gdje RADIUS klijent na temelju korisničkog zahtjeva poslužitelju šalje *Access – Request* upit s navedenom lozinkom i korisničkim imenom, na što će mu poslužitelj odgovoriti s dvije poruke: *Access – Accept* ili *Acces – Reject* ovisno prihvaća li sesiju ili ne. Na slici 2. će se detaljnije prikazati komunikacija između klijenta i poslužitelja.



Slika 2. Komunikacija RADIUS klijenta i poslužitelja[3]

Kod samog procesuiranja spomenutog postupka klijent je taj koji zahtijeva od poslužitelja autentikacijsku provjeru lozinke i korisničkog imena, dok s druge strane poslužitelj je taj koji pristupa sustavu baze podataka, koja sadrži autentikacijsku arhivu korisničkih parametara.

Na temelju postavljenih upita RADIUS klijenta, poslužitelj može obrađivati korisnički zahtjev, a zatim na temelju primljenih parametara odlučiti hoće li dozvoliti ili zabraniti pristup mrežnim resursima.

2.1 Upit klijenta

Sama sjednica započinje na način da klijent šalje upit s postavljenim *Access – Request* kodom. Upit minimalno mora sadržavati dva korisnička atributa, a to su: *User – Name i User – Password.* Bajt identifikacije (ID) tog paketa klijent sam odabire i kao takav on nije definiran RADIUS protokolom. Generiranje ovog broja se uglavnom provodi na način da se većinom provodi u obliku brojila, te se taj broj prilikom svakog upita povećava za jedan. *Authenticator* polje unutar paketa sadrži *Request Authenticator* vrijednost. Takva vrijednost predstavlja 16-bajtni znakovni niz, a algoritam njegovog generiranja je vrlo važan za sigurnost. Ne gledajući *User – Password* atribut, RADIUS paket ne sadrži nikakve druge zaštite.

Klijent i poslužitelj međusobno dijele neku vrstu tajnog ključa koji je temeljni dio za kriptiranje korisničke lozinke. U sljedećih nekoliko koraka će se prikazati način kriptiranja lozinke:

- *Request – Authenticator* – spajanje se vrši tajnim ključem kojeg dijele klijent i poslužitelj.
- U sljedećem koraku vrši se obrada MD5 *hash* funkcijom, koja daje 16-bajtni znakovni niz.
- Između dobivenog znakovnog niza i korisničke lozinke primjenjuje se XOR funkcija kako bi se došlo do štićene lozinke. U slučaju da je lozinka veća od 16 bajta, izvode se dodatne MD5 kalkulacije, zbog izbjegavanja neželjenog rezultata.

U narednih nekoliko matematičkih operacija će se prikazati dobiveni konačni rezultat. Prije samih operacija bitno je spomenuti označavanje svakog segmenta. Tajni ključ i poslužitelj se označavaju sa (S), dok se pseudo-slučajna 128- bitna vrijednost *Request – Authenticator* označava sa (RA). Lozinka se dijeli na 16-bajtne blokove *p1,…,pn.* Zadnji blok se dopunjava s nulama kako bi se dobilo 16 blokova veličine 1 bajta.

Matematičke operacije:

$$c1 = p1 \text{ XOR } MD5 (S + RA)$$
$$c2 = p2 \text{ XOR } MD5 (S + c1) \quad (1)$$
$$.cn = pn \text{ XOR } MD5 (S + cn – 1)$$

2.2 Odgovor poslužitelja

Nakon što poslužitelj primi RADIUS upit *Access – Request*, vrši se provjera postoji li praktički tajni ključ za tog klijenta kojeg bi oni trebali međusobno dijeliti. Ukoliko se dogodi da ne postoji spomenuti ključ za tog klijenta, poslužitelj odbija zahtjev i šalje određenu poruku.
S druge strane, kod prihvaćanja tajnog ključa dolazi do drugačijeg procesa kriptiranja, kako bi se došlo do originalne korisničke lozinke.

Ukoliko se pojavi neispravnost lozinke tj. lozinka se ne preklapa s bazom podataka, klijent prima *Access – Reject* paket, kojim se odbija ikakav daljnji proces.
S druge strane, ako se lozinka preklapa s bazom podataka poslužitelja, klijent dobiva *Access-Accept* paket. Oba paketa sadrže identičnu vrijednost bajta identifikacije (ID), kao što sadrži i originalan *Access – Request* upit klijenta. *Response Authenticator* vrijednost atributa vraćenog paketa se dobije primjenom MD5 hash funkcije u kombinaciji sa vrijednosti polja *Response – Authenticator* originalnog upita klijenta.
Matematičko prikazivanje spomenutih atributa:

$$RA = MD5 (Code + ID + Length + RequestAuth + Attributes + S) \qquad (2)$$

Na slici u nastavku će se prikazati tijek razmjene RADIUS poruka.

Slika 3. Tijek razmjene RADIUS poruka[3]

2.3 Procesiranje odgovora poslužitelja

Kada klijent na svojoj strani primi odgovor od strane RADIUS poslužitelja, on će na temelju identifikacijskog bajta pokušati odrediti da li se zaista odgovor slaže s njegovim upitom.

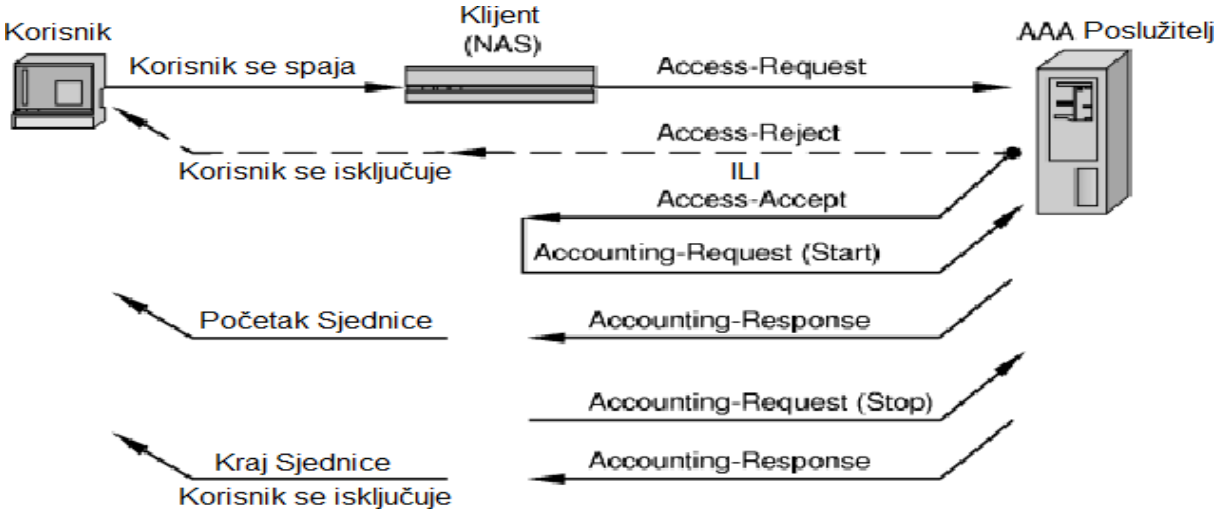
Klijent može identificirati ispravnost odgovora na način da usporedi vrijednosti ID polja poslanog (*Access – Accept)* i primljenog (*Access – Accept ili Access – Reject)* paketa. Ukoliko postoji mogućnost da se dvije spomenute tvrdnje ne podudaraju, klijent smatra odgovor ne regularnim i sjednica se automatski prekida. U sljedećem koraku se vrši provjera *Response Authenticator* polja primljenog paketa korištenjem identične matematičke operacije kao na strani poslužitelja, da bi se dobila potvrda da li zaista odgovor stiže od strane poslužitelja. Kao što je već spomenuto, ukoliko se rezultati ne podudaraju također se sjednica prekida.

- Autentikacija se smatra uspješnim ukoliko je klijentu vraćen *Access – Accept* RADIUS paket s valjanim sadržajem, korisničkim imenom i lozinkom.
- Autentikacija se smatra neregularnom ukoliko je klijentu vraćen *Access – Reject* RADIUS paket s valjanim sadržajem, korisničkim imenom i lozinkom te će se autentikacija smatrati neuspješnom.

2.4 Sažetak sjednice

Cijeli proces izmjene poruka između RADIUS klijenta i poslužitelja, zahtjevi koji se šalju, te zapravo cijela komunikacija prikazati će se u nekoliko koraka te slici u nastavku.

1. Na samom početku korisnik šalje svoje identifikacijske podatke RADIUS klijentu, koji bi mu trebao omogućiti pristup mreži.
2. Klijent obavlja proces autentikacije i autorizacije izmjenom poruka s RADIUS poslužiteljem
   a) Klijent šalje *Access – Request*
   b) U ovom slučaju poslužitelj uzvraća s *Access – Reject* porukom jer mu se odbacuje pristup na mreži, ali mu također u drugom slučaju može odgovorit s *Access – Accept* porukom.
3. Provodi se administracija korisnika (*accounting)*
   a) Prva poruka u nizu je *Accounting – Request (Start)*
   b) sjednica započinje na način da poslužitelj odgovara porukom *Accounting – Response*
   c) ukoliko je korisnik iz nekog razloga odlučio da prekine sjednicu, klijent šalje poruku *Accounting – Request (Stop)*
   d) sjednica se završava porukom *Accounting – Response* nakon čega se korisnik isključuje iz mreže.



Slika 4. Sjednica koja koristi RADIUS protokol[3]

4. PROBLEMI RADIUSA

RADIUS protokol zasigurno kao i svaki protokol u telekomunikacijskoj mreži, sadrži određene propuste, u ovom slučaju sigurnosne. Takvi propusti su posljedica u provođenju samog protokola ili neispravnog, odnosno nepotpunog provođenja programske podrške. U sljedećih nekoliko poglavlja prikazat će se i opisati neki od sigurnosnih propusta koji se pripisuju RADIUS protokolu.

4.1 Napad na tajni ključ *Response – Authenticator* polja

Ovakav tip napada na RADIUS protokol se zapravo odnosi na način generiranja vrijednosti *Respose – Authenticator* polja, kada se gledaju *Access – Accept* ili *Access – Reject* RADIUS paketi.

Pregledavanjem upravo spomenutih paketa i korištenjem algoritama za razbijanje, postoje mogućnosti za probijanje vrijednosti tajnog ključa.

U jednom od prethodnih poglavlja se spominje korištenje MD5 hash funkcije koje poslužitelj koristi za generiranje odgovora klijentu. Ukoliko se detaljnije promotre argumenti spomenute funkcije može se primijetiti jedina nepoznanica u tom izrazu, odnosno tajni ključ kojeg dijele klijent i poslužitelj.

Napadač pred sobom ima sljedeći problem :

$$RA = MD5 (Code + ID + Length + RequestAuth + Attributes + X) \quad (3)$$

X predstavlja tajni ključ koji se pokušava odgonetnuti.

S obzirom na poznate argumente napadač može izračunati slijedeći izraz:

$$RA = MD5 (Code + ID + Length + RequestAuth + Attributes) \quad (4)$$

Snažnim računalnim algoritmom, te metodom pokušaja i pogreške postoje velike šanse za otkrivanje tajnog ključa klijenta i poslužitelja.

4.2 Enkripcija *User – Password* atributa

Za enkripciju korisničke lozinke, odnosno *User – Password* atributa, koristi se algoritam koji spada u grupu *stream chipper* algoritama za enkripciju podataka. MD5 *hash* funkcija se u tom slučaju koristi kao generator pseudo slučajnih brojeva (PRNG).

Sigurnost ovakvog postupka zaštite korisničke lozinke ovisi o kvaliteti i snazi odabrane MD5 *hash* funkcije, odnosno odabiru tajnog ključa između klijenta i poslužitelja. Sigurnost postupka se podiže na višu razinu ovisno o kvaliteti odabira.

MD5 *hash* funkcija se u slučaju RADIUS protokola praktički smatra neprikladnim alatom. Razlog tomu je što MD5 *hash* funkcija nije predviđena da se koristi kao *stream chipper* grupa algoritama, već kao čisti alat za enkripciju podataka.

U sljedećim poglavljima će se moći primijetiti kako je neregularno korištenje MD5 *hash* funkcije zapravo jedan od bitnih razloga sigurnosnih propusta, koje neki neovlašteni korisnik može nelegalno iskoristiti za neautorizirani pristup povjerljivim korisničkim podacima.

4.3 Napad na tajni ključ pomoću *User – Password* atributa

Još jedan slučaj omogućavanja odgonetanja tajnog ključa između klijenta i poslužitelja je korištenje *stream chipper* algoritma za kriptiranje korisničke lozinke prilikom slanja upita poslužitelju.

Sam napad kreće na način da se osmišljava korisnička lozinka koja je samo poznata napadaču i traži se autentikacija kod RADIUS klijenta. RADIUS klijent će na temelju primljenog zahtjeva formirati *Access – Request* upit koji se dalje prosljeđuje poslužitelju da bi mu se provjerili korisnički podatci.

User – Password atribut se dobiva na način kako je opisano u poglavlju 2.2. Vrlo je važno napomenuti da je kao argument enkripcije korištena lozinka koja je poznata napadaču.

Analizom mrežnog prometa napadač može uhvatiti generirani RADIUS *Access – Request* upit, zatim primijeniti XOR na User – Password atribut i na taj način dobiti izlaznu vrijednost slijedeće matematičke operacije:

MD5 (Shared Secret + Request Authenticator) *(5)*

Budući da je vrijednost *Request – Authenticator* poznata, opet ostaje jedna nepoznanica, a to je upravo tajni ključ kojeg se pokušava odgonetnuti.

Kao što je već spomenuto u jednom od prethodnih poglavlja kod ovog slučaja je također, uz primjenu metode pokušaja i pogreške te snažnih računalnih algoritama, moguće doći do tajnog povjerljivog ključa klijenta.

4.4 Napad na korisničku lozinku pomoću *User – Password* atributa

Neprikladna upotreba *stream chipper* algoritma dovodi do još jednog sigurnosnog propusta za kriptiranje korisničke lozinke. Naime, neovlaštenom korisniku se omogućava uspješno nagađanje lozinke, a samim time i uspješna autentikacija kod poslužitelja. Bitan preduvjet je taj da poslužitelj ne posjeduje ograničenje za neuspjele pokušaje autentikacije. Prvi dio napada se odvija kao i što je opisano u prethodnom poglavlju. Napadač klijentu šalje zahtjev za autentikaciju s valjanim korisničkim imenom i nekom proizvoljno odabranom lozinkom koja je najvjerojatnije pogrešno. Nakon toga se dolazi do izlazne vrijednosti sljedeće matematičke operacije:

MD5 *(Shared secret + Request Authenticator)* *(6)*

Kada bi se ponovno vratili na izraz (1) može se vidjeti da napadač ima mogućnost generirati novi *Access – Request* paket s istim korisničkim imenom ,ali ovog puta s novo odabranom korisničkom lozinkom. Ako postoji mogućnost da poslužitelj nema već spomenuto ograničenje za slanje neuspjelih pokušaja, napadač slanjem velikog broja upita ima mogućnost za odgonetanje korisničke lozinke.

4.5 Napadi bazirani na *Response – Authenticator* atributu

Cjelokupna sigurnost RADIUS protokola se bazira na kvaliteti algoritma za generiranje *Request – Authenticator* atributa. Veoma je bitno da je spomenuti algoritam jedinstven i nepredvidljiv.

Specifikacija ovog protokola ne prikazuje dovoljno važnost postupka generiranja ovog atributa. Određeni broj implementacija koristi loše i površne mehanizme za generiranje slučajnih brojeva, koji se koriste u svrhu generiranja vrijednosti ovog atributa. Naime, poznata je činjenica da je za kvalitetu algoritama za kriptiranje bitan mehanizam za generiranje slučajnih brojeva (PRNG). Što su više zastupljena deterministička svojstva, algoritam je teže provaliti. Identična situacija je i s RADIUS protokolom. U sljedećim poglavljima će se opisati pasivni i aktivni napad korištenjem spomenutog atributa.

4.5.1 Pasivni napad pomoću *Request – Authenticator* atributa

Promatranjem prometa koji se događa na mreži, napadač s vremenom ima priliku kreirati RADIUS rječnik s *Request – Authenticator* atributima i određenim *User – Password* atributima. Ukoliko se radi o većoj količini mrežnog prometa, postoji mogućnost uklanjanja utjecaja tajnog ključa i samim tim dođe do nezaštićene korisničke lozinke. Prvi korak napada je primjena XOR logičkog operatora nad zaštićenim korisničkim lozinkama, a kao rezultat će se dobiti XOR kombinacija nezaštićenih lozinki. Ako se radi o lozinkama jednake duljine, ovakva vrsta napada neće biti uspješna. Vodeći se praksom, lako se može doći do zaključka da su korisničke lozinke uglavnom različitih duljina i svojstava, ovakva vrsta napada bi ipak u nekim slučajevima mogla dati uspješan rezultat. Situacija koja ide u prilog napadaču je lozinka kraća od 16 bajtova. Neovlašteni korisnik korištenjem različitih statističkih metoda, a i metoda ponavljanja pokušaja ima veliku mogućnost za otkrivanje korisničkih lozinki.

4.5.2 Aktivni napad pomoću *Request – Authenticator* atributa

U slučaju aktivnog napada neovlašteni korisnik šalje veliki broj RADIUS zahtjeva klijentu, sa svojim nasumce odabranim korisničkim lozinkama, što dovodi do toga da se aktivira *Access – Request* upit poslužitelju. Sljedeći korak je presretanje generiranih paketa prema poslužitelju, te upisivanje gore spomenutih atributa unutar tih paketa. U ovakvim paketima se također nalazi zaštićena lozinka poznata neovlaštenom korisniku, s obzirom da je on sam pokrenuo upit.

Neovlašteni korisnik dolazi do MD5 *(Shared secret + Request Authenticator)* vrijednosti generiranih *Access – Request* paketa primjenom XOR logičkog operatora. U ovom slučaju se opet može kreirati već spomenuti rječnik sa spomenutim atributom i njegovim pripadajućim vrijednostima.

Ukoliko se detektira regularni *Access – Request* upit s nekom od vrijednost atributa iz prethodne faze napada, opet postoji mogućnost za laganim odgonetanjem korisničke lozinke. Primjenom već spomenute XOR operacije između MD5 (*Shared secret + Request Authenticator)* vrijednosti koja prema rječniku odgovara *Request - Authenticator* atributu i zaštićenog *User – Password* polja detektiranog paketa, također se dolazi do nezaštićene korisničke lozinke.

4.6 Napomene vezane za tajni ključ

RADIUS protokol dozvoljava uporabu istog tajnog ključa za nekoliko korisnika RADIUS sustava. Naime, praksa pokazuje da je na taj način sigurnost upitna i ne preporučuje se za korištenje u nijednom slučaju.

Još jedan veliki problem je činjenica da se dozvoljava upotreba samo ASCII znakovnih nizova što napadaču uvelike olakšava uspješno obavljanje neregularnih radnji. Kao što je poznato brojka se s ukupnih 256 znakova smanjuje na samo 94, što predstavlja još jedan od većih sigurnosnih propusta.

Također, neke implementacije RADIUSA stavljaju ograničenja na tajni ključ tako što se smanjuje duljina na brojku od 16 znakova, a u nekim slučajevima čak i manje.

5. ALTERNATIVNI PROTOKOLI

RADIUS je sigurnošću jedan od najpopularnijih protokola, no međutim ne i jedini koji koristi „AAA“ princip. Kroz nekoliko sljedećih poglavlja će se ukratko opisati alternativni protokoli koji se koriste za sličnu ili istu namjenu.

5.1 TACACS

TACACS (*Tereminal Access Controler Access – Control System*) je autentikacijski protokol koji omogućava komunikaciju između pristupnog poslužitelja s udaljenim poslužiteljem u UNIX mreži. S obzirom da se radi o protokolu sličnom RADIUS – u, poslužitelj vrši autentikaciju kada korisnik zatraži pristup mreži.

Spomenuti protokol omogućava klijentu preuzimanje korisničkog imena i lozinke, a zatim i slanje upita TACACS poslužitelju pod nazivom TACACS *deamon* ili TACACSD. Radi se o poslužitelju koji se ponaša kao program koji se izvršava na domaćinu, s tim da domaćin odlučuje o odbijanju ili prihvaćanju zahtjeva te slanju odgovora. Algoritmi i podatci koji se koriste su pod kontrolom domaćina na kojem se izvršava sam TACACS.

5.2 TACACS +

RADIUS i TACACS + protokoli su u novijim mrežama istisnuli TACACS iz upotrebe. TACACS + je sasvim novi proizvod i zapravo nema dodirnih točaka s prethodnim verzijama. Ono što ga čini drugačijim od RADIUS protokola je što koristi TCP protokol (*Transmission Control Protocol)* dok RADIUS kao što je spomenuto u jednom od prethodnih poglavlja za transport koristi UDP protokol koji je manje pouzdan od TCP – a. Još jedna bitna razlika je odvajanje autorizacije i autentikacije.

Spomenuti protokol se može rastaviti na 3 segmenta gdje svaki obavlja jednu od funkcija „AAA“ modela. Također se mogu provesti na odvojenim poslužiteljima. Ciscovo poboljšanje TACACS protokola je ta da TACACS + vrši operaciju enkripcije cijelog tijela paketa koji omogućava sigurnu komunikaciju.

Kriterij	RADIUS	TACACS +
Transportni protokol	UDP (nepouzdani prijenos)	TCP (pouzdani prijenos)
Autentikacija i autorizacija	Povezani	Mogu se odvojiti čime se postiže veća fleksibilnost
Podrška drugih protokola	Samo IP	Podržava (IP, Apple, NetBIOS, X.25
Pristup naredbenom sučelju usmjeritelja	Ne podržava	Podržava 2 metode kontroliranja autorizacije naredbi usmjeritelja – po osobi i grupi
Enkripcija	Samo lozinke	Enkripcija cijelog paketa

Tablica 3 Usporedba RADIUS i TACACS + protokola [3]

5.3 Diameter protokol

Još od samih početaka RADIUS protokola, počele se rasprave o kreiranju bolje, poboljšane verzije. Velike su se rasprave vodile oko samog naziva novije verzije. Isprva se protokol trebao zvati RADIUS v2, ali ga IETF (*Internet Engineer Task Force*) nije dozvolio zbog ratifikacije RADIUS v1 verzije. Umjesto tih verzija, novi protokol dobiva naziv Diameter (jer je „dvostruko“ bolji od RADIUS – a).

Jedna od prednosti Diameter protokola je ta što pruža jaču kontrolu pristupa, koja je zapravo jedan veliki nedostatak RADIUS modela. Primjerice, RADIUS protokol, kao što je već prethodno spomenuto, koristi nepouzdani UDP mrežni protokol, dok Diameter s druge strane podržava TCP I STCP *(Stream Transmission Control Protocol*) protokole. Diamater protokol je time upotrebljiviji za razne aplikacije.

Karakteristike	RADIUS	Diameter
Transportni protokol	Nepouzdani (UDP)	Pouzdani (TCP ili STCP)
Transportna sigurnost	Neobavezni IPSec	Obvezni IPSec ili TLS (*Transport Layer Security)*
Konfiguracija klijenta	Statička konfiguracija	Statička konfiguracija i otkrivanje korisnika
Status poslužitelja	Poslužitelj ne objavljuje svoj status (radi ili ne radi)	Podržava poruke o stanju poslužitelja (*keepalive, running, going down)*
Potvrda o prijemu	Klijent ne zna da li je poslužitelj primio poruku ili je ona odbačena (zbog greške ili netočnih podataka)	Poslužitelj može slati poruke o greškama, autentikaciji i prekidu sjednice
Sigurnosni model	Podržava sigurnost „korak-po- korak“ (Hop – by – hop). Svakim skokom podaci se mijenjaju te im se ne može utvrditi podrijetlo	Podržava sigurnost s „s kraja na kraj“ i „ korak – po – korak“. Sigurnost „s kraja na kraj“ osigurava da se podaci ne mogu mijenjati bez upozorenja
Veličina atributa	Rezervirano je 8 bitova za kod atributa u zaglavlju	Rezervirana su 32 bita za kod atributa u zaglavlju
Podrška različitih nabavljača	Podržava specifične atribute	Podržava specifične atribute i poruke

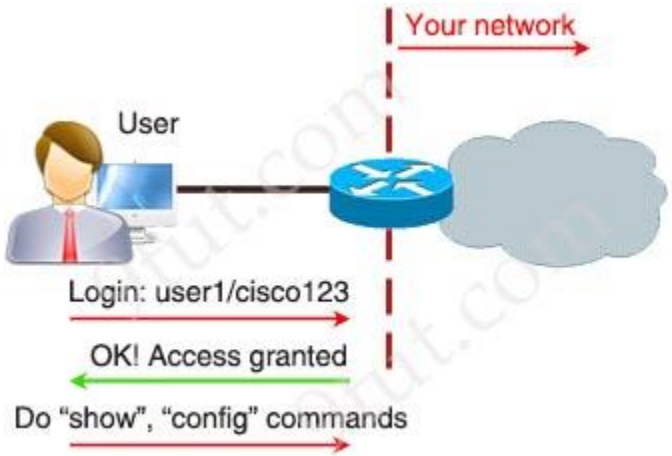
Tablica 4 Usporedba RADIUS i Diameter protokola [3]

6. „AAA“ KONFIGURACIJA NA MREŽNOJ OPREMI

U današnje vrijeme sigurnost je jako važna u svim kompanijama. Bez sigurnosnog rješenja implementiranog u mreži, neovlašteni korisnik se može jednostavno „uključiti i igrati“ na istoj. Korisnik jednostavno može uzeti valjanu IP adresu ili mu ona može biti dodijeljena automatski putem DHCP. To je pogodno, ali nije dobar način ako mreža sadrži osjetljive podatke. Još gore, taj korisnik može imati sva prava na tu mrežu te time činiti i neregularne radnje.

Kako kompanija raste, tako se u jednom trenutku pojavi i potreba za implementiranjem sigurnosnog sustava u mrežu. Postoji mnogo načina na koji se može osigurati mreža, ali AAA nudi potpuno rješenje. U sljedećih nekoliko primjera prikazati će se detaljnije karakteristike sigurnosnog sistema.

Prije detaljnije analize „AAA“ prikazat će se primjer korisnika koji se želi priključiti na mrežu.

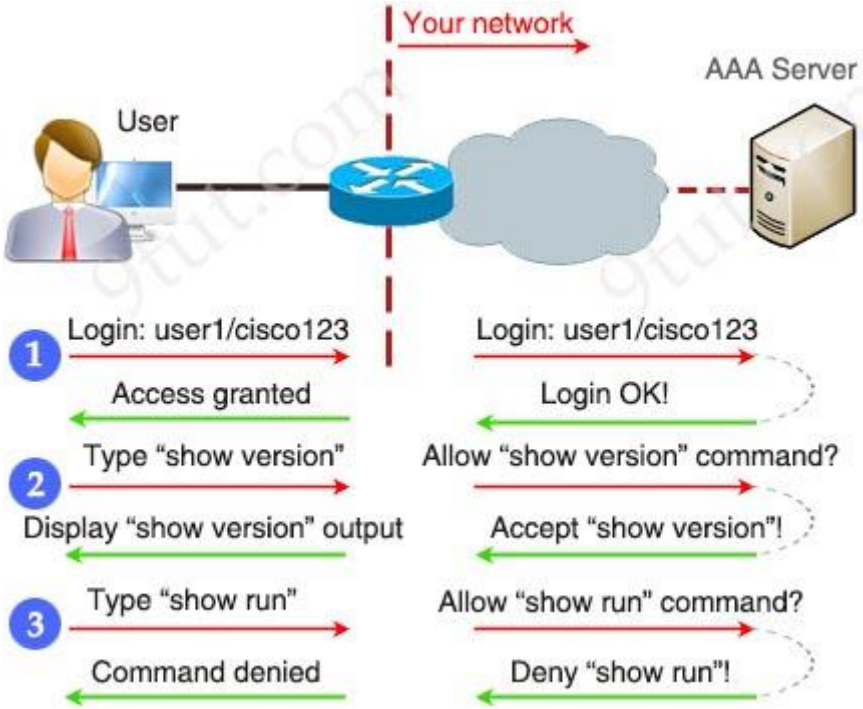


Slika 5. Zahtjev za prijavu na mrežu

Na slici 5. se prikazuje korištenje korisničkog imena i lozinke za pristup na mrežu. Iako ju je lako implementirati ova metoda ima jako puno nedostataka.

- Nesigurna metoda prijave
- Ne postoji nikakva odgovornost
- Svaki uređaj se mora ručno konfigurirati
- Loše podnosi napad
- Sprema na svaki uređaj korisničko ime i lozinku

Koristeći model „AAA“, spajanja korisnika na mrežu je prikazano na slici u nastavku.



Slika 6. „AAA“ model spajanja na mrežu

Svaka radnja korisnika mora biti predana na „AAA“ poslužitelj kako bi vidjelo da li mu je pristup dozvoljen ili odbijen. Ovaj proces ima mnoge prednosti i nedostatke

Prednosti:

- Sigurna prijava (AAA poslužitelj nije izložen korisnicima i samo je nekim protokolima dozvoljeno da budu poslani inicijalno)
- Lako upravljanje s jednog ili nekoliko centraliziranih poslužitelja
- Različiti sigurnosni uređaji se mogu postaviti ispred poslužitelja zbog zaštite
- Može prihvatiti ili odbiti različite naredbe
- Svaka naredba koju korisnik utipka može se zabilježiti za kasniju analizu

Nedostatak:

- Zahtjeva snažan poslužitelj (za upravljanje prometom i zahtjevima)

„AAA“ model kao što je već spomenuto predstavlja autentičnost, autorizaciju i administraciju.

- Autentikacija određuje tko si (obično putem korisničkog imena i lozinke)
- Autorizacija određuje koje su radnje dozvoljene, te kojim se izvorima smije pristupiti
- Administracija promatra što se i koliko dugo radi (naplata i revizija)

Primjer „AAA“ će se prikazati u primjeru ispod:

Autentikacija: „Ja sam normalan korisnik. Moje korisničko ime/lozinka su user_darko/završni rad123“.

Autorizacija: „user_Darko može pristupiti LearnCCNA poslužitelju putem HTTP I FTP“.

Administracija: „user_Darko koji je pristupio LearnCCNA poslužitelju 2 sata“. Ovaj korisnik koristi samo „show“ komande.

Koristeći „AAA“ model korisnik mora potvrditi autentičnost prije dobivanja IP adrese. U protivnom mora koristiti određene protokole za potvrdu autentičnosti.

Za potvrdu autentičnosti može se koristiti lokalna baza podataka, 802.1 x standard (koja se i razvila da bi se mogla osigurati autentičnost uređaja koji pokušavaju pristupiti switchportu/LAN-u ili putem dodijeljenih „AAA“ poslužitelja. RADIUS i TACACS + su dva najpoznatija klijent/poslužitelj „AAA“ protokoli za ovjeravanje autentičnosti između udaljenih poslužitelja i uređaja. U sljedećim poglavljima će se opisati način konfiguracije „AAA“.

6.1 Konfiguracija na Cisco 2811 usmjerivaču

U sljedećih nekoliko koraka će se opisati konfiguracija na Cisco 2811 usmjerivaču kako bi se osigurao telnet pristup. RADIUS poslužitelj je domaćin na uređaju Server – PT. Lozinka korisnika RADIUS – a mora biti konfigurirana na AAA *tab of the* Server – PT uređaja.

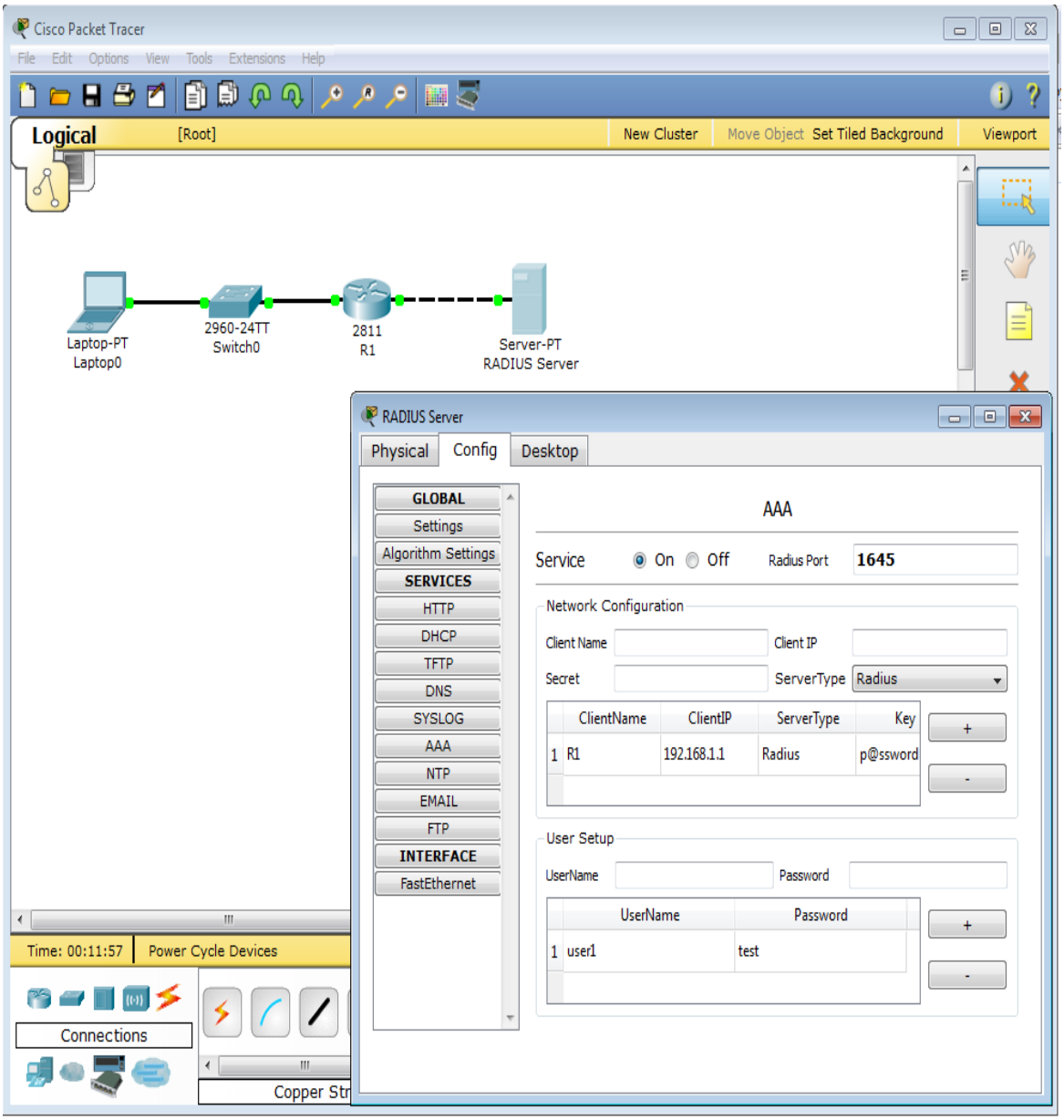
Usmjerivač R1:

- *FastEthernet 0/0 : 192.168.1.1 / 24*
- *FastEthernet 0/1 : 12.168.2.1 / 24*

RADIUS poslužitelj : *192.168.1.2 / 24*

Klijent (laptop) : *192.168.2.1 / 24*

Konfiguracija će biti prikazana na slici u nastavku.



Slika 7. Cisco konfiguracija

7.KONFIGURACIJA RADIUS HOTSPOT USLUGE NA MIKROTIK OPREMI

U ovom poglavlju će se prikazati način konfiguriranja RADIUS *Hotspot* usluge na MikroTik opremi. Prije samog prikaza konfiguriranja potrebno se istaknuti najbitnije činjenice vezane za RADIUS protokol. Sam protokol je danas često korišten protokol za autorizaciju, autentikaciju i administraciju korisnika. RADIUS protokol se zasniva na „klijent-poslužitelj“ modelu koji koristi UDP mrežni protokol. Kod klijentskog dijela koristi se *Network Access Server* (NAS) programski paket, koji prosljeđuje korisničke parametre RADIUS poslužitelju i obrađuje primljene odgovore. S druge strane RADIUS poslužitelji provjeravaju primljene korisničke parametre te vraćaju konfiguracijske parametre potrebne za kvalitetnu uslugu koja se pruža korisnicima. U nastavku će se opisati kreiranje jedne od usluga korištenjem RADIUS protokola te će se prikazati i detaljno analizirati promet koji se odvija prilikom zahtjeva za spajanje na mrežu.

7.1 Uvodna analiza

Kao što se navelo u prethodnim poglavljima, RADIUS je protokol koji koristi klijent-poslužitelj arhitekturu. Klijent je obično računalo, odnosno poslužitelj na računalu. U ovom slučaju u mreži postoji jedan poslužitelj koji svim „klijentima“ dozvoljava ili zabranjuje priključak na mrežu. Poslužitelj je kod ove mreže MikroTik usmjerivač na kojeg se prethodno instalira *SW „User manager*“ koji je zapravo MikroTik verzija RADIUS poslužitelja. Kod prijave na mrežu, korisnik šalje svoje podatke RADIUS klijentu (RADIUS klijent je „SW“ instaliran na samom korisničkom računalu) koji zatim izmjenjuje poruke određenog formata s RADIUS poslužiteljem, odnosno MikroTik usmjerivačem na kojem je instaliran *SW „User Manager.* Razlog izmjenjivanja poruka je ostvarivanje tri funkcije „AAA“ formata: autorizacije, autentikacije i administracije korisnika.

7.2 MikroTik usmjerivač RB2011UAS

U ovom poglavlju prikazat će se usmjerivač potreban za izradu RADIUS *Hotspot* usluge. MikroTik oprema je namijenjena različitim mrežnim inženjerima, tvrtkama koje pružaju IT usluge, telekom operaterima i sl. U nastavku će biti prikazan MikroTik usmjerivač RB2011UAS.

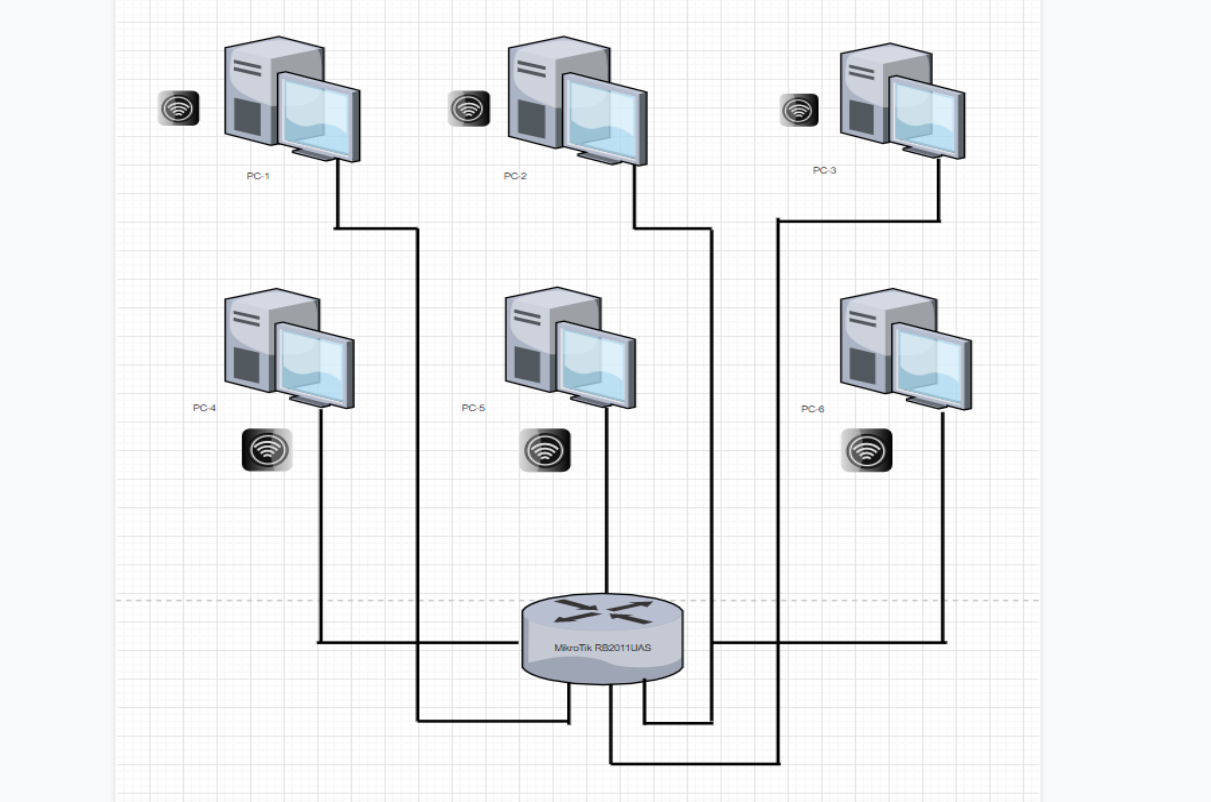
Slika 8. MikoTik RB2011UAS[1]

Na slici 8. prikazan je Mikrotik usmjerivač RB2011UAS. Radi se o usmjerivaču s 5 *Gigabit Ethernet* priključaka i 5 *Fast Ethernet* priključaka. Postoji više vrsta ovog modela, neki se razlikuju u cijeni, ali RB2011UAS prednjači zbog svojih vrhunskih karakteristika. Svi modeli imaju integriran *Atheros 600 Mhz 74 K MIPS* procesor.

7.3 RADIUS Hotspot

U poglavljima koji slijede prikazat će se nekoliko koraka konfiguracije same RADIUS Hotspot usluge. Također će se prikazati autentikacija korisnika koristeći se RADIUS poslužiteljem. Prije same konfiguracije potreban je i prikaz topologije mrežnih elemenata.

7.3.1 Topologija mreže

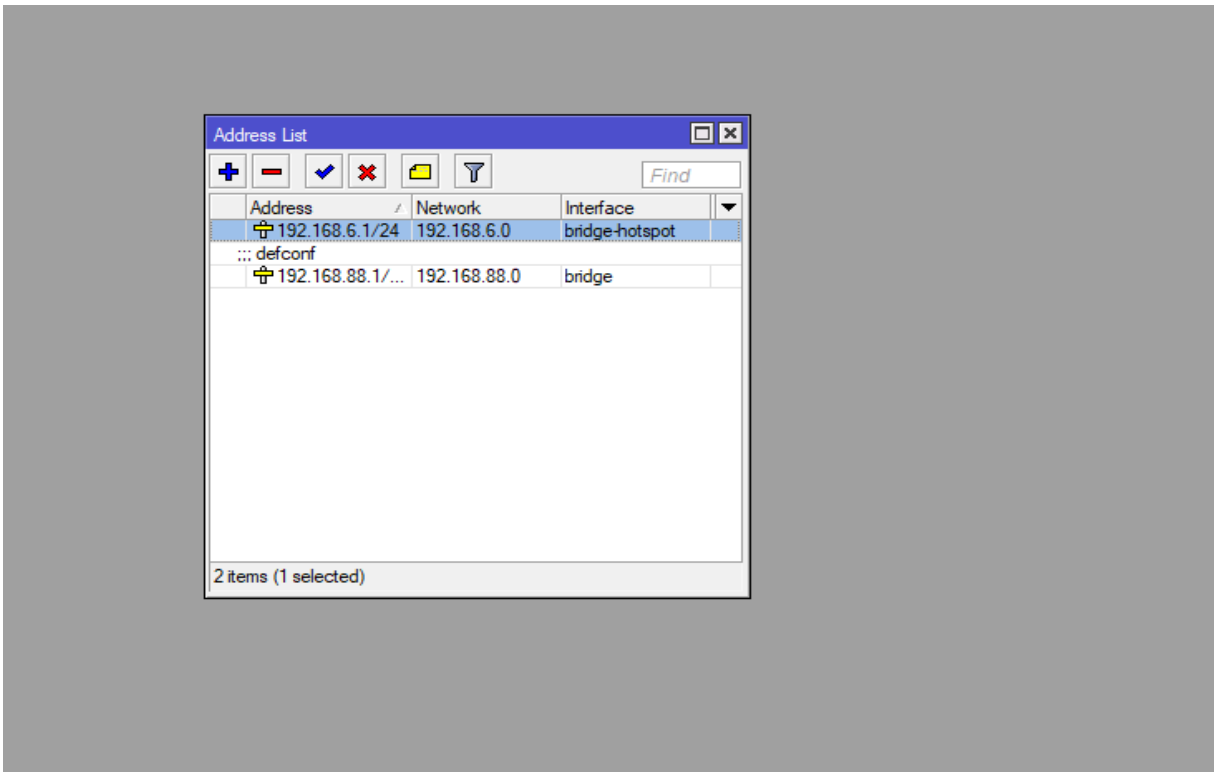


Slika 9. Topologija mreže

Na slici 9. prikazana je topologija mreže. Kao što se može primijetiti na slici svi PC-evi su spojeni na MikroTik usmjerivač bežično. Na PC-u nije potrebno dodjeljivanje statičkih IP adresa već se ostavljaju na automatski dodijeljenim IP adresama od strane DHCP usluge koja je također konfigurirana na Mikrotik usmjerivaču.

7.3.2 Postavljanje IP adresa

U ovom poglavlju će se prikazati dodjeljivanje IP adresa unutar programa *Winbox*. Prva IP adresa koja se dodaje je tzv. *bridge – hotspot*. U ovom slučaju je to 192.168.6.1 /24 , a njena mrežna adresa je 192.168.6.0. Prethodno spomenute adrese se mogu vidjeti iz sljedeće slike.

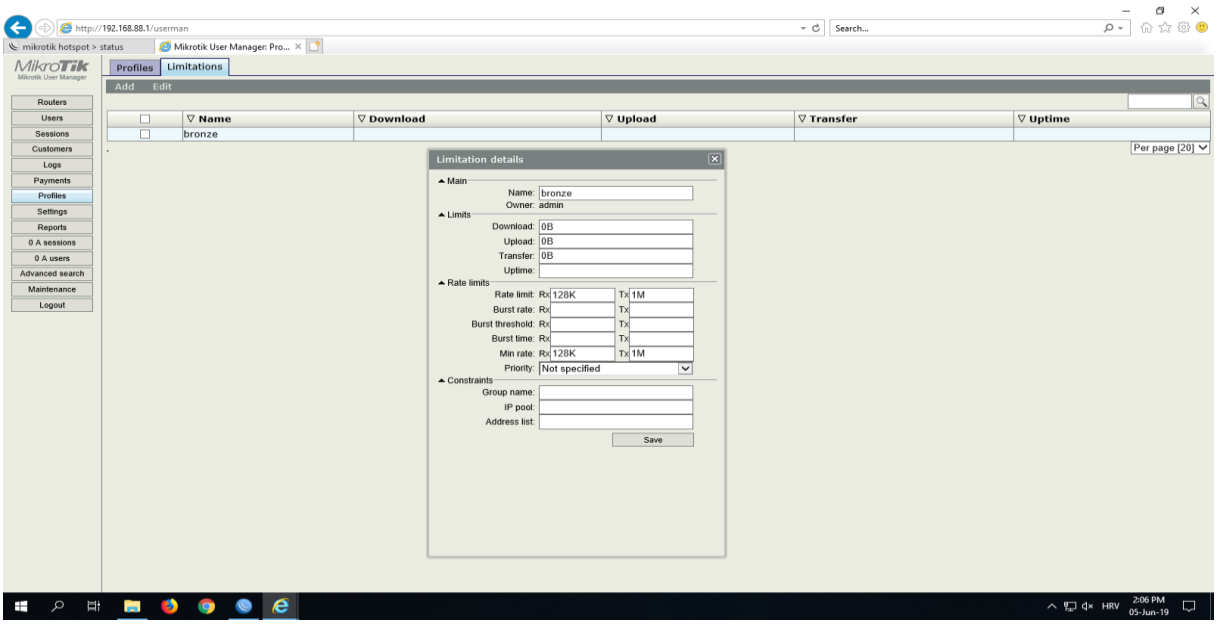


Slika 10. Postavljanje IP adresa

Na slici 10. može se primijetiti IP adresa koja predstavlja *bridge - hotspot*. Također se može iščitati još jedna adresa koja je zapravo zadana IP adresa samog MikroTik usmjerivača. U *Wireless* umrežavanju *bridge - hotspot* omogućuje dvije ili više bežičnih pristupnih točaka za komunikaciju i pridruživanje njihovim lokalnim mrežama.

7.3.3 Postavljanje limita profila korištenjem User managera

„*User manager*“ ili upravitelj postavkama se može koristiti u različitim primjenama. Neki od primjera korištenja User managera su Hotspot, DHCP, PPP itd. Upravitelj postavkama je RADIUS poslužiteljska aplikacija koja je podržana na svim *RouterOS* arhitekturama. Cilj završnog rada je nadzor pristupa velikog broja korisnika u mrežu. Kako bi se izbjeglo postavljanje pravila za svakog korisnika, odmah na početku se kreira nekoliko različitih „profila“ npr. gost, radnik, direktor itd. Na svakom od tih profila postavi se nekoliko različitih parametara kao što su maksimalna brzina pristupa, stranice kojima je dozvoljen pristup itd. U kasnijim fazama nakon kreiranja korisnika dodijelimo mu jedan od prethodnih profila i na taj način se olakšava posao mrežnom administratoru. Za ulazak u konfiguracijsko sučelje profila potrebno je upisati IP adresu koja je dodana u prethodnom poglavlju u Internet pretraživač. U nastavku će biti prikazana spomenuta IP adresa i prikaz sučelja profila.

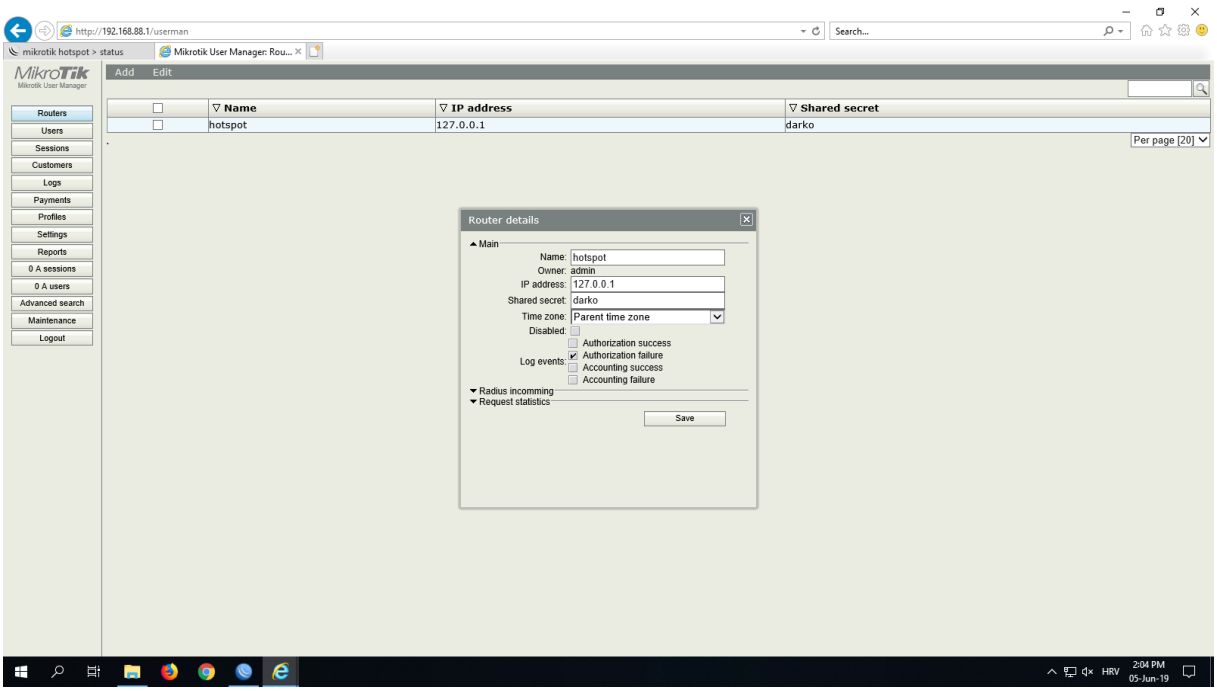


Slika 11. Postavljanje limita profila

Na slici 11. se mogu vidjeti neki od detalja u profilu. Naime, unutar profila se mogu postavljati različita spomenuta ograničenja. U ovom slučaju radi se o postavljanju limita za prijenos podataka od 1 megabajt i limit za primanje podataka od 128 kilobajta. Također se mogu postaviti i vremenska ograničenja prisutnosti na *Hotspot* usluzi te mnogi drugi spomenuti limiti.

7.3.4 Postavljanje profila usmjerivača

Nakon kreiranja profila unutar „*User manager*“ konfiguracijskog sučelja potrebno je dodati nekoliko parametara unutar profila samog usmjerivača. U jednom od prethodnih poglavlja je spomenuto kako MikroTik koristi „*User manager*“ verziju RADIUS poslužitelja. Unutar usmjerivačkog sučelja svakom korisniku pojedinačno se može dodjeljivati korisničko ime *i* lozinka, te mu pridružiti jedan od prethodno definiranih profila (gost, radnik ili direktor). U nastavku će biti prikazano sučelje profila usmjerivača te će se analizirati pojedini parametri.

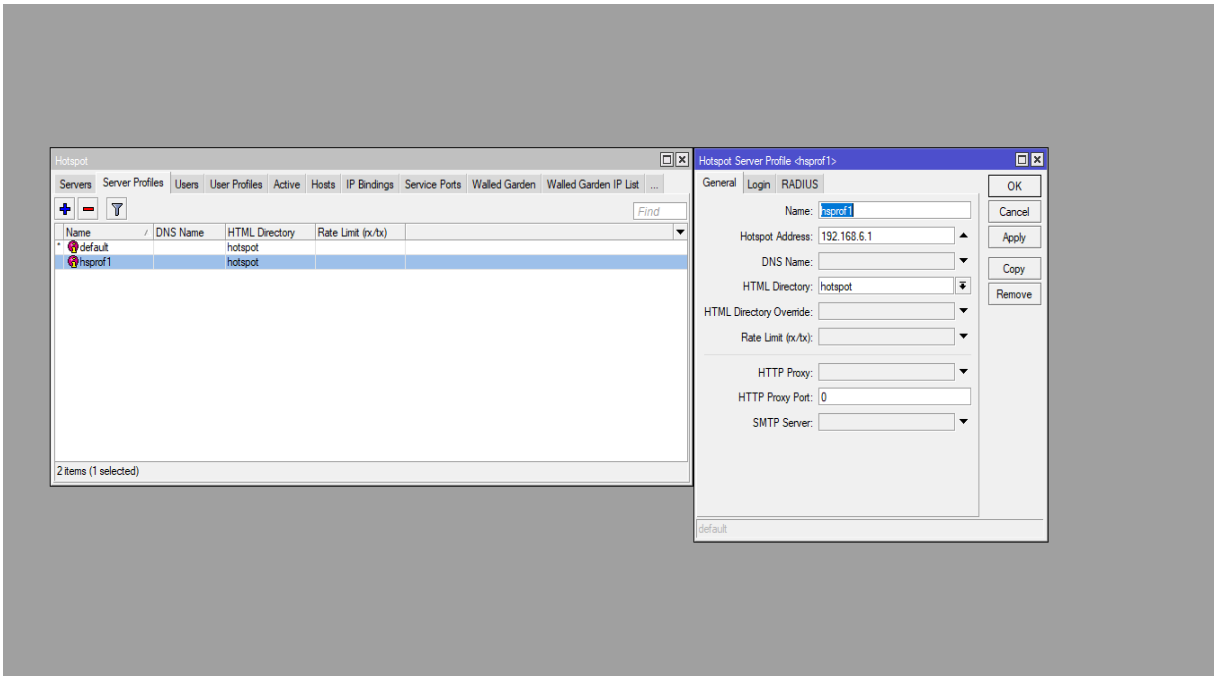


Slika 12. Profil usmjerivača

Na slici 12. vide se također različiti parametri unutar profila. Može se vidjeti *loopback* adresa 127.0.0.1. *Loopback* ili povratna adresa se također postavlja unutar jednog od sučelja u aplikaciji *Winbox*. Razlog postavljanja povratne adrese je taj što RADIUS poslužitelj kojim se autentificira *Hotspot* usluga je isti poslužitelj koji zapravo pokreće *Hotspot* uslugu. *Unutar Log events* opcije mogu se vidjeti funkcije RADIUS „AAA“ formata. U ovom slučaju označena je opcija *Authorization failure*. Ona predstavlja pogrešku koja se događa kada usluga ne dozvoljava povezivanje jer ne prepoznaje korisničko ime ili zaporku koju je sam administrator postavio unutar konfiguracijskog sučelja.

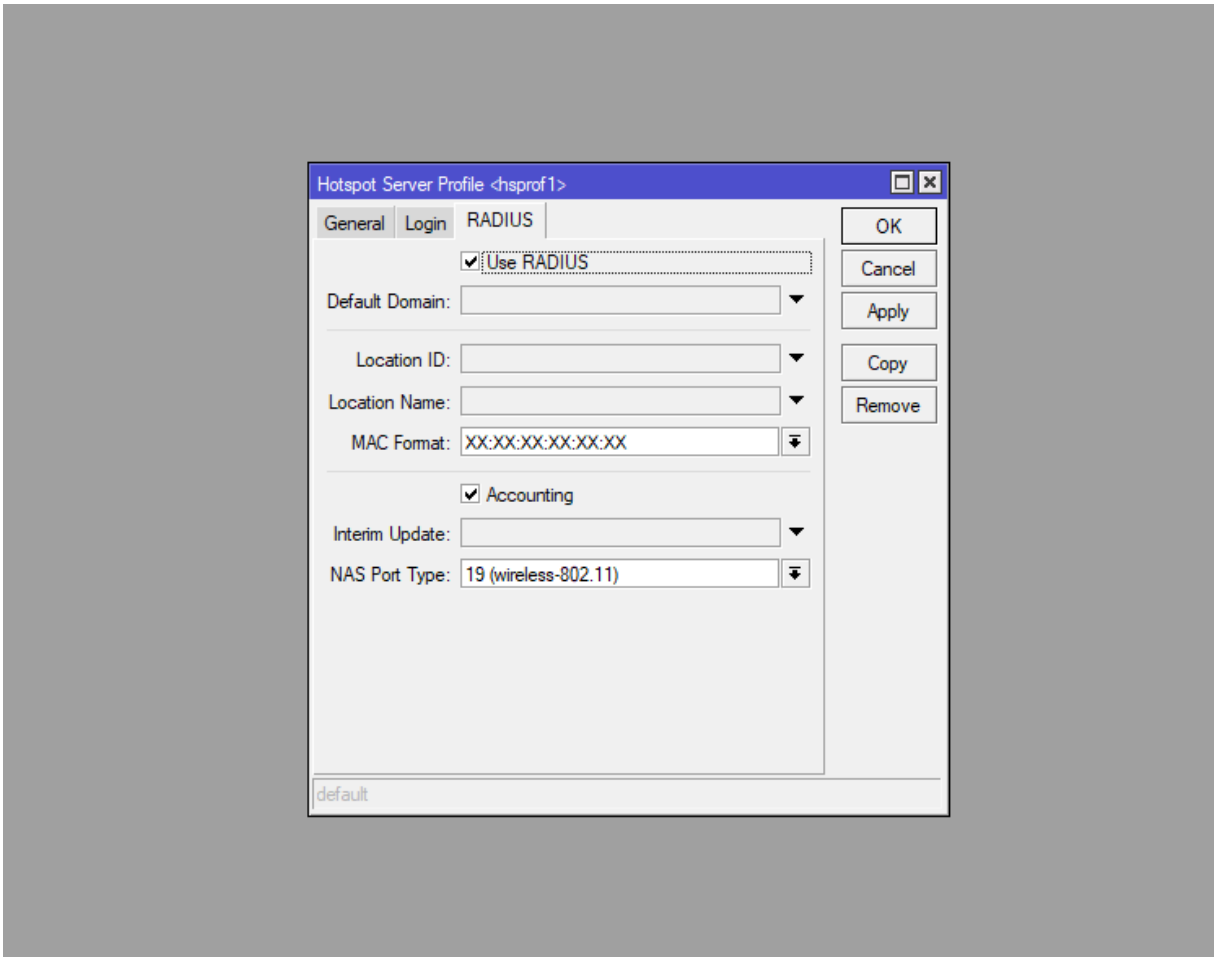
7.3.5 Hotspot profil i postavljanje RADIUSA

Jedan od sljedećih koraka je i samo postavljanje Hotspot usluge i zaštita iste RADIUS opcijom koji će biti prikazani na slikama u nastavku.



Slika 13. Hotspot sučelje profila

Na slici 13. može se vidjeti sučelje *Hotspot* profila. Kao i u ostalim profilima koji se vide u prethodnim poglavljima *Hotspot* profil sadrži mnoštvo opcija. Prvenstveno, takav profil služi za postavljanje same IP adrese koja je u ovom slučaju 192.168.6.1. Također se može vidjeti ime HTML direktorija koje je postavljeno kao *Hotspot.* Direktorij je definiran kao organizacijska jedinica ili kontejner koji se koristi za organiziranje mapa ili datoteka u hijerarhijsku strukturu. U nastavku će biti prikazano sučelje u kojem aktiviramo opciju RADIUSA.



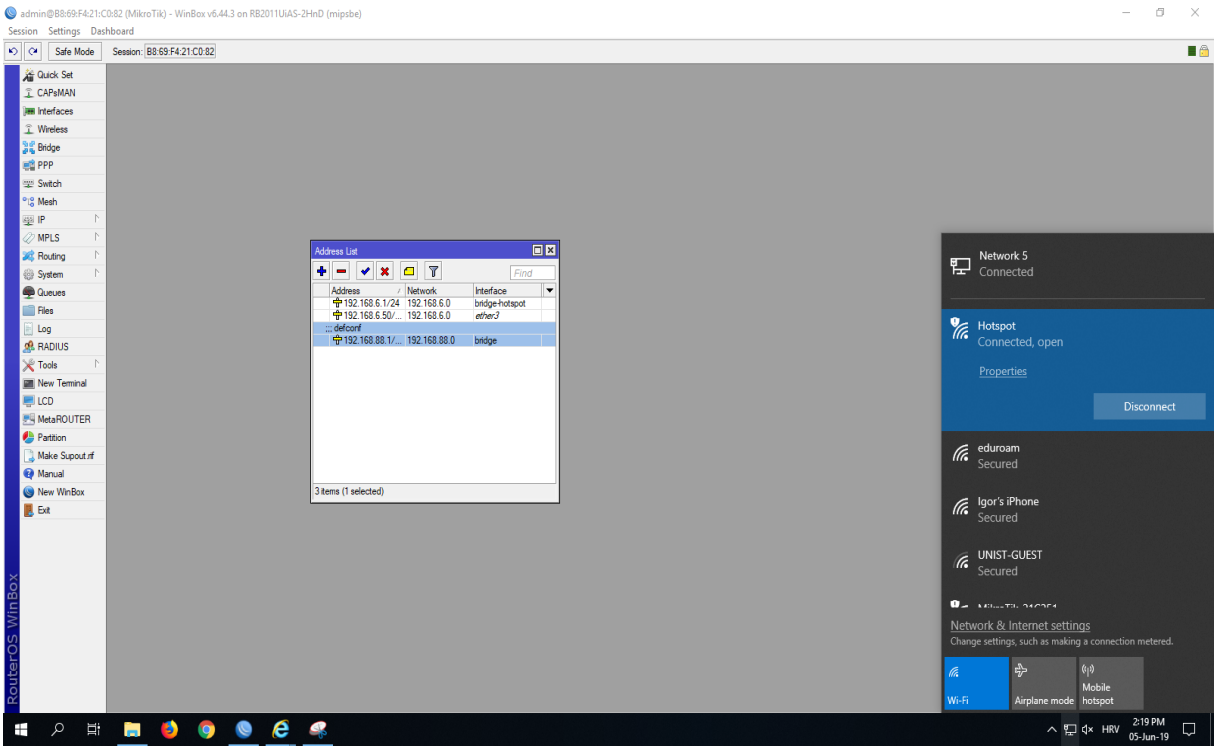
Slika 14. Zaštita Hotspot profila

Na slici 14. može se vidjeti sučelje u kojem se nalazi opcije korištenja RADIUSA. Također se može vidjeti kako je označena i opcija *Accounting* ili računovodstvo. Kada se koristi RADIUS *Accounting* opcija klijent i poslužitelj mogu izmjenjivati sljedeće dvije vrste poruka:

- Računovodstveni zahtjev – šalje ga klijent (NAS) koji traži računovodstvo
- Računovodstveni odgovor – šalje ga RADIUS poslužitelj koji potvrđuje računovodstvo

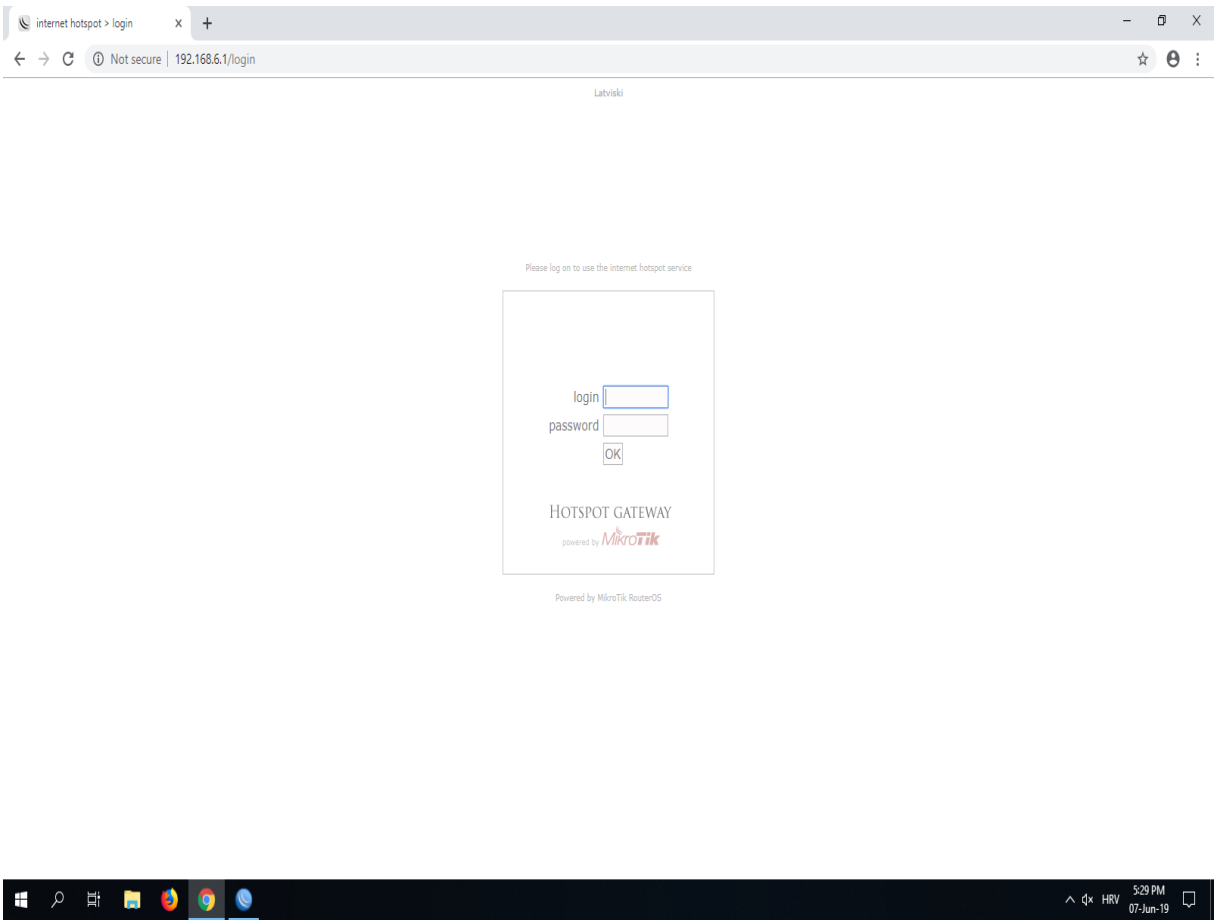
7.3.6 Konačni rezultat konfiguracije

U ovom poglavlju će se pokazati kako izgleda *Hotspot* usluga autentificirana RADIUS poslužiteljem. Naime cilj postavljanja samog RADIUS-a na Hotspot uslugu je takav da joj se može pristupiti samo uz korisničko ime i lozinku postavljenu od strane mrežnog administratora. Na sljedećim slikama će biti prikazana sama opcija *Hotspot* i što se događa u slučaju spajanja na istu.



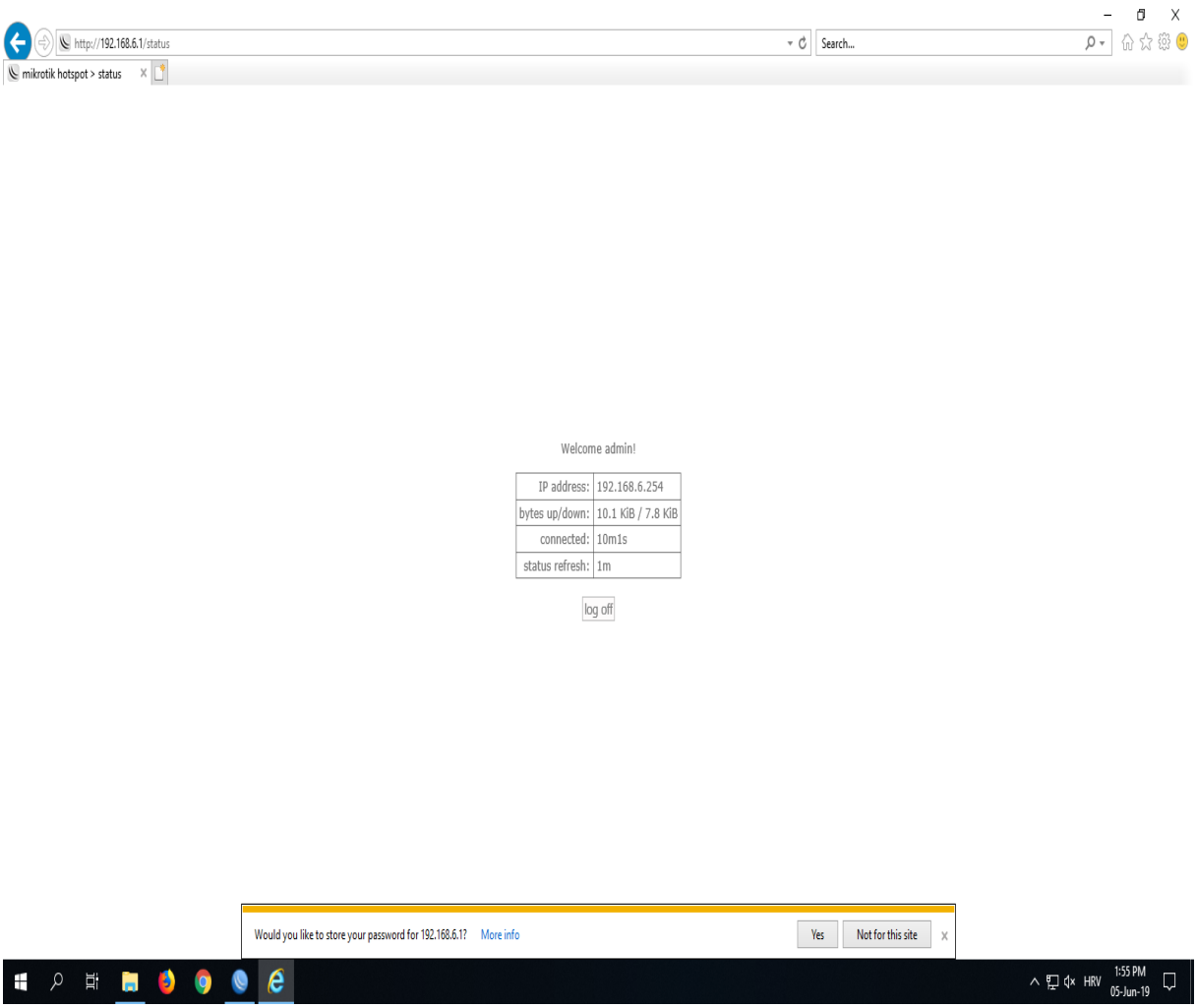
Slika 15. Hotspot

Na slici 15. se može vidjeti kreirani *Hotspot*. Danas je ta usluga većinom besplatna, ali ponekad je potrebna registracija ili pregledavanje različitih reklama prije odobravanja pristupa Internetu. Postavlja ga se na različitim lokacijama od hotela, aerodroma, zračnih luka itd. U ovom slučaju nakon što se pritisne opcija za spajanje događa se preusmjeravanje na IP adresu samog *Hotspot-a* (192.168.6.1) što će biti prikazano na sljedećoj slici.



Slika 16. Prozor s korisničkim imenom i lozinkom

Na slici 16. vidi se rezultat preusmjeravanja na spomenutu IP adresu (192.168.6.1). Naime, pojavljuje se prozor koji zahtjeva upisivanje korisničkog imena i lozinke prije same konekcije na uslugu. Nakon upisivanja korisničkog imena i lozinke otvara se prozor koji će biti prikazan na sljedećoj slici.



Slika 17. Prijava na uslugu

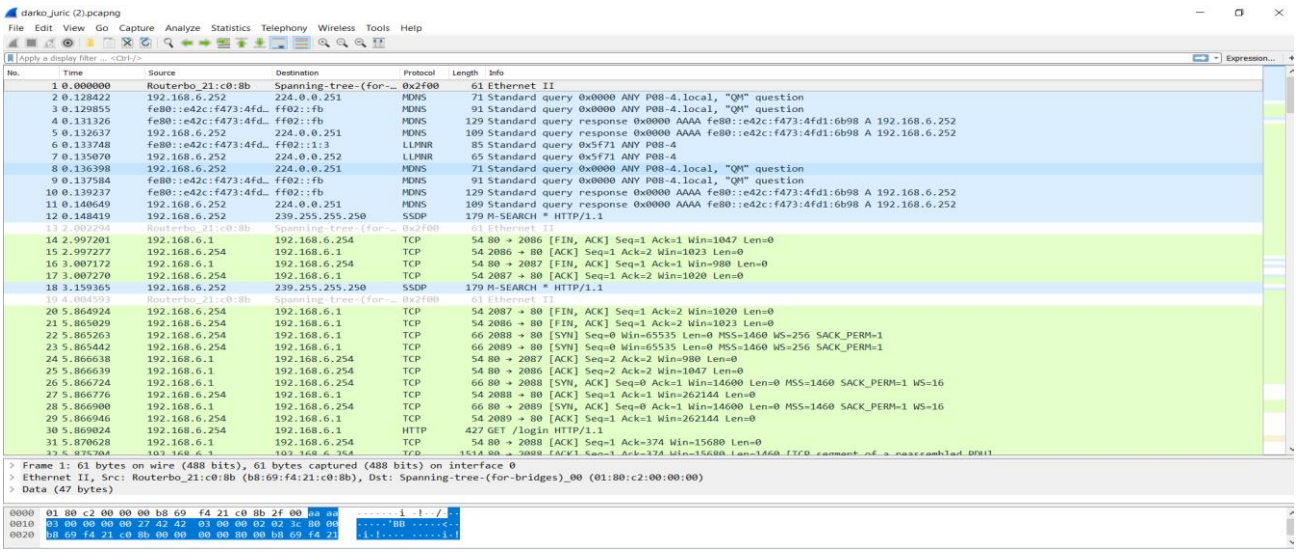
Na slici 17. se konačno može vidjeti i aktivacija *Hotspot* usluge. Nakon što se upiše ispravno korisničko ime i lozinka otvara se prozor s IP adresom računala s kojeg se prijavljuje, prenošenje i primanje podataka, koliko dugo traje konekcija na mrežu itd.

8.SNIMANJE PODATKOVNOG PROMETA WIRESHARKOM

U ovom poglavlju će se prikazati što se događa prilikom određenih aktivnosti na Internet pretraživaču. Snimanje prometa vršit će se alatom *Wireshark*. Tim alatom se vrše različite analize, razvoj komunikacijskih protokola, razvoj *software-a* i sl. *Wireshark* dozvoljava korisniku postavljanje različitih kontrolora mrežnog sučelja, tako da se nakon toga može vidjeti sav promet na tom sučelju, uključujući i *unicast* promet koji se ne nalazi na *MAC* adresi kontrolera mrežnog sučelja. U sljedećem poglavlju će biti prikazano koliko se paketa šalje nakon zahtjeva za prijavu na *Hotspot* uslugu unutar određenog vremenskog intervala.

8.2 Wireshark prikaz prometa

U ovom poglavlju prikazat će se dio podatkovnog prometa. Nakon upisivanja ispravnog korisničkog imena, lozinke i slanja zahtjeva za prijavu na uslugu šalje se mnoštvo paketa. Dio tih paketa će se moći vidjeti na slici u nastavku.

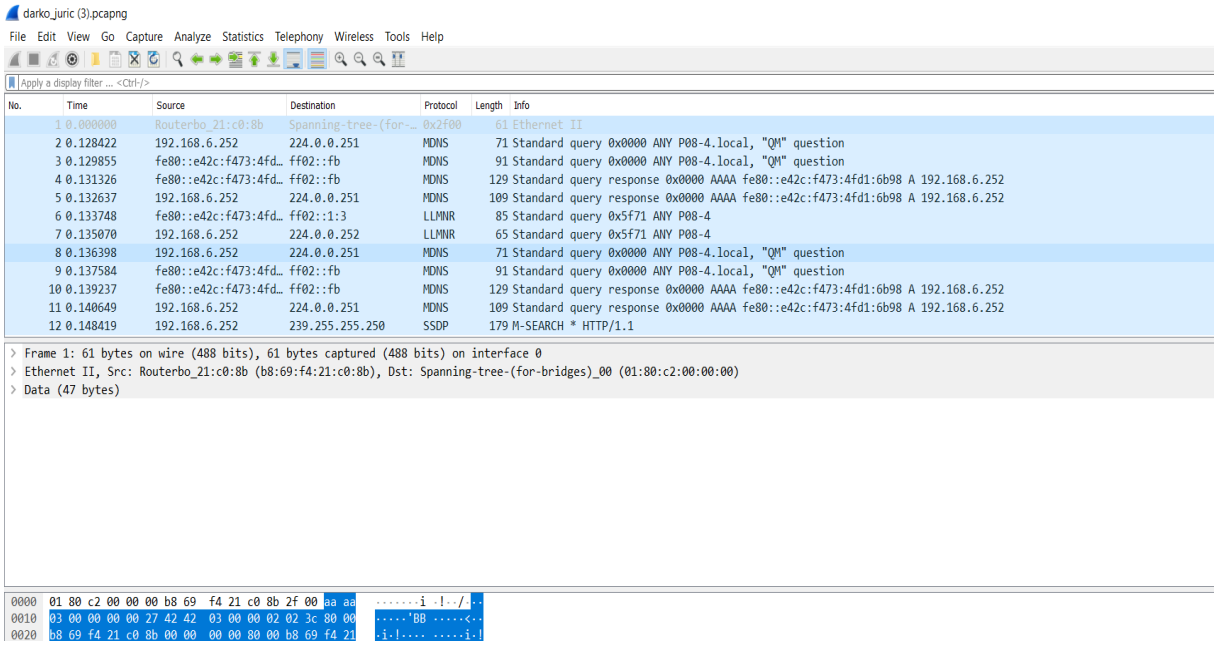


Slika 18. Prikaz podatkovnog prometa

Na slici 18. mogu se vidjeti različite paketi unutar alata *Wireshark.* Postoji mnoštvo stavki koje se mogu primijetiti bez da se otvara paket. Sa slike se mogu uočiti izvorišna i odredišna adresa, zatim koji se protokol koristi na kojem paketu, traka za filtriranje protokola te informacijski dio svakog paketa. U sljedećem poglavlju će se prikazati i samo otvaranje nekoliko paketa i što se nalazi unutar istih.

8.2 Analiza paketa

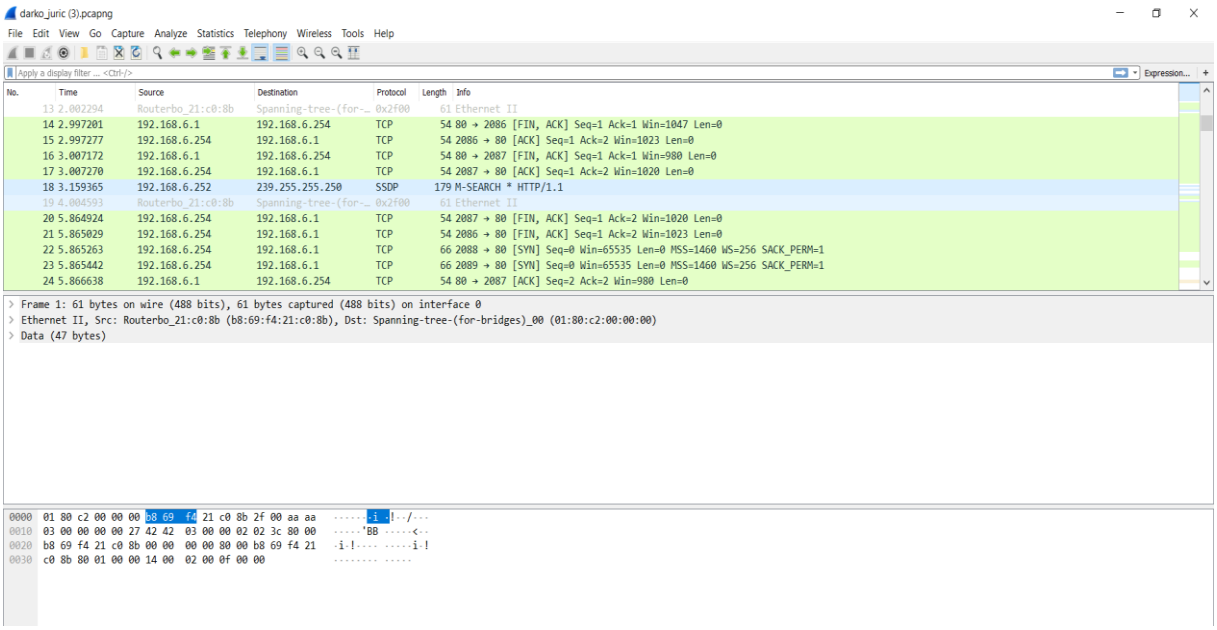
U nastavku ovog poglavlja prikazat će se prikaz prvih nekoliko paketa od samog zahtjeva i uspostave na uslugu, zatim početak konekcije te paket koji prikazuje specifikacije RADIUS protokola. Svaki paket se sastoji od svog podatkovnog, mrežnog, transportnog i korisnog dijela. Na slici u nastavku će se prikazati početak podatkovnog prometa prije dozvole za konekciju na samu uslugu te će se objasniti neki od protokola koje paketi koriste.



Slika 19. Početak slanja paketa

Na slici 19. se prikazuje početak slanja paketa na mreži. U prvim paketima se koristi MDNS protokol. To je protokol koji rješava imena *hostova* na IP adrese u malim lokalnim mrežama na način da šalje IP poruku višestrukog odašiljanja s ciljem identifikacije *hosta*. Nadalje, SSDP protokol se temelji na paketu Internet protokola i služi za otkrivanje mrežnih usluga i informacija o prisutnosti.

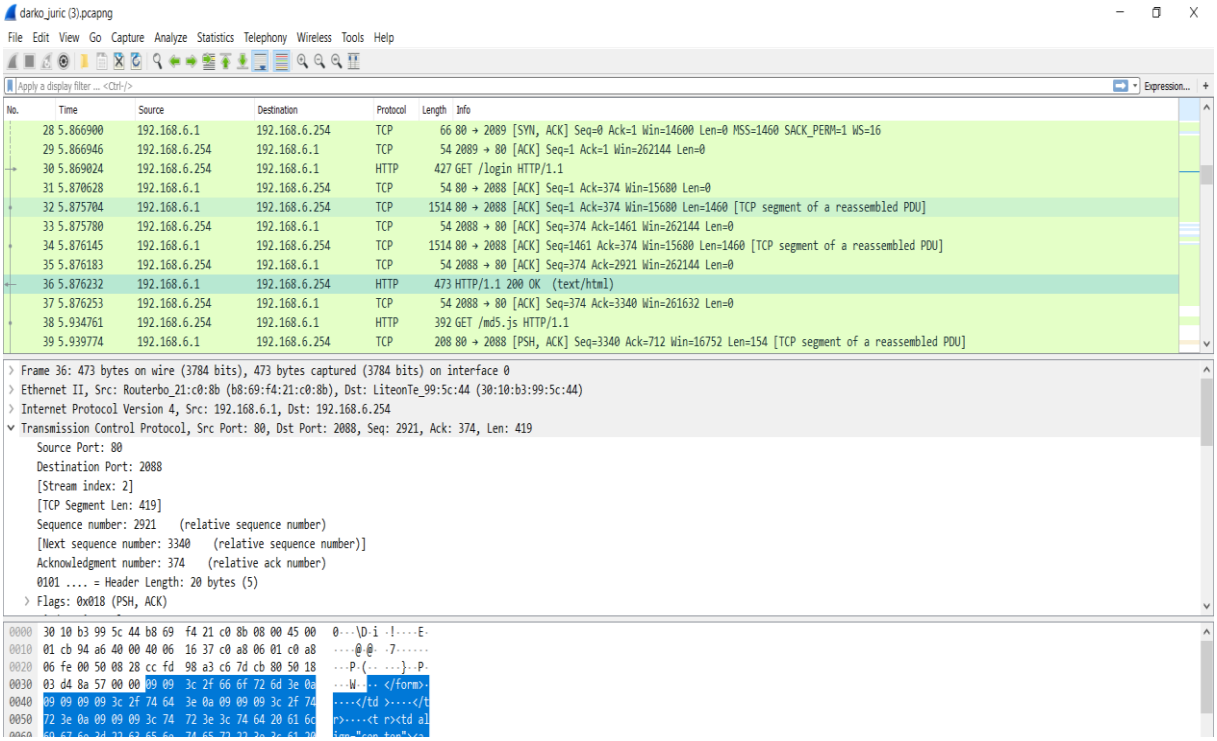
Nakon slanja početnih paketa, uspješnog otkrivanja mrežnih usluga i identificiranja *hosta,* nastavlja se sa daljnjim slanjem paketa. U nastavku će se prikazati paketi koji se izmjenjuju kad se procesuiraju početni paketi. Od posebne je važnosti 14. paket koji označava sam početak uspješne konekcije. U informacijskoj traci spomenutog paketa se može vidjeti ta prva ACK ili *acknowledge* poruka što znači potvrditi. Prikaz nastavka izmjene paketa će biti prikazan na sljedećoj slici.



Slika 20. Nastavak izmjene paketa

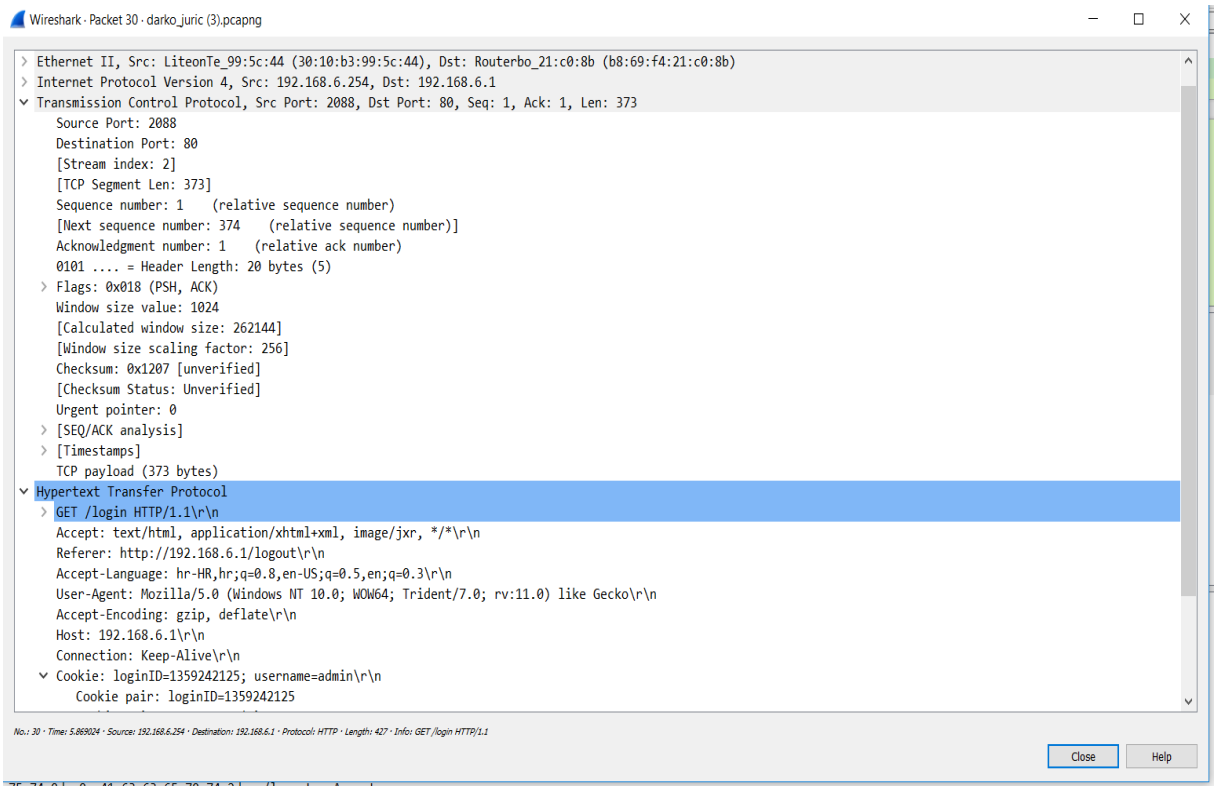
Na slici 20. se može vidjeti nastavak izmjene paketa. Može se primijetiti 14. paket koji je prvi u redoslijedu nakon izmjene paketa sa MDNS I SSDP protokolima. Također, vidi se da svi paketi u glavnini koriste TCP protokol. Taj protokol se koristi za kreiranje virtualne veze prema poslužitelju i tom vezom prenosi podatke. Stoga ovaj protokol spada u grupu tzv. spojnih protokola, za razliku od bez spojnih protokola kakav je primjerice UDP. Nadalje, TCP garantira pouzdanu isporuku podataka u kontroliranom redoslijedu od pošiljatelja prema primatelju.

U nastavku će biti prikazan možda i najbitniji paketi kroz snimak podatkovnog prometa. Spomenuti paketi su jako bitni zbog toga što približavaju zapravo samu važnost RADIUS-a. Na slici u nastavku će se prikazati još nekoliko paketa uz 30. i 36. paketi na koje posebno treba obratiti pozornost.



Slika 21. Prikaz paketa u Wiresharku

Na slici 21. kao što je već spomenuto treba posebno obratiti pozornost na 30. i 36. paket. Oba paketa sadrže HTTP protokole, no ono što je najbitnije je sadržaj njihove informacijske trake. Kod 30-og paketa potrebno je primijetiti izvorišnu IP adresu (192.168.6.254) u ovom slučaju PC-a, koja šalje odredišnoj adresi (192.168.6.1), odnosno adresi *Hotspota-a*, poruku *get/login.* U 36-om paketu su odredišna i izvorišna adresa zamijenila svoja mjesta. Naime, sada IP adresa šalje natrag IP adresi PC-a poruku OK i na taj način se daje do znanja kako su korisničko ime i lozinka ispravni, te je moguća konekcija na *Hotspot* uslugu. Otvaranje i detaljniji prikaz sadržaja 30-og paketa će biti prikazan na slici u nastavku.



Slika 22. Sadržaj 30 – og paketa

Na slici 22. je prikazan sadržaj 30-og paketa koji koristi HTTP protokol. HTTP je *request/response* protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent kao što je Web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu sa poslužiteljem. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom portu, čekajući da klijent pošalje niz znakova kao što je „*GET/HTTP/1.1*“- kojim se zahtjeva uspostava komunikacije. Nakon GET poruke klijent mora poslati niz određenih znakova [4]. Kao što je prethodno spomenuto 30-i paket sadrži poruku *get/login.* Na slici 21. se mogao primijetiti upravo takav redoslijed paketa.

9. ZAKLJUČAK

RADIUS protokol dokazano povećava kontrolu i sigurnost mreže. Pored toga što traži utvrđivanje vjerodostojnosti i autorizacije, primjena RADIUS protokola također podrazumijeva prijenos informacija o tarifiranju između NAS i tarifnog poslužitelja. Također, postoji i nekoliko prijedloga za poboljšanje samog protokola. Jedno od rješenja je korištenje simetričnog *block chipper* algoritma za enkripciju korisničke lozinke. Potrebno je istaknuti da je jako malo toga napravljeno u smjeru poboljšavanja sigurnosti same komunikacije između klijenta i poslužitelja. Sigurno je da i bez značajnijeg modificiranja protokola, uvijek postoji mogućnost za uvođenje manjih preinaka koji bi zasigurno unaprijedili RADIUS protokol, te ga učinili sigurnijim, a samim tim bi se zadržala kompatibilnost s prethodnim verzijama.

Trenutno je situacija u telekomunikacijskom svijetu takva, da još uvijek ne postoji potreba za polagano izbacivanje RADIUS protokola iz upotrebe. Ne iznenađuje ni činjenica da korisnici još uvijek ne osjećaju potrebu za prelazak na „dvostruko“ jači Diameter protokol. No, kako vrijeme ide prema naprijed tako se Internet, a i tehnologija razvijaju velikom brzinom. Zaključno, sigurno je da će se u dogledno vrijeme uporaba Diameter protokol ipak više prepoznati, a nakon toga se očekuje njegova brza ekspanzija i dugo očekivano preuzimanje RADIUS –ovog mjesta.

POPIS LITERATURE

[1]https://www.spectrumvoipstore.com/Mikrotik_Router_RB2011UAS/p2278465_12376008.aspx

[2]https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2001-07-05.pdf

[3]https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-07-306.pdf

[4]https://hr.wikipedia.org/wiki/HTTP

POPIS SLIKA I TABLICA

Popis slika

Popis tablica