LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

”SOHO” TĪKLA APARATŪRAS IZMANTOŠANA: PROBLĒMAS UN DROŠĪBAS ASPEKTI

MAĢISTRA DARBS

Autors: **Artjoms Inkins**
Studenta apliecības Nr. ai09003
Vadītājs: Dr. Sc.Comp. Leo Trukšāns

RĪGA 2015

ANOTĀCIJA

Maģistra darbs vērsts uz padziļinātu tēmas „"SOHO" maršrutētāju pielietojums lokālajos tīklos un ar to saistītas problēmas” izpēti, kas iepriekš daļēji tikusi pētīta bakalaura darba ietvaros.

Darba mērķis ir SOHO aparatūras problēmu un īpatnību izpēte, gan no programmatūras darbības, gan no to konfigurācijas skatupunktiem, kas pārsvarā ir saistīta ar drošības jautājumiem. Viens no galvenajiem uzdevumiem ir apkopot rekomendācijas izstrādātājiem, balstoties uz veiktajiem pētījumiem. Vēl viens uzdevums ir parādīt lasītājam, pat ja tas nav saistīts ar IT nozari, ka nepareizi nokonfigurēts maršrutētājs var apdraudēt lietotāju drošību, atsaucoties uz publiskā pētījumu datiem, kuru ir veicis pats autors.

Atslēgvārdi

Bezvadu maršrutētāji

Drošība

Datortīkli

SOHO

ABSTRACT

The master's thesis aims to deeper analyze and research the topic “Usage of SOHO Routers in local networks and problems with them”, which has previously been partly studied in the Bachelor's thesis.

The objective is the research of SOHO hardware problems and features from the points of view of software activity and their configuration, which is mainly focused on safety questions. One of the main tasks is to summarize recommendations to hardware developers, based on the executed research. One task is to show the reader, even if they are not familiar with the IT industry, that incorrect SOHO hardware configuration can imperil the safety of users, based of public research data, which the author has done by himself.

Keywords

Wireless routers

Security

Networks

SOHO

AUTOREFERĀTS

Maģistra darbā tika veikti sekojoši pētījumi un darbi:

- Tika atrasta iespējamā ievainojamība, kurai ir vajadzīga tālāka izpēte: veicot ARP pieprasījumu uz lokālo IP adresi, publiskā pieslēguma portā, maršrutētājs atbildēja ar publiskā interfeisa MAC adresi, bet ar lokālo IP adresi.
- Izpētīts Rīgas iedzīvotāju bezvadu maršrutētāju bezvadu tīklu drošības īpatnības, kopēji ievācot datus par vairāk nekā 22 tūkstošiem bezvadu piekļuves punktiem.
- Veiktas maršrutētāju grafisko interfeisu analīzes.
- Tika piedāvāti ieteikumi, kas ir balstīti gan uz veiktajiem pētījumiem, gan uz autora pieredzi, darbā ar bezvadu maršrutētājiem.

Pētījums ar ARP pakešu atbildēm darbā ir svarīgākais, jo šāda veida parādība, pēc autora domām, iepriekš netika pētīta. Autora meklējumi sakarā ar šo pētījumu nedeva nekādus rezultātus, nekāds līdzīgs pētījums netika atrasts.

Pētījums par Rīgas iedzīvotāju bezvadu piekļuves punktu drošību apkopoja datus, un secinājums ir viens – ne visi cilvēki rūpējas par savu bezvadu maršrutētāju pareizu konfigurēšanu un aizsardzības līmeni. Tas noved pie tā, ka to dati var būt pārķerti ar ļaundariem un izmantoti saviem mērķiem.

Tīkla pakešu pārķeršana neaizsargātā bezvadu tīkla tika pierādīta kā elementāra darbība. Tas tika izdarīts atsevišķā pētījumā.

Par katru no veiktajiem pētījumiem autors veic secinājumus un problēmu analīzi.

Darba noformējums atbilst visām prasībām, gramatikas kļūdas tika pārbaudītas, izmantojot tehniskos risinājumus.

SATURS

APZĪMĒJUMI

Apzīmējums	Nozīme
SOHO	Small office, Home office, tirgus segmenta nosaukums, kurš nosaka, ka ofisa darbinieku skaits ir mazāks par desmit cilvēkiem.
ARP	Address Resolution Protocol, tīkla līmeņa protokols, ar kura palīdzību tiek uzzināta iekārtas MAC adrese, zinot tās IP adresi tīklā.
WEP	Wired Equivalent Privacy, novecojis bezvadu aizsardzības algoritms
WPA2	Wi-Fi Protected Access, bezvadu aizsardzības otrās versijas protokolu un sertifikātu apkopojums.
MAC adrese	Unikāls identifikators, kas tiek pielietots katrai ar datortīklu saistītai ierīcei.
IGMP	Internet Group Management Protocol – tīkla līmeņa protokols, kuru izmanto saziņai ar maršrutētājiem, lai saņemtu multicast grupas biedrību.
ICMP	*Internet Control Message Protocol* - tīkla līmeņa protokols, kuru izmanto, lai informētu par kļūdām un citiem gadījumiem, kas radušies datu pārraides laikā.
NAT	*Network Address translation* – ir metodoloģija, kas pārveido vienu IP adresi citā, labojot IP protokola datagrammu pakešu galvenēs, kad tie tiek pārsūtīti caur maršrutēšanas ierīci.

IEVADS

Informācijas tehnoloģiju pasaulē jau sen ir ieviests termins “maršrutētājs”. Laikam ejot, sākumā sauktais “residental gateway” sāka gūt lielāku un lielāku popularitāti gan mājās, gan mazos uzņēmumos. To parādīšanās stimulēja industrijā cenu kritumu gan uz šāda veida ierīcēm, gan arī daļēji uz serveriem, kas stipri veicināja “SOHO” aparatūras izplatīšanos pasaulē.

“SOHO” maršrutētāju masveida izmantošanas rezultātā var secināt, ka šāda veida ierīces, iespējams, lietotāji var izmantot nepareizi. Tas noved pie tā, ka to informācija var būt apdraudēta jau lokālajā tīklā. Šo problēmu pastiprina arī tas, ka jau vairāk nekā 15 gadu ilgajā pieredzē, aparatūras ražotāji arī pieļauj kļūdas gan programmatūras izstrādē, gan dzelžu izstrādē. Tas, protams, ir daļēji saistīts ar konkurenci un centieniem samazināt ražošanas izmaksas, kas būtiski nemaina kopējo situāciju. Praksē ir sastopamas arī tādas kļūdas, kuras var novest pie aparatūras nestandarta darbības.

Galvenais darba uzdevums ir izpētīt “SOHO” aparatūras darbības īpašības. Atrast un apskatīt gan no lietotāja, gan no ražotāju puses nepilnības un ievainojamības, kuras ir radušās dažādu iemeslu dēļ. Iespējams, dažas no problēmām ir iespējams novērst ar programmatūras ielāpa izveidošanu.

Darba rezultātus apkopot un piedāvāt sastapto problēmām risinājumus. Katrai no atrastajai problēmām izpētīt cik krasi tā var ietekmēt pašas aparatūras un arī citu iekārtu darbību, kuras atrodas ar to vienā lokālajā tīklā vai pat ārpus tā.

Galvenie maģistra darba mērķi:

1. Atrast problēmas, kas ir saistītas ar “SOHO” maršrutētāju nestandarta uzvedību. Atrast, vai pēc iespējas tuvāk patiesībai, minēt to cēloņus.
2. Veikt visu atrasto problēmu analīzi, mēģināt ar tām problēmām panākt to, ka tās var apdraudēt maršrutētāja drošību.
3. Izveidot ieteikumus gan maršrutētāju ražotājiem, gan parastiem lietotājiem, kuri vēlas pareizi nokonfigurēt savu bezvadu maršrutētāju.
4. Atrisināt kaut daļu no izvirzītām un atrastām problēmām, tādējādi padarot stabilāku un drošāku “SOHO” aparatūras darbību.

Darbs sastāv no piecām nodaļām:

- Pirmajā nodaļā tiek apskatīta ”Plaši pielietotā “SOHO” aparatūra”. Nodaļā tiks paskaidrots kas tā par aparatūru, kam tā ir domāta un kādiem mērķiem, tiek mūsdienās izmantota.
- Otrajā nodaļā tiks apskatītas “SOHO” aparatūras problēmu iespējamie cēloņi.
- Trešajā nodaļā, kurā tiks veikti pētījumi ar dažādu ražotāju “SOHO” aparatūru un pierādīt izvirzītie drošības problēmu riski.
- Ceturtajā Nodaļā “Pētījumu analīze un to secinājumi” tiks analizēta informācija no pētījumu nodaļas.
- Piektajā nodaļā tiks izvirzīts ieteikumu un rekomendāciju apkopojums, kuros tiks iekļauts visu konstatēto problēmu iespējamie risinājumi.

1. PLAŠI PIELIETOTĀ SOHO APARATŪRA

Nodaļa sevī ietvers teorētisko daļu, ar kuras palīdzību būs iespējams gūt priekšstatu par to kas ir "SOHO" aparatūra, kam tā ir domāta un kādiem mērķiem tiek izmantota.

1.1. Kas ir "SOHO" aparatūra

Termins "SOHO" radies biznesa industrijā 80-o gadu sākumā, kas nozīmē "Small office/Home office" un atspoguļo mājas vai nelielus birojus ar darbinieku skaitu no 1 līdz 10 cilvēkiem[1]. "SOHO" aparatūra var būt dažādu tipu un tā tiek dalīta pēc darbības OSI līmeņos:

- Koncentratori – jau gandrīz netiek izmantoti mūsdienās. Darbojas OSI pirmajā līmenī un tika izstumti no industrijas ar komutatoriem, savu daudzo trūkumu dēļ. Galvenais to trūkums bija saņemto pakešu izsūtīšana uz visiem koncentratora portiem, tādējādi koncentrators nezin kur atrodas paketes saņēmējs. Vēl viens liels trūkums bija maz pārraides ātruma atbalsta [2].
- Komutatori, kas tikai un vienīgi veic tīkla mezglu savienošanu vienam ar otru. Atšķirībā no koncentratoriem komutatori darbojas OSI otrajā (kanāla) līmenī un prot nodrošināt neatkarīgu pakešu pārraidi, kas samazina lieko un nevajadzīgo datu pārraidi. Komutatori spēj lasīt pakešu virsrakstus un pārsūtīt tās portos, balstoties uz saņēmēja MAC adresi. Atšķirībā no koncentratoriem komutatori tiek izmantoti arī mūsdienās. Evolucionējot šobrīd, tie prot strādāt gan dažādos režīmos, gan dažādos pārraides ātrumos, atkarībā no pieslēgtas pie porta ierīces. Dārgie komutatori, kuri jau nav attiecināmi pie "SOHO" aparatūras prot darboties OSI otrajā un trešajā līmenī un veikt sarežģītas operācijas, kā VLAN (802.11q) izmantošanu, QOS, agregēšana, portu spoguļošana, IP televīzijas izmantošanu (IGMP) utt. Eksistē arī tā saucamie "Layer 2+" komutatori un to pieprasījums aug ik dienu. Tiem piemīt tikai daļēja OSI trešā līmeņa funkcionalitāte, kā IGMP un ICMP, un kuri ir faktiski attiecināmi pie "SOHO" aparatūras segmenta, to lētās cenas dēļ[2].
- Maršrutētāji – darbojas daļēji OSI trešajā līmenī un prot veikt jau maršrutēšanu starp tīkliem, piemēram, ārējo un lokālo, izmantojot NAT metodoloģiju. Tie ietver sevī visu iepriekšējo OSI līmeņu funkcionalitāti un ir papildināti ar citu. Cenas ziņā, "SOHO" maršrutētāju ir iespējams iegādāties sākot no 7 eiro, bet ir arī pieejami daudz dārgāki produkti. Atkarībā no cenas maršrutētājiem mainās to

maksimālais bezvadu tīkla ātrums, funkcionalitātes klāsts, pieslēguma portu skaits un to ātrums, USB portu esamība utt.

1.2. Kam ir domāta "SOHO" aparatūra

"SOHO" aparatūra ir domāta neliela skaita cilvēku vai maza uzņēmuma datortehnikas un citu ierīču savienošanai lokālajā tīklā, kā arī ar iespēju no šī tīkla piekļūt internetam. Lielākā daļa no funkcionalitātes, kā jau tika aprakstīt iepriekšējā apakšnodaļā, ir atkarīga tieši no tā, kāda veida "SOHO" aparatūra tiek izmantota. Galvenais kritērijs šādu ierīču iegādei ir to ļoti liela pieejamība tirgū ar elastīgu funkcionalitāti, kura pārsvarā arī diktē ierīces cenu. Tomēr, ir arī izņēmumi, piemēram, Cisco ražotājs piedāvā klientiem "Small business" sērijas komutatorus, kuri pēc funkcionalitātes ir ļoti elementāri, bet pēc cenas ir daudz dārgāki par citu ražotāju piedāvātājiem analoģiskiem risinājumiem.

Šāda veida aparatūru nedrīkst izmantot uzņēmumos, kura tīklā tiek pārsūtīti dažādi sensitīvi dati, piemēram, finansiāli vai personīgi dati, kas var apdraudēt to drošību, pat ja iekšējais tīkls ir ļoti labi aizsargāts. Šādos uzņēmumos izmanto dārgākus risinājumus par "SOHO" maršrutētājiem.

1.3. Kā izmanto "SOHO" aparatūru

Apakšnodaļā aprakstīts "SOHO" aparatūras pielietojums dažādos izmantošanas apstākļos. Tās mērķis ir veikt priekšstatu par to, cik liels cilvēku daudzums un kādu funkcionalitāti izmanto "SOHO" maršrutētājos, tādējādi parādot kopējo bildi, cik lielā masveidā tiek izmantota šāda aparatūra.

1.3.1. Pielietojums mājas apstākļos

Interneta lietotājam, kurš ikdienā nav saistīts ar IT nozari, būs pilnīgi pietiekams pat ar lētu maršrutētāju, kas ļaus tam izmantot internetu ikdienišķām vajadzībām, tai skaitā pārlūkot interneta lapas, lejupielādēt dažādus failus, spēlēt tiešsaistes spēles utt. Pat ja būs nepieciešama kāda elementāra papildus funkcionalitāte – tā būs pieejama lētajiem maršrutētājiem. Vienīgais, ko lietotājs varēs just, ir maksimālais bezvadu tīkla pārraides ātrums, kas vislētākajiem maršrutētājiem var būt dažas reizes mazāks par ātrumu, kuru piedāvā dārgāki modeļi.

1.3.2. Pielietojums Birojos

"SOHO" maršrutētāju pielietojums birojos variē atkarībā no tā, kāda funkcionalitāte ir vajadzīga tā darbiniekiem. Neskaitot standarta funkcionalitāti, maršrutētājos izmanto arī:

- DHCP rezervāciju, kura ir vajadzīga, lai izvēlētiem datoriem rezervētu statisku lokālo IP adresi. Šāda veida piesaiste tiek veidota, izmantojot datora MAC adresi un izvēlētu lokālo IP adresi. (piemērs) Ja uzņēmumā vēlas, lai vienam datoram vienmēr būtu statiska IP adrese, piemēram, grāmatvedības programmatūras serverim.
- Portu pāradresāciju (port forwarding), ar kura palīdzību ir iespējams no ārējā tīkla piekļūt izvēlētā datora vai neliela servera konkrētajiem portiem. Pārsvarā šo iespēju izmanto ar DHCP rezervāciju. (piemērs) Ja grāmatvedības serverim ir vajadzīga piekļuve, izmantojot Remote desktop protokola palīdzību, tad RDP portu 3389 no globālās IP adreses pāradresēs uz grāmatvedības servera rezervētu lokālo IP adresi un uzņēmuma darbinieki varēs slēgties klāt serverim attālināti, no globālā tīkla.
- Viesu bezvadu tīklu, ar kura palīdzību būs iespējams sadalīt tīklu tā, lai galvenajam lokālajam tīklam, kurā atrodas biroja darbinieku datori un ierīces, nevarētu piekļūtu sveši cilvēki.

Pēdējā laikā lielu popularitāti arī ir ieguvuši maršrutētāji ar vienu vai pat vairākiem USB portiem. Pie šiem portiem ir iespējams pieslēgt dažādas USB ierīces:

- USB printeri vai skeneri. Ja printeris neatbalsta pieslēgumu izmantojot tīkla vadu, iespēja pieslēgt USB printeri pie maršrutētāja ir liela priekšrocība, atšķirībā no Windows Printer Sharing iespējām, kura gadījumā ir vajadzīgs atstāt ieslēgtu datoru, lai printeri varētu izmantot citi lokālā tīkla lietotāji.
- 3G/4G modemu, ar kura palīdzību ir iespējams nodrošināt interneta pieeju pat tad, kad primārais interneta pieslēgums nav pieejams.
- USB zibatmiņu vai USB cieto disku, lai varētu lokālajā tīklā koplietot failus un mapes. Dārgākajiem modeļiem ir iespējams nokonfigurēt FTP pieeju, lai failiem varētu piekļūt arī attālināti no ārējā tīkla.

Papildus tam, maršrutētājus var nokonfigurēt veikt elementārākas lietas, kā – atkārtot kādu no eksistējošiem bezvadu tīkliem, tādējādi palielinot tā bezvadu tīkla raidīšanas

diapazonu. Kā piemēru var minēt nelielas viesnīcas, kuras pārsvarā arī izmanto šāda veida risinājumus, lai to bezvadu tīkla pārklājums būtu pieejams visos ēkas nostūros.

1.4. Ar ko tiek darbināta "SOHO" aparatūra

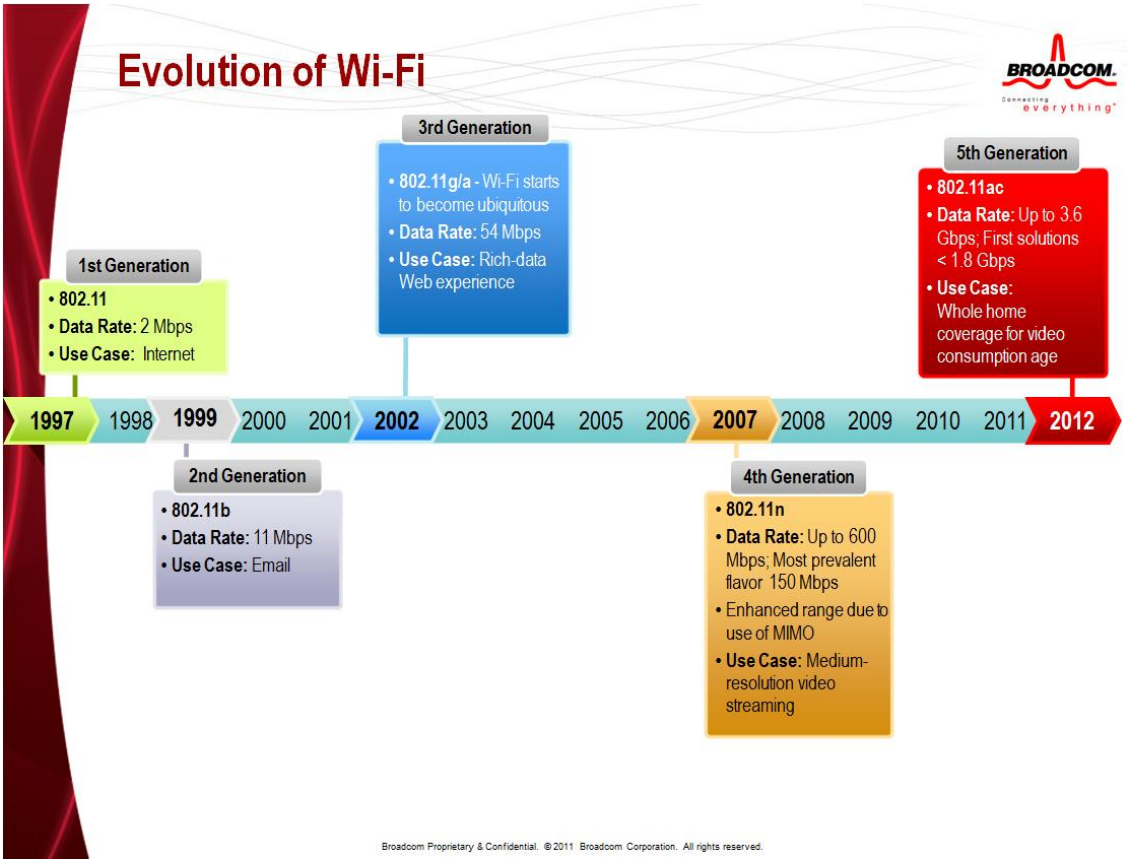
Katrs ražotājs izmanto savu operētājsistēmu, lai darbinātu maršrutētāju. Pārsvarā visas šīs operētājsistēmas ir balstītas uz Linux kodola[3]. To konfigurācijai lielākoties tiek izmantots tīmekļa interfeiss, kas tiek darbināts ar iebūvētā tīmekļa servera palīdzību. Daži dārgāki modeļi atbalsta arī Telnet vai SSH pieslēguma iespējas, ļaujot konfigurēt maršrutētājus, izmantojot komandrindu. Ir redzēti modeļi, kuriem komplektācijā nāk CD disks ar atzīmi atvērt uz tā ierakstītu programmatūru un sekot uzstādīšanas instrukcijām, tādējādi lietotājam pirmajā uzstādīšanas reizē nav vajadzīgs pat vērt konfigurācijas lapu.

Paralēli ražotāju operētājsistēmām, dažādu ražotāju maršrutētājiem, atkarībā kāds mikroprocesors darbina maršrutētāju, ir iespējams nomainīt operētājsistēmu uz trešo personu izstrādātu operētājsistēmu. Populārākie ir OpenWRT, DD-WRT un Tomato. To galvenās priekšrocības ir palielināta funkcionalitāte un lielāka stabilitāte, salīdzinot ar maršrutētāju ražotāju izveidotām operētājsistēmām. Katra no minētajām trešo personu operētājsistēmām ir ar ko īpaša un, izvēloties uzstādīt tās uz maršrutētāja, ir jāpiedomā kas tieši datortīkla administratoram būs vajadzīgs – visvieglākā un intuitīvākā konfigurācija ir Tomato un DD-WRT operētājsistēmām, bet maksimālai funkcionalitātes palielināšanai būs jāizmanto OpenWRT. Tomēr tā ir grūtāk konfigurējama un pieejamā papildus funkcionalitātes pievienošanai dažreiz būs jāizmanto skripti un programmēšana.

1.5. "SOHO" maršrutētāji pēdējo 15 gadu laikā

Apakšnodaļā tik aplūkota "SOHO" aparatūras vēsture, protokolu un standartu evolūcija un izplatība pēdējo 15 gadu laikā.

Pārsvarā, mūsdienu bezvadu tīklu pasaulē tiek veikts uzsvars uz pārraides ātruma palielināšanu starp ierīcēm, lai ātrāk varētu veikt datu apmaiņu starp tām, jo ik gadu palielinās datu pārraides apjomi. Sākot ar 1997. gadu un līdz mūsdienām, datu pārraides ātrumi ir daudzkārt palielinājušies (sk. 1.1 att.), kā arī mainās datu pārraides protokoli un modulācijas, kas ļauj palielināt datu pārraides stabilitāti [4]. Tomēr, bezvadu tīklu aizsardzības protokoli nav tikuši daudz tālāk par 2004. gadu, kad tika prezentēts WPA2 aizsardzības protokols.



1.1 att. **Bezvadu tīklu evolūcija [5]**

Tātad, ātrumam augot, bezvadu tīklu aizsardzība netika palielināta vai pat modificēta. Ir pagājušas jau divas jaunas bezvadu tīklu paaudzes, bet WPA2 joprojām tiek izmantots primāri un ir vienīgais vislabāk aizsargājamais drošības protokols.

Ja šāds protokols nesaturētu kļūdas un visu tā dzīves laiku nebūtu uzlauzts vai arī netiktu atrastas tā ievainojamības, to varētu izmantot arī tālāk, bet diemžēl internetā parādās vairāk un vairāk ziņu par to, ka ir atrastas WPA2 ievainojamības un iespējas to uzlauzt.

1.6 Jauninājumi "SOHO" maršrutētājos un bezvadu tīklu industrijā

Apakšnodaļā tiks aprakstīti jaunumi, kas ir ieviesti "SOHO" aparatūrā tuvākajos gados. Vai arī to ieviešana ir, kaut kādā mērā izdzēsusi vai, samazinājusi eksistējošās problēmas, kas ir saistītas ar maršrutētāju darbību un bezvadu tīkliem.

1.6.1 802.11ac standarts

Prezentēts 2011. gadā un apstiprināts 2014. gada janvārī 802.11ac standarts palielināja trīsreiz iespējamo teorētisko pārraides ātrumu bezvadu tīklā, salīdzinot ar iepriekšējo 802.11n standartu, tāpēc to ir sākuši saukt par "Gigabit Wi-Fi", kas kļuva pirmais, kas spēja pārvarēt

gigabita ātruma izmantošanu bezvadu tīklos[6][7]. Izmantojot visdārgāko aparatūru ar 8xMU-MIMO antenām, teorētiskais pārraides ātrums var būt līdz 6.77 gigabitiem sekundē. Tomēr, galvenais šī standarta ieviešanas mērķis ir jaunas modulācijas shēma 256-QAM, kas palielina signāla modulācijas iespējas, tādējādi palielinot gan pārraides ātrumu un tā uztveršanas stabilitāti[4]. Tātad, apkopojot visu informāciju par šo standartu, ir iespējams izveidot sarakstu ar 802.11ac standarta priekšrocībām:

- Jauna modulācijas shēma;
- Kopējā ātruma palielinājums, kas mājās apstākļos spēs realizēt gigabita lokālo bezvadu tīklu, neizmantojot vadu pieslēgumus.
- Lielāks klientu skaita atbalsts lokālajā tīklā;
- Datu pārraidei samazinās enerģijas patēriņš.

Bet tik un tā, līdz pat šim brīdim mājas bezvadu maršrutētāja ar 802.11ac standartu cena ir divas pat trīs reizes dārgāka par līdzīgu N standarta maršrutētāju. Ir jāņem vērā arī fakts, ka pat šodien visās modernās ierīces, kuras izmanto bezvadu savienojumus, netiek izmantots 802.11ac standarts. To izmanto tikai dārgajos produktos [8].

1.6.2 Viesu bezvadu tīkls

Vidējās cenu kategorijas maršrutētāji atbalsta tā saucamo "viesu" bezvadu tīklu vai arī papildus virtuālo bezvadu tīklu izveidošanu, kas ļauj izveidot divus atsevišķus tīklus. Šāda funkcionalitāte noder, ja uzņēmumā, piemēram, strādā ar sensitīviem datiem un bezvadu tīklam ir jābūt maksimāli iespējami aizsargātam. Viesu tīklam, pārsvarā, iekšējais maršrutētāja DHCP serveris izdala atsevišķu IP adrešu loku citā zem-tīklā, tādējādi pasargājot darbinieku datorus no nevēlamiem viesu datoriem savā zem-tīklā [9].

Ja viesi un darbinieki slēgtos pie viena un tā paša bezvadu tīkla – tie atrastos vienā zem-tīklā, kas var ļoti apdraudēt datu drošību, piemēram, ja viesa portatīvais dators saturēs programmatūru, tā varēs skenēt un daļēji vai pilnībā saņemt darbinieku datus.

2. “SOHO” APARATŪRAS PROBLĒMAS

Nodaļā tiks apkopota informācija par to, kāda veida problēmas ir iespējamas “SOHO” maršrutētājiem un kā tos ir iespējams sadalīt.

2.1 Tehniskās problēmas

Tehniskās problēmas radušās no ražotāja puses un dalās uz dzelžu līmeni un programmatūras līmeni. Iespējams arī tas, ka pēc problēmu konstatēšanas, to izcelsmi nevarēs precīzi attiecināt uz vienu vai otru kategoriju, jo līdz beigām nav skaidrs, kas konkrētu problēmu veido.

2.1.1 Dzelžu līmenis

Ņemot vērā to, ka WAN un LAN tiek apstrādāts ar vienu un to pašu mikroprocesoru, iespējami gadījumi – kad no WAN puses būs “redzama” lokālā tīkla adrese, kas tiks pierādīts apakšnodaļā 3.1. Ar to nebūs iespējams savienoties, vai arī veikt kādas darbības, bet fakts paliek – uz ARP pieprasījumiem lokālā maršrutētāja IP adrese atbildēs.

Ja maršrutētājs darbojas 802.11 B/G/N režīmā 2.4 gigahercos (GHz) un 10 lietotāji izmanto 802.11n standartu, bet viens 802.11G – savienojums starp visiem lietotājiem samazinās līdz 802.11g standartam. Kā viens no risinājumiem varētu būt – izmantot divus maršrutētājus – vienu 802.11n standartam, otru – vecākiem 802.11b un 802.11g standartiem.

2.1.2 Programmatūras līmenis

Ņemot vērā to, ka jau masveidā ir pieejami bezvadu maršrutētāji cenā sākot no 7 eiro, ir iespējams uzdot jautājumu – ar ko tad atšķīrās maršrutētāji, kas ir, balstīti uz vienu un to pašu mikroprocesoru, bet to maksa atšķiras par 10 vai pat 20 eiro? Atbilde varētu būt elementāra – funkcionalitāte, vai dažādi trūkumi programmatūras izstrādē.

Ir arī redzēti gadījumi maršrutētāju grafiskajos interfeisos, kad to attēlošana izskatās sabojāta vai neproporcionāla citām izvēlnes sadaļām, kas var būt iemesls ne līdz beigām uzrakstītam programmatūras kodam.

2.2 Cilvēciskās problēmas

Iespējamas situācijas, kad cilvēks pat nekonfigurēto maršrutētāju pieslēdz pie interneta un, teorētiski, viņam to nav jākonfigurē, lai to sāktu izmantot. Tas ir liels risks, jo lielākā daļa maršrutētāju pēc noklusējuma nenāk ar bezvadu tīkla aizsardzību, un to standarta lietotājvārds un parole, ar kuru ir jāveic konfigurāciju interfeisā, ir viegli uzminami.

Cits iemesls cilvēciskām problēmām var būt dažu konfigurācijas parametru nepareiza saprašana vai nevēlēšanās saprast. Veicot bāzes konfigurāciju, cilvēks var, piemēram, nesaprast atšķirību starp WEP un WPA bezvadu tīkla drošības protokoliem un izvēlēties novecojušo WEP standartu, kas var beigās novest pie slikti aizsargāta bezvadu tīkla.

2.3 Bezvadu maršrutētāju izmantošana dažādās valstīs

Apakšnodaļa apkopos nianšu sarakstu ar ierobežojumu vai specifisko "SOHO" aparatūras izmantošanu dažādās pasaules valstīs:

- Ziemeļamerikā 2.4 gigahercu frekvencē ir iespējams izmantot tikai no 1 līdz 11 frekvenču kanālam, atšķirībā no Eiropas, kurā drīkst izmantot no 1 līdz 13 frekvenču kanālam. 12 un 13 kanālu Amerikas Savienotajās Valstīs ir atļauts izmantot tikai un vienīgi ja tās ir mazjaudīgas [10].
- 5 gigahercu izmantošana atsevišķās pasaules daļās ļoti atšķiras ar atļauto kanālu izmantošanu.

3. PĒTĪJUMI

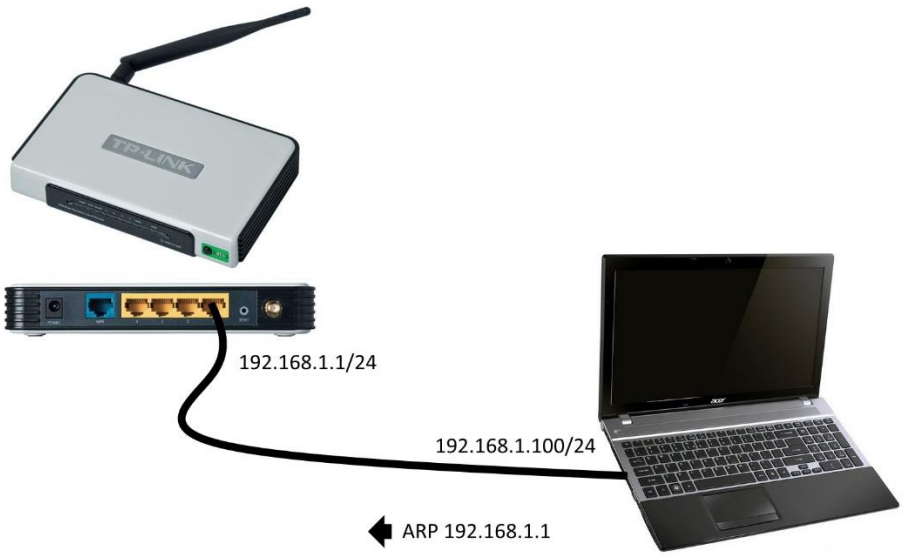
3.1 Lokālā tīkla IP un MAC adreses uzrādīšana no globālā (WAN) tīkla puses

Pētījums vērsts uz to lai pārbaudītu vai "SOHO" maršrutētāji, darbojoties, neizplata savā WAN portā lokālā tīkla IP un MAC adresi. Pētījumam tiks izmantota arp-ping.exe[11] neliela brīvi pieejamā programmatūra, kas darbināma uz Windows 8.1. Ar šīs programmatūras palīdzību Windows operētājsistēmas komandrindā būs iespējams veikt ARP pieprasījumu uz izvēlētu IP adresi[12]. Šī pētījuma gadījumā – pieprasījumi tiks sūtīti uz lokālo maršrutētāja IP adresi 192.168.1.1.

Pētījumam tiks izmantoti maršrutētāji, kuri bija pieejami autoram uz darba rakstīšanas brīdi un visi attiecināmi pie "SOHO" maršrutētāju kategorijas:

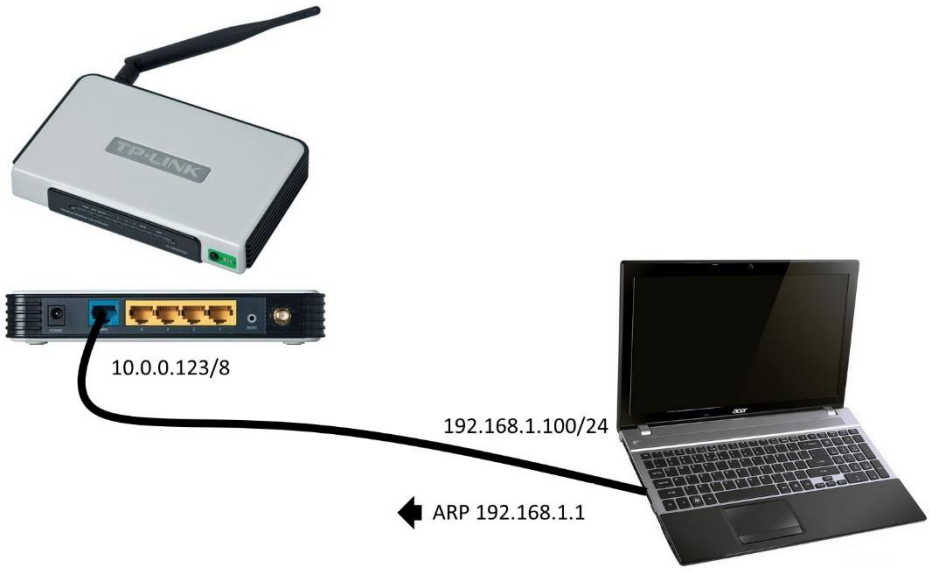
- TP-Link TL-WR740N
- TP-Link TL-WR740N ar OpenWRT programmnodrošinājumu
- TP-Link TL-WR320G
- LevelOne WBR-6005
- D-Link DAP-1155 (B1)
- Netis WF2411
- Netis WF2419
- Linksys WR54G
- Linksys Cisco E2500

ARP pieprasījumi tiks sūtīti, izmantojot divas shēmas, vienas – pieslēdzot datoru pie maršrutētāja LAN porta (sk. 3.1 att.), tādējādi pārbaudot, ka maršrutētājs darbojas, un atbild ar lokālā tīkla MAC adresi, otras – pieslēdzot pie maršrutētāja WAN porta (sk. 3.2 att.).



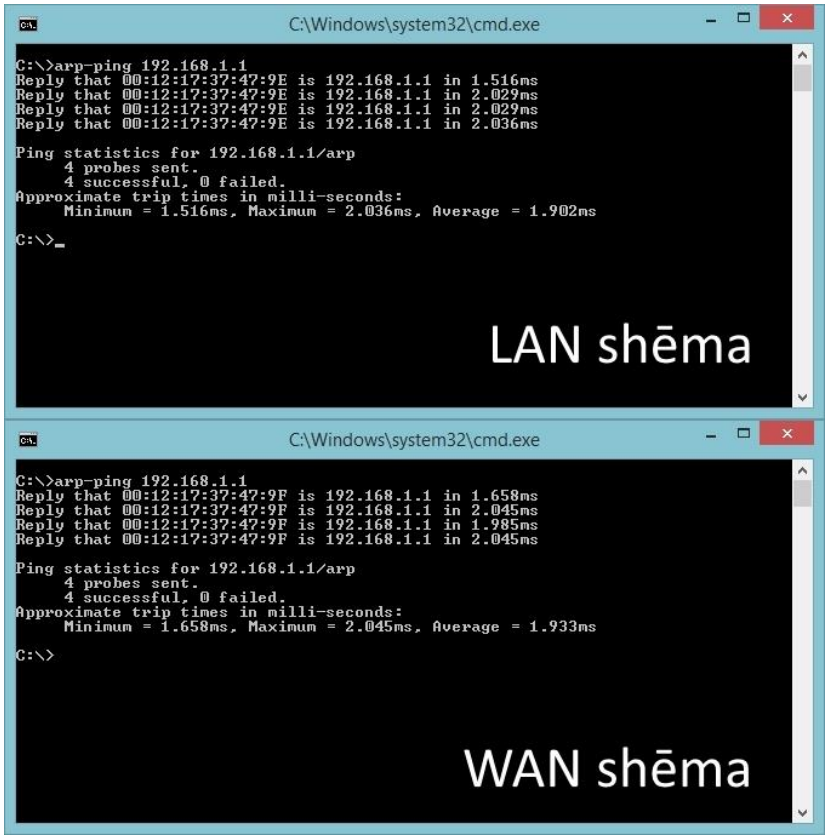
3.1 att. **Pieslēguma shēma pie lokālā (LAN) tīkla porta**

Pētījuma mērķis ir pārliecināties par to, ka "SOHO" maršrutētāju darbība pat no paša ieslēgšanas brīža nav pielīdzināma pasaules standartiem un protokoliem, ka maršrutētājs globālajā tīklā translē savu lokālo IP un MAC adresi.



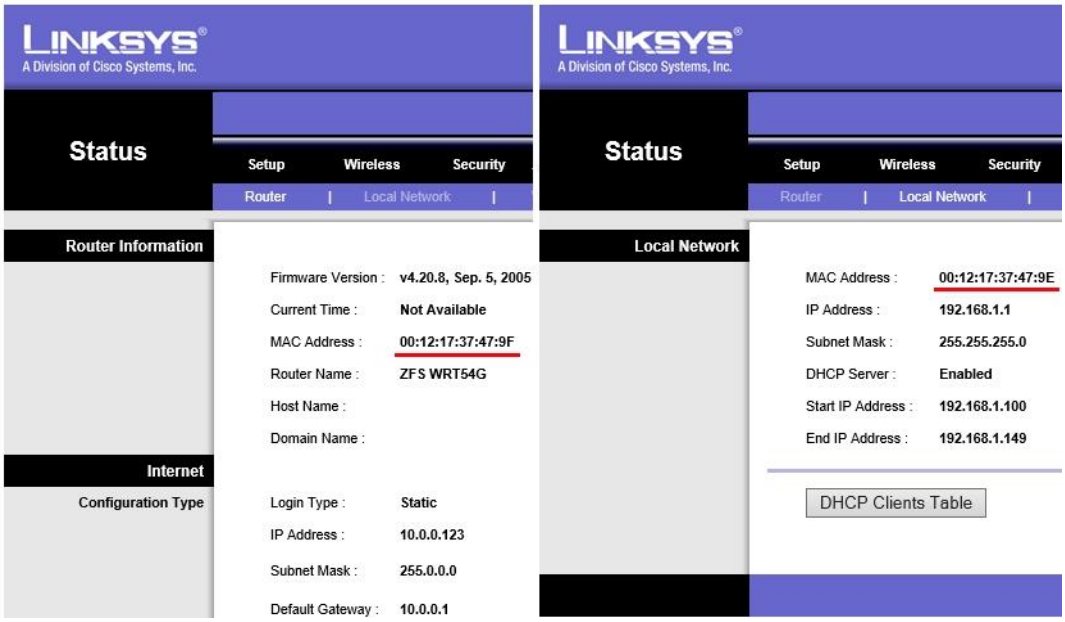
3.2 att. **Pieslēguma shēma pie globālā (WAN) tīkla porta**

Veicot pētījumu, sākumā tika izmantota lokālā tīkla pieslēguma shēma, veikti ARP pieprasījumi, bet pēc tam tika pārslēgts uz globālā tīkla pieslēguma shēmu. Viens no pieprasīju logiem, izmantojot maršrutētāju ir parādīts att. 3.3.



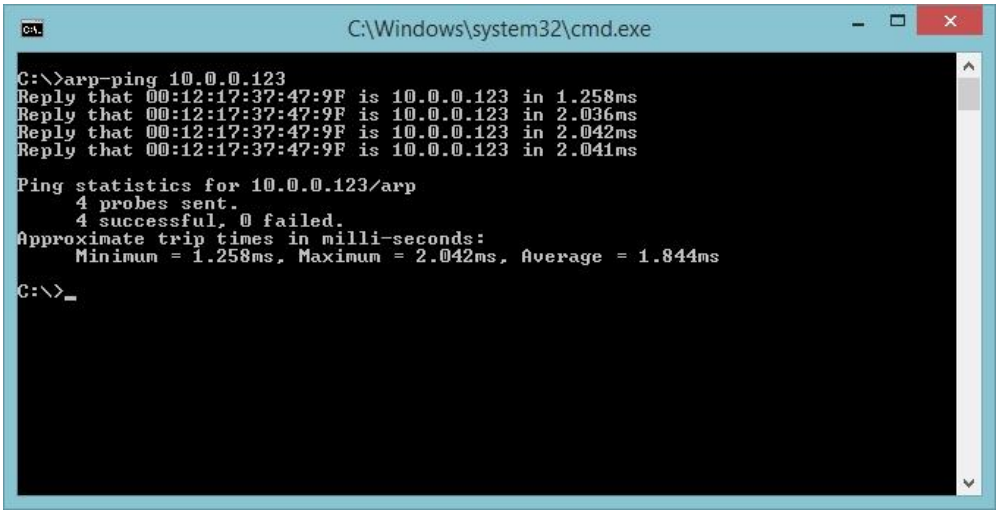
3.3 att. **ARP pieprasījumu atbildes no Linksys WRT54G v2 abās shēmās**

Abos shēmu gadījumos uz ARP pieprasījumu tika atbildēts, tikai no atšķirīgām MAC adresēm. Pārbaudot šīs MAC adreses Linksys maršrutētāja grafiskajā interfeisā, ir jāsecina, ka maršrutētājs uz LAN un WAN portiem izmanto dažādas MAC adreses – vienu priekš lokālā tīkla apkalpošanas, bet otru – darbībai ar globālo tīklu (sk. 3.4 att.).



3.4 att. **Linksys WR54G globālā un lokālā MAC adrese**

Tomēr, no teorētiskā viedokļa, WAN shēmā minētajai MAC adresei ir jādarbojas tikai ar globālā tīkla IP adresi (sk. 3.5 att.).



3.5 att. **ARP pieprasījumu atbildes no Linksys WR54G veicot pieprasījumu uz globālo IP adresi**

Zemāk minētajā tabulā parādīts, kurš no pētījuma maršrutētājiem ir atbildējis uz lokālās adreses ARP pieprasījumu (tabula 3.1).

Tabula 3.1

ARP atbilžu no WAN porta apkopojums

Maršrutētājs	**ARP no WAN porta**
Linksys WR54G v2	✓
TP-LinkTL-WR740N	-
TP-LinkTL-WR740N OpenWRT	-
TP-Link TL-WR320G	-
LevelOne WBR-6005	✓
D-Link DAP-1155	✓
Linksys Cisco E2500	-
Netis WF2411	✓
Netis WF2419	✓

Paralēli ARP pieprasījumiem autors sūtīja arī PING pieprasījumus, veicot šo pētījumu un neviens no testējamiem maršrutētājiem nav uz tiem atbildējis.

Interesants fakts – maršrutētājs D-Link DAP-1155 no LAN porta ir atbildējis ar ”Realtek semiconductor corp.” MAC adresi (sākuma simboli: 00:E0:4C), bet no WAN porta ar ”Shenzhen Gongjin Electronics Co.,Ltd” MAC adresi (sākuma simboli: 2C:AB:25). Tikmēr maršrutētājs Netis WF2419 no LAN porta ir atbildējis ar “Netcore Technology Inc.” (sākuma simboli: 04:8D:38), bet no WAN porta atbildējis ar “Liteon Technology corporation” (sākuma simboli: 20:68:9D). Ekrānuzņēmumi ir pieejami pielikumos Nr.1 un Nr.2.

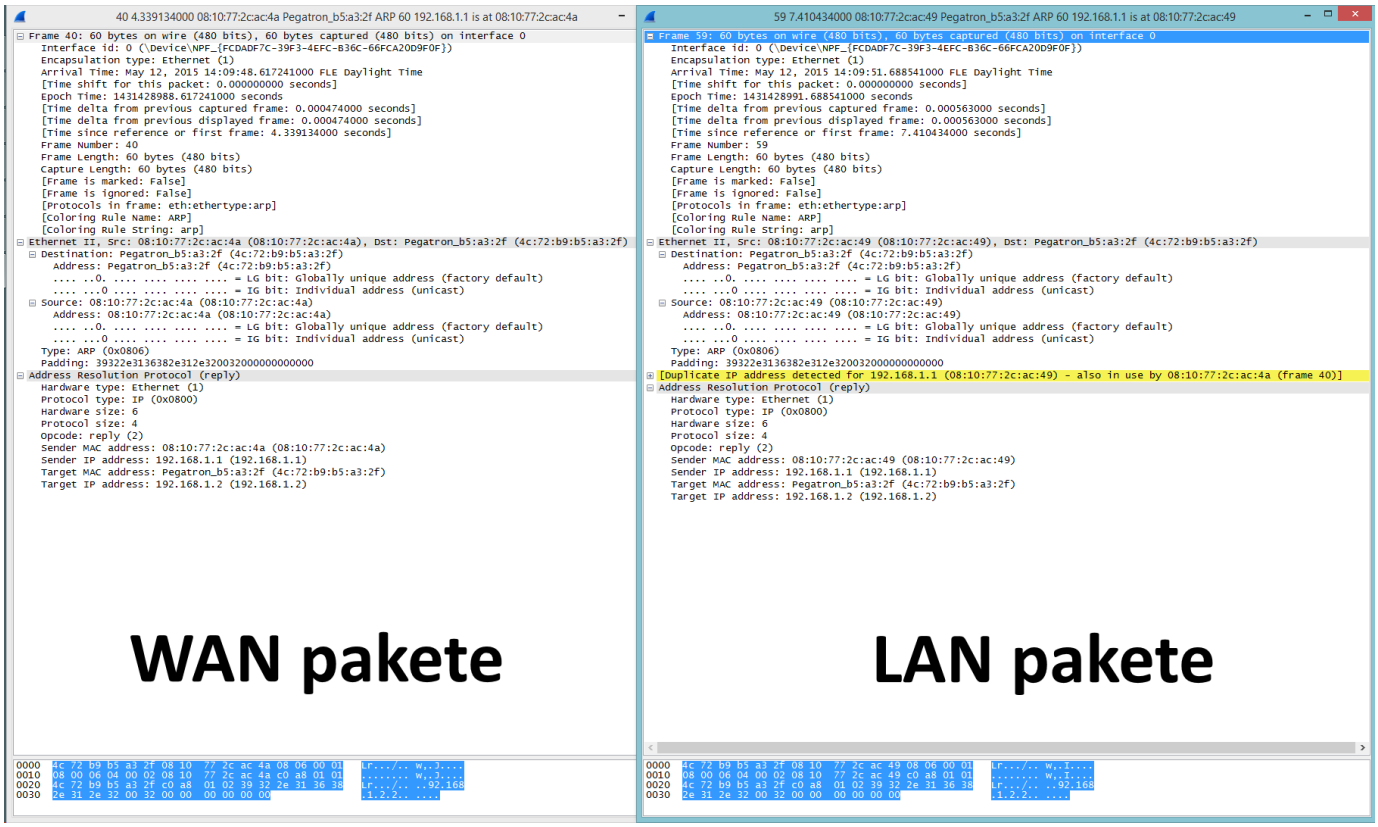
Pārējiem testējamajiem maršrutētājiem mainījās tikai MAC adreses pēdējie simboli.

No izveidotā pētījuma var secināt, ka puse no testējamiem "SOHO" maršrutētājiem tomēr uzrāda savu lokālo IP adresi WAN portā, bet to dara zem WAN porta MAC adreses, nevis zem lokālās MAC adreses. Arī tas, ka maršrutētāji atbild uz ARP, bet neatbild uz PING pieprasījumiem liek aizdomāties par to, ka šāda veida parādība iespējama, slikti uzrakstītas programmatūras gadījumā.

3.1.1 WAN un LAN portu ARP atbilžu salīdzinājums

Ņemot vērā to, ka ir jāmēģina dziļāk izpētīt ARP atbildes no WAN un LAN portiem, iespējams, ir laba doma tos notvert ar Wireshark programmatūru un salīdzināt. Pētījums tika veikts, izmantojot Netis WF2411 bezvadu maršrutētāju.

Pētījums sastāvēja no tā, ka autors saņemot ARP atbildi no WAN porta, pārslēdz patch vadu LAN portā un tādējādi ar wireshark notver abas atbildes paketes.

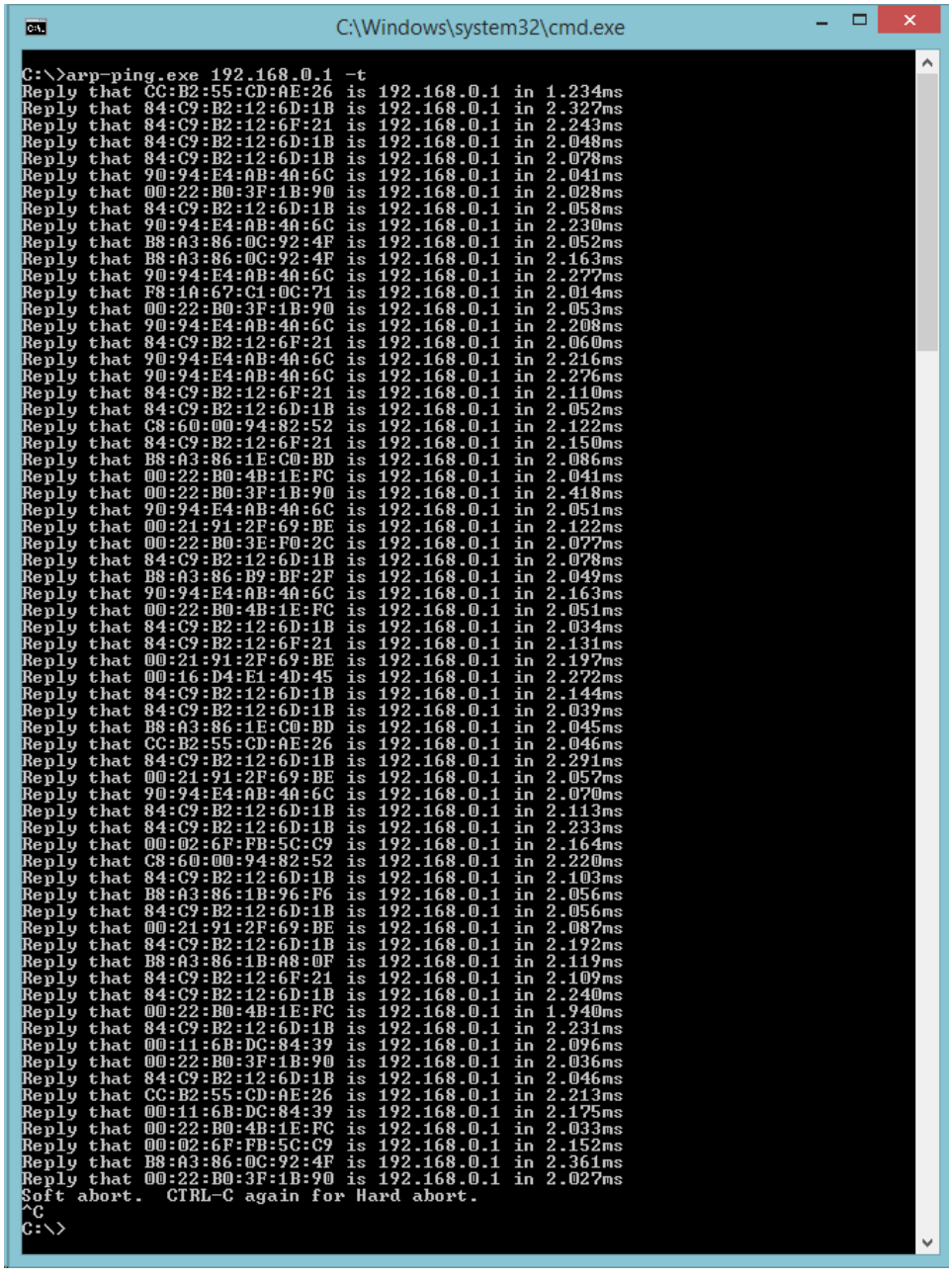


3.6 att. **Netis WF2411 WAN un LAN ARP pakešu salīdzinājums**

Salīdzinot to struktūru ir jāsecina, ka ir mainījies MAC adreses pēdējais simbols (no 4**9** uz 4**A**), kā arī Wireshark programmatūra parāda to, ka šāda IP adrese jau pieder citai MAC adresei.

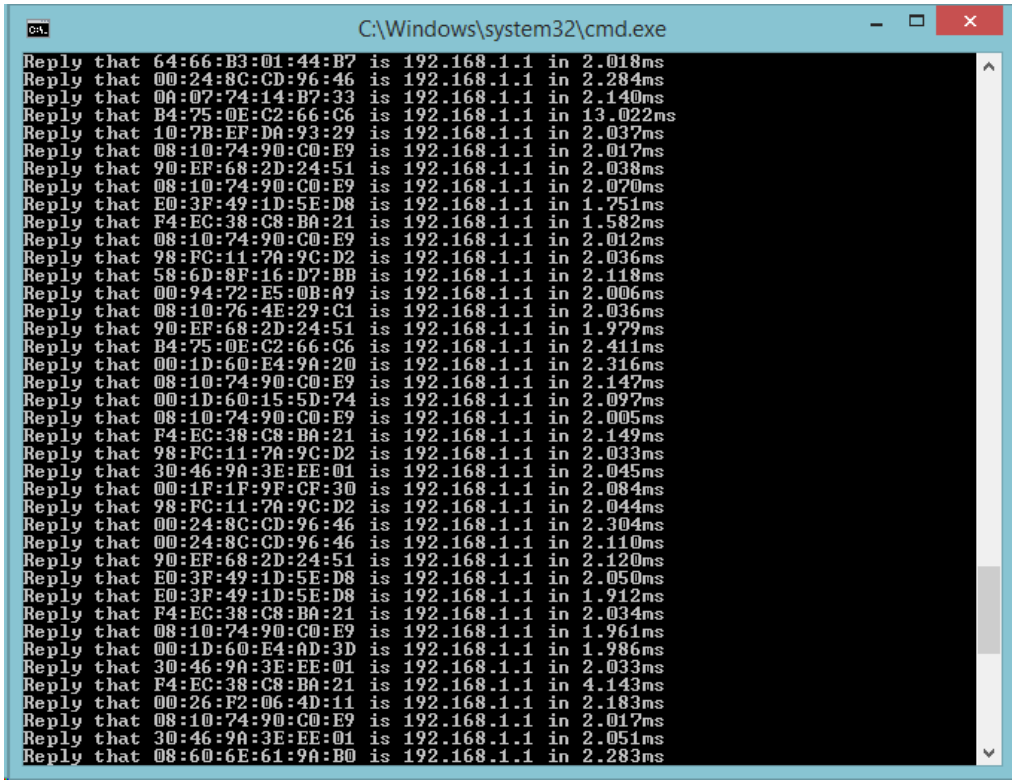
3.1.2 ARP pieprasījumi interneta pakalpojumu sniedzēja tīklā

Iepriekšējā pētījuma pareizību un aktualitāti arī pierāda tas, ka autors ir izsūtījis sava mājas interneta pakalpojumu sniedzēja tīklā iepriekšminētos arp-ping pieprasījumus un saņēmis ļoti daudz atbilžu no dažādām MAC adresēm (sk. 3.7 att.).



3.7 att. **ARP pieprasījumu atbildes izsūtot tās pakalpojumu sniedzēja tīklā**

Pilnīgi identiski ir arī ar arp-ping pieprasījumu izsūtīšanu uz 192.168.1.1 lokālo IP adresi (sk. 3.8 att.).



3.8 att. **ARP pieprasījumu atbildes izsūtot tās interneta pakalpojumu sniedzēja tīklā**

Kopējais MAC adrešu skaits gan 192.168.0.1, gan 192.168.1.1 ARP pieprasījumiem ir bijis ap 50. Ņemot vērā to, ka tīkla kopējais aktīvo IP adrešu skaits, uz pētījuma veikšanas brīdi, ir bijis ap 300, var secināt, ka 16% no visām aktīvām IP adresēm, iespējams, uzrāda savu lokālo IP adresi, globālajā portā.

Interneta pakalpojumu sniedzējs izmanto tikai un vienīgi statistiskās IP adreses tīklā. Tāpēc gandrīz neiespējams, ka ap 50 atbildēto MAC adrešu atbildēja, būdami pieslēgti pie LAN portiem, jo šādā veidā maršrutētāja lietotāji nevarētu izmantot internetu, izmantojot maršrutētāja bezvadu tīklu. Kā arī uz testēšanas brīdi tika uzzvanīts interneta pakalpojumu sniedzējam un jautāts par izsaukumiem konkrētajā rajonā un konkrēti ar manu savienojumu, uz ko tika atbildēts, ka viss šajā rajonā darbojas un ar manu savienojumu viss ir kārtībā.

3.1.3 Maršrutētāju atjaunošana līdz pēdējai programmatūras versijai

Veicot pētījumu 3.1 un, atklājot, ka maršrutētāja WAN portā ir, iespējams saņemt ARP pieprasījuma atbildi no lokālās IP adreses, autors nolēmis pārbaudīt, vai šo problēmu ir iespējams novērst, atjaunojot maršrutētāja iekšējo programmatūru līdz pēdējai versijai. Tas daļēji varētu atbildēt uz jautājumu par problēmas cēloni – ka vaina var slēpties slikti uzrakstītajā programmatūrā.

Tabula 3.2

ARP atbildes no WAN porta pēc programmatūras atjaunošanas līdz pēdējai versijai

Maršrutētājs	Pētījuma laikā	Pēdējā versija	ARP no WAN porta pēc atjaunošanas
Linksys WRT54G v2	V4.20.8	4.21.5	✓
LevelOne WBR-6005	0.0.1.13	0.0.1.14	✓
D-Link DAP-1155	1.0.0	2.5.0	-
Netis WF2411	V1.1.21610	V1.1.29433	-
Netis WF2419	V1.1.25087	V1.2.29433	-

Veicot programmatūras atjauninājumus līdz pēdējai versijai, kas, uz darba uzrakstīšanas brīdi, bija pieejama maršrutētāju ražotāju mājaslapās, izrādījās, ka Netis ražotāja pēdējie atjauninājumi šo problēmu ir novērsuši.

LevelOne WBR-6005 maršrutētāja programmatūras atjaunināšana neko nav devusi, uz ARP pieprasījumiem tik un tā tiek atbildēts no WAN porta. Iespējams, tas ir tādēļ, ka pēdējā maršrutētāja atjauninājuma izvietošanas datums ir 2011. gadā 11. janvāris. Kaut gan viens no Latvijas interneta veikaliem to vēl tirgo (balstoties uz resursu www.salidzini.lv), kas nozīmē, ka šādas ierīces parādās Latvijā vēl joprojām.

Tieši tāda pati situācija ir ar Cisco divīzijas Linksys WRT54G v2 maršrutētāju, ir pamainījies grafiskais interfeiss, tas kļuvis daudz izskatīgāks, bet problēma ar ARP pieprasījumiem ir palikusi. Pēdējā maršrutētāja programmatūras versija tika izlaista 2012. gada februārī.

Autors ir pamēģinājis arī veikt maršrutētāju TP-Link programmatūras atjaunošanu uz viss vecākām versijām, lai pārbaudītu vai maršrutētājiem arī bija problēmas ar WAN porta ARP atbildēm. Tomēr, pat ar vecāku TP-Link maršrutētāju versijām netika konstatēta šī problēma.

3.2 "SOHO" maršrutētāju grafisko interfeisu izpēte

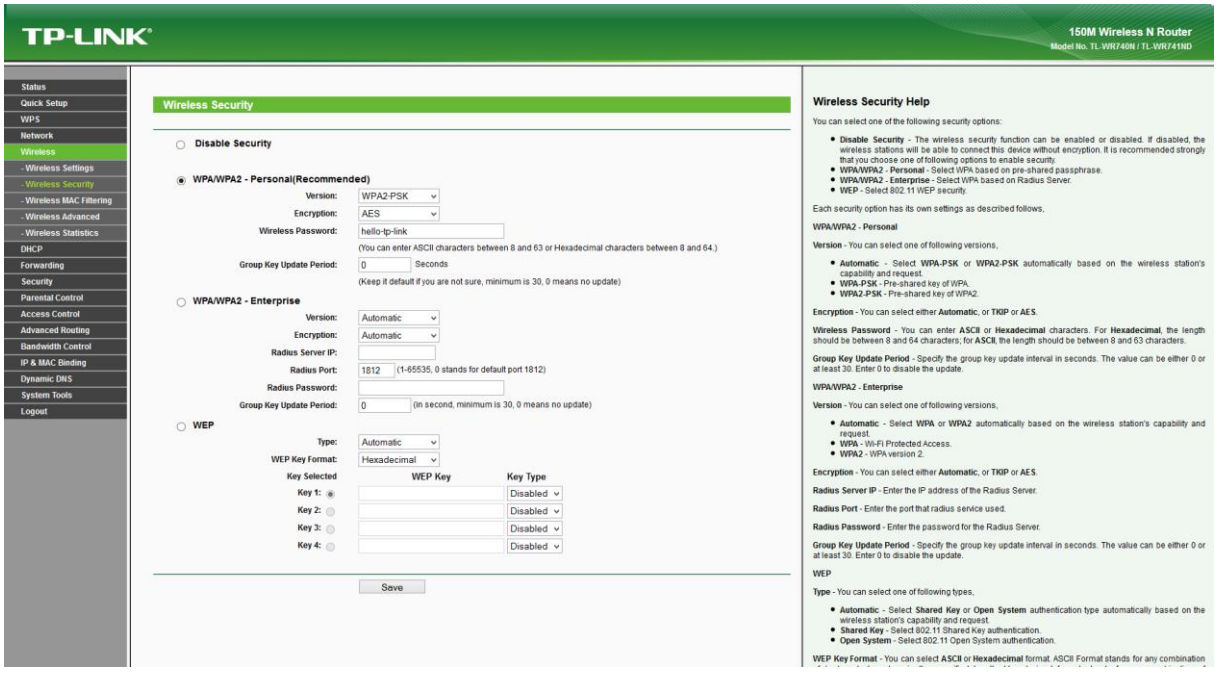
Liela nozīme jebkurā konfigurācijas procesā vienmēr aizņem grafiskais konfigurācijas interfeiss. Katrs no ražotājiem mēģina realizēt savas idejas, kā izskatīsies interfeiss un cik viegli to būs nokonfigurēt, bet pārsvarā tiek pieturās pie vienotas politikas – horizontālā vai vertikālā galvenā izvēlne ar zem izvēlnēm. Pētījuma mērķis ir veikt dažu grafisko interfeisu izpēti un mēģināt apkopot to labās un sliktās puses. Pētījumā tiks izmantoti tie paši maršrutētāji, kas tika izmantoti pētījumā 3.1.

Pārsvarā maršrutētāju ražotāji tomēr mēģina atvieglot ierīces konfigurāciju, bet tas, tomēr, ne vienmēr izdodas. Izvēlnes dažreiz ir ļoti nepārdomātas un neintuitīvas, kas noved ierīces nepareizas konfigurācijas vai arī funkcionalitāte netiek pareizi saprasta. Dažu maršrutētāju ražotāji pat nav veltījuši laiku, lai lietotājam paskaidrotu, ko katrs no konfigurācijas izvēlnes punktiem nozīmē, tāpēc arī sanāk pārpratumi no galēju lietotāju puses, ja vien konfigurāciju neveic datorspeciālists.

Kā vienu no galvenajiem punktiem autors izvēlējies pārbaudīt vai ražotāji iesaka izvēlēties WPA2 bezvadu aizsardzību, nevis jau sen novecojušu WEP protokolu, kuru iespējams uzlauzt ātrāk par vienu minūti [13].

3.2.1 TP-Link TL-WR741N grafiskais interfeiss

Viens no interesantākajiem grafiskā interfeisa piemēriem, nenoliedzami, ir TP-Link veidotais interfeiss. TP-Link ražojumi Latvijā ierindojas pirmajās vietās pēc lētas cenas un pirkšanas daudzuma, tāpēc tā interfeiss ir viens no populārākajiem un atpazītākajiem.



3.9 att. **TP-Link grafiskais interfeiss**

Pētījumu atvieglo arī tas, ka ražotājs ir pacenties, un savā mājaslapā izveidoja maršrutētāju grafisko interfeisu emulatorus, pat balstoties uz dzelžu versiju. Tāpēc pētāmā modeļa grafiskie interfeisi ir pieejami četrās versijās (V1, V2, V4, V5). Links uz šī modeļa emulatoriem pieejams atsaucē [14].

Ražotājs ir izvēlējies vertikālu galvenās izvēlnes izvietojumu, un jebkura no konfigurācijas lapām nāk kopā ar iebūvētu rokasgrāmatu, kas atrodas pa labi no konfigurācijas loga, kas atvieglo katra konfigurācijas parametra saprašanu (sk. 3.9 att.).

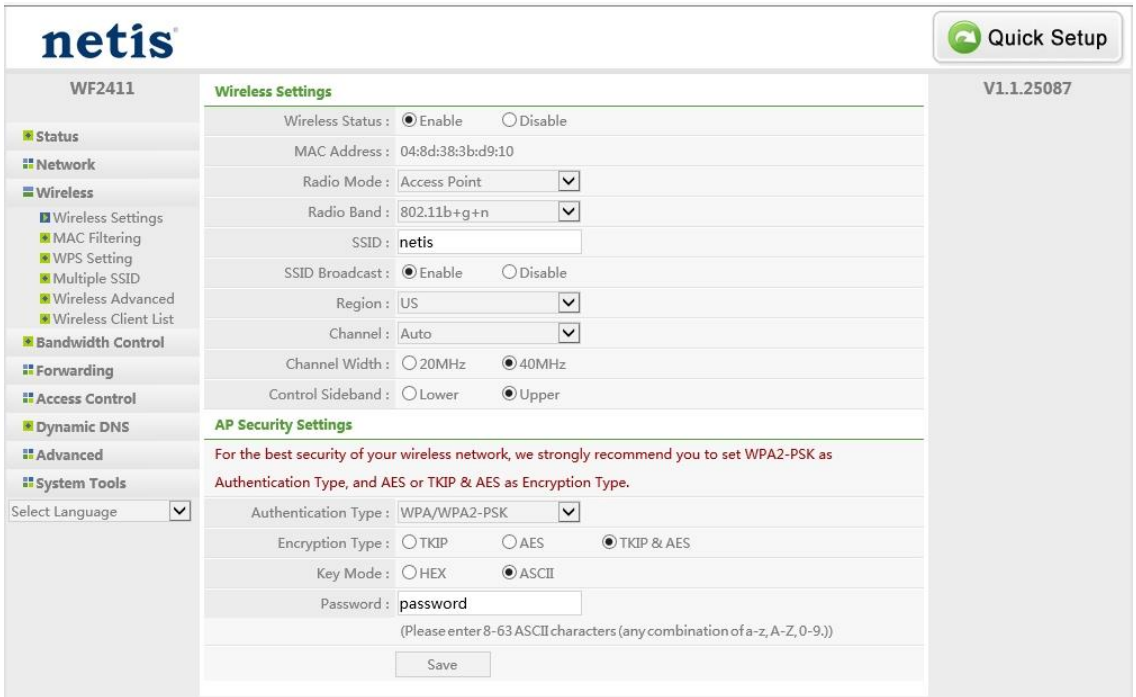
Sākot ar V4 programmatūras versiju, ražotājs ir pārvietojis ”WPA/WPA2-Personal” sadaļu augstāk par ”WEP” un ”WPA/WPA2 – Enterprise”, kā arī pievienoja iekavās to, ka WPA/WPA2 ir rekomendējams.

Ir pieejams arī ērts ātrās maršrutētāja konfigurācijas logs, kurā lietotājam lūdz ievadīt tikai visu nepieciešamāko: datus par interneta pakalpojumu sniedzēju (IP adresi, masku, vārteju, DNS serverus), bet nākamajā logā – bezvadu tīkla iestatījumus, kur pēc noklusējuma ir uzstādīts neizmantot paroli un nekādas rekomendācijas netiek sniegtas par to, ka drošāk ir izmantot WPA2 šifrēšanu.

Grafiskā konfigurācijas interfeisa valodas izvēle nav pieejama, tāpēc lietotājam ir obligāti jāzin angļu valoda, lai varētu to nokonfigurēt.

3.2.2 Netis WF2411 grafiskais interfeiss

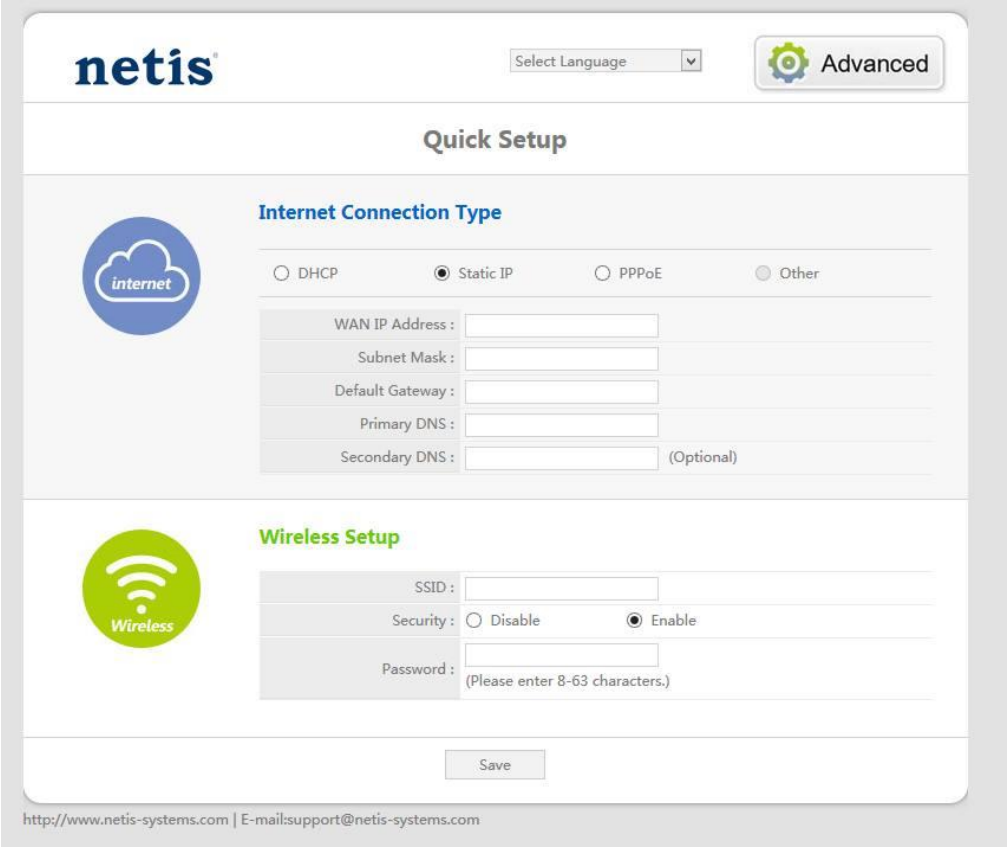
Netis maršrutētāja grafiskais interfeiss pēc struktūras līdzinās TP-Link interfeisiem.



3.10 att. **Netis sarežģītais grafiskais interfeiss**

Vienīgā lielā atšķirība – ražotājs nav padomājis par to, ka lietotājs var būt nepieredzējis, tāpēc interfeisā pilnīgi nav nekādas rokasgrāmatas un palīdzības par konfigurāciju, neskaitot jau ierasto ātrās konfigurācijas izvēlni.

Tā gan ir ļoti saprotama un elementāra. Un ja lietotājam ir vajadzīgais tikai standarta funkciju komplekts, pārejot uz maršrutētāja konfigurācijas mājaslapu (jeb http://192.168.1.1/), to sagaidīs ļoti elementārs interfeiss, un tikai pēc pāriešanas "progresīvajā" izvēlnē tiks parādīta galvenā maršrutētāja izvēlne. Papildus tam, šī izvēlne parādās vienkārši pārejot uz konfigurācijas mājaslapu, tāpēc nav jāspiež vai jāmeklē ātrās konfigurācijas izvēlne, kā tā ir jādara citu maršrutētāju ražotāju grafiskajos konfigurācijas interfeisos (sk. 3.11 att.).



3.11 att. **Netis standarta interfeiss**

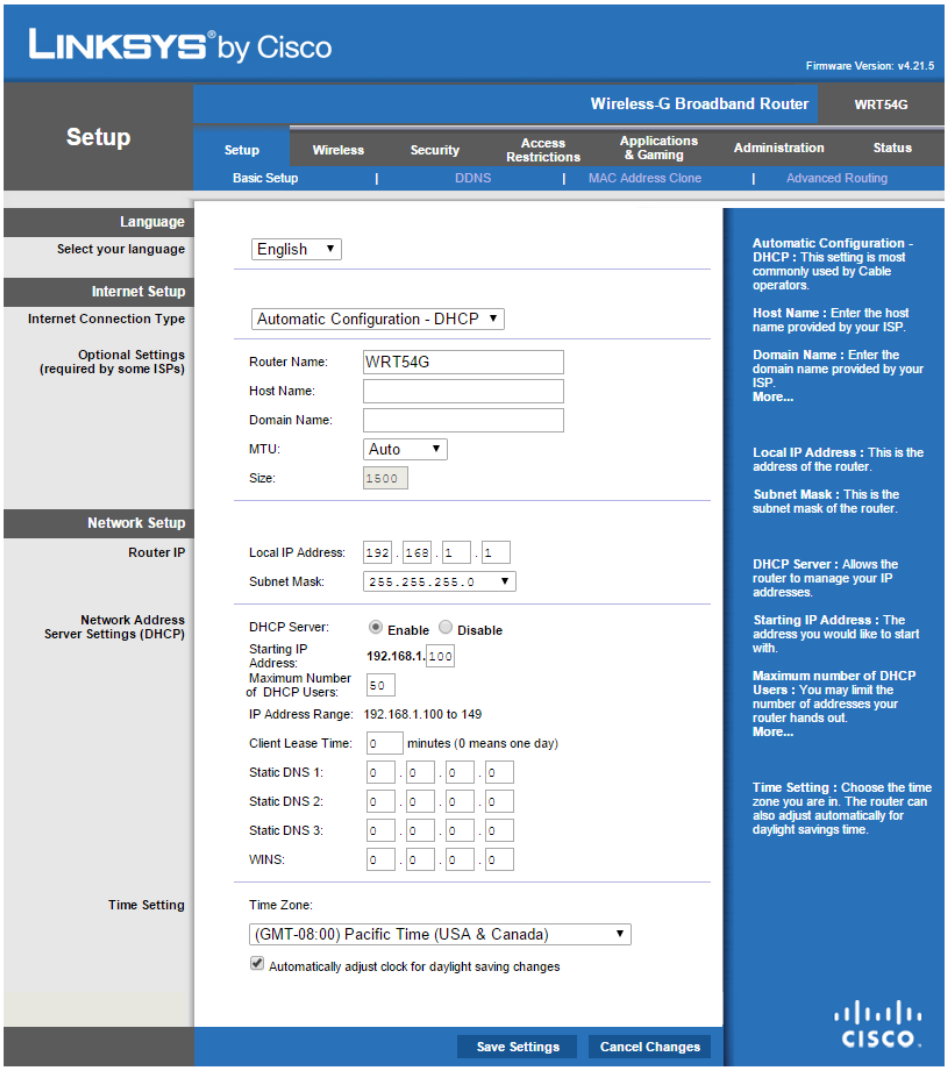
Balstoties uz to, ka lielākā daļa šāda maršrutētāja pircēju izmantos tikai pamata funkcionalitāti, šāds konfigurācijas logs ir ļoti pārdomāta izvēle no ražotāja puses. Tomēr, tiklīdz lietotājam būs vajadzīga papildus funkcionalitāte – izvēlnē tam nebūs pieejami palīdzības logi, jo tādi šeit vienkārši neeksistē.

Bezvadu tīkla konfigurācijas logs neparedz aizsardzības protokola izvēli – tas pēc noklusējuma ir WPA2. Bet ir iespējams izvēlēties arī to, ka maršrutētāja bezvadu tīkls būs bez paroles. Arī, pārejot uz galveno konfigurācijas lapu, bezvadu tīkla sadaļā ir minēts, ka ražotājs iesaka izvēlēties WPA2 protokolu.

Papildus tam, jebkurā izvēlnē ir pieejama valodas maiņa, kurā ir pieejamas 12 populārākās pasaules valodas.

3.2.3 Linksys-Cisco WRT54G grafiskais interfeiss

Linksys-Cisco modeļu tīmekļa interfeiss jau nemainās vairāk nekā 10 gadus. Ražotājs pieturās pie unificēta interfeisa visos savos produktos, tādējādi atvieglojot darbu ar to konfigurāciju dažādos produktos. Interfeiss katrā no konfigurācijas logiem satur gan rokasgrāmatu, gan aprakstus lielākajai daļai no konfigurācijas parametriem, kurš atveras atsevišķā logā. Atverot konfigurācijas interfeisa mājaslapu (http://192.168.1.1/) ir jāpiemin, ka parādās ātrais maršrutētāja konfigurācijas interfeiss, bet tajā nav neviena uzsvara uz bezvadu tīklu. Tā ir jākonfigurē atsevišķi, pārejot uz "Wireless" nodaļu.



3.12 att. **Linksys WRT54G konfigurācijas interfeiss**

Nodaļā "Wireless", veicot bezvadu tīkla aizsardzības konfigurāciju, ražotājs A4 lapas lielā palīdzības logā, visu bezvadu protokolu aprakstā nemin to, ka visdrošāk ir izmantot WPA2.

Diemžēl, tāpat kā TP-Link maršrutētāju interfeisos, valodas izvēle nav pieejama, un konfigurācijas interfeiss ir tikai angļu valodā, kas var apgrūtināt konfigurāciju lietotājiem, kuri nezina angļu valodu.

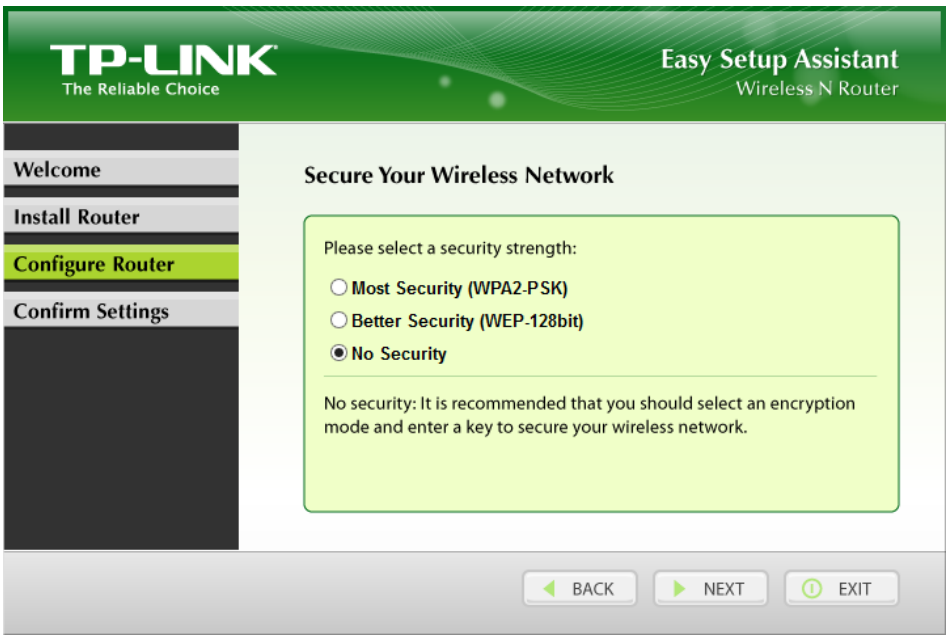
Kā arī lielākajai daļai no maršrutētājiem, ražotājs nav parūpējies par to, lai piedāvātu lietotājam nomainīt noklusējuma administratora konta paroli.

Kā izrādījās vēlāk, veicot maršrutētāja programmatūras atjauninājumu līdz pēdējai pieejamajai versijai, valodas izvēlnē parādās ar sešām valodām.

3.2.4 CD diska konfigurācijas interfeiss

Uz darba uzrakstīšanas brīdi autoram bija pieejams tikai viens CD konfigurācijas disks, kurš piederēja TP-Link ražotāja TL-WR740N modelim. Tā kā šis modelis ir viens no izplatītākajiem un lētākajiem 2.4Ghz 150 megabitu maršrutētājiem tirgū, autors uz tā notestēs, cik viegli ar to ir konfigurēt un kā pietrūkst konfigurācijas programmatūrā.

Veicot šo pētījumu, autors ir nolēmis nosimulēt standarta pircēja situāciju. Personas dators, kurš ir pieslēgts pie interneta ar kabeļa palīdzību, un statiskām IP adresēm ir nopircis šādu maršrutētāju un sekojis instrukcijai – palaist programmatūru, kas ir uz CD diska, un sekot tālākām norādēm.



3.13 att. **CD grafiskais interfeiss – bezvadu aizsardzība**

Pat ja uz datora tīkla kartes iepriekš tika nokonfigurētas statiskās IP adreses, programmatūra pamainīs konfigurāciju uz automātisko IP adrešu saņemšanu, lai dators varētu saņemt dinamiskās IP adreses no maršrutētāja.

Pēc pilnas maršrutētāja konfigurācijas, izmantojot maršrutētāja komplektācijā iekļauto CD disku, kas ir domāts, lai nevajadzētu izmantot tīmekļa bāzētu konfigurācijas interfeisu, ir jāsecina, ka šādai konfigurācijai arī ir savi trūkumi:

- Netiek piedāvāts nomainīt administratora paroli, ar kuras palīdzību ir iespējams tikt tīmekļa bāzētajā grafiskajā konfigurācijas interfeisā.
- Veicot bezvadu tīkla aizsardzības konfigurāciju pēc noklusējuma piedāvā izvēlēties ierakstu "No Security", kas nozīmē neizmantot WPA2 aizsardzību. Kaut gan tie tiek piedāvāti un rekomendējamais ir WPA2 un tas tiek rekomendēts (sk. 3.13 att.).
- Netiek piedāvāts izvēlēties valsti, kurā tiek konfigurēts maršrutētājs. Pēc konfigurācijas beigām tika pārbaudīta valsts, kas izrādījās, pēc noklusējuma ir ASV.

Tātad, CD disks, kas nāk komplektā ar maršrutētāju, spēj tikai veikt pamata maršrutētāja konfigurāciju, kas, protams, nav ļoti pareizi. Ja jau tiek veidota šāda veida konfigurācijas iespēja, ražotājam būtu jāpiedāvā nokonfigurēt pilnīgi visu nepieciešamo, kas ir svarīgs, maršrutētāju konfigurācijā, nevis tikai pamata iestatījumus.

3.3 Novecojušu maršrutētāju un protokolu trūkumi

Apakšnodaļā tiks apkopota informācija par novecojušajiem protokoliem un funkcionalitāti, no kuru izmantošanas ir ieteicams izvairīties. Šāda veida trūkumi pārsvarā ir iespējami, ja maršrutētājs ir salīdzinoši vecs. Tomēr, arī jaunajiem maršrutētājiem ir pieejama šāda funkcionalitāte. Ražotāji to dara tādēļ, lai mēģinātu atstāt atpakaļ saderību (backward compatible) ar vecākām bezvadu ierīcēm. Galvenie šādi trūkumi ir:

- WEP drošības protokols.
- WPA drošības protokols.
- Ilgtermiņā netiek piedāvātas programmatūras atjauninājumu iespējas – nozīmē, ka, ja tiks konstatēta kāda no maršrutētāja programmatūras ievainojamība – ražotājs neizveidos atjauninājumu, lai šo problēmu novērstu, jo produktam ir beidzies atbalsta termiņš.
- Ja maršrutētājs ir samērā vecs, tā īpašniekam, iespējams, nebūs pieejamas pēdējās no parādītām mūsdienu maršrutētājos funkcionalitātēm, piemēram, tādiem kā viesu bezvadu tīkli.

- Ir iespējams arī tas, ka vecākajos maršrutētājos nebūs pieejama visa iespējamā ugunsmūra funkcionalitāte, filtrācijas iespējas vai arī vecāku kontroles rīks, kas jaunajiem maršrutētājiem ir pieejama.

3.4 Publiskais pētījums: Rīgas iedzīvotāju bezvadu piekļuves punktu drošība

Pētījums ir vērsts uz to, lai pārbaudītu, cik daudz Rīgā maršrutētāju izmanto novecojušos bezvadu tīkla protokolus vai arī neizmanto tos vispār. Pētījums pārsvarā tiks veikts atsevišķos Rīgas mikrorajonos, tādējādi veicot analīzi tieši starp mājas bezvadu maršrutētāju segmentu.

Pētījumam tiks izmantota maza izmēra brīvi pieejamā programmatūra WirelessNetView 1.52, ar kuras palīdzību ir iespējams tiešsaistes režīmā skenēt un saglabāt datus par bezvadu tīkliem, kuri atrodas bezvadu adaptera tuvumā. Tālāk visus saglabātos datus ir iespējams eksportēt HTML tabulā.

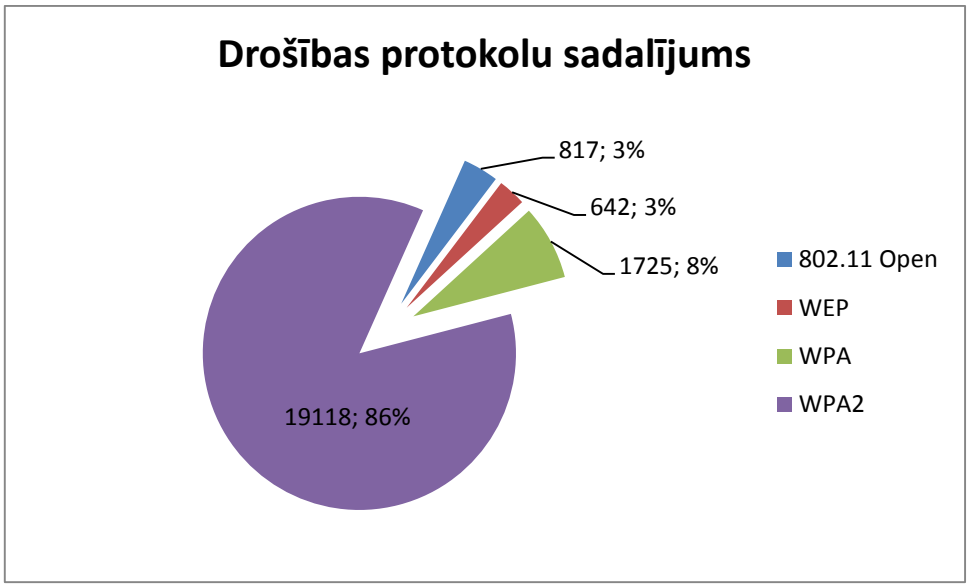
Lai varētu saņemt vairāk informācijas par bezvadu tīkliem, tika iegādāts USB „High gain" bezvadu adapteris (TP Link TL-WN722NC), kuram tika nomainīta antena no 4dBi uz 5dBi. Adapteris tika uzstādīts uz automašīnas jumta, bet portatīvais dators tika pieslēgts pie elektrības, izmantojot 220 voltu pārveidotāju. Apmēram trīs stundu braucienā cauri Rīgas mikrorajoniem un galvenajiem ceļiem ir izdevies iegūt informāciju par vairāk nekā 23 tūkstošiem bezvadu piekļuves punktiem, kas, protams, sastāda ne vairāk par 10% no Rīgas kopējā piekļuves punktu skaita.

Pēc filtrācijas un lielākās daļas publiski pieejamo piekļuves punktu dzēšanas no statistikas, tādu kā Lattelecom bezmaksas piekļuves punkti, lielāko universitāšu bezvadu piekļuves punkti, kafejnīcu utt., ir iespējams secināt, ka mājas bezvadu maršrutētāji ir nokonfigurēti dažādos veidos:

- Pilnīgi nenokonfigurēti un darbojas ar standarta iestatījumiem
- Daļēji nokonfigurēti, bet nav nokonfigurēti bezvadu tīkla drošības iestatījumi (iespējams, daļa no šiem piekļuves punktiem ir publiskie interneta piekļuves punkti)
- Nokonfigurēti ar novecojušajiem bezvadu tīkla iestatījumiem, tādiem kā WEP vai WPA
- Pareizi nokonfigurēti, izmantojot WPA2 vai citus mūsdienu risinājumu veidus

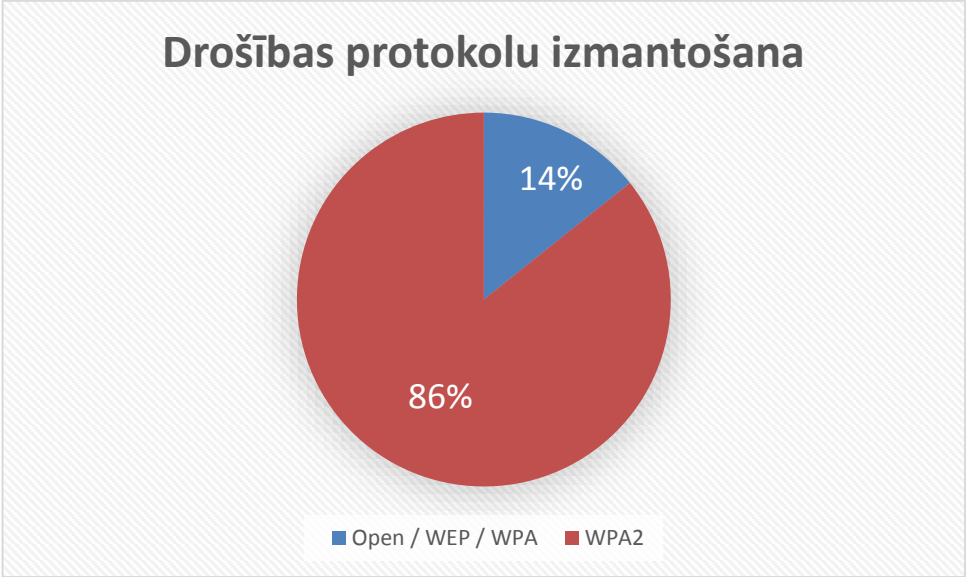
Kopējais aktuālais skaits ar savāktiem piekļuves punktu datiem, pēc atlasīšanas, sastāda 22302 piekļuves punkti.

Grafiks 3.1 parāda procentuālo sadalījumu starp drošības protokoliem.



3.1 grafiks. **Drošības protokolu izmantošanas sadalījums**

Veicot tālāku analīzi, tika izpētīts cik daudz maršrutētāju ir nenokonfigurēti vispār vai izmanto novecojušās metodes.



3.2 grafiks. **Drošu un nedrošu drošības protokolu sadalījums**

Tie ir veseli **14%** no visiem statistikā eksistējošajiem bezvadu piekļuves punktiem, jeb 3184 no kopumā 22302 piekļuves punktiem! Grafiks 3.2 parāda procentuālo sadalījumu starp šāda veida piekļuves punktiem.

Veicot bezvadu piekļuves punktu saraksta izpēti, ir jāpiemin vispopulārākie, neaizsargātie bezvadu tīklu nosaukumi:

- ASUS
- default
- DD-WRT
- TP-LINK_XXXXXX (kur "XXXXXX" ir pēdējie bezvadu tīkla interfeisa MAC adreses simboli).
- Tenda, TENDA_XXXXXX (kur "XXXXXX" ir pēdējie bezvadu tīkla interfeisa MAC adreses simboli).
- airlive
- DIR-300, DIR-600
- dlink
- linksys
- Zyxel

Visi šāda veida nosaukumi, pārsvarā nozīmē tikai to, ka to īpašnieki, pieslēdzot pie maršrutētāja interneta vadu, un ja interneta pakalpojumu sniedzējs izmanto DHCP serveri, lai izdalītu IP adreses tīklā, neturpina konfigurāciju pēc tam, kad internets kļūst pieejams.

Secinot visu apakšnodaļā pieminēto, ir iespējams droši apgalvot, ka mūsdienu Rīgas iedzīvotāji ne visi ir parūpējušies par to, lai aizsargātu savu bezvadu tīklu. Tas var nozīmēt arī to, ka šādai darbībai ir daži cēloņi, nevis viens. Tā varētu būt cilvēku nevēlēšanās to darīt, neprašana vai arī slikti izveidots bezvadu maršrutētāja grafiskais konfigurēšanas interfeiss.

Ētisku apsvērumu un ļoti lielas tabulas izmēra dēļ, bezvadu tīkla piekļuves punktu saraksts, kas iegūts šī pētījuma laikā, netiek pievienots pielikumam.

3.5 Kā var attālināti izvest no ierindas bezvadu maršrutētāju

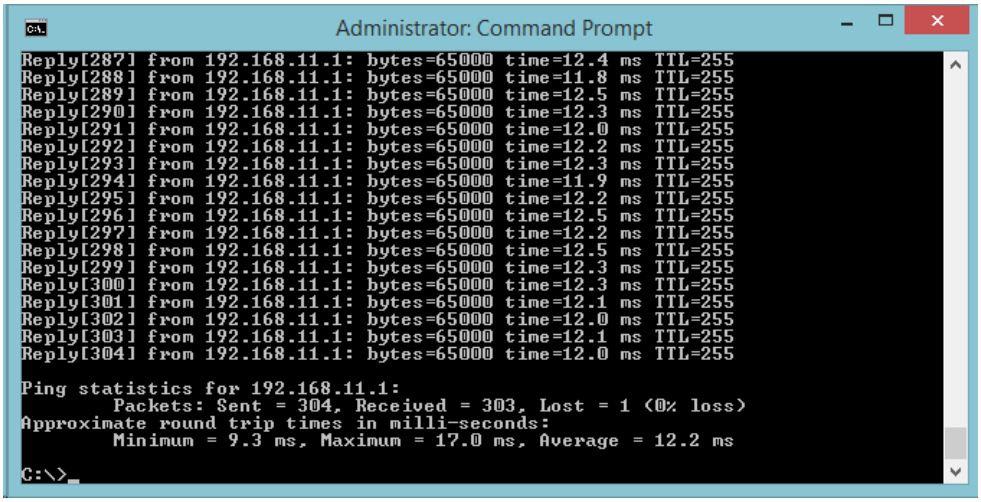
3.5.1 Ping Flood

Jau ar parastu PING-flood programmatūru, veicot ICMP PING pieprasījumus no diviem datoriem, testa Netis WF2411 maršrutētājs ir sācis izlaist 10-30% (no lokālā tīkla) PING pieprasījumiem, bet no ārējā tīkla vairāk uz 50% pieprasījumu netika atbildēts un tas ļoti grūti

spējis atvērt savu tīmekļa bāzētu interfeisu. Kā arī, maršrutētāja grafiskais interfeiss uzrādījis 100% maršrutētāja procesora noslodzi. Šāda veida darbība tika novērota arī ar citu ražotāju maršrutētājiem.

Izmantotā programmatūra: fping.exe

Komandrinda: fping 192.168.11.1 –c –s 65000 –t



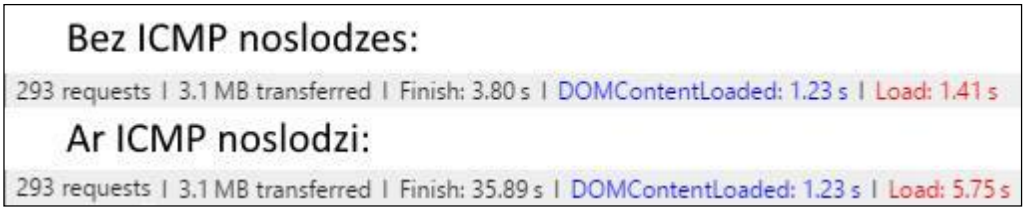
3.14 att. **Fping izmantošana, veicot pieprasījumus no viena datora**

Šāda komanda veic ātru liela izmēra ICMP pakešu izsūtīšanu, tādējādi mēģinot noslogot maršrutētāja iekšējo procesoru, jo tam ir jāapstrādā liels pakešu pieprasījumu skaits, un uz katru no pieprasījuma ir jāatbild.

Veicot lielāku izpēti, pēc 3 datoru pieslēgšanas lokālajā tīklā un ar tiem veicot augstākminēto ICMP pieprasījumu sūtīšanu maršrutētājiem, interneta izmantošana kļuvusi daudz lēnāka vai pat apgrūtinoša, nekā bez ICMP pakešu izsūtīšanas.

Tika veikti arī pakešu sūtīšana kombinēti – gan no datoriem, kas pieslēgti pie LAN portiem, gan no datoriem, kuri pieslēgti pie bezvadu tīkla – rezultāts bija līdzīgs. Izskatās, ka bezvadu tīkla apstrādei tomēr procesors velta vairāk laika un ICMP pieprasījumi bezvadu tīklā parādās ar ļoti lielām aizturēm, bet pārslodzes brīžos – pilnībā pārstāj atbildēt.

Veicot šo pētījumu, autors ir pamēģinājis salīdzināt mājaslapu ielādes laikus. Attēls 3.15 uzrāda maršrutētāja Netis WF2419 ielādes laikus ar un bez noslodzes. Pārbaudei tika izmantots pārlūkprogrammas Google Chrome nodaļas ”Developer Tools” testēšanas rīku “Network”, kas veic tīmekļa lapu ielādes testus.



3.15 att. **www.delfi.lv mājaslapas ielādes laiks, ar ICMP noslodzi un bez tās**

Pēc visu pieejamo autoram maršrutētāju izpētīšanas, ir iespējams veikt secinājumus, balstoties uz maršrutētāju darbību, kuri saņem lielu daudzumu ICMP pieprasījumu:

- Divi no maršrutētājiem – LevelOne WBR-6005 un TP-Link TL-WR340G – pēc dienas testiem ir pilnībā pārstājuši darboties, un pat pēc ICMP pieprasījumu sūtīšanas pārtraukšanas nespēja normāli darboties. Tie neatbildēja ne uz parastajiem PING pieprasījumiem, ne deva DHCP IP adresi pievienojot kādu jaunu ierīci lokālā tīkla portiem, nevarēja dot ierīcēm pieeju internetam, kā arī nevarēja atspoguļot savas grafiskās konfigurācijas mājaslapas. Pārtraukt šādu stāvokli maršrutētājiem bija iespējams tikai atslēdzot tiem elektrības padevi, un pēc brīža to atkal pieslēdzot, tādējādi tos pārstartējot.
- Lielākā daļa no maršrutētājiem, nespējot apstrādāt visu pakešu plūsmu, ir sākuši mest (drop) saņemtās paketes, uz tām neatbildot, tādējādi pasargājot procesoru no pārslodzes. Pakešu zudumi maršrutētājiem sastādīja no 5% līdz 80%, atkarībā no noslodzes un pakešu daudzuma, kuri tika tam sūtīti. Visvecākais maršrutētājs TP-Link TL-WR340G pat ar viena datora pieslēgumu jau nevarēja atbildēt uz visām ICMP paketēm.
- Tikai viens no visiem testējamiem maršrutētājiem – Cisco-Linksys E2500, iespējams, vispareizāk ir veicis lielas pakešu plūsmas apstrādi. Kā autoram licies, tas ir veicis tikai ICMP pakešu mešanu (drop), tādējādi arī pasargājot procesoru no pārslodzes, tomēr tā darbība ar internetu un maršrutētāja grafisko konfigurācijas interfeisu netika skarta un nebija jūtamas aiztures. Iespējams, šāda darbība ir saistīta ar to, ka maršrutētājs ir dārgākais no visiem testējamiem maršrutētājiem un vienīgais, kurš atbalstīja 5GHz tīklu, tādējādi tā procesora arhitektūra vai programmatūra ir vairāk piesardzīga pret šāda veida darbībām.

3.5.2 Switch loop

Pieslēdzot patch vada abus galus pie maršrutētāja LAN portiem ir iespējams pilnīgi vai daļēji izvest no ierindas bezvadu maršrutētāju. Lielākajai daļai testēto maršrutētāju tika pilnīgi nesasniedzams internets, kā arī konfigurācijas tīmekļa interfeiss.

Bija arī gadījumi, kad maršrutētājs nespēja sniegt internetu, bet konfigurācijas tīmekļa interfeiss bija pieejams.

Šāds eksperiments, protams, paredz iespēju tikt pie maršrutētāja LAN portiem, bet ir arī variants, piemēram, kad ir pieejams tikai vads vai arī rozete, kura ir pieslēgta pie maršrutētāja. Tad, šādu eksperimentu arī var atkārtot, izveidojot speciālu patch vadu, kura 1 un 2 dzīsla ir savienota ar 3 un 6 dzīslu, tādējādi visus saņemtos datus pārsūtot uz izsūtītām dzīslām.

Ņemot vērā dažādas infrastruktūras, ir iespējami gadījumi, kad paši lietotāji var izveidot aprakstīto apakšnodaļā gadījumu, tādējādi paralizējot visu lokālo tīklu, ja vien tīkls netiek būvēts jau ar komutatoriem, kuri atbalsta „Loop detection" funkcionalitāti, kura spēj identificēt portus, uz kuriem šāds gadījums darbojas, un tos nobloķēt.

3.6 Cik nedrošs "tikko-no-iepakojuma" maršrutētājs.

Ņemot vērā statistikas datus no apakšnodaļas 3.4, ir iespējams secināt, ka maršrutētāji, kuri ir izņemti, tikko no iepakojuma, ir pakļauti riskam, ka tie netiks nokonfigurēti.

Interneta pakalpojumu sniedzēji, kuri savā tīklā izmanto DHCP serveri IP adrešu izdalīšanai, nevis statiskās IP, kuras jāievada klientam ar roku savā maršrutētājā, ir pakļauti riskam, ka to klients, nopērkot jaunu maršrutētāju un, pieslēdzot to, interneta tīklam nerūpējas par to, ka maršrutētājs tiks pareizi nokonfigurēts.

Veicot šo pētījumu ar desmit dažādu ražotāju maršrutētājiem ir iespējams izveidot sarakstu ar statistiku:

- 6 no 10 maršrutētāju bezvadu tīkliem pēc noklusējuma nav uzstādīta WPA2 drošības parole.
- 8 no 10 maršrutētājiem nav uzstādīta parole administratora kontam vai arī tā ir viegli uzminama. Tikai divi no testējamiem maršrutētājiem, pirmo reizi pieslēdzoties maršrutētāja grafiskajam interfeisam, palūdza šo paroli nomainīt.

3.16 att. **Netis WF2411 ražotāja maršrutētāja uzlīme ar bezvadu tīkla SSID un tā paroli [15]**

Labi šajā pētījumā sevi ir parādījis Netis WF2411 maršrutētājs, kurš gan nesaturēja pēc noklusējuma administratora konta paroli, tomēr, tā bezvadu tīkla parole bija grūti uzminama, jo saturēja frāzi ar burtiem(sk. 3.16 att.). Tas nozīmē to, ka pat ja lietotājs nebūs vispārībā konfigurējis maršrutētāju, ir mazāka iespēja, ka kāds no ļaundariem varēs viegli to uzminēt.

3.7 DHCP servera darbība un IP adreses izdalīšana WAN portā

Ņemot vērā to, ka autors ir sastapies ar gadījumiem, kad bezvadu maršrutētāju DHCP serveris ir dalījis IP adreses WAN tīkla portā, autors centīsies veikt pētījumu, kas pārbaudīs vai to ir iespējams izveidot laboratorijas apstākļos. Diemžēl neviens no pieejamiem autoram maršrutētājiem uz darba uzrakstīšanas brīdi nedalīja DHCP IP adreses globālajā tīklā, tāpēc pierādīt šo teoriju nav sanācis.

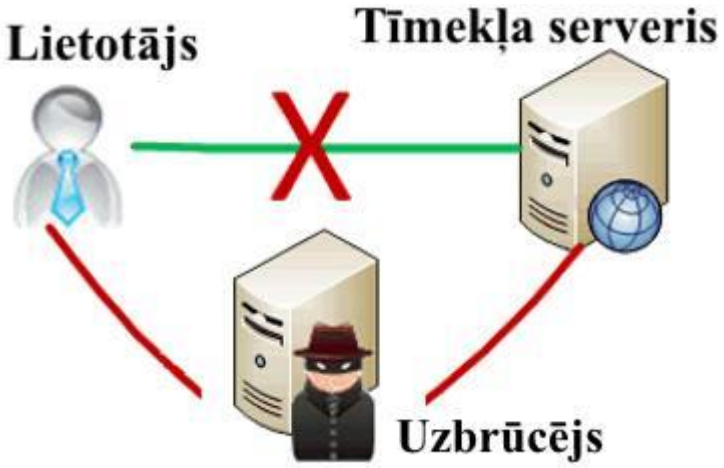
Tomēr, autors grib pieminēt to, ka ir redzējis šādu darbību, savas darba pieredzes laikā.

3.8 „Man in the middle" uzbrukuma pielietojums

Pētījumi 3.1 un 3.4 parāda to, ka gan maršrutētāji satur dažādas ievainojamības, gan maršrutētāju īpašnieki ne vienmēr pareizi vai arī vispār neaizsargā savus bezvadu tīklus. Balstoties uz tiem, autors ir nolēmis pārbaudīt – cik tad ir grūti veikt datu pārķeršanu neaizsargātā bezvadu tīklā, izmantojot „Man in the middle" uzbrukuma veidu. Ņemot vērā to, ka šāds uzbrukums ir, pārsvarā, pielietojams kustīgos apstākļos, autors nolēmis izmantot par

piemēru planšetdatoru kā ierīci, ar kuras palīdzību būs iespējams veikt lietotāju datu pārķeršanu, kas ir pieslēgti, piemēram, pie neaizsargāta bezvadu tīkla un izmanto internetu.

Šāda veida uzbrukums, būtībā, ļaundara ierīci nostāda starp lietotāju un maršrutētāju, tāpēc ierīce ir spējīga pārķert datus no lietotāja datora vai ierīces (sk. 3.17 att.).

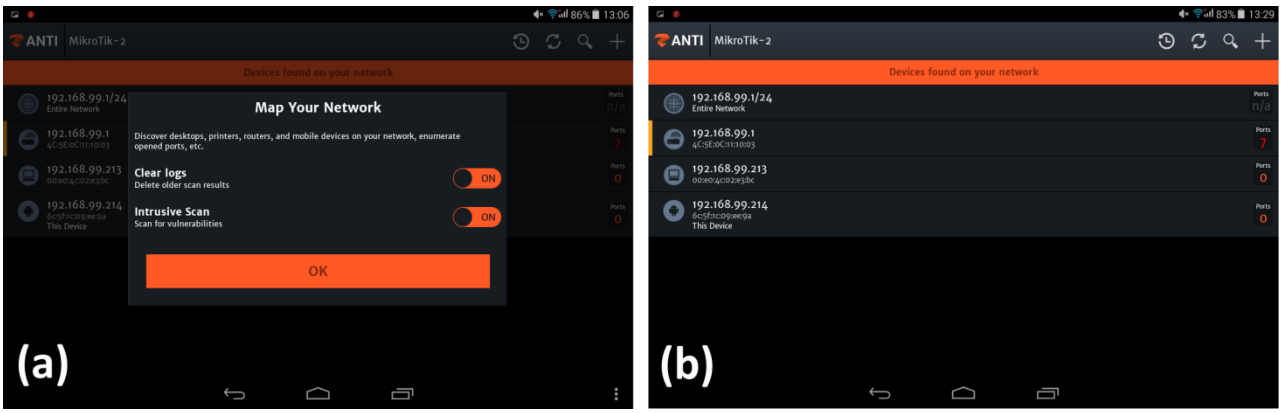


3.17 att. **„Man In The Middle" uzbrukuma attēlojums[16]**

Viss kas ļaundarim ir nepieciešams ir Android planšetdators ar uz tā aktivētām root privilēģijām. Mūsdienās, gandrīz katrai Android ierīcei to ir iespējams uzstādīt, tāpēc tā, pat parastam lietotājam nevajadzētu būt problēma, jo internetā ir pieejamas daudz un dažādas instrukcijas, kas soli-pa-solim ļaus to uzstādīt. Root tiesību uzstādīšana autora Lenovo Yoga 8 planšetdatorā ir aizņēmusi 20 minūtes. Pēc root tiesību saņemšanas, atliek tikai uzstādīt programmatūru, ar kuras palīdzību tiks veikts uzbrukums.

Mūsu gadījumā šī programmatūra ir zANTI2. Programmatūra ir brīvi pieejama internetā, kas ir uzstādāma viena klikšķa laikā, un domāta, lai jebkurš cilvēks varētu pārbaudīt, cik drošs ir viņa datortīkls. Pārsvarā, šāda veida programmatūru, tomēr, lieto IT speciālisti un dažāda veida testētāji. Bet tas nenozīmē to, ka to nevar lietot ļauniem mērķiem. Tās pielietojums ir ļoti plašs: tā veic atvērtu portu skenēšanu, skenē un pārbauda tīkla iekārtas un datorus uz zināmām programmatūras ievainojamībām, kā arī veic jau augstākminēto „Man in the middle" uzbrukumu.

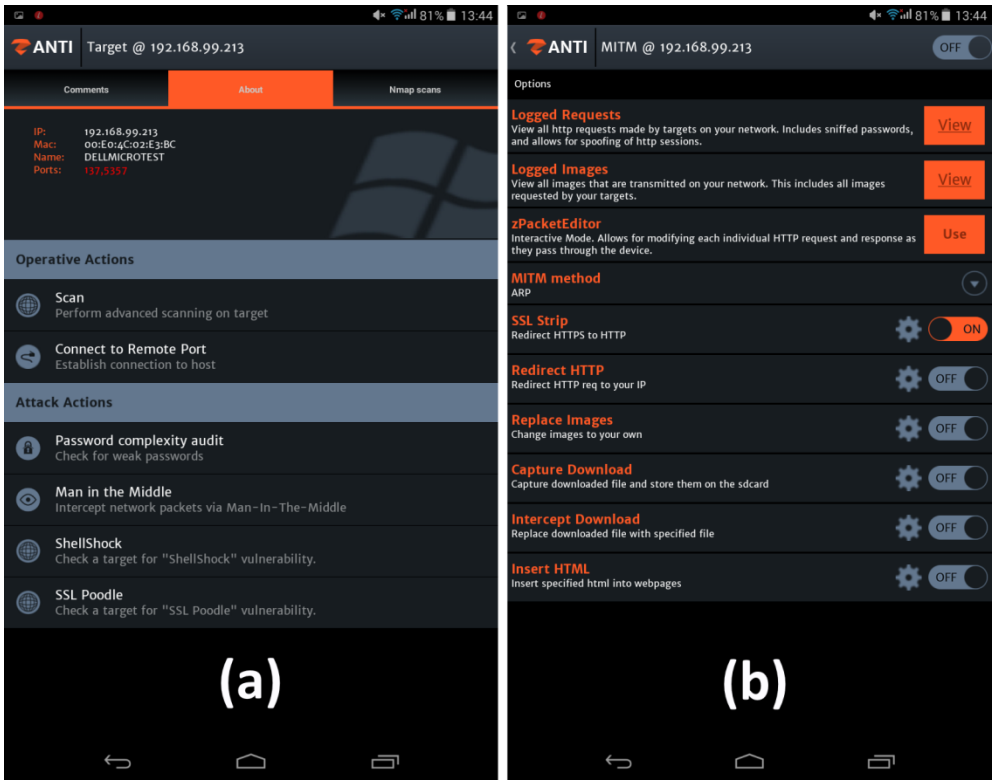
Pēc zANTI2 uzstādīšanas uz planšetdatora, ir jāpieslēdzas pie izvēlētā bezvadu tīkla, pēc kā tiks piedāvāts noskenēt visu bezvadu tīklu un atrast visas pie tā pieslēgtas ierīces, ievainojamības utt.



3.18 att. **zANTI2 programmatūra**

(a) Skenēšanas uzsākšana **(b)** Tīkla ierīču saraksts

Pēc bezvadu tīkla skenēšanas ir jāizvēlas no saraksta datora IP adresi, kuras datus vēlamies pārķert un uzspiežam „Man in the Middle" pogu, lai nonāktu pārķeršanas izvēlnē. Izvēlnē tika izvēlēta opcija „SSL Strip", kas veiks HTTPS pāradresāciju uz HTTP, ar kuras palīdzību būs iespējams iegūt vairāk pakešu informācijas.

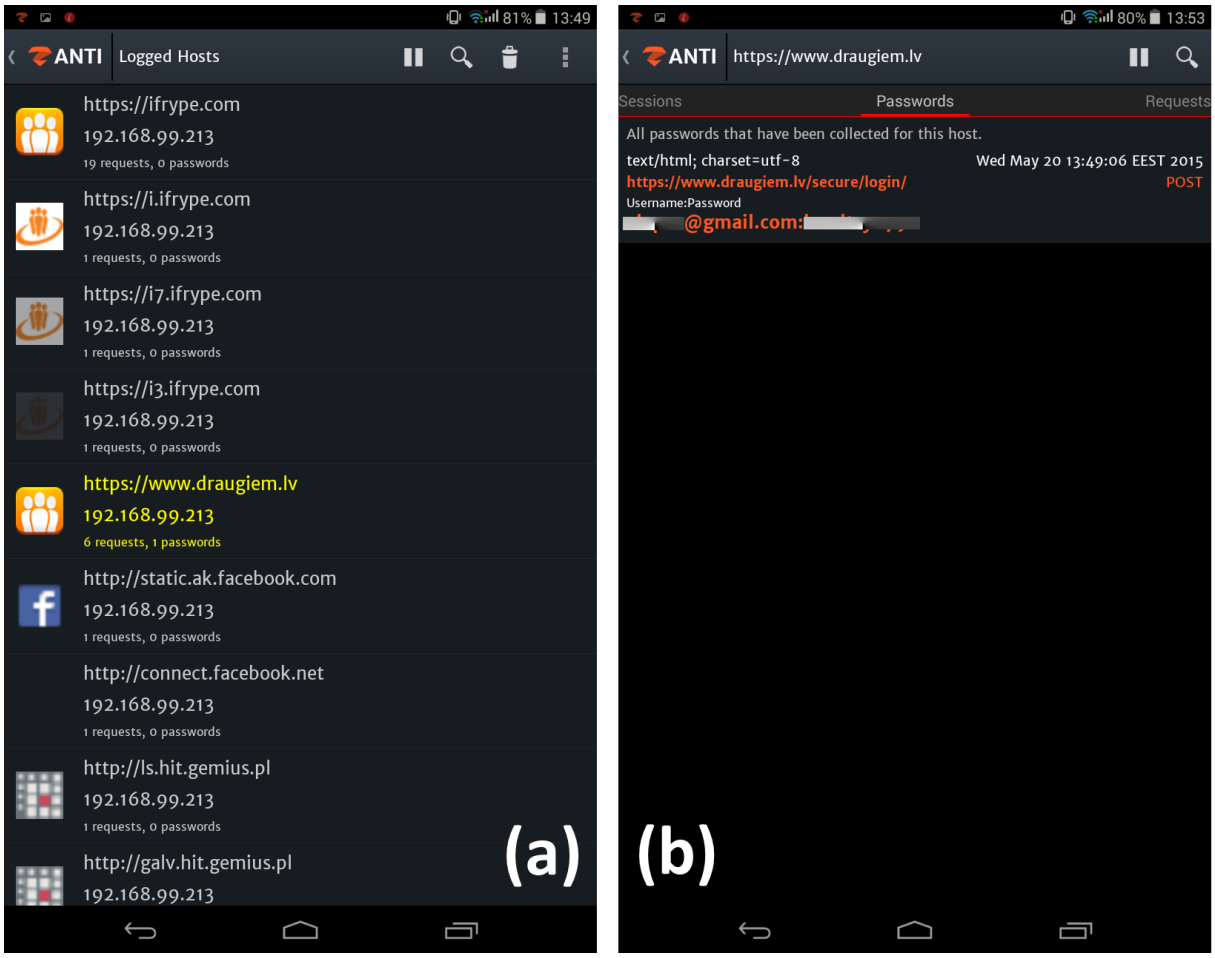


3.19 att. **zANTI2 programmatūra**

(a) Iespējas, izvēloties ierīci (pēc IP adreses) **(b)** „Man in the middle" izvlēne

Pēc pārķeršanas funkcionalitātes ieslēgšanas, ir jāuzspiež uz „View" pogas, sadaļā „Logged Requests" un jāvēro HTTP pieprasījumi. Ja kāds no pieprasījumiem saturēs Lietotājvārda un paroles kombināciju, programmatūra šo pieprasījumu izdalīs dzeltenā krāsā.

Kā piemēru, autors veica Latvijas lielākā sociālā tīkla autentifikācijas datu pārķeršanu, tādējādi saņemot savā rīcībā lietotājvārdu un paroli, ar kuras palīdzību cilvēks uz portatīvā datora ir ierakstījis www.draugiem.lv mājaslapā.

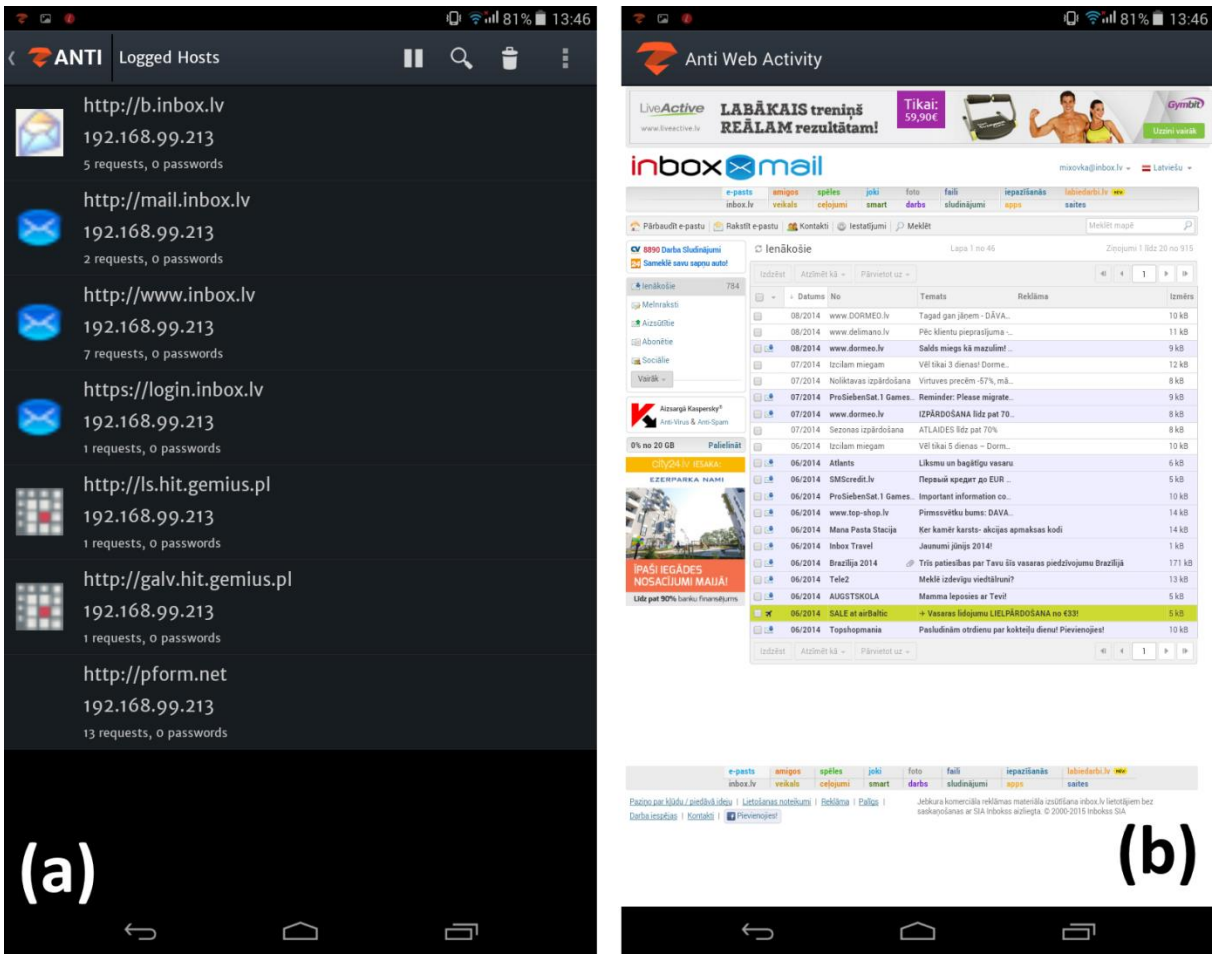


3.20 att. **zANTI2 programmatūra**

(a) draugiem.lv paroles pārķeršana **(b)** draugiem.lv paroles attēlošana

Ar šīs programmatūras palīdzību, paralēli pārķertajiem lietotājvārdiem un parolēm ir iespējams arī novērot portatīvā datora sesiju, pārķerot ”cookie” failus un citus datus.

Veicot šādu identisku darbību ar www.inbox.lv – vienu no lielākajiem Latvijas e-pasta servisa sniedzējiem, paroli pārķert neizdevās, bet lietotāja sesija tika pārķerta un ar programmatūras palīdzību bija iespējams, bez nekādiem ierobežojumiem, lasīt lietotāja e-pastu un veikt visas citas darbības, kuras ir pieejams, kad lietotājs ir pieteicies sistēmā.



3.21 att. **zANTI2 programmatūra**

(a) inbox.lv pakešu pārķeršana **(b)** inbox.lv sesijas pārķeršana, ar iespēju pārskatīt e-pastus

Protams, šāda programmatūra ir noderīga tad, ja ir vēlme pārķert nešifrētus datus, jo HTTPS pieprasījumus tā attēlot nevar. Kaut gan ir zināmi gadījumi, kad bija uzlauzts arī HTTPS[17].

4. PĒTĪJUMU ANALĪZE UN TO SECINĀJUMI

Nodaļā tiks veikta visu pētījumu analīze un tiks mēģināts veikt gan secinājumus par katru pētījumu un tā iespējamām problēmām, gan apkopot kopējās problēmas.

Ņemot vērā pētījumu 3.1, kurā tika pierādīts, ka daļa no bezvadu maršrutētājiem atbild arī no WAN porta ar lokālo IP adresi, tikai ar WAN porta MAC adresi un to, ka interneta pakalpojumu sniedzēju tīklos ir manāmi vairāki desmiti ARP pieprasījumu atbildes no lokālām IP adresēm, iespējams, var minēt to, ka autora bakalaura darba atrastais lokālo IP adrešu konflikts ir saistīts ar pētījumā atrasto problēmu.

No.	Time	Source	Destination	Length	Protocol	Info
106	0.018887000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
107	0.019193000	Tp-LinkT_47:74:f6	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request) (duplicate use of 192.168.0.1 detected!)
108	0.019194000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
109	0.019444000	Tp-LinkT_47:74:f6	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request) (duplicate use of 192.168.0.1 detected!)
110	0.019519000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
111	0.019845000	62.84.0.222	225.1.1.6	1358	YAMI	[Malformed Packet]
112	0.019846000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
113	0.020049000	62.84.0.213	225.6.1.7	1358	YAMI	[Malformed Packet]
114	0.020050000	Tp-LinkT_47:74:f6	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request) (duplicate use of 192.168.0.1 detected!)
115	0.020121000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
116	0.020570000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
117	0.020860000	Tp-LinkT_47:74:f6	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request) (duplicate use of 192.168.0.1 detected!)
118	0.020940000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
119	0.021147000	Tp-LinkT_47:74:f6	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request) (duplicate use of 192.168.0.1 detected!)
120	0.021147000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
121	0.021579000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
122	0.021731000	62.84.0.222	225.1.1.1	1358	YAMI	[Malformed Packet]
123	0.021809000	Tp-LinkT_47:74:f6	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request) (duplicate use of 192.168.0.1 detected!)
124	0.021885000	Tp-LinkT_98:d4:42	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request)
125	0.022203000	Tp-LinkT_47:74:f6	Broadcast	60	ARP	Gratuitous ARP for 192.168.0.1 (Request) (duplicate use of 192.168.0.1 detected!)

4.1 att. **Divu TP-Link maršrutētāju ARP atbilžu konflikts [15]**

Šāda veida konflikti ir reti, bet, iespējams, tiek veidoti, parādoties kādai specifiskai situācijai, piemēram, ja globālajā tīklā tiek izsūtīts kāds liels ARP pieprasījumu daudzums, kas beigās var novest pie šāda liela pakešu daudzuma konflikta, kas būtībā ir vienkārši nevajadzīga tīkla datu plūsma. Interesants liekas arī fakts, ka pētījumā 3.1 neviens no TP-Link bezvadu maršrutētājiem nav atbildējis ar lokālo adresi no WAN porta. No tā var secināt to, ka vai nu ir tikai daļa no maršrutētājiem, kuri atbild no WAN porta, vai arī augstākminētais ir kādas citas situācijas iemesls.

Šāds ARP pieprasījumu konflikts noved arī pie tā, ka komutatoru ARP tabulas nemitīgi mainās. Kopumā, tas viss noved pie ātrdarbības krituma interneta pakalpojumu sniedzēja tīklā. Cik stipri tas ietekmē ātrdarbību ir grūti spriest, un tas ir pārsvarā atkarīgs no tā, cik jaudīgu aparatūru izmanto interneta pakalpojumu sniedzējs savā tīklā.

Diemžēl, ja ICMP PING pieprasījumu atbilžu sūtīšanu ir iespējams nobloķēt, izmantojot maršrutētāja ugunsmūra funkcionalitāti, tad ARP pieprasījumus nobloķēt nav iespējams, jo tie

tiek izmantoti, lai varētu uzzināt MAC adresi, zinot IP adresi un ir neatņemama datortīkla darbības sastāvdaļa.

Apskatot pētījumu 3.1.3 ir jāsecina, ka ARP pieprasījumu atbildes, tomēr, radušās slikti uzrakstītas programmatūras dēļ, jo atjauninot dažu maršrutētāju programmatūru līdz pēdējām versijām, šī problēma pazūd. Dažiem maršrutētājiem, kuriem, izskatās, ka ir beidzies atbalsta termiņš, programmatūras atjauninājumi nav palīdzējuši novērst šo problēmu, bet ir jāņem vērā fakts, ka to pēdējais programmatūras atjauninājums tika izvietots ražotāju mājaslapā 2012. gadā, kad, iespējams, šī problēma vēl netika atrasta.

Pētījums 3.2 parāda to, ka maršrutētāju grafiskie interfeisi dažiem ražotājiem nemainās jau desmitiem gadu un to izpildījums, ergonomika un funkcionalitāte ne vienmēr pietuvinās pie labākajiem variantiem. No tā var secināt, ka, pat gribot, parasti lietotāji, kas nav saistīti ar IT nozari, iespējams, varēs apmaldīties maršrutētāja konfigurācijas logos un kļūdīties veicot to uzstādīšanu savā tīkla infrastruktūrā. Palīdzības logu un valodas izvēles trūkums arī noved pie maršrutētāja nekorektas uzstādīšanas.

Daži no maršrutētāju ražotājiem ar saviem produktiem piedāvā CD disku, ar kuras programmatūras palīdzību būs iespējams vieglāk un pareizāk to nokonfigurēt. Balstoties uz pētījumu 3.2.4 šāds konfigurācijas veids nav pilnīgs un tā interfeisu un izvēlni būtu ražotājiem jālabo.

Pētījums 3.4 pierāda to, ka 3% no maršrutētāju īpašniekiem, kas ir ievākti, apbraucot Rīgas mikrorajonus, pilnībā nenokonfigurē savus maršrutētājus, tāpēc to drošība ir ļoti apdraudētā. Tas ne tikai ļauj citiem brīvi izmantot maršrutētāja piekļuvi internetam, bet arī apdraud pašus maršrutētāja īpašniekus, kad tie sērfo internetā, veic maksājumus utt. Piemēram, ļaundaris, izmantojot neaizsargāto maršrutētāja konfigurācijas interfeisu, var pamainīt konfigurācijā DNS serveru IP sarakstu, kuru izdala DHCP serveris, uz savu, kas var novest pie lietotājvārdu un paroļu nokļūšanai ļaundara rokās. Vēl viens variants ir tas, ka ļaundaris, atrodoties vienā lokālajā tīklā ar maršrutētāja īpašnieka ierīcēm, var pielietot zināmu caurumu ievainojamības, tādējādi gūstot kontroli par konkrētu ierīci. Šāds gadījums ir iespējams, piemēram, ja maršrutētāja īpašnieka datora operētājsistēmai nav uzstādīti pēdējie atjauninājumi. Vai arī ja tīklā atrodas vēl kāda neaizsargāta ierīce, piemēram, tīkla cietais disks. Iespējams arī tas, ka ļaundaris var iegūt informāciju arī, izmantojot kādu no pakešu ķeršanas rīkiem, piemēram, Wireshark.

Tomēr, 3 procenti neliekas tik daudz, lai liktu lasītājam domāt, ka Rīgā ir daudz neaizsargātu bezvadu piekļuves punktu. Bet jāņem vērā tas, ka pat apbraucot visus mikrorajonus ir savākts tikai, pieņemsim, ap 10% no visa kopējā bezvadu piekļuves punktu

skaita, jo bezvadu tīkla karte, ar kuru tika savākta informācija, braucot gar deviņu stāvu ēku, augstāk par 3-4 stāvu jau nevarēja ievākt informāciju par bezvadu piekļuves punktiem, kas atradās augstākajos stāvos.

Ja statistikas datus pareizināt kaut par 10, vai nu vismaz 5 reizēm, kopējā bilde pēc procentiem nemainīsies, bet skaitliski kļūs daudz sliktāka.

Pētījums 3.5.1 parāda, ka maršrutētāji ir ļoti sensitīvi pret lielām pakešu plūsmām. Ņemot vērā to, jāsecina, ka apraides (broadcast) datu plūsma arī ietekmē maršrutētāju darbību.

Apkopojot visu uzrakstīto apakšnodaļā 3.8, ir iespējams veikt secinājumus par to, ka pieslēgšanās publiskiem bezvadu piekļuves punktiem var būt diezgan bīstama un šāda bezvadu tīkla lietotājs pakļauj sevi un savu informāciju riskam. Vai nu tā būtu kāda dienasgrāmatas (bloga) pieslēgšanās, vai e-pasta dati, lietotāja pieslēgšanās citiem portāliem, kuri neizmanto HTTPS vai arī kad nostrādā programmatūras HTTPS uz HTTP pārveidošanas opcija, nodot svešām personām. Protams, interneta banku dati, google kontu dati un citu lielu uzņēmumu vai sociālo tīklu dati tiek labāk aizsargāti un ar apskatītās programmatūras palīdzību nav pārķerami, jo tie neatļauj HTTP izmantošanu pilnībā. Bet, ja autoram, kurš nespecializējas datu pārķeršanā, ir izdevies aprakstītos pētījumā datus iegūt pāris stundu laikā, tad cilvēks, kurš ir šādas nozares speciālists ar to, ka Jūs esat pieslēdzies pie neaizsargāta bezvadu tīkla, varēs izdarīt daudz vairāk par pētījumā apskatītajām situācijām.

5. IETEIKUMU UN REKOMENDĀCIJU APKOPOJUMS

Nodaļā tiks apkopota visa uzkrātā gan maģistra darba ietvaros atrastā informācija, gan papildus rekomendācijas. Ieteikumi un rekomendācijas tiks sadalītas divās apakšnodaļās – vienā tiks apkopotas rekomendācijas, kas būs vajadzīgas maršrutētāju ražotājiem, otrā – kas noderēs datortīklu administratoriem vai arī cilvēkiem, kuri grib nokonfigurēt maršrutētāju paša spēkiem.

5.1 Ieteikumi un rekomendācijas "SOHO" maršrutētāju ražotājiem

- Slikti veidota drošība maršrutētājiem "izņemot no kastes". Risinājums - atslēgt lielāko daļu funkcionalitātes un piedāvāt vieglu un drošu konfigurācijas iespēju, liedzot daļēju maršrutētāja izmantošanu, līdz brīdim, kad tas tiks, pareizi nokonfigurēts.
- CD disku konfigurācijas interfeisu veidot tā, lai tā tiktu skarti visi konfigurācijas parametri, nevis tikai to minimālais apjoms, ar kura palīdzību maršrutētājs varēs darboties. Pēc noklusējuma konfigurācijas parametru izvēli veikt tā, lai lietotājs pamana, ka izvēlas drošāko risinājumu.
- Izslēgt WAN portu pilnībā maršrutētājiem "izņemot no kastes", un slēgt to tikai tad, kad ir pilnībā nokonfigurēts bezvadu tīkls ar visiem drošības elementiem, nomainīta administratora parole.
- Brīdināt lietotāju, kad tas grib izmantot novecojušus bezvadu tīkla aizsardzības standartus.
- Atslēgt WiFi līdz tā pareizai nokonfigurēšanai, vai arī ģenerēt nejaušu paroli katram maršrutētājam, tādējādi tikai maršrutētāja īpašnieks varēs pieslēgties bezvadu tīklam.
- Eiropas modeļiem liegt izmantot ne-Eiropas frekvenci, jeb 2.4Ghz 14 kanālu, tādējādi padarot drošāku bezvadu tīkla izmantošanu. Daži ražotāji, mēģinot unificēt ražošanu, piedāvā lietotājiem pašiem izvēlēties reģionu, kur tika nopirkts maršrutētājs, tādējādi nododot pareiza reģiona izvēles atbildību uz lietotāju.
- Pie katra konfigurācijas parametra uzrādīt atbalsta ("help") logu ar paskaidrojumu, ko dara konkrēts konfigurācijas parametrs, tādējādi samazinot risku tam, ka nekvalificēts lietotājs nepareizi sapratīs specifiski uzrakstīto tekstu.

Ir jāpiekrīt, ka daļēji, aparatūras izstrādātāji ir izveidojuši šādus paskaidrojošus logus, bet tie apraksta tikai populārākos konfigurācijas parametrus.

- Pārsvarā maršrutētāja dizains un to grafiskais konfigurācijas interfeiss visiem ražotājiem izskatās vienveidīgi. Tikai dārgie modeļi tiek parādīti interesantos izpildījumos.
- Pie pirmās pieslēgšanas reizes lūgt nomainīt administratora lietotājvārdu un paroli. Šāda darbība bija pamanāma tikai diviem testa maršrutētājiem – TP-Link TL-WR740N ar OpenWRT programmnodrošinājumu un D-Link DAP-1155 (šajā gadījumā, tikai ar 23.04.2015 v2.5.0 programmatūras atjauninājumu) maršrutētājiem. Tad, pat ja ļaundari atminēs vai uzlauzīs bezvadu tīkla paroli, tie nevarēs veikt izmaiņas maršrutētāja konfigurācijā.
- Pašreizējā situācijā, lietotājiem izmantot lokālajam tīklam ne tik populāras IP adreses, piemēram 10.1.2.1 vai 192.168.32.1. Šo variantu var izmantot arī maršrutētāju izstrādātāji. Iespējams, vislabāk būtu, ja maršrutētājs pats varētu nejauši ģenerēt zem-tīklu.
- "SOHO" maršrutētāju izstrādātājiem veikt analīzi, kāpēc pētījumā 3.1 aprakstītā situācija nostrādā, un izstrādāt programmatūras atjauninājumu visām pakļautām šādam riskam ierīcēm, ja šī pētījuma rezultāts, tomēr, izrādās ar iekšēji darbināmo programmatūru saistīts.
- Vienmēr izsūtīt komūnas reģistrētiem lietotājiem ziņas par maršrutētāju programmatūras atjauninājumiem.
- Mēģināt ieviest maršrutētāja programmatūrā automatizēto atjauninājumu lejupielādēšanas un uzstādīšanas rīku, vai ko līdzīgu, tādējādi atņemot darbu ar programmatūras atjauninājumiem no gala lietotāja. Šāda veida modulis daudzkārt palielinās "SOHO" maršrutētāju drošību, jo tiklīdz jauns atjauninājums būs izstrādāts un publicēts – tas tiks uzstādīts uz maršrutētāja.
- Pēc noklusējuma atslēgt multividi un citu papildus funkcionalitāti, piemēram, USB portu izmantošana vai cieto disku koplietošanas iespējas, lai ļautu tos sākumā pareizi nokonfigurēt un tikai tad sākt to lietošanu, nepieļaujot standarta konfigurācijas uzstādīšanu.

- Ražotājiem savās mājaslapās uzrādīt modeļu sarakstu, kuri vairāk netiek atbalstīti, tādējādi lietotāji varēs zināt, ka, iespējams, ir vērts aizdomāties par jauna maršrutētāja iegādi.

5.2 Ieteikumi un rekomendācijas "SOHO" maršrutētāju konfigurācijā un lietošanā

- Pašreizējā situācijā, lietotājiem izmantot lokālajam tīklam ne tik populāras IP adreses, piemēram 10.1.2.1 vai 192.168.32.1, tādējādi samazinot IP konfliktus starp maršrutētājiem, kuri uzrāda lokālo IP adresi WAN portā.
- Obligāti mainīt maršrutētāja administratora konta paroli.
- Izmantot tikai un vienīgi WPA2 aizsardzību bezvadu tīkla konfigurācijā. Nepieļaut WEP vai WPA izmantošanu.
- Ik laiku pārbaudīt, vai maršrutētāja ražotājs nav, izlaidis programmatūras atjauninājumus. Izmantot atjauninājumus tikai un vienīgi no oficiālās maršrutētāja mājaslapas.
- Ja iespējams, izmantot HTTPS savienojumu, sērfojot internetā, īpaši gadījumos, kad esat pieslēdzies pie publiskā bezvadu tīkla. Tas ir attiecināms pret maršrutētāja grafiskā interfeisa izmantošanu.

REZULTĀTI

Darba gaitā tiks izpildīti visi izvirzītie uzstādījumi:

- Pētījumos tika atrastas problēmas, kas ir saistītas ar "SOHO" maršrutētāju nestandarta uzvedību.
- Tika atrastas problēmas, kuras ir pieļāvuši maršrutētāju ražotāji.
- Veikta visu atrasto problēmu analīze.
- Izpētīts Rīgas iedzīvotāju bezvadu maršrutētāju bezvadu tīklu drošības īpatnības.
- Veikti secinājumi par to, ka „tikko-no-iepakojuma" bezvadu maršrutētāju, pat ar iebūvēto maršrutētāja „ātrās uzstādīšanas" interfeisi vai CD diski ar tiem joprojām nav izveidoti tā, lai to aizsardzība būtu labi izveidota. Tik un tā ir jāizmanto pilns interfeiss, lai labāk aizsargātu bezvadu maršrutētāju.
- Pārbaudīts, ka ir diezgan viegli pārķert lietotāju datus, kuri izmanto neaizsargātu bezvadu tīklu.
- Daļēji izpētīti populārāko maršrutētāju ražotāju tīmekļa interfeisi, veikti secinājumi, balstoties uz drošības aspektiem.
- Apkopoti maršrutētāju iespējamie problēmu veidi.

SECINĀJUMI

Rezumējot visas atrastās "SOHO" maršrutētāju īpatnības un problēmas, ir vērts izteikt viedokli, ka pat aptuveni 15 gadu laikā, šī aparatūra joprojām nav maksimāli pilnveidojusi sevi. Pēdējo gadu laikā, neskaitot 802.11ac standarta ieviešanu, mūsdienu maršrutētāji nav ieguvuši nekādu papildus funkcionalitāti vai kādu lielu drošības papildinājumu. Tas liek aizdomāties, vai par šo laiku ražotāji nevarēja novērst jau gadiem eksistējošu programmatūru vai dzelžu trūkumus, vai arī šīs rīcības ir saistītas ar mārketingu un daļēji ar ražošanas izmaksām?

Ir arī iespējams, ka darbā atrastā nestandarta bezvadu maršrutētāju uzvedība dažiem ražotājiem joprojām nav zināma.

Ņemot vērā to, ka tika atrasta nestandarta maršrutētāju uzvedība un salīdzinātas APR paketes, kas izrādījās pilnīgi identiskas, iespējams, ir nepieciešama dziļāka šādas uzvedības analīze un ievainojamības pārbaude. Tad varētu gan noteikt, gan pārbaudīt, vai šāda nestandarta darbība, ir maršrutētāja operētājsistēmas koda kļūda, kas ir novēršama, vai arī tā nav novēršama, jo vainīgs ir mikroprocesors, kas to darbina.

Pētījums, kas pārbaudīja kādu aizsardzību Rīgas iedzīvotāji izmanto savos bezvadu maršrutētājos (apakšnodaļa 3.4), pierādījis, ka ne visiem mūsdienu cilvēki, kuriem pieder vairākas bezvadu ierīces, ir parūpējušies par to, ka viņu bezvadu tīkls ir droša vieta. Salīdzinot šo pētījumu ar kādu no ikdienišķām darbībām, autors grib minēt to, ka, noteikti, visi automašīnu īpašnieki, atstājot savu mašīnu uz ielas vai, piemēram, pie mājām, kur ir diezgan droši, tomēr, aizejot aizslēdz automašīnu. Kāpēc tad tie paši cilvēki nerūpējās par savu datu drošību, kas, reāli, var būt arī nedrošs pasākums, un beigās var novest pie datu nokļūšanas trešo personu rokās.

Tāpēc, ka bezvadu maršrutētāja konfigurācija, parastam lietotājam, kas ar IT nozari nav saistīts, var būt apgrūtinoša, autors iesaka, tomēr, vērsties pie IT speciālista, un nepažēlot naudu sava bezvadu tīkla pareizai konfigurācijai, ņemot vērā to, ka tas ir vienreizējs pasākums un maršrutētājs, kā minimums, tiks izmantots pāris gadus.

To, ka maršrutētāju drošība ir tāla no ideāla, apstiprina arī tas, ka 2015. gada 19. maijā, tika publicēts raksts[18] par to, ka 26 dažādu ražotāju maršrutētāju 92 ierīcēs, kurās atrodas USB ports vai porti, tiek apdraudēti. To drošība ir, iespējams, apdraudēta ar ievainojamību, kas jau ir zināma kopš 90-jiem gadiem, kas ir saistīta ar NetUSB kodola draiveri. Ja datora vārda garumu izveidot lielāku par 64 simboliem, tas var novest pie steka bufera pārpildes bezvadu maršrutētājā. Pēc šādas darbības maršrutētājs pats pārstartējas un ļaundarim ir iespējams uz tā attālināti palaist ļaundarīgu programmatūras kodu.

Ir jāpiebilst arī to, ka ierīces kas satur USB portus, cenas ziņā, nav lētas un nāk tikai ar dārga segmenta bezvadu maršrutētājiem. Daļa no ievainojamiem maršrutētājiem ir izlaisti pavisam nesen.

Apkopojot visu uzrakstīto, ir jāsecina, ka „SOHO" bezvadu maršrutētāju gan konfigurācija, gan izmantošanas īpašības ir, tiešām, tālu no ideāla un, izmantojot to ikdienā, ir jācenšas pieturēties pie ļoti pareizas to konfigurācijas. Balstoties uz to, ka, pārsvarā, konfigurācija notiek tikai un vienīgi ierīces iegādes brīdī, to īpašniekiem ir jāvelta padziļināta uzmanība tās pareizajai uzstādīšanai vai šī darbība jānodod speciālista rokās.

PATEICĪBAS

Liels paldies Leo Trukšānam, par darba vadīšanas uzņemšanos.

Par sniegto atbalstu, diskusijām un ieteikumiem, kuras palīdzēja šo darbu virzīt uz priekšu, izsaku pateicību Filipam Skutelim.

IZMANTOTĀ LITERATŪRA UN AVOTI

[1] Small office/home office - Wikipedia, the free encyclopedia [tiešsaiste]. – [atsauce 20.05.2015.]. Pieejams: https://en.wikipedia.org/wiki/Small_office/home_office

[2] Hubs Versus Switches — Understand the Tradeoffs" (PDF), ccontrols.com, [tiešsaiste]. – [atsauce 21.01.2015.]. Pieejams: http://www.ccontrols.com/pdf/Extv3n3.pdf

[3] Wireless Router - Wikipedia, the free encyclopedia [tiešsaiste]. – [atsauce 15.03.2015.]. Pieejams: http://en.wikipedia.org/wiki/Wireless_router

[4] 802.11ac: A Survival Guide [tiešsaiste]. – [atsauce 26.02.2015.]. Pieejams: http://chimera.labs.oreilly.com/books/1234000001739/ch02.html#modulation_and_coding_set_mcs

[5] Broadcom blog – WiFi timeline [tiešsaiste]. – [atsauce 10.05.2015.]. Pieejams: http://www.broadcom.com/blog/wp-content/uploads/2012/05/wifi_timeline.jpg

[6] IEEE, Proposed TGac Draft Amendment [tiešsaiste]. – [atsauce 10.03.2015.]. Pieejams: mentor.ieee.org/802.11/dcn/10/11-10-1361-03-00ac-proposed-tgac-draft-amendment.docx

[7] New IEEE 802.11ac™ Specification Driven by Evolving Market Need for Higher, Multi-User Throughput in Wireless LANs [tiešsaiste]. – [atsauce 10.03.2015.]. Pieejams: http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html

[8] Гигабит без проводов. Тест пяти роутеров стандарта 802.11ac, [tiešsaiste]. – [atsauce 10.04.2015.]. Pieejams: http://www.thg.ru/network/test_5_routerov_standarta_802_11ac/index.html

[9] Linksys Official Support - Guest Network Frequently Asked Questions [tiešsaiste]. – [atsauce 10.04.2015.]. Pieejams: http://www.linksys.com/us/support-article?articleNum=140727

[10] IEEE 802.11-2007 — Tabula 18-9

[11] ARP-PING programmatūras mājaslapa [tiešsaiste]. – [atsauce 23.01.2015.]. Pieejams: http://www.elifulkerson.com/projects/arp-ping.php

[12] David C. Plummer (November 1982). "RFC 826, An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware". Internet Engineering Task Force, Network Working Group. [tiešsaiste]. – [atsauce 26.02.2015.]. Pieejams: http://tools.ietf.org/html/rfc826

[13] *Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin*, Breaking 104 bit WEP in less than 60 seconds, [tiešsaiste]. – [atsauce 21.02.2015.]. Pieejams: http://eprint.iacr.org/2007/120.pdf

[14] TP-LINK Emulators, [tiešsaiste]. – [atsauce 22.03.2015.]. Pieejams: http://www.tp-link.com/en/support/emulators/?model=TL-WR741ND

[15] A. Inkins, bakalaura darbs - "SOHO" maršrutētāju pielietojums lokālajos tīklos un ar to saistītas problēmas, 2013

[16] Certificate Pinning Plugin for PhoneGap to prevent Man in the Middle Attacks [tiešsaiste]. – [atsauce 25.04.2015.]. Pieejams: http://www.x-services.nl/certificate-pinning-plugin-for-phonegap-to-prevent-man-in-the-middle-attacks/734 (http://www.x-services.nl/wp/wp-content/uploads/2013/09/man-in-the-middle-attack.gif)

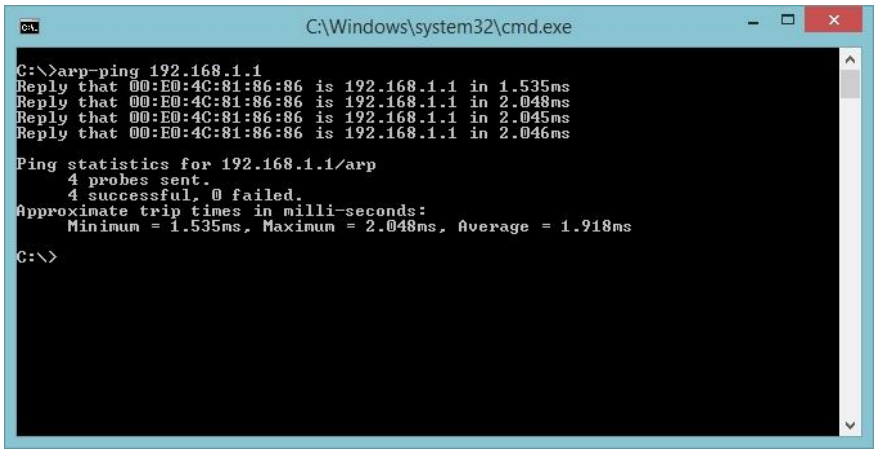
[17] Red alert: HTTPS has been hacked | InfoWorld [tiešsaiste]. – [atsauce 10.05.2015.]. Pieejams: http://www.infoworld.com/article/2620383/security/red-alert--https-has-been-hacked.html

[18] KCodes NetUSB: How a Small Taiwanese Software Company Can Impact the Security of Millions of Devices Worldwide [tiešsaiste]. – [atsauce 20.05.2015.]. Pieejams: http://blog.sec-consult.com/2015/05/kcodes-netusb-how-small-taiwanese.html

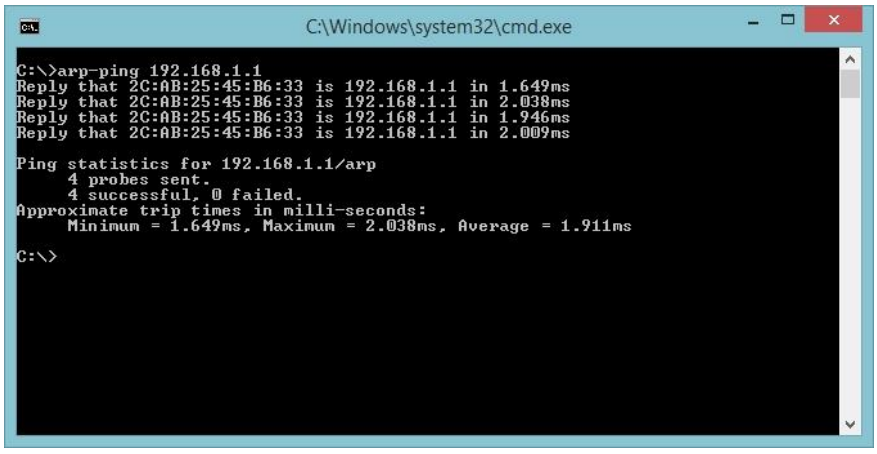
PIELIKUMI

Pielikums 1. D-Link DAP-1155 ARP atbildes no WAN un LAN portiem

LAN shēma:

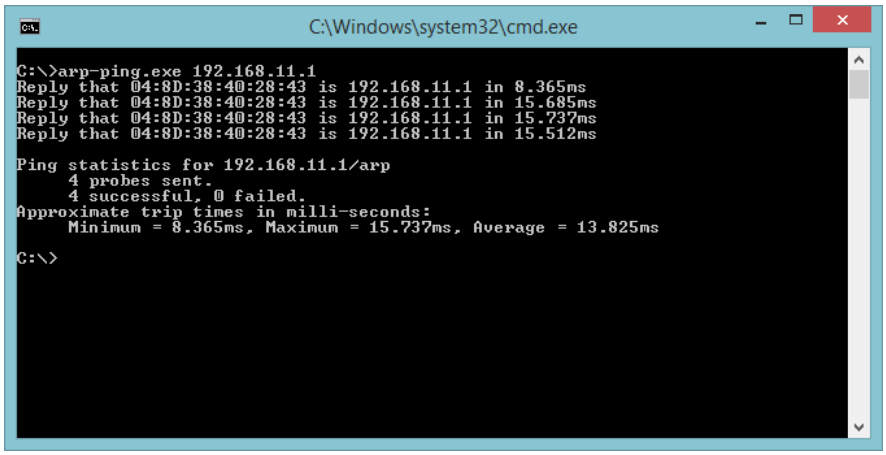


WAN shēma:



Pielikums 2. Netis WF2419 ARP atbildes no WAN un LAN portiem

LAN shēma:



WAN shēma: