RĪGAS TEHNISKĀ UNIVERSITĀTE

DZELZCEĻA TRANSPORTA INSTITŪTS

V.POPOVS, J.GOLOVINS, A.STURME

802.11 STANDARTA BEZVADU LOKĀLO TĪKLI (WLAN).

LEKCIJU KONSPEKTS

RĪGA 2006

UDK 681.3.07

Popovs V., Golovins J., Sturme A. 802.11 standarta bezvadu lokālo tīkli (WLAN). Lekciju konspekts. Rīga: RTU Izdevniecība, 2006, 60.lpp.

Lekciju konspekts tiek apskatīti 802.11 standarta bezvadu lokālie tīkli, kuri mūsdienās plaši tiek izmantoti mobilajos tīklos, kā arī telekomunikāciju tīklos uz dažādiem transporta veidiem.

Lekciju konspekts paredzēta telekomunikāciju speciālistiem un RTU elektronikas un telekomunikācijas fakultātes studentiem.

ISBN……

SATURS

IEVADS.

Wi-Fi šodien – ta ir ātra, ērta mobila piekļūšana internetam. Mūsdienu Wi-Fi pielietošana sola grandiozu ekonomiju kompānijām, kas pielieto šīs tehnoloģijas. Jauni lēmumi šajā nozarē, būtībā, ver vaļā jaunus biznesa modeļus.

Piekļūšanas vietas internetā caur Wi-Fi Latvijas Republikā parasti atrodas trešdaļa no visiem komerciālu Wi-Fi spētiem novietoti dzelzceļš, lidostās un hoteļos.

Un tāpēc dotā lekciju konspekta temats ir ļoti aktuāls.

Tas apgaismo sekojošās problēmas:

- Wi-Fi tīkla standarti,
- Wi-Fi tīkla uzbūves apskats,
- Wi-Fi tīkla aprīkojumu tehniskie raksturojumi,
- Wi-Fi tīkla darbspējas kvalitātes pārbaude,
- Wi-Fi tīkla drošība.

Standarta 802.11 bezvadu lokālie tīkli.

Izejas standarts 802.11 nosaka divas pārraides metodes fizikālajā slānī:

- Spektra paplašināšanas tehnoloģija, izmantojot lēcienveidīgu frekvences pārslēgšanu (FHSS) 2,4GHz diapazonā.
- Šaurjoslas modulācijas tehnoloģija (DSSS) ar spektra paplašināšanu pēc tiešās sekvences metodes 2,4GHz diapazonā.

Abas šīs tehnoloģijas strādā 2,4GHz diapazonā, kurā ASV Federālā sakaru komisija (FCC) izdalīja 82MHz platu joslu rūpniecības, zinātnes un medicīnas pielietošanai (ISM).

Standarta 802.11b bezvadu lokālie tīkli.

1999. gadā parādījās standarts 802.11b, kurš reglamentēja augstas ātrdarbības DSSS (HR-DSSS) tehnoloģijas, kura nodrošina pārraides ātrumu bezvadu lokālajos tīklos ISM 2,4GHz diapazonā līdz pat 5,5 un 11Mbit/s, izmantošanas noteikumus. Bez tam pielieto arī kodēšanu, izmantojot komplementāros kodus (complementary code keying, CCK) vai bināro pakešu konvolūcijas kodēšanas tehnoloģija (packet binary convolutional coding, PBCC). HR-DSSS tehnoloģijā izmanto to pašu kanālu organizēšanas shēmu, kuru DSSS tehnoloģijā, - frekvences joslas platums 22MHz, 11 kanāli, 3 nepārklāti, 2,4GHz ISM-diapazons.

Standarta 802.11a bezvadu lokālie tīkli.

Tai pašā laikā, kad 1999.gadā standarta projektā tika aprakstīts HR-DSSS tehnoloģijas fizikālais kanāls, standarta 802.11a projektā tika piedāvāts izmantot fizikālo kanālu, kurā izmanto multipleksēšanas tehnoloģiju ar sadalījumu pēc ortogonālajām frekvencēm (orthogonal frequency division multiplexing, OFDM) 5GHz diapazonā. Tā leģitimēja pārraides ātrumu līdz 24Mbit/s un – līdz 54Mbit/s ASV nacionālās informācijas infrastruktūras U-NII (unlicensed national information infrastructure) bez licences diapazonos: 5,15-5,25GHz, 5,25-5,35GHz un 5,725—5,82GHz. Standarts 802.11a reglamentē 20MHz platu kanālu izmantošanu un nosaka četrus kanālus katram no trim diapazoniem.

Standarts 802.11j.

Lokālo/pilsētas tīklu (MAN) standarta korekciju projekts 802.11j reglamentē darbu saskaņā ar standarta 802.11a noteikumiem 4,96GHz diapazonā, izdalītu Japānā un ASV sabiedriskai pielietošanai, ievērojot drošības pasākumus, kā arī 5,03-5,091 diapazonā Japānā. Kanālu numerācijas shēmā (channel numbering scheme) šiem kanāliem doti numuri no 240 līdz 255, katra platums sastāda 5MHz.

Standarta 802.11g lokālie tīkli.

2003.gada jūnijā piedāvātais standarts 802.1lg tehnoloģiju EPR noteica kā pārraides ātruma līdz 54Mbit/s 2,4GHz ISM diapazonā nodrošināšanas līdzekli; tas pārņēma standarta 802.11a OFDM metodes. Pretēji standartam 802.11a, šis nodrošināja apgriezto saderību ar standartu 802.11b, jo standartam 802.1lg atbilstošās iekārtas spēj mainīt datu pārraides ātrumu līdz vērtībām, kuras ir mazākas par standartā 802.11b reglamentētajām. Noteiktas trīs modulācijas shēmas: ERP-ORFM, ERP-PBCC и DSSS-OFDM. Izmantojot ERP-ORFM, sāk darboties speciāli tai izstrādātie mehānismi, kuri nodrošina 6, 9, 12, 18, 24, 36, 48, un 54Mbit/s lielus pārraides ātrumus, no tiem obligāti ir ātrumi 6, 12 un 24Mbit/s papildinājumā ar datu pārraides ātrumiem 1, 2, 5,5 un 11Mbit/s. Tāpat standarts ļauj izmantot PBCC režīmus ar ātrumiem 22 un 33Mbit/s, kā arī DSSS-OFDM režīmus ar ātrumiem 6, 9, 12, 18, 24, 36, 48 un 54Mbit/s.

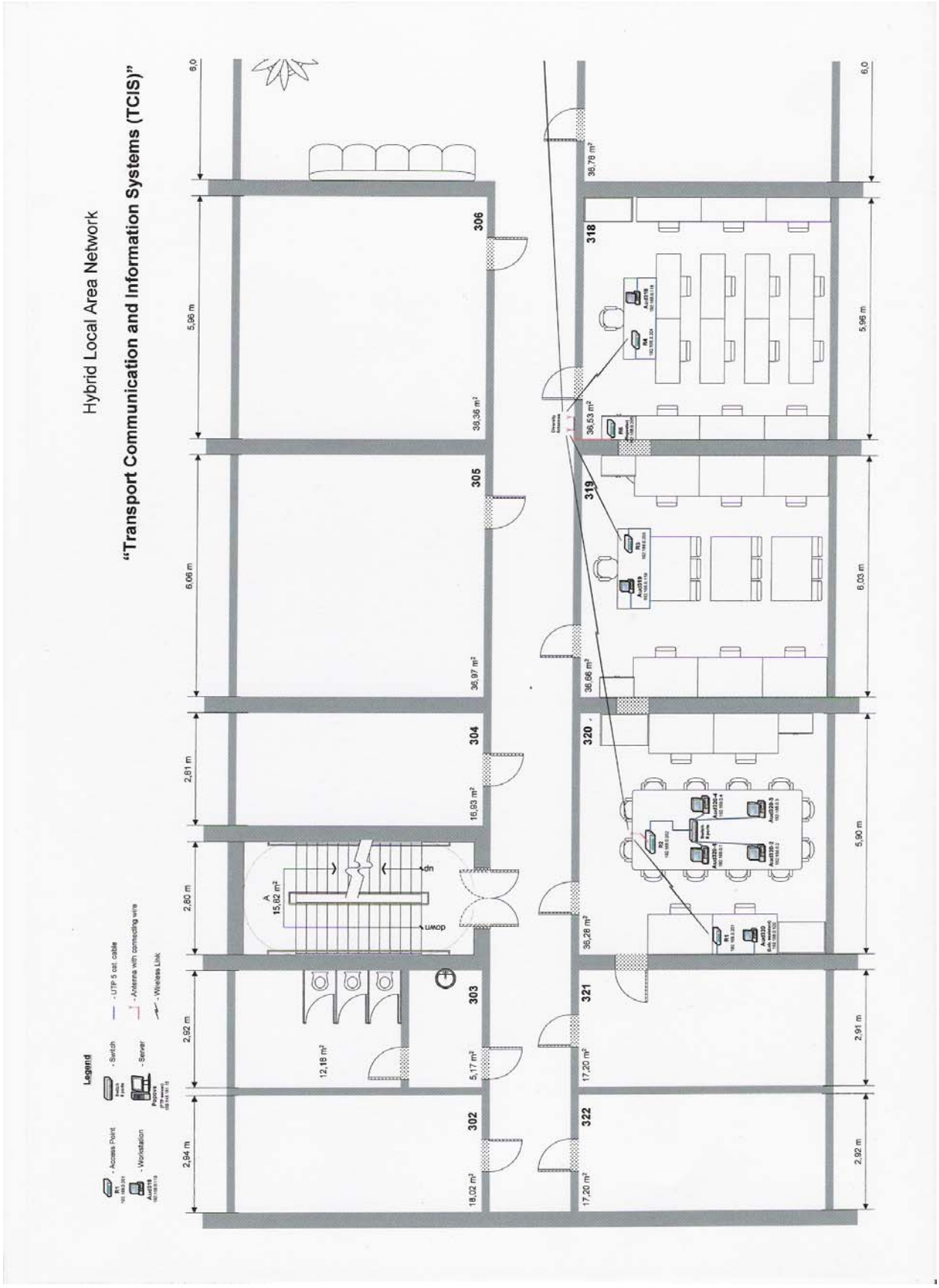
Tab.1 minēti dažādu tehnoloģiju, kuras pielieto uz PHY slāņa un ir izskatītas dotajā nodaļā, pamata parametri. Lai gan FHSS tehnoloģija ļoti ātri izplatās, to cenšas panākt DSSS un HR-DSSS tehnoloģijas. Laikā, kad tika rakstītas šīs rindas, rūpniecība atradās uz

tehnoloģijas otrās revolūcijas viļņa, jo lietotāji pārgāja uz standartu 802.11a un 802.1lg bāzētu iekārtu izmantošanu.

Tabula 1. Standarti 802.11

Parametrs	**802.11 FHSS**	**802.11 DSSS**	**802.11b HR-DSSS**	**802.11a OFDM**	**802.11g ERP**	**802.11j**
Frekvences diapazons (GHz)	2,4	2,4	2,4	5	2,4	4,9
Datu pārraides maksimāls ātrums (Mbits/s)	2	2	11	54	54	54

1. TĪKLA TOPOLOĢIJA.



Att.1.

1.1.Tīkla topoloģijas izvēle.

Pielikumā parādīta ***WLAN (Wireless Local Area Network) 802.11b standartā*** shēma (Att.1.), kura minēta TCIS ("Transport Communication and Information Systems") virzienu grupas lokālo tīklu projektā.

Katrai tīkla darba stacijai ir dots vārds un IP adrese, kuru izmanto iekšējā tīkla adresācijai un kurš viennozīmīgi translējas MAC adresē savienojuma uzstādīšanai kanāla slānī. Piekļuves punktam ir viena IP adrese (izņemot vārteju R6, kurai ir divas dažādas IP adreses – ārējā un iekšējā), nepieciešama administratora piekļuvei pie viņu iestatījumiem, un katram interfeisam – vadu vai bezvadu - pa vienai MAC adresei.

1.1.1. Bezvadu sadales sistēma.

TCIS tīklā pieejas punkti A032 veido bezvadu sadales sistēmu (WDS – Wireless Distribution Systems) daudzkomponentu tīkla tilta veidā, kurš jebkurām divām tīklam pieslēgtām darba stacijām nodrošina "punkts - punkts" savienojumu (wireless point-to-point bridge). Šis bezvadu tilts kalpo par ESS maģistrāli un savā starpā savieno Ethernet segmentus, kuri iziet uz atsevišķiem piekļuves punktiem.

Attiecībā uz bezvadu tilta konfigurāciju, nepieciešams norādīt svarīgas piezīmes:

1) Visām ESS komponentēm jāstrādā vienā un tai pašā kanāla frekvencē (TCIS tīklā tā ir – Channel 1, kura funkcionē 2412MHz).
2) Bezvadu sadales sistēmai jābūt ar kokveidīgu topoloģiju.

Lai izveidotu daudzkomponentu ESS bezvadu tiltu, katra piekļuves punkta iestatījumos nepieciešams norādīt, kuri citi pieejas punkti būs tās partneri pēc tilta (to MAC adreses). Piemēram, TCIS tīklā R1 partneris ir R2, R5 partneri – R2, R3, R4 un R6 (skat. shēmu). Pirms tam tiek sastādīta tīkla topoloģijas karte. Tai noteikti jābūt ar kokveidīgu topoloģiju. Nepieciešams izvairīties no cilpu rašanās, pa kurām nepārtraukti cirkulēs dati, bloķējot sakarus.

3) Bezvadu klientu roumings no viena piekļuves punkta pie otra ir iespējams, taču netiek rekomendēts.

Pie audzsegmentu infrastruktūras nosacījumiem ESS bezvadu klienti automātiski tiek pievienoti pie tā piekļuves punkta, kura signāla jauda ir vislielākā. Lai novērstu roumingu, nepieciešams katram piekļuves punktam ESS iekšienē noteikt unikālu BSS tīkla vārdu (Network Name vai BSSID), kurā tas ir centrālais mezgls. Pēc tam klienta iestatījumos var

norādīt, pie kāda piekļuves punkta pievienoties (piemēram, TCISx, kur x – TCIS tīkla piekļuves punkta kārtas numurs).

Tab.1.1. parādīta piekļuves punktu pakotnes iziešanas secība, kad notiek datu pārraide no vienas darba stacijas uz otru.

Tabula 1.1

Kadru kustības kārtība caur WDS mezgliem

		Kadra noteikšanas stacija					
		Aud309	**Aud318**	**Aud319**	**Aud320**	**Aud320-x (x=1…4)**	**Popovs (ārējā tīklā)**
Kadra stacija-avots	**Aud309**	-	R7-R6-R5-R4	R7-R6-R5-R3	R7-R6-R5-R2-R1	R7-R6-R5-R2	R7-R6
	Aud318	R4-R5-R6-R7	-	R4-R5-R3	R4-R5-R2-R1	R4-R5-R2	R4-R5-R6
	Aud319	R3-R5-R6-R7	R3-R5-R4	-	R3-R5-R2-R1	R3-R5-R2	R3-R5-R6
	Aud320	R1-R2-R5-R6-R7	R1-R2-R5-R4	R1-R2-R5-R3	-	R1-R2	R1-R2-R5-R6
	Aud320-x (x=1…4)	R2-R5-R6-R7	R2-R5-R4	R2-R5-R3	R2-R1	-	R2-R5-R6
	Popovs (ārējā tīklā)	R6-R7	R6-R5-R4	R6-R5-R3	R6-R5-R2-R1	R6-R5-R2	-

1.1.2. Ethernet segmenti lokālā tīkla sastāvā.

Nokia A032 piekļuves punkti ir aprīkoti ar 10BaseT Ethernet interfeisu, lai savienotos ar LAN vadiem. Šis interfeiss nodrošina maksimālu pārraides ātrumu 10Mbit/s dupleksa režīmā, kas pilnībā pietiekams, ņemot vērā ierobežoto 11Mbit/s WLAN 802.11b summāro caurlaides spēju, kura reālos gadījumos ir divas un pat vairākas reizes mazāka par norādīto vērtību.

Ethernet 802.3 segmenti, kurus pieslēdz pie piekļuves punkta caur interfeisu 10BaseT, var būt divu veidu:

1) tiešs savienojums ar darba staciju pa kabeli UTP 5cat., kuram ir crossover izvadīšanas vadi (piemēram, savienojumi Aud320-R1, Aud319-R3 u.t.t.);

2) savienojums pa parastu kabeli UTP 5cat. ar centrmezglu vai komutatoru (piemēram, R2 savienojums ar 8-portu komutatoru Eusso USH5008-XL), kurš ir pēc zvaigžņu topoloģijas sakopotā lokālā tīkla Ethernet centrālais posms.

Datu pārraide caur Fast Ethernet standarta komutatoru, kura viens ports savienots ar piekļuves punktu A032, ir iespējama ar vairāk kā 10Mbit/s (līdz 100Mbit/s) lieliem ātrumiem. Šajā gadījumā failu apmaiņā jāpiedalās stacijām, kuru tīklu adapteri atbilst Fast Ethernet specifikācijām.

TCIS tīklā datu pārraide starp darba stacijām Aud320-1, Aud320-2, Aud320-3 un Aud320-4 notiek ar maksimālo ātrumu 100Mbit/s, pateicoties 4 vienlaicīgiem 100Mbit/s savienojumiem ar 8-portu Eusso USH5008-XL komutatoru. Tai pašā laikā, savienojuma ar piekļuves punktu R2, caurlaides spēja nepārsniedz 10Mbit/s.

1.1.3. Piekļuves punkti, kā "Ethernet-WLAN" tilti un WDS atkārtotājs.

Parastā nozīmē "Wireless bridge" (bezvadu tilts) – tā ir iekārta, kura paredzēta LAN vadu segmenta savienošanai ar pārraides bezvadu vidi. Piemēram, piekļuves punkts R2 ar tiltu savieno bezvadu maģistrāli un Eusso USH5008-XL komutatoru (skat. TCIS tīkla shēmu). Pie tam no vada Ethernet-segmenta, pieslēgts pie R2, pa tiltu tiek pārraidīti tikai paketes, kuras ir adresētas stacijām citos vadu segmentos. Tai pašā laikā lokāli pārraidāmie dati šajā segmentā starp stacijām Aud320-1, Aud320-2, Aud320-3 un Aud320-4 netiek pārraidīti radio-ēterā. Tas ļauj nenoslogot bezvadu savienojumus un pārraidīt datus vada Ethernet-segmenta robežās ar lielāku ātrumu, kuru atbalsta radio-savienojums.

Liels piekļuves punktu skaits sadales sistēmas sastāvā var negatīvi atsaukties uz datu pārraides ātrumiem. Tā kā piekļuves izejas punkts katru saņemto apraides ziņojumu individuāli izplata visām tilta komponentēm, tad, jo vairāk ir šādu ziņojumu, jo lēnāk strādā tīkls. Līdz ar to, ESS sastāvā izmantojot vairāk kā 3-4 piekļuves punktus, nepieciešams pārdomāt tīkla topoloģiju. Nepieciešams ņemt vērā arī to, ka daži nelieli lokālā tīkla segmenti bieži dod daudz augstāku veiktspēju, ja iekārtas var sadalīt grupās tā, lai trafiks segmenta iekšienē būtiski pārsniegtu datu apmaiņu starp segmentiem.

Tiltam jābūt ar pietiekamu bufera apjomu, lai varētu strādāt maksimāla pieprasījuma apstākļos, kad īsā laika posmā kadri pienāk ātrāk, kā tiek pārraidīti.

Darbam ar adresēm un maršrutiem tilts tiek aprīkots ar maršrutēšanas līdzekli, kurš ņem vērā tīklu apvienošanas topoloģiju. Piekļuves punktam, kurš izpilda retranslēšanas tilta

funkcijas, pieņemot kadru, jāizlemj, vai to pārraidīt tālāk vai nē, un ja pārraidīt, tad kuram mezglam.

A032 realizē vienkāršāko fiksētās maršrutēšanas algoritmu bez cikla atļaujas. Šī metode ir piemērota nelieliem tīklu apvienojumiem. Pēc tam, kad ar rokām visiem piekļuves punktiem ir norādīti tilta savienojuma partneri, tīkla funkcionēšanas procesā uz katra tilta dinamiski formējas maršrutu tabula. Katrai iespējamai mērķa MAC-adresei tabula rāda, uz kuru nākamo mezglu tiltam ir jāvirza kadrs.

Izņemot bezvadu tilta Nokia funkcijas A032 var strādāt kā bezvadu atkārtotāji (wireless repeaters), palielinot radio-pārklājuma tīkla atttālumu. TCIS tīklā par radio signāla atkārtotāju kalpo piekļuves punkti R2, R5 un R6 (bez tam R2 un R6 vienlaicīgi izpilda tilta un atkārtotāja funkcijas). Piemēram, ja notiek datu pakotnes pārraide no darba stacijas Aud320 uz staciju Aud309, tad no sākuma to sūta atkārtotājs R2 pa tiltu R1, tad R2 pārsūta uz R5 un pēc tam pakotne tiek nodota atkārtotājam R6, kurš, savukārt, nosūta to uz tiltu R7, kas ir savienots ar staciju Aud309.

Pieslēdzot bezvadu klientu staciju pie piekļuves punkta, pēdējais kalpo par atkārtotāju pārraidot datus starp klientu un pārējām ESS infrastruktūras komponentēm.

Nepieciešams atzīmēt, ka jo lielāks atkārtotāju skaits tiek izmantots, jo būtiskāks ir pārraides ātruma kritums. Saskaņā ar Nokia rekomendācijām: pārraides ātruma samazināšanās = saites/(atkārtotāju skaits +1) caurlaides spēja, t.i., pie viena atkārtotāja ātrums samazinās uz pusi, pie diviem – 3 reizes. Jāatzīmē arī tas, ka tāda pieeja, novērtējot WDS veiktspēju, ir pamatota tikai tajos gadījumos, kad bezvadu savienojumu starp atkārtotājiem caurlaides spēja ir aptuveni vienāda. Sīkāks TCIS tīkla caurlaides spējas aprēķins dots 6. nodaļā.

2. WLAN IEKĀRTAS

2.1. Tīkla iekārtas tehniskie raksturojumi

2.1.1. Standarta IEEE 802.11B WLAN iekārta.

2.1.1.1. Nokia C110/C111 WLAN Card.

Nokia C110/111 – tie ir WLAN adapteri, kuriem ir Extended Type II PC Card formāts un paredzēti uzstādīšanai portatīvajās darba stacijās. C110/C111 pilnībā atbilst IEEE 802.11b specifikācijai un ir aprīkoti ar divām kompaktām iekšējām antenām.

Nokia C110/111 specifikācijas

Formāts	PC Card (Extended Type II)
Standarts	IEEE 802.11b
Kanālu skaits	13 (atkarībā no reģiona)
Pārraides ātrums	11, 5.5, 2 и 1Mbit/s
Modulācijas tehnoloģija	DSSS
Antenas	2 integrētas antenas platē (C111 tāpat ir vietas ārējām antenām)
Pārraides jauda	35 mW (iekšējo antenu gadījumā)
Uztvērēja jūtība	Min. -84 dBm
Pārklājuma zonas rādiuss	Atklātā apvidū: maks. 400 m Ēkā: 20-100 m
Drošība	WEP ar slepenās atslēgas garumu līdz 128 bit
Enerģijas patēriņš (3.3V/5V)	Sleep: 10mA/10mA Receive: 240mA/180mA Transmit: 360mA/310mA

2.1.1.2. Nokia A032 WLAN Access Point.

Nokia A032 piekļuves punkts ir kā kompakta bāzes stacija, kura paredzēta WLAN BSS formēšanai slēgtās telpās. A032 tāpat funkcionē kā tilts starp Ethernet un WLAN stacijām, kas mobilajām stacijām, aprīkotām ar 802.11-kopīgiem adapteriem, ļauj iegūt pieeju pie vadu tīkla resursiem. Dažus A032 piekļuves punktus, integrētus ar Ethernet vadu segmentiem, var savā starpā sasaistīt ar bezvadu tiltu, lai izveidotu vienotu lokālo tīklu.

Kā radio moduli, A032 izmanto Nokia C111 adapteri. Piegādes komplektā tāpat ietilpst viena nevērsta (omni-directional) vertikāli polarizēta antena – Nokia C950, kura paredzēta radio pārklājuma zonas paplašināšanai.

Savienojot lokālo apakštīklu ar ārējo tīklu, A032 aktivizē tīkla ekrānu (Firewall), kas pasargā piekļuvi iekšējam tīklam no ārienes.

Nokia A032 specifikācijas

Standarti	IEEE 802.11b (WLAN) IEEE 802.3 (Ethernet)
Radio interfeiss	Nokia C111 PC Card
Antena	Nevirzīta ārējā antena ar 2m koaksiālo savienošanas kabeli
Ethernet-interfeiss	10BaseT (RJ-45): 10 Mbit/s
Seriālā pieslēgvieta	Interfeisa DCE atbalstīts konektors DB9
Dial-up Modem	9600-57600 bit/s
Mobilo staciju enerģijas taupīšanas režīma atbalstīšana	Power Save Poll atbalsts saskaņā ar standartu 802.11
Piekļuves drošība	WEP šifrēšana ar atslēgas garumu 40 un 128 bit

Šifrēšanas atslēgas	Glabāšana līdz 200 WEP-atslēgām
DHCP (Dynamic Host Configuration Protocol) funkcija	Piekļuves punktiem pieslēgto staciju (kā WLAN, tā arī Ethernet) TCP/IP automātiskā konfigurācija
Bāzes DHCP maksimālais adrešu skaits	64
Interneta pieslēgums	Tīkla ekrāna (Firewall) ar adrešu translāciju (NAT) ieslēgšana
Vadības programmu interfeisi	Administrēšana ar Web-pārlūka palīdzību; termināla pieslēgšana caur seriālo pieslēgvietu; Telnet; SNMP
LED-indikatori	Padeve, asociēto staciju skaits, utilizācija, radio un Ethernet-interfeisa statuss
Elektropadeve	DC 12V, 1A
Patērētā jauda	5.1 W

2.1.2. Standarta IEEE 802.3u Fast Ethernet iekārta.

2.1.2.1. Eusso UEC2200-S 10/100 Mbps PCI Fast Ethernet Card

UEC2200-S – tas ir standarta Fast Ethernet tīkla adapteris, kurš automātiski izvēlas nepieciešamo pārraides ātrumu (10 vai 100Mbit/s), pamatojoties uz pārrunām ar partneriem savienojumu jomā.

Eusso UEC2200-S specifikācijas

Atbalstāmie LAN standarti	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX
Interfeiss	RJ45

Pārraides režīms	Full/Half duplex: 10 un 100Mbit/s
Pārraides vide	10BASE-T: UTP Cat. 3, 4, 5 100Base-TX: UTP Cat. 5
Iestatīšanas interfeiss	32-bit maģistrāle PCI
Chipset	Realtek RTL8139
LED-indikators	Link/Activity

2.1.2.2. Eusso USH5005-XPB 5-Port 10/100 Mbps Nway Switch

USH5005-XPB – tas ir standarta Fast Ethernet komutators, kura visi 5 porti, pamatojoties uz pārrunām ar tīklu iekārtām, spēj automātiski izvēlēties pārraides režīmu (Full/Half Duplex) un ātrumu (10/100Mbit/s). Visi porti atbalsta Auto MDI/MDI-X funkciju, kura ļauj savienot Ethernet komutatorus ar parastiem (ne crossover) UTP kabeļiem.

USH5005-XPB nodrošina izdalīto 10/100Mbit/s savienojumu katrai pie tā pieslēgtajai stacijai ar pilnvērtīgu caurlaides spējas izmantošanu (salīdzinājumā ar savienojumu caur koncentratoru ar kopējo caurlaides spēju visiem portiem). Dupleksa režīmā 100Base-TX vienlaicīgi izdalās 100Mbit/s uztveršanai un 100Mbit/s pārraidei.

Komutators satur adrešu tabulu MAC, kura sastāv no ļoti daudziem ierakstiem. Katrs ieraksts glabā informāciju par mezgla adresi tīklā (MAC adrese, porta identifikators u.t.t.). Pamatojoties uz šo informāciju, tiek īstenota pakotņu filtrācija un pārvirzīšana. Adrešu tabulas MAC saturs dinamiski atjaunojas ar ienākošo pakotņu avotu adrešu datiem.

Kad uz vienu no komutatora portiem pienāk datu pakotne, komutators meklē piešķiršanas adresi MAC adrešu tabulā. Ja tāda adrese nav atrasta, tad pakotne tiek pārsūtīta

uz visiem portiem, izņemot avota portu. Ja tabulā ir norādītā adrese, un tās ports atšķiras no avota porta, tad pakotne tiek novirzīta uz to portu, kas atbilst tabulas ierakstam. Savukārt, ja piešķiršanas adrese pieder tam pašam portam, kam arī avota adrese, tad pakotne tiek izfiltrēta.

Komutatora USH5005-XPB darba princips ir pamatots uz starpglabāšanas (store-and-forward) tehnoloģiju ar zemu aizturi: komutators uztver kadru no ieejas signāla, ievieto to buferī pagaidu glabāšanai, pēc tam pa maršrutu virza uz attiecīgo izejas kanālu. Šis mehānisms ļauj efektīvi cīnīties ar kļūdām, jo komutators pārbauda CRC kadrus pirms retranslācijas.

USH5005-XPB ir Plug-n-Play iekārta, un tā neprasa programmatūras iestatīšanu.

Eusso USH5005-XPB specifikācijas

Atbalstāmie LAN standarti	IEEE 802.3 10BASE-T IEEE802.3u 100BASE-TX
Interfeiss	5 portu RJ-45 NWay
Protokola NWay atbalsts	Pārraides ātrums: 10/100 Mbit/s Pārraides režīms: Full/Half Duplex
Auto MDI/MDI-X atbalsts	Visi 5 porti realizē Auto MDI/MDI-X funkciju
Adrešu tabula MAC	2048 ieraksti
Sistēmas atmiņa	1 Mbit
Filtrācijas/pāradresācijas ātrums (Filtering/Forwarding Rate)	10Mbps: 14880pps/14880pps 100Mbps: 148800pps/148800pps
Kabeļa savienojums	10BASE-T: UTP Cat. 3, 4, 5 līdz 100 m 100Base-TX: UTP Cat. 5 līdz 100 m
LED-indikatori	System: Power Port: 100M, Link/Activity
Elektropadeve	External Power Supply: +12VDC 0.5A

2.1.2.3. Eusso USH5005-XPB 8-Port 10/100 Mbps Nway Switch

USH5005-XPB – standarta Fast Ethernet 8-portu komutators, kura tehniskie raksturojumi ir analoģiski USH5005-XPB.

Eusso USH5008-XL specifikācijas

Atbalstāmie LAN standarti	IEEE 802.3 10BASE-T IEEE802.3u 100BASE-TX
Interfeiss	8 portu RJ-45 NWay
Protokola NWay atbalsts	Pārraides ātrums: 10/100 Mbit/s Pārraides režīms: Full/Half Duplex
Auto MDI/MDI-X atbalsts	Visi 8 porti realizē Auto MDI/MDI-X funkciju
Adrešu tabula MAC	8192 ieraksti
Bufera atmiņa	2Mbit
Filtrācijas/pāradresācijas ātrums (Filtering/Forwarding Rate)	10Mbps: 14880pps/14880pps 100Mbps: 148800pps/148800pps
Kabeļa savienojums	10BASE-T: UTP Cat. 3, 4, 5 līdz 100 m 100Base-TX: UTP Cat. 5 līdz 100 m
LED-indikatori	System: Power Port: Speed, Link/Activity, FDC/Collision
Elektropadeve	External Power Adapter: +12VDC 1A

3. TĪKLA INSTALĀCIJA UN KONFIGURĀCIJA.

3.1. Lokālā tīkla mezglu konfigurācija.

Nokia A032 programmatūra piedāvā ērtu piekļuvi vairumam iestatījumu, izmantojot standarta pārlūku uz jebkuru klientu staciju (vadu vai bezvadu). Paplašināta konfigurācija pieejama caur komandu rindas interfeisu, pieslēdzoties piekļuves punktam caur seriālo pieslēgvietu vai savienojoties ar protokola Telnet starpniecību.

3.1.1. Konfigurāciju parametri.

Tab.2.2. parādīti WLAN iekārtu konfigurācijas parametri (piekļuves punktu un darba staciju), kuru iestatīšana nepieciešama lokālā tīkla izveidošanai.

Tabula 3.1

WLAN bāzes parametri

Parametrs	**Vērtība (TCIS tīklam)**	**Paskaidrojumi**
Regulatory Domain	ETSI	Reģiona (valsts) izvēle, kurā tiek uzstādīts bezvadu tīkls
Radio Channel	1	Frekvenču kanāla uzstādīšana
Network Name	TCISx (x=1…7 – piekļuves punkta numurs)	Identifikators BSS (BSSID)
IP Address	192.168.0.1-192.168.0.254	Iekārtas IP adrese apakštīklā
IP Subnet Mask	255.255.255.0	Apakštīkla IP maska, pie kuras pieslēgta stacija
IP Gateway	192.168.0.206	Uz ārējā tīkla vedošā apakštīkla vārtejas adrese

Tab.3.2. aprakstīti paplašinātās konfigurācijas opcijas parametri, kuri palīdz optimizēt WLAN veiktspēju.

Tabula 3.2.

802.11 bezvadu savienojuma optimizācijas parametri

Parametrs	**Vērtība (Nokia default)**	**Paskaidrojumi**
RTS Threshold	2301 bytes	Uzstāda sliekšņa vērtību, lai noskaidrotu, vai konkrētajam datu kadram ir nepieciešama RTS/CTS kadru apmaiņa. Ja servisa datu modulim MAC (MSDU – MAC Service Data Unit), iegūts no daudz augstākiem protokolu steka slāņiem, ir lielāks izmērs, kā RTS Threshold, tad ir nepieciešama RTS/CTS apmaiņa pārraides vides rezervēšanai. Pie noklusēšanas šī vērtība netiek norādīta, t.i., neatkarīgi no MSDU izmēra RTS/CTS apmaiņa netiek noteikta. Kad RTS/CTS kadru apmaiņa ir ieslēgta, tad pie kadru pārraides parādās papildus pieskaitāmās izmaksas. Lai gan RTS/CTS apmaiņa uzlabo datu pārraides drošību, kanāla rezervēšanas laiks datu kadra pārraidei var pieaugt.
Short Retry Limit	15	Šis parametrs norāda maksimālo pārraides mēģinājumu skaitu līdz tam, kamēr kadrs tiks nomests. Šo ierobežojumu pielieto datu kadriem, kuru MSDU izmērs ir mazāks vai vienāds ar RTS Threshold (t.i., kadrs, kuram nav nepieciešama RTS/CTS apmaiņa). Pēc noklusēšanas IEEE 802.11 uzstāda šo vērtību vienādu ar 7 mēģinājumiem.
Long Retry Limit	15	Šis parametrs izpilda to pašu funkciju, kuru iepriekšējais, tikai to pielieto datu kadriem, kuru MSDU izmērs lielāks par RTS Threshold (kadrs, kuram ir nepieciešama RTS/CTS apmaiņa). Pēc noklusēšanas priekš 802.11 – 4 mēģinājumi.
SIFS Time	0 (10 μs)	Īsa starpkadru intervāla ilguma iestatīšana (SIFS – Short InterFrame Spacing). Dotajai vērtībai 802.11-saderīgos WLAN jābūt standarta (10 μs).
Fragmentation Threshold	2346 bytes	Nosaka sliekšņa vērtību, lai pieņemtu lēmumu par MSDU, iegūtu no daudz augstāka slāņa, fragmentācijas nepieciešamību pirms pārraides. Kadri, kuru izmērs ir lielāks par Fragmentation Threshold, tiek raidīti pa daļām. Fragmentu skaitu aprēķina izejot no MSDU un sliekšņa fragmentācijas izmēra. Stacija-saņēmēja saņems šos fragmentus un tos glabās montāžas buferī, līdz visi fragmenti tiks pieņemti. Pēc noklusēšanas fragmentācija ir atslēgta (2346 biti – maksimāli pieļaujamais MPDU izmērs). Liela izmēra pakotņu fragmentācijas izmantošana palielina datu apmaiņas starp stacijām drošību. Tā kā katrs datu fragments prasa apstiprinājumu, apmaiņā piedalošo kadru skaits ir lielāks, kā bez fragmentācijas. Līdz ar to, zemās Fragmentation Threshold vērtības var

		palielināt lietderīgo caurlaides spēju pie sliktiem radio signāla izplatīšanās nosacījumiem, toties samazina lietderīgo caurlaides spēju pie stabiliem sakariem.

3.1.2. Statistiskie parametri.

A032 attēlo sīku tīkla aktivitātes statistikas pārskatu, kura veidojas kā radio-interfeisā, tā arī 10BaseT Ethernet-interfeisā. Pamatojoties uz šiem datiem, ir iespējams lokālā tīkla sadales sistēmas veiktspējas novērtējums.

Statistikas tabulās sekundēs norādīts periods, kurā dati tika apkopoti (tas ir nepieciešams vidējo vērtību aprēķināšanai) un skaitītāju ..... laiks (parasti tas ir .....).

Uzskaitīsim dažus statistikas parametrus, kurus izmanto tīkla darba novērtēšanai.

Ethernet-interfeisa A032 statistiskie raksturojumi uzskaitīti tab.3.3.

Tabula 3.3.

Ethernet-savienojuma statistika

Parametrs	Paskaidrojumi
Frames Transmitted	Kadru skaits, kuru pieejas punkts nosūtīja uz Ethernet LAN
Bytes Transmitted	Nosūtīto kadru baitu skaits
Total Frames Seen	Uz Ethernet LAN pārraidīto kadru skaits, kurus redz pieejas punkts
Frames Accepted	Kadru skaits, kurus pieejas punkts saņēma no Ethernet LAN
Data Bytes Rcvd	Saņemto kadru baitu skaits

Tab.3.4. ataino bezvadu savienojumu A032 raksturojumus.

Tabula 3.4.

WLAN-savienojumu statistika

Parametrs	Paskaidrojumi
Frames Transmitted	Nosūtīto datu kadru un administratīvo kadru skaits
Bytes Transmitted	Nosūtīto datu baitu skaits
Frames Received	Saņemto datu kadru un administratīvo kadru skaits
Data Frames Rcvd	Pa radio-savienojumu saņemto datu kadru skaits
Data Bytes Rcvd	Saņemto datu kadru baitu skaits

Svarīgi atzīmēt, ka norādītā statistika apkopojas starp A032 procesoru un PCMCIA radio karti. Ja radio karte uztver kadrus ar kļūdām, tad tās tiks ņemtas vērā MIB (Management Information Base), bet netiks pārraidītas apstrādei uz A032 pamata moduli.

Tab.3.5.. atspoguļo informāciju no MIB saskaņā ar standarta IEEE 802.11 specifikāciju.

Tabula 3.5.

Radio kartes statistika

Parametrs	**Paskaidrojumi**
aTransmitted_MPDU_Count	Uz radio-ēteru pārraidīto MPDU skaits (MAC Protocol Data Unit)
aTransmitted_MSDU_Count	Uz radio-ēteru pārraidīto MSDU ieskaits (MAC Service Data Unit)
aMulticast_Transmitted_Frame_Count	Uz radio-ēteru pārraidīto grupveida ziņojumu skaits
aFailed_Count	Kadru skaits, kurus neizdevās pārraidīt, ņemot vērā atkārtotus mēģinājumus, un kuri tika noņemti
aRetry_Count	Atkārtoti pārraidīto (viens mēģinājums) kadru skaits
aMultiple_Retry_Count	Gadījumi, kad bija nepieciešami vairāki kadra pārraides mēģinājumi
aFrame_Duplicate_Count	Saņemto (un noņemto) dublējošo kadru daudzums
aRTS_Success_Count	Atbildē uz RTS saņemto CTS skaits
aRTS_Failure_Count	RTS skaits, kuri nesaņēma atbildi
aACK_Failure_Count	Reižu skaits, kad apstiprinājums (ACK) netika saņemts pārraides atbildē
aReceived_Frame_Count	Uztverto kadru skaits
aMulticast_Received_Count	Uztverto grupveida ziņojumu skaits
aFCS_Error_Count	Ar kontroles summas kļūdām uztverto kadru skaits

3.1.3. TCP/IP uzstādīšana un vārtejas iestatīšana.

TCIS lokālais tīkls savieno 8 stacionārās darba stacijas, sadalītas 5 segmentos, vienu ar otru un ārējo tīklu, kurš piešķir piekļuvi Web un FTP pakalpojumiem. Bez tam pie jebkura sadales sistēmas mezgla TCIS ir atļauta atklāta pieslēgšanās līdz 32 mobilajām stacijām, kuras atbilst IEEE 802.11 specifikācijai.

TCIS apakštīkla adreses telpa maksimāli atbalsta 254 mezglus (IP maska – 255.255.2555.0). IP adrešu sadalījums starp iekārtām uzbūvēts sekojošā kārtībā (skat. shēmu

pielikumā 1). Adreses 192.168.0.1-192.168.0.10 iedalītas darba stacijām, kuras ietilpst Fast Ethernet segmenta sastāvā uz Eusso komutatora bāzes, kuram nav nepieciešama individuālās IP adreses noteikšana (mijiedarbība starp komutatoru un stacijām notiek uz MAC slāņa). Pārējām stacionārajām darba stacijām (pa vienai uz auditoriju) IP adreses noteiktas pēc kārtulas: 192.168.0.1xx, kur xx – divi pēdējie auditorijas numura skaitļi (piemēram, stacijas Aud309 adrese - 192.168.0.109). Piekļuves punktiem piešķirtas adreses 192.168.0.20y, kur y – piekļuves punkta numurs (piemēram, R1 IP adrese - 192.168.0.201). Mobilās stacijas var saņemt adreses, kuras nav aizņēmušas stacionārās iekārtas (visieteicamāk 192.168.0.210-192.168.0.254 diapazonā).

Vārteja Nokia A032 (ar iekšējo IP adresi 192.168.0.206) nodrošina iekšējā apakštīkla drošību, novēršot nevēlamu piekļuvi tā resursiem no Internet. Šiem mērķiem kalpo tīkla ekrāns (Firewall) ar adrešu translāciju NAT (Network Address Translation), kurā visas iekšējās lokālā tīkla IP adreses pārveido vienā ārējā IP adresē Internet izmantošanai. Lietotāji ārpus tīkla ekrāna neredz reālo lokālā tīkla IP adresi. Līdz ar to, vārteja pārvirza pieprasījumus no vietējā apakštīkla uz Internet ārējo adresi, un šķērso jebkuras tiešās piekļuves no ārējā tīkla uz iekšējo mēģinājumus.

Gadījumā, ja lokālajam tīklam ir ārējā statiskā IP adrese, ir iespējama lietotāju piekļuves organizācija no ārējā tīkla pie iekšējā resursiem, piemēram, FTP vai Web-servera. Tāpēc uz vērtēju tiek uzstādītas NAT holes katram atsevišķam tīkla dienestam, kuri nosaka maršrutu caur tīkla ekrānu pie konkrētas LAN iekārtas.

TCIS apakštīkla vārteja savienota ar reālu IP adrešu ārējo tīklu ar interfeisa 10Base Ethernet palīdzību. Tīkla ekrāna NAT ārējās puses konfigurācija:

External IP address **159.148.161.2**
External DNS IP address **159.148.108.1**
External Gateway **159.148.161.30**
External Subnet Mask **255.255.255.224.**

FTP Popovs serverim ir tieša izeja uz ārējo tīklu (tam ir piešķirta reāla IP adrese - **159.148.161.15**). Piekļuve servera resursiem no iekšējā tīkla īstenojas caur vārteju R6 un komutatoru Eusso USH5005-XPB.

4. BEZVADU LOKĀLĀ TĪKLA AR WDS DROŠĪBA UN VAJIBAS.

4.1. Lokālā tīkla ar WDS drošība.

4.1.1. Pieejas punktu vadības aizsardzība

Lai novērstu nesankcionētu piekļuvi vadības funkcijām Nokia A032, pastāv iespēja izvēlēties nepieciešamo drošības līmeni un uzstādīt paroli.

TCIS tīklā piekļuve interfeisiem A032 ir atļauta tikai no administratora datora, kura MAC adrese norādīta piekļuves punktu iestatījumos. Pastāv arī tāda iespēja, kā klientu staciju selektīvā autentifikācija pēc viņu MAC adresēm, kuras ierakstītas speciālā reģistrā.

4.1.2. Autentifikācijas politika bezvadu tīklā.

Nokia A032 piedāvā būtiskus aizsardzības pasākumus no pa radiokanālu pārraidītās informācijas pārķeršanas un nesankcionētas tīkla pieejamības. Pieejamības vadīšana, galvenokārt, balstās uz autentifikāciju (aizsardzība ar paroli). Informācijas pārtveršanu (noklausīšanos) var novērst izmantojot IEEE 802.11 standarta noteiktu WEP šifrēšanas metodi. Dati skremblējas tā, ka tos saprot tikai avots un adresāts. A032 dod iespēju izvēlēties dažus autentifikācijas un šifrēšanas līmeņus.

TCIS tīklā izmanto atklātu autentifikāciju bez pārraides vides pieejamības ierobežojumiem (līmenis 0). Šajā režīmā visi WEP šifrēšanas algoritmi ir atslēgti. Tāda risinājuma iemesls ir nepieciešamība dot tādu iespēju, kā operatīvais pieslēgums pie jebkuras lietotāju kategorijas (studentu un pasniedzēju no citām profesoru grupām) mobilo klientu darba staciju tīkla resursiem. Pie tam viss, kas jānorāda klienta iestatījumos – tā ir BSSID infrastruktūra, pie kuras tiek plānots pieslēgums. Pārējie iestatījumi tiek noteikti automātiski. Lai nodrošinātu efektīvu resursu pieejamības drošību šajā režīmā, izmanto paroļu aizsardzību operētājsistēmas līmenī.

Līmenis 1 no līmeņa 0 atšķiras ar to, ka piekļuvi tīklam saņem tikai tie klienti, kuru MAC adreses norādītas reģistrā A032.

Pirmie divi līmeņi neaizsargā no pa radiokanālu pārraidītās informācijas pārtveršanas. Lai vienlaicīgi novērstu arī nesankcionētu piekļuvi un noklausīšanos, izmanto WEP šifrēšanu, kuru pielieto otrajā un trešajā aizsardzības līmenī un kuras sarežģītības pakāpe ir atkarīga no atslēgas garuma (2 līmenī 40 bit, 3 līmenī 128 bit).

4.1.2.1. Standarta 802.11 autentifikācijas mehānismi.

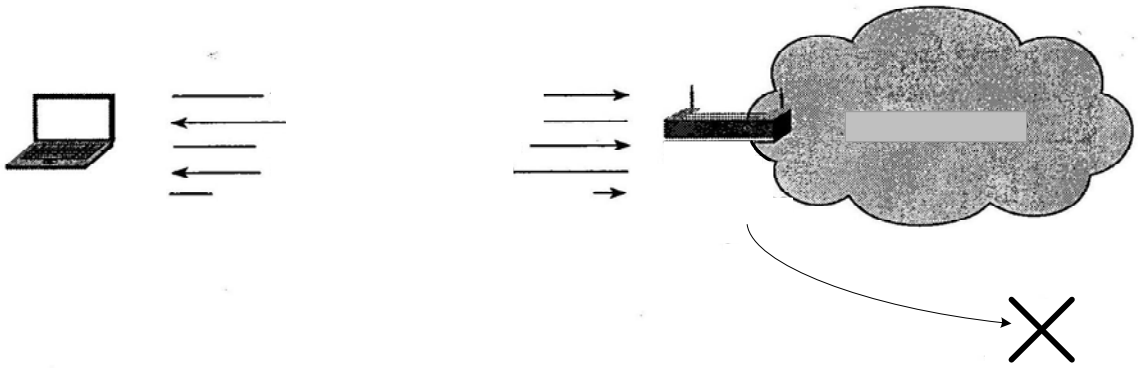
Standarta 802.11 specifikācija atrunā divus mehānismus, kurus var pielietot WLAN klientu autentificēšanai.

- Atklātā autentifikācija (open authentication).
- Autentifikācija ar koplietošanas atslēgu (shared key authentication).

Pēc būtības atklātā autentifikācija ir algoritms ar nulles autentifikāciju (null authentication algorithm). Piekļuves punkts pieņem jebkuru autentifikācijas pieprasījumu. Tas var būt vienkārši bezjēdzīgs signāls, kuru izmanto, lai norādītu tieši uz šī autentifikācijas algoritma pielietošanu. Tomēr atklātā autentifikācija spēlē noteiktu lomu standarta 802.11 tīklos. Tik vienkāršas autentifikācijas prasības ļauj iekārtām ātri saņemt piekļuvi tīklam.

Piekļuves kontrole pie atklātās autentifikācijas īstenojas, izmantojot iepriekš konfigurētu WEP-atslēgu piekļuves punktā un klientu stacijā. Šai stacijai un piekļuves punktam jābūt ar vienādu atslēgu, jo tad tie var saistīties savā starpā. Ja stacija un piekļuves punkts neatbalsta WEP algoritmu, BSS nav iespējams nodrošināt aizsardzību. Pie tāda BSS var pieslēgties jebkura iekārta, un visi datu freimi tiek pārraidīti nešifrētā veidā.

Pēc atklātās autentifikācijas izpildes un asociēšanas procesa pabeigšanas, klients var sākt datu pārraidi un uztveri. Ja klients ir konfigurēts tā, ka viņa atslēga atšķiras no piekļuves punkta atslēgas, tad viņš nevarēs pareizi nošifrēt un atšifrēt freimus, un tādus freimus nometīs kā piekļuves punkts, tā arī klientu stacija. Šis process ir diezgan efektīvs BSS pieejamības kontroles līdzeklis (Att. 4.1.).

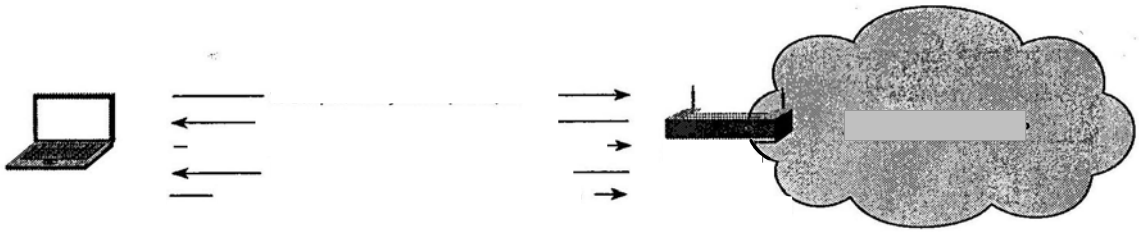


Att. 4.1. Atvērtās autenfikacijas process pie WEP-atslēgu dažādības

Atšķirībā no atklātās autentifikācijas, pie autentifikācijas ar koplietošanas atslēgu ir nepieciešams, lai klientu stacija un piekļuves punkts spētu atbalstīt WEP un būtu ar vienādām WEP-atslēgām. Autentifikācija ar koplietošanas atslēgu process īstenojas sekojošā veidā.

1. Klients piekļuves punktam pārraida autentifikācijas ar koplietošanas atslēgu pieprasījumu.
2. Piekļuves punkts atbild ar izsaukuma freimu (challenge frame), kas satur atklātu tekstu.
3. Klients šifrē izsaukumu un pārraida to atpakaļ piekļuves punktam.
4. Ja piekļuves punkts var pareizi atšifrēt šo freimu un saņemt savu izejas izsaukumu, klientam tiek nosūtīts ziņojums par veiksmīgu autentifikāciju.
5. Klients saņem piekļuvi WLAN.

Priekšnosacījumi, uz kuriem balstīta autentifikācija ar koplietošanas atslēgu, ir tieši tādi paši, kuri tika paredzēti pie atklātās autentifikācijas, kura izmantoja WEP-atslēgu kā piekļuves kontroles līdzekli. Atšķirība starp šīm abām shēmām ir tāda, ka, izmantojot autentifikāciju ar koplietošanas atslēgu mehānismu, klients sevi nevar asociēt no piekļuves punkta, ja viņa atslēga nav konfigurēta vajadzīgajā veidā. Att. 4.2. shematiski parādīts autentifikācijas ar koplietošanas atslēgu process.

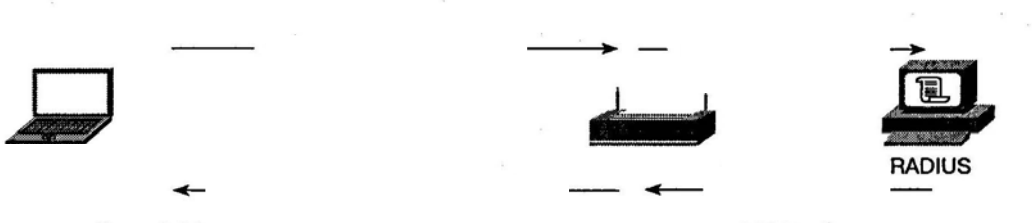


Att. 4.2. Autentifikacijas process ar kopīgi izmantojamo atslēgu

4.1.2.2. Autentifikācija izmantojot MAC-adreses.

Autentifikācija izmantojot MAC-adreses nav ar standartu 802.11 specificēta, tomēr daudzi ražotāji ir ar to nodrošinājušies. Autentifikācijas izmantojot MAC-adreses gaitā tiek pārbaudīta klienta MAC adreses atbilstība lokāli konfigurētam atļauto adrešu sarakstam vai arī sarakstam, kurš glabājas uz ārējā autentifikācijas servera (Att. 4.3.). Autentifikācija izmantojot MAC-adreses pastiprina atklātās autentifikācijas un autentifikācijas ar koplietošanas atslēgu darbību, ko nodrošina standarts 802.11, līdz ar to potenciāli samazinot varbūtību, ka neautorizētas iekārtas saņems piekļuvi tīklam. Piemēram, tīkla administrators var vēlēties ierobežot piekļuvi noteiktam pieejas punktam trim konkrētām iekārtām. Ja visas

stacijas un visi BSS piekļuves punkti izmanto vienādas WEP-atslēgas, tad, izmantojot atklāto autentifikāciju un autentifikāciju ar koplietošanas atslēgu, tādu scenāriju ir grūti realizēt. Lai pastiprinātu standarta 802.11 autentifikācijas mehānisma darbību, viņš var pielietot autentifikāciju izmantojot MAC-adreses.



Att. 4.3. Autentifikācijas process ar MAC- adrešu izmantošanu

4.1.3. Šifrēšanas sistēmu apskats.

Šifrēšanas mehānismu pamatā ir algoritmi, kuri randomizē datus. Izmanto divus šifru veidus.

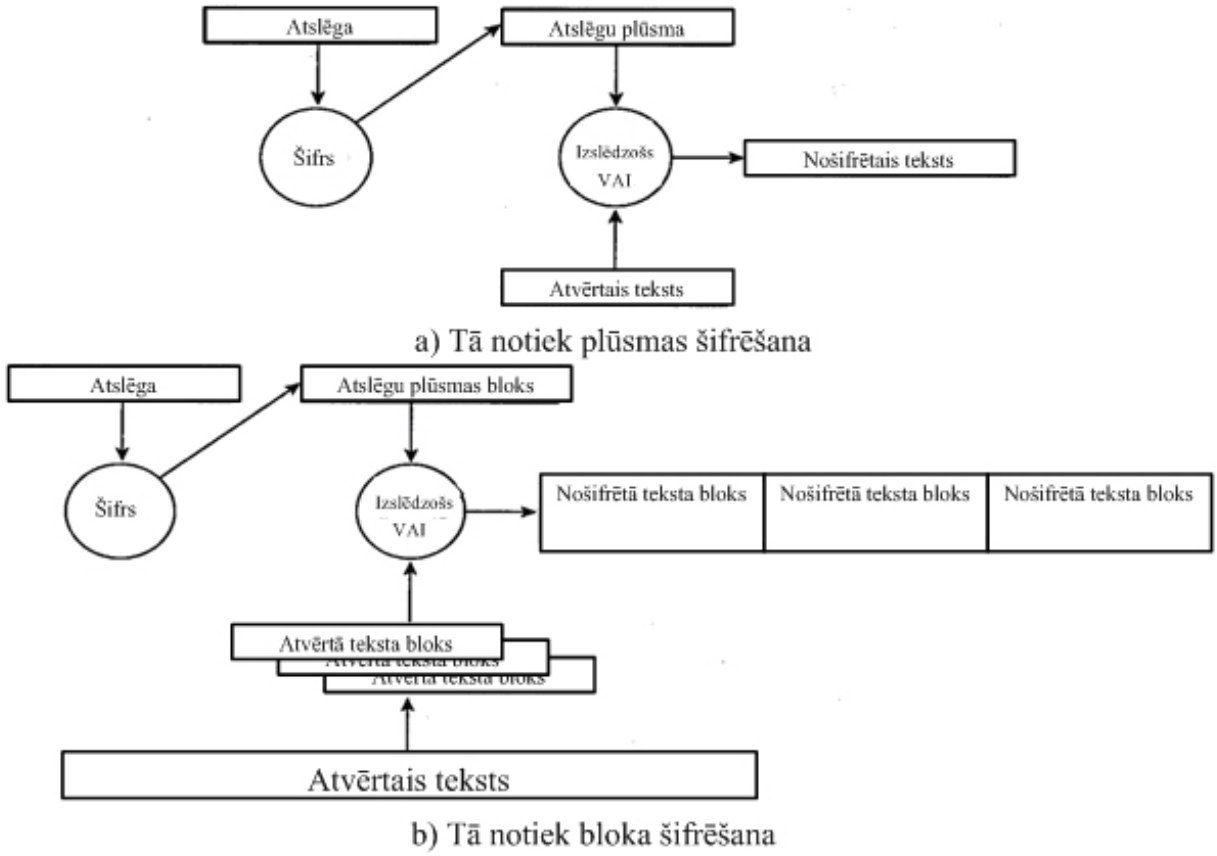
- Plūsmas (grupas) šifrs.
- Bloku šifrs.

Abu veidu šifri darbojas ģenerējot atslēgas plūsmu (key stream), iegūtu pamatojoties uz slepenās atslēgas vērtību. Atslēgas plūsma sajaucas ar datiem vai atklātu tekstu, kā rezultātā tiek iegūts kodēts izejas signāls vai šifrēts teksts. Nosauktie divu veidu šifri atšķiras pēc datu apjomiem, ar kuriem tie var strādāt vienlaicīgi.

Plūsmas šifrs ģenerē nepārtrauktu atslēgas plūsmu, balstoties uz atslēgas vērtību. Piemēram, plūsmas šifrs spēj ģenerēt 15-kārtu atslēgas plūsmu viena freima šifrēšanai un 200-kārtu atslēgas plūsmu cita freima šifrēšanai. Att. 4.4. a) ilustrēts plūsmas šifra darbs. Plūsmas šifri – tie ir nelieli un efektīvi šifrēšanas algoritmi, pateicoties kuriem, slodze uz centrālo procesoru ir neliela. Visizplatītākais ir plūsmas šifrs RC4, kurš ir balstīts WEP algoritma pamatā.

ABC klienta MAC- adrese

Bloku šifrs, otrādi, ģenerē vienīgo fiksēta izmēra šifrēšanas atslēgas plūsmu. Atklāts teksts dalās blokos, un katrs bloks ar atslēgas plūsmu sajaucas neatkarīgi. Ja atklātā teksta bloks ir mazāks, kā atslēgas plūsmas bloks, tad pirmais papildinās, lai iegūtu vajadzīgā izmēra bloku. Att. 4.4. b) ilustrēts bloka šifra darbs. Fragmentācijas process, kā arī citas šifrēšanas īpatnības, izmantojot bloku šifru, izsauc paaugstinātu pieladi centralajam procesoram.



Att. 4.4. a) Plūsmas šifrēšana; b) Bloka šifrēšana

Aprakstītais šifrēšanas process plūsmu un bloku šifriem, tiek saukts par *šifrēšanas režīmu ar elektronisko kodu grāmatas palīdzību* (Electronic Code Book, ECB). ECB šifrēšanas režīms raksturojas ar to, ka viens un tas pats atklātais teksts pēc šifrēšanas pārveidojas vienā un tajā pašā nošifrētā tekstā. Šis faktors potenciāli rada draudus drošībai, jo ļaundari var iegūt nošifrētā teksta paraugus un izvirzīt kaut kādus nodomus par izejas tekstu.

Dažas šifrēšanas metodes ļauj šo problēmu atrisināt.

- Inicializācijas vektori (initialization vectors, IV).
- Atgriezeniskās saites režīmi (feedback modes).

4.1.3.1. Šifrēšana pēc algoritma AES.

Ir zināms, ka šifrēšanai un autentifikācijai, kuras izpilda saskaņā ar standartu 802.11, ir vājās puses. IEEE un WPA ar protokola TKIP palīdzību pastiprināja algoritmu WEP un piedāvā spēcīgu autentifikācijas mehānismu pēc standarta 802.Hi, kurš nodrošina standarta bezvadu LAN aizsardzību. Tai pašā laikā IEEE izskata iespēju pastiprināt šifrēšanas

mehānismu. Tāpēc IEEE adaptēja algoritmu AES, lai to pielietotu attiecībā pret nodaļu, kas skar standarta 802.1N piedāvātos aizsargājamos datus. WPA komponentes nenodrošina atbalstu šifrēšanai pēc algoritma AES. Tomēr pēdējās WPA versijas, iespējams, tiks realizētas saskaņā ar standartu 802.1N, un lai nodrošinātu mijiedarbību, atbalstīs šifrēšanu pēc algoritma AES

Algoritms AES sevī ietver nākamās paaudzes šifrēšanas līdzekļus, kurus ir atbalstījis ASV Nacionālais standartu un tehnoloģiju institūts (NIST). Nosauktais institūts piedāvāja kriptogrāfijas asociācijai izstrādāt jaunus šifrēšanas algoritmus. Šiem algoritmiem jābūt pilnībā atklātiem, un tos var izmantot bez maksas. Kandidāti bija pārbaudīti jautājumos par "kriptogrāfisko izturību" un tās praktisko pielietojumu. Par finālistu un pieņemto metodi kļuva tā saucamais *Rijndela algoritms* (Rijndael algorithm). Tāpat kā daudzi citi šifri, AES prasa atgriezeniskākas saites režīmu, lai izvairītos no riska, kas saistīts ar ECB režīmu (atgādināsim, tas ir šifrēšanas režīms ar elektronisko kodu grāmatas palīdzību). IEEE izstrādāja AES režīmu, kas paredzēts izmantošanai bezvadu LAN. Šo režīmu sauc par *šifra bloku konkatenāciju skaitīšanas režīmu* (Cipher Block Chaining Counter Mode, CBC-CTR) ar ziņojumu par šifra bloku konkatenācijām autentifikācijas kontroli (Cipher Block Chaining Message Authenticity Check, CBC-MAC), visu kopā to apzīmē ar abreviatūru AES-CCM. CCM režīms sevī ietver šifrēšanas režīma CBC-CTR un ziņojumu autentifikācija kontroles algoritma kombināciju. Šīs funkcijas kombinētas, lai nodrošinātu šifrēšanu un pārbaudītu ziņojumu integritāti vienā risinājumā.

CBC-CTR šifrēšanas algoritms strādā izmantojot skaitītāju, lai papildinātu atslēgas plūsmas. Šī skaitītāja vērtība pieaug par 1 pēc katra bloka šifrēšanas. Tāds process nodrošina unikālas atslēgas plūsmas iegūšanu katram blokam. Atklāta teksta freims dalās 16-baitu blokos. Pēc katra bloka šifrēšanas skaitītāja vērtība palielinās par 1, un tā līdz tam brīdim, kamēr būs pabeigta visu bloku šifrēšana. Katram jaunam freimam skaitītājs pārstādās.

CBC-MAC šifrēšanas algoritms izpildās izmantojot CBC šifrēšanas rezultātu attiecībā pret visu freimu, saņēmēja adresi, avota un datu adresi. Rezultāta 128-kārtu izeja nošķeļas līdz 64 bitiem, lai to varētu izmantot pārraidāmajā freimā.

CBC-MAC strādā ar pazīstamām kriptogrāfijas funkcijām, taču tam ir izdevumi, saistīti ar divu operāciju izpildīšanu – šifrēšana un ziņojumu integritāte. Šis process prasa nopietnus aprēķinus un būtiski palielina šifrēšanas "pieskaitāmās izmaksas".

4.1.3.2. Inicializācijas vektori.

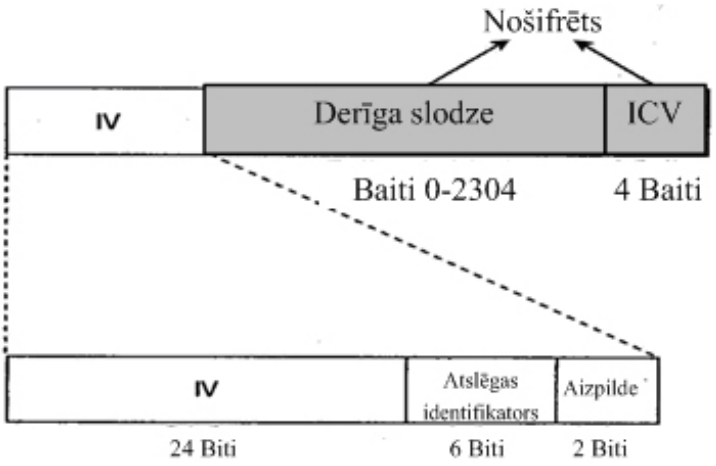
Inicializācijas vektors – tas ir numurs, kuru pievieno atslēgai, kā rezultātā rodas atslēgas plūsmas informācijas izmaiņas. Inicializācijas vektors saistās ar atslēgu pirms atslēgas plūsmas ģenerācijas sākuma. Inicializācijas vektors visu laiku mainās, tas pats notiek ar atslēgas plūsmu. Teksts sajaucas ar atslēgas plūsmu, papildinātu ar inicializācijas vektoru, cita šifrēta teksta iegūšanai.

Pievērsiet uzmanību, ka otrā gadījumā šifrētais teksts atšķiras no pirmā. Standarts 802.11 rekomendē izmainīt inicializācijas vektoru uz pēcfreima (on a per-frame basis). Tas nozīmē, ja viens un tas pats freims tiks pārraidīts divreiz, diezgan liela izrādīsies varbūtība tam, ka nošifrētais teksts būs dažāds.

4.1.3.3. Kodēšana pēc standarta 802.11.

Standarta 802.11 specifikācija paredz datu aizsardzības nodrošināšanu izmantojot algoritmu WEP. Šis algoritms balstās uz simetriska plūsmas šifra RC4 izmantošanu. RC4 simetriskums nozīmē, saskaņotas WEP-atslēgas ar 40 vai 104 bitu lielu izmēru statiski konfigurējas klientu iekārtās un pieejas punktos. WEP algoritms tika izvēlēts, galvenokārt, tāpēc, ka tas neprasa apjomīgus aprēķinus. Lai gan personālie datori ar standarta 802.11 bezvadu tīklu platēm tagad ir plaši izplatīti, 1997gadā situācija bija savādāka. Lielākā daļa no bezvadu LAN iekļautajām iekārtām ir specializētās iekārtas (application-specific devices, ASD). Piemēram, par tādu iekārtu var kalpot svītru kodu lasītājs, plakanvirsmu PD (tablet PC) un standarta 802.11 telefoni. Lietojumprogrammas, kuras izpildīja šīs specializētās iekārtas, parasti neprasīja lielu aprēķinu jaudu, tāpēc ASD tika aprīkoti ar vājiem procesoriem. WEP – vienkārši pielietojams algoritms, kura pierakstam dažos gadījumos pietiek ar 30 kodu rindām. Mazie ražošanai neparedzētie izdevumi, kuri rodas pielietojot šo algoritmu, veido to par ideālu šifrēšanas algoritmu.

Lai izvairītos no šifrēšanas ECB režīmā, WEP izmanto 24-kārtu inicializācijas vektoru, kurš tiek pievienots atslēgai pirms apstrādes pēc RC4 algoritma veikšanas. Att. 4.5. parādīts freims, kurš šifrēts pēc WEP algoritma izmantojot inicializācijas vektoru.



Att. 4.5. Freims, kurš ir nošifrēts pa WEP algoritmu

Inicializācijas vektoram jāmainās pēcfreima veidā, lai izvairītos no IV-kolīzijām. Tāda veida kolīzijas notiek tad, kad izmanto vienu un to pašu inicializācijas vektoru un vienu un to pašu WEP-atslēgu, kā rezultātā freima šifrēšanai tiek izmantota viena un tā pati atslēgas plūsma. Tāda kolīzija dod ļaundariem lielāku iespēju atminēt atklātā teksta datus, līdzīgu elementu salīdzināšanas ceļā. Izmantojot inicializācijas vektoru, ir svarīgi novērst līdzīgu scenāriju, tāpēc inicializācijas vektoru bieži nomaina. Vairums ražotāju savās bezvadu LAN paredzētajās iekārtās piedāvā pēcfreimu inicializācijas vektorus.

Standarta 802.11 specifikācija prasa, lai vienādas WEP-atslēgas tiktu konfigurētas kā uz klientu, tā arī uz iekārtām, kas veido tīkla infrastruktūru. Var noteikt līdz četrām atslēgām uz vienu iekārtu, taču vienlaicīgi pārraidāmo freimu šifrēšanai izmanto tikai vienu no tām.

WEP-šifrēšanu izmanto tikai attiecībā uz datu freimiem un autentificēšanas ar koplietošanas atslēgu procedūras laikā. Pēc WEP algoritma šifrējas nākamie standarta 802.11 datu freima lauki.

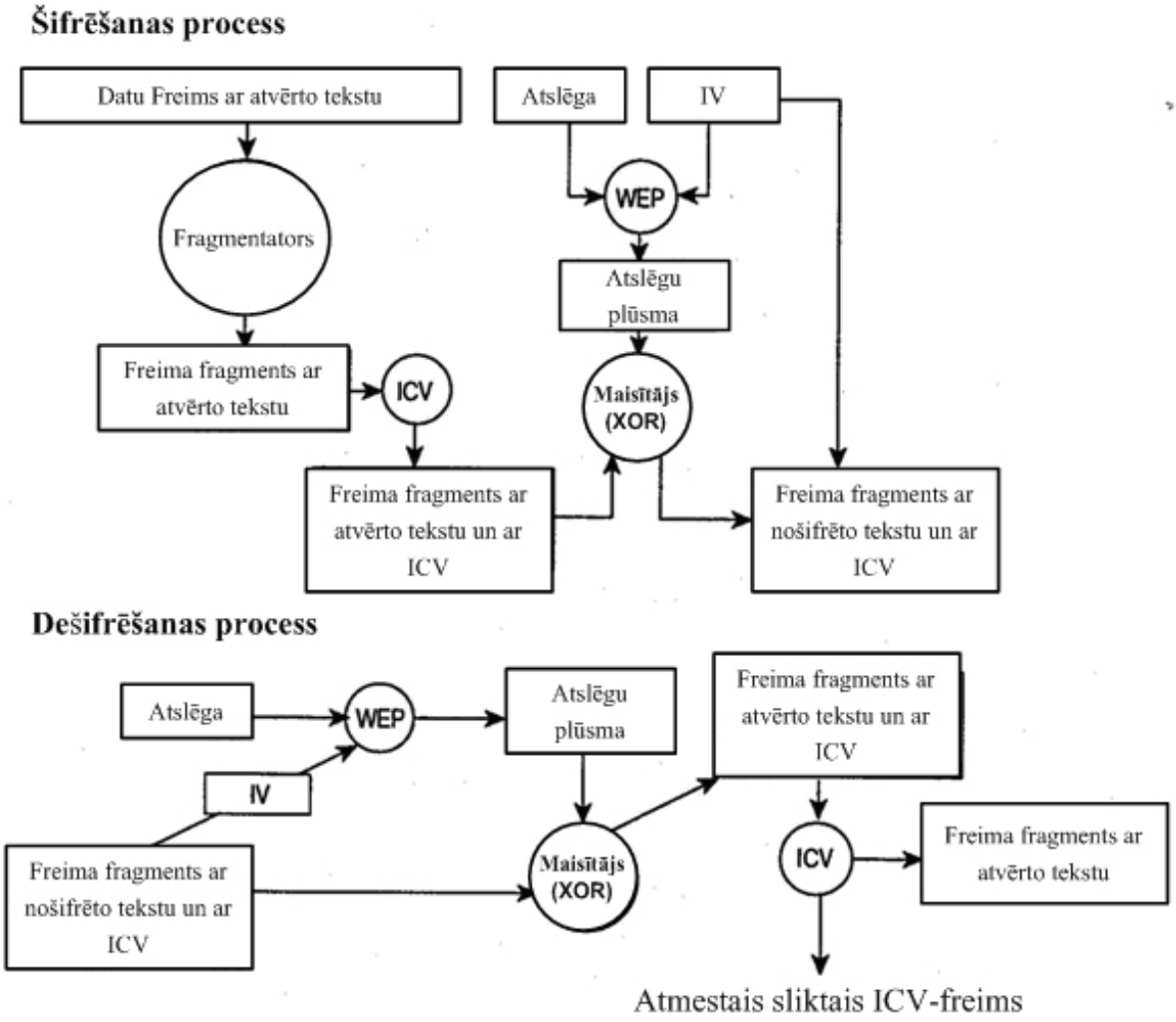
- Dati vai lietderīgā slodze (payload).
- Integritātes kontroles pazīme (integrity check value, ICV).

Visu pārējo lauku vērtības tiek pārraidītas bez šifrēšanas. Inicializācijas vektors jāpārraida nenošifrēts freima iekšienē, lai uztverošā stacija varētu to saņemt un izmantot korektai lietderīgās slodzes un ICV atšifrēšanai. Att. 4.6. shematiski parādīts datu freima šifrēšanas, pārraides, uztveršanas un atšifrēšanas process saskaņā ar WEP algoritmu.

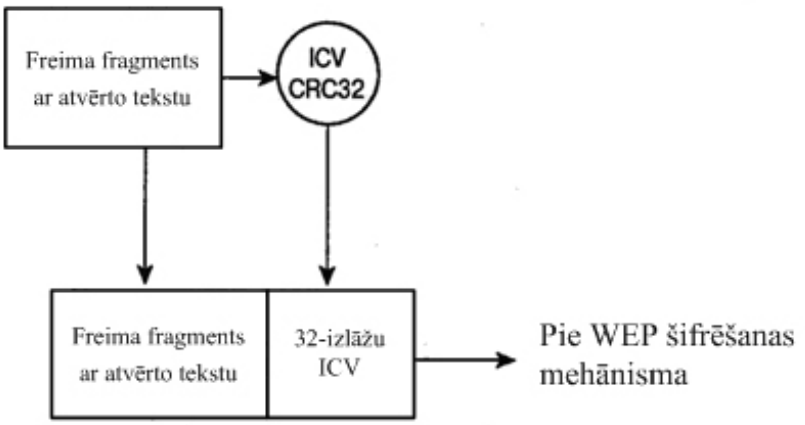
Standarta 802.11 specifikācija datu šifrēšanas pielikumā piedāvā izmantot 32-kārtas vērtību, kuras funkcijas – īstenot integritātes kontroli. Šī integritātes kontroles pazīme uztvērējam paziņo par to, ka freims pārraides procesā saņemts bez bojājumiem. Tā pastiprina

freima kontroles secības (FCS) darbību 1 un 2 līmenim, kuras uzdevums – atklāt pārraides procesā radušās kļūdas.

Integritātes kontroles pazīmi aprēķina pēc visiem freima laukiem, izmantojot 32-kārtas polinoma kontroles funkciju un ciklisko redundances kodu (CRC-32). Stacija-nosūtītāja izskaitļo šo vērtību un rezultātu ievieto ICV laukā. ICV lauka vērtība tiek iekļauta freima daļā, kuru šifrē pēc WEP algoritma, tāpēc ļaundari tik viegli to nevar "ieraudzīt". Freima saņēmējs to atšifrē, aprēķina ICV vērtību un rezultātu salīdzina ar saņemtā freima ICV lauka vērtību. Ja šīs vērtības sakrīt, freims tiek uzskatīts par īstu, neviltotu. Ja tās nesakrīt, tāds freims tiek nomests. Att. 4.7. parādīta ICV mehānisma funkcionēšanas diagramma.



Att. 4.6. Šifrēšanas un dešifrēšanas process



Att. 4.7. ICV mehānisma funkcionēšanas diagramma

4.2. WLAN ievainojamība.

4.2.1. Standarta 802.11 aizsardzības sistēmas ievainojamība.

Iepriekšējā nodaļā tika stāstīts par to, kā īstenojas autentifikācija un šifrēšana izmantojot standarta 802.11 iekārtas. Nav noslēpums, ka standartā 802.11 specificētā aizsardzības sistēma ir nepilnīga. Drīz pēc standarta 802.11 apstiprināšanas parādījās raksti, kuros tika norādītas standarta 802.11 autentificēšanas un šifrēšanas pēc WEP algoritma vājās vietas.

4.2.2. Atklātās autentifikācijas ievainojamība.

Izmantojot atklātās autentifikācijas mehānismu, piekļuves punktam netiek dota iespēja pārbaudīt klienta tiesības. Šādas iespējas nepastāvēšana ir aizsardzības sistēmas trūkums, ja bezvadu lokālajā tīklā neizmanto WEP-šifrēšanu. Atklātās autentifikācijas mehānisms nepiedāvā līdzekļus, lai noteiktu, kurš izmanto WLAN iekārtu – statiskā WEP piekļuves punkts vai klients. Autorizēta iekārta neautorizēta lietotāja rokās - tas ir drauds drošībai, vienlīdz spēcīgs kā kaut kādas tīkla aizsardzības trūkums.

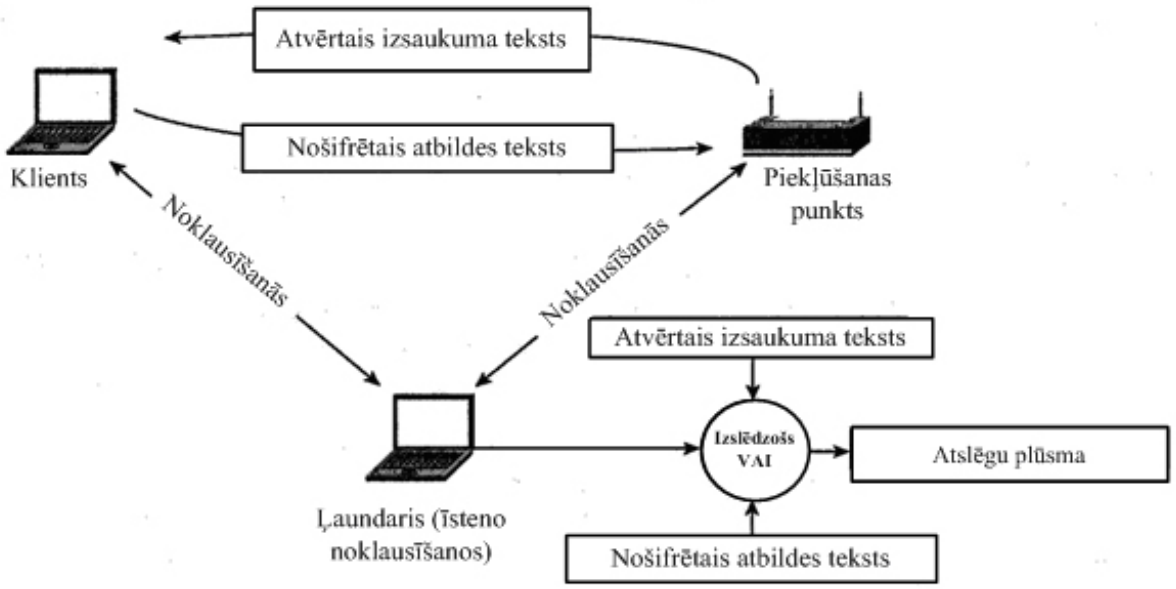
4.2.3. Autentifikācijas ar koplietošanas atslēgu ievainojamība.

Autentifikācijas ar koplietošanas atslēgu gadījumā nepieciešams, lai klients izmantotu iepriekš izdalītu koplietošanas atslēgu un šifrētu no piekļuves punkta saņemto izsaukuma

tekstu. Piekļuves punkts autentificē klientu atšifrējot nošifrēto, izmantojot atbildes koplietošanas atslēgu, un pārbaudot, vai izsaukuma iegūtais teksts pilnībā atbilst nosūtītajam.

Izsaukuma teksta apmaiņas process īstenojas pa bezvadu sakaru kanālu un ir uzbrukumu ievainojams, kas ir iespējams zinot atklāto tekstu. Šī ievainojamība, autentifikācijas ar koplietošanas atslēgu gadījumā, ir pamatota ar matemātiskām metodēm, kuras atrodas šifrēšanas pamatā. Iepriekš šajā nodaļā tika runāts par to, ka kodēšanas process sastāv no atklātā teksta sajaukšanās ar atslēgas plūsmu un no rezultātā nošifrētā teksta iegūšanas. Sajaukšanās process sevī ietver binārās matemātiskās operācijas izpildīšanu, kuru sauc par 'izslēgšanas VAI' (XOR). Ja atklātu tekstu sajauc ar attiecīgu nošifrētu tekstu, šīs operācijas izpildīšanas rezultātā tiks iegūts sekojošs pāris: atslēgas plūsma, kuru izmanto WEP-atslēgai, un inicializācijas vektors.

Ļaundaris var pārtvert kā atklātu, tā arī nošifrētu atbildes tekstu. Ja viņš, attiecībā pret šīm vērtībām, izpilda 'izslēgšanas VAI', tad ļaundaris var iegūt spēkā esošu atslēgas plūsmu. Pēc tam viņš šo atslēgas plūsmu var izmantot freimu atšifrēšanai. Šo freimu izmērs ir vienāds ar atslēgas plūsmas izmēru, jo atslēgas plūsmas iegūšanai izmantotais inicializācijas vektors ir tāds pats, kā atšifrētajam freimam. Att. 4.8. parādīts, kā uzbrūkot tīklam ļaundaris spēj izsekot autentifikācijas ar koplietošanas atslēgu procesam un iegūt atslēgas plūsmu.



Att. 4.8. Autentifikacijas mehānisma vārīgums ar kopīgi izmantojamu atslēgu

4.2.4. Autentifikācijas izmantojot MAC-adreses ievainojamība.

MAC-adreses tiek pārsūtītas ar nenošifrētu standarta 802.11 freimu palīdzību, kā tas arī ir atrunāts šī standarta specifikācijā. Rezultātā bezvadu LAN, kuros pielieto autentifikāciju izmantojot MAC-adreses, ir uzbrukumu ievainojami, kuru gaitā ļaundari nokļūst autentifikācijā izmantojot MAC-adreses, imitējot likumīgo MAC-adresi.

MAC-adreses imitācija iespējama standarta 802.11 tīklu platēm, kuras ļauj universāli-noteikto adresi (universally administered address, UAA) aizvietot ar lokāli-noteikto (locally administered address, LAA). Universālā adrese – tā ir MAC-adrese, kuru ražotājs ir nokodējis tīkla kartei. Uzbrucējs var izmantot protokola analizatoru, lai noteiktu BSS atļauto MAC-adresi un tīkla palti, kura pieļauj adreses lokālo misiju, atļautās MAC-adreses imitācijai.

4.2.5. WEP-šifrēšanas ievainojamība.

Visnopietnākās un grūtāk pārvaramās standarta 802.11 tīklu aizsardzības problēmas izvirzīja kriptogrāfijas analītiķi Flurers (Fluhrer), Mantins (Mantin) un Šamirs (Shamir). Savā rakstā viņi parādīja, ka WEP-atslēgu var iegūt atsevišķu freimu, izplatītu bezvadu LAN, pasīvās uzkrāšanas ceļā.

Ievainojamība pamatota ar to, kā WEP mehānisms pielieto atslēgas sastādīšanas algoritmu (key scheduling algorithm, KSA), balstoties uz plūsmas šifru RC4. Daļa inicializācijas vektoru (tos sauc par vājie IV — weak IV) spēj atklāt atslēgas bitus statiskas analīzes veikšanas rezultātā. Kompānijas AT&T un universitātes Rice pētnieki, kā arī AirSnort pielikuma izstrādātāji izmantoja šo ievainojamību un noskaidroja, ka WEP-atslēgu ar 40 vai 104 bitu lielu garumu var iegūt pēc 4miljonu freimu apstrādes. Pirmajiem standarta 802.11b bezvadu LAN tas nozīmē, ka tiem aptuveni vienu stundu freimi ir jāpārraida, un pēc tam var izvest 104-kārtu WEP-atslēgu. Līdzīga ievainojamība padara WEP par neefektīvu informācijas aizsardzības nodrošināšanas mehānismu.

Uzbrukums ir pasīvs, ja uzbrucējs vienkārši noklausās BSS un pārraidītos freimus uzkrāj. Atšķirībā no autentificēšanas ar koplietošanas atslēgu ievainojamības, uzbrucējs, kā parādīja Flurers, Mantins un Šamirs, var iegūt ne tikai atslēgas plūsmu, bet arī funkcionējošu WEP-atslēgu. Šī informācija ļaus uzbrucējam saņemt pieeju BSS kā autentificēšanas iekārtai bez tīkla administratora ziņas. Ja tāda veida uzbrukumi izrādīsies nepietiekami, tad, kā rāda teorija, veikt tos uz WEP vai citu mehānismu (tiesa, praksē tāda veida uzbrukumi nav veikti). Šis loģiski iespējamais uzbrukums var būt balstīts uz metodēm, kuras pielieto aizsardzības

pārvarēšanai, ko nodrošina autentifikācijas ar koplietošanas atslēgu mehānisms: lai iegūtu atslēgas plūsmu: izmanto atklāto tekstu un tam atbilstoši nošifrēto tekstu.

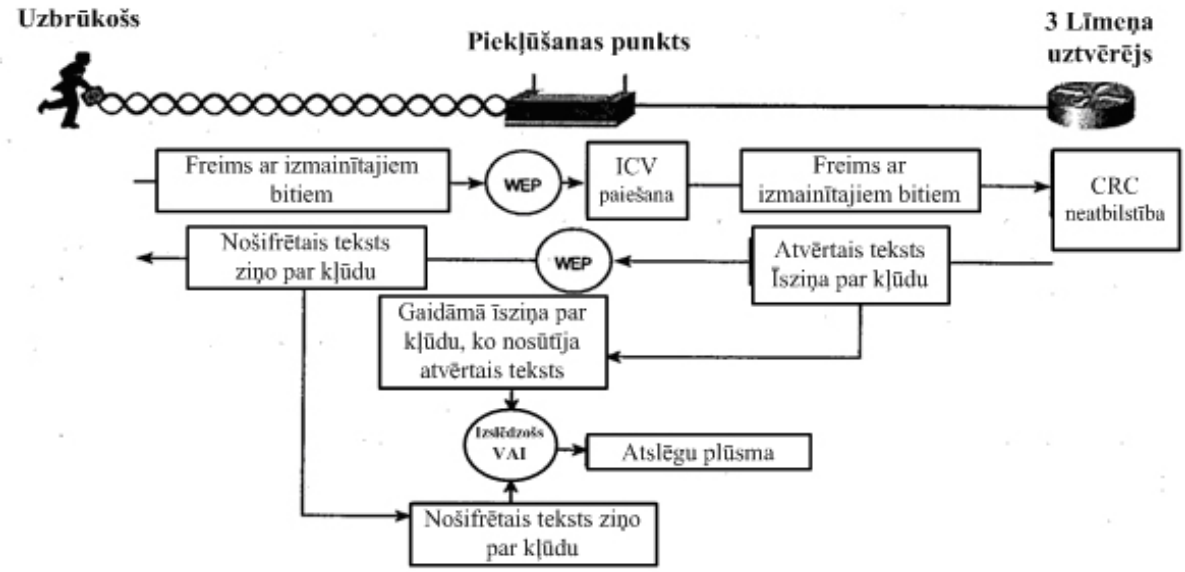
Kā jau tika sacīts, izvesto atslēgas plūsmu var izmantot, lai atšifrētu pāra 'inicializācijas vektors – WEP-atslēga' un noteikta garuma freimus. Abstrakti var pieņemt, ka uzbrucējs noklausīsies tīklu ar mērķi uzkrāt pēc iespējas lielāku tādu atslēgu plūsmu skaitu, lai izveidotu atslēga-plūsma datu bāzi, uzlauztu tīklu un saņemtu iespēju atšifrēt freimus. Bezvadu LAN, kurā neizmanto autentificēšanu ar koplietošanas atslēgu, uzbrukums izmantojot freima bitu apstrādi ļauj ļaundariem īsā laikā izvest lielu atslēgu plūsmu daudzumu.

Uzbrukumi izmantojot bitu apstrādi (vai "bitu žonglēšana", bit flipping) balstās uz integritātes kontroles pazīmes ievainojamību (ICV). Dotais mehānisms bāzējas uz polinomu funkciju CRC-32. Taču šī funkcija, kā ziņojuma integritātes kontroles līdzeklis, ir neefektīva. Funkcijas CRC-32 matemātiskās īpatnības ļauj viltot freimu un modificēt ICV vērtību, pat ja freima izejas saturs nav zināms.

Lai gan dažādiem freimiem lietderīgo datu izmērs var būt dažāds, daudz standarta 802.11 datu freimu elementi paliek vieni un tie paši un vienās un tajās pašās pozīcijās. Uzbrucējs šo faktu var izmantot savā labā un freima daļu ar lietderīgo informāciju viltot, lai modificētu daudz augstāka slāņa pakotni. Uzbrukuma, izmantojot bitu apstrādi, realizācijas scenārijs var būt sekojošs (Att. 4.9.).

1. Uzbrucējs satver bezvadu LAN freimu.
2. Uzbrucējs izmaina freima lietderīgās slodzes gadījuma bitus (flips random bits).
3. Uzbrucējs modificē ICV (sīkāk par to - zemāk).
4. Uzbrucējs pārraida modificēto freimu.
5. Uztvērējs (klients vai pieejas punkts) saņem freimu un izskaitļo freima satura ICV.
6. Uztvērējs salīdzina aprēķināto ICV ar vērtību, kura glabājas ICV freima laukā.
7. Uztvērējs pieņem modificēto freimu.
8. Uztvērējs pārraida modificēto freimu uz daudz augstāka līmeņa iekārtu (atkārtotājs vai vadītāja-datora).
9. Tā kā pakotnē 3 līmeņa biti ir izmainīti, 3 līmeņa kontroles summa izrādās nepareiza.
10. Uztvērēja IP protokols izdod kļūdas ziņojumu.
11. Uzbrucējs saņem ziņas par bezvadu LAN, analizējot nenošifrēto kļūdas ziņojumu.
12. Saņemot kļūdas ziņojumu, uzbrucējs izved atslēgas plūsmu, kā gadījumā ar atkārtošanos IV.

Tāda uzbrukuma pamats ir ICV neatbilstība prasītai vērtībai. ICV vērtība atrodas ar WEP palīdzību nošifrētā freima daļā



Att. 4.9. Uzbrukums ar bitu apstrādāšanas izmantošanu

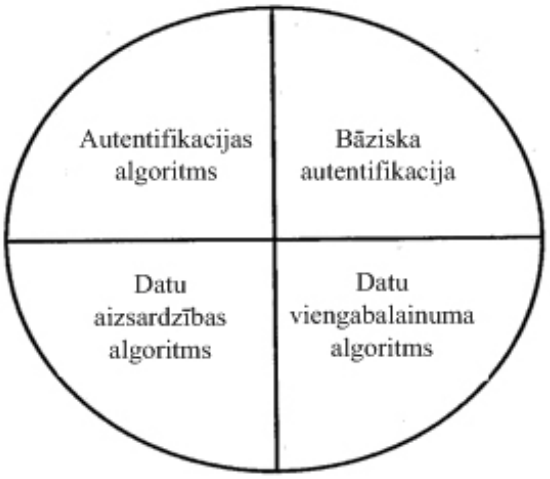
4.3. Standarta 802.11 aizsargātie LAN.

Rūpniecība pārvarēja standarta 802.11 autentificēšanas un tīklu aizsardzības mehānismu pašas vājākās vietas. Lai piedāvātu lietotājiem aizsardzības nodrošināšanas, tīklu mērogošanas un vadīšanas risinājumus, IEEE palielināja standarta 802.11 tīklu aizsardzību, izstrādājot uzlabotu autentifikācijas un šifrēšanas mehānismu. Šī izmaiņas tika ieviestas standarta 802.11i projektā. Uz šodien 802.11i projekts kā standarts nav apstiprināts, tāpēc Alianse Wi-Fi (Wi-Fi Alliance) apkopoja standartam 802.11i atbilstošu komponenšu apakškopu, kura ieguva nosaukumu "aizsargātā Wi-Fi pieeja" (Wi-Fi Protected Access, WPA). Dotajā sadaļā sīki aprakstīti standarts 802.11i un WPA komponentes.

Lai gan līdz šim brīdim šajā sadaļā tika aplūkoti standarta 802.11 tīklu aizsardzības, kā arī WEP-šifrēšanas un autentificēšanas – atklātās vai ar koplietošanas atslēgu – koplietošanas jautājumi, daudzi kļūdaini uzskata, ka WEP – tā ir vienīgā bezvadu LAN aizsardzības nodrošināšanas komponente. Patiesībā bezvadu tīklu aizsardzībai ir četras komponentes.

- **Bāzes autentifikācija** (authentication framework). Tas ir mehānisms, kurš pastiprina autentificēšanas algoritma darbību, organizējot aizsargātu ziņojumu apmaiņu starp klientu, pieejas punktu un autentificēšanas serveri.
- **Autentifikācijas algoritms.** Tas ir algoritms, ar kura starpniecību tiek apstiprinātas lietotāja pilnvaras.
- **Datu aizsardzības algoritms.** Nodrošina datu freimu aizsardzību, pārraidot to caur bezvadu vidi.
- **Datu integritātes nodrošināšanas algoritms** (data integrity algorithm). Nodrošina datu integritāti pārraidot tos caur bezvadu vidi, ļaujot uztvērējam pārliecināties par to, ka dati netika samainīti.

  Nosauktās četras komponentes parādītas Att. 4.10.



Att. 4.10. Četri bezvadu tīklu aizsardzības sastādošās sistēmas

4.3.1. Pirmā komponente: bāzes autentifikācija.

Standarta 802.11 autentifikācijas pamats ir standarta 802.11 autentifikācijas dienesta freims. Šis dienesta freims palīdz realizēt autentifikācijas un autentifikācijas ar koplietošanas atslēgu algoritmus, lai gan pats freims nav apveltīts ar īpašību - autentificēt klientu. Tā kā par standarta 802.11 autentificēšanas trūkumiem mēs jau runājām, mēģināsim izprast to, kas ir nepieciešams, lai nodrošinātu aizsargātu autentifikāciju bezvadu LAN.

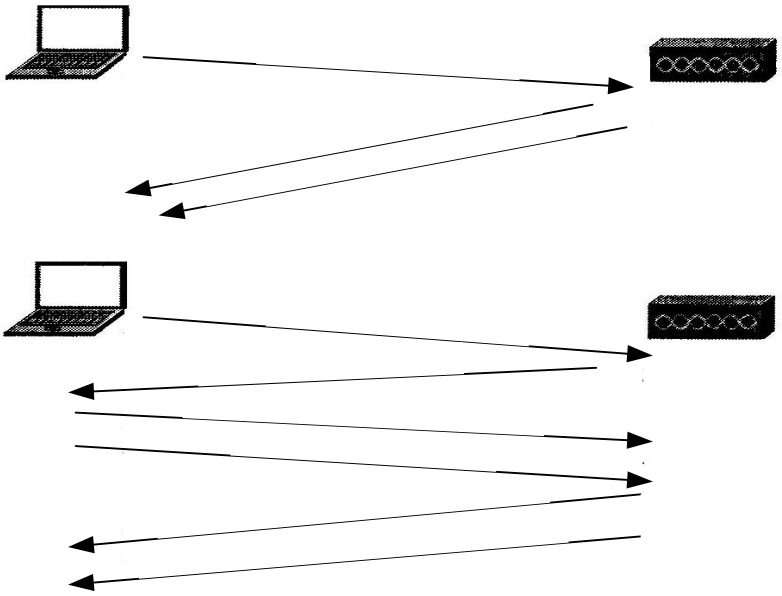
Standartā 802.11 nav noteiktas pamata komponentes, kuras spēj nodrošināt efektīvu autentifikāciju (uzskaitītas zemāk).

- Centralizētā autentifikācija, orientēta uz lietotāju.
- Dinamiski šifrējamās atslēgas.

- Nošifrētu atslēgu vadīšana.
- Savstarpējā autentifikācija.

Uz lietotāju orientēta autentifikācija ir īpaši svarīga tīkla aizsardzības nodrošināšanai. Uz iekārtu orientēta autentifikācija, līdzīga atklātajai autentifikācijai un autentifikācijai ar koplietošanas atslēgu, nespēj neautorizētiem lietotājiem aizliegt izmantot autorizētas iekārtas. No tā var secināt, ka pie tādas iekārtas pazaudēšanas vai zādzības vai pēc tās darba beigšanas, tīkla administ00rators būs spiests manuāli izmainīt visus standarta 802.11 tīkla pieejas punktu un klientu atslēgas. Pie centralizētās, uz lietotāju orientētas vadīšanas caur autentifikācijas, autorizācijas un uzskaites serveri (authentication, authorization, and accounting, AAA), tādas kā RADIUS, administrators var aizliegt tīkla pieejamību atsevišķiem lietotājiem, bet nevis viņu iekārtām. Prasībai veikt uz lietotāju orientētu autentifikāciju ir pozitīvs blakus efekts: atsevišķas šifrēšanas atslēgas katram lietotājam. Autentifikācijas varianti, kuri atbalsta dinamisku šifrēšanas atslēgu izveidošanu, piemēroti, lai uzlabotu bezvadu LAN aizsardzību un viņu vadīšanas modeli. Katram lietotājam individuālās dinamiskās atslēgas atbrīvo tīkla administratoru no nepieciešamības izmantot statiski vadāmās atslēgas. Šifrēšanas atslēgas dinamiskie tiek nozīmētas un anulētas, kad lietotājs iziet autentifikācijas procedūru vai iziet no tīkla. Lai kādu lietotāju varētu no tīkla izraidīt, pietiek anulēt viņa uzskaites pierakstu un viņš zaudē tīkla pieejamības iespēju.

Savstarpējā autentifikācija – tā ir divpusējā autentifikācija. Tās "divpusējā" daba pamatota ar to, ka ne tikai tīkls autentificē klientu, bet arī klients autentificē tīklu. Izmantojot atklāto autentifikāciju un autentifikāciju ar koplietošanas atslēgu, piekļuves punkts vai tīkls autentificē klientu. Pēdējais noteikti nezina, vai ir pieslēdzies tieši pie tā tīkla, pie kura tas ir vajadzīgs, jo standartā 802.11 nav paredzēts mehānisms, kurš ļauj klientam autentificēt tīklu. Rezultātā ļaundarim piederošais pieejas punkts vai klienta stacija var sevi uzdot par 'likumīgu' piekļuves punktu un bojāt klienta mašīnas datus. Att. 4.11. parādītas diagrammas, kuras ilustrē vienpusējās un savstarpējās autentifikācijas procesus.



Klien

Att. 4.11. Vienpusīga un savstarpēja autentifikacija

Standarta 802.11 un IEEE tīklu piegādātāji apzinās nepieciešamību pastiprināt un aizstāt pastāvošos aizsardzības nodrošināšanas mehānismus – kā autentifikācijas, tā arī šifrēšanas. Standarta 802.11 I pētniecības grupa tagad ar to strādā, un pēc tam, kad izmaiņas būs pilnībā sagatavotas, aizsardzības specifikācijas tiks apstiprinātas kā standarta 802.1 li specifikācijas.

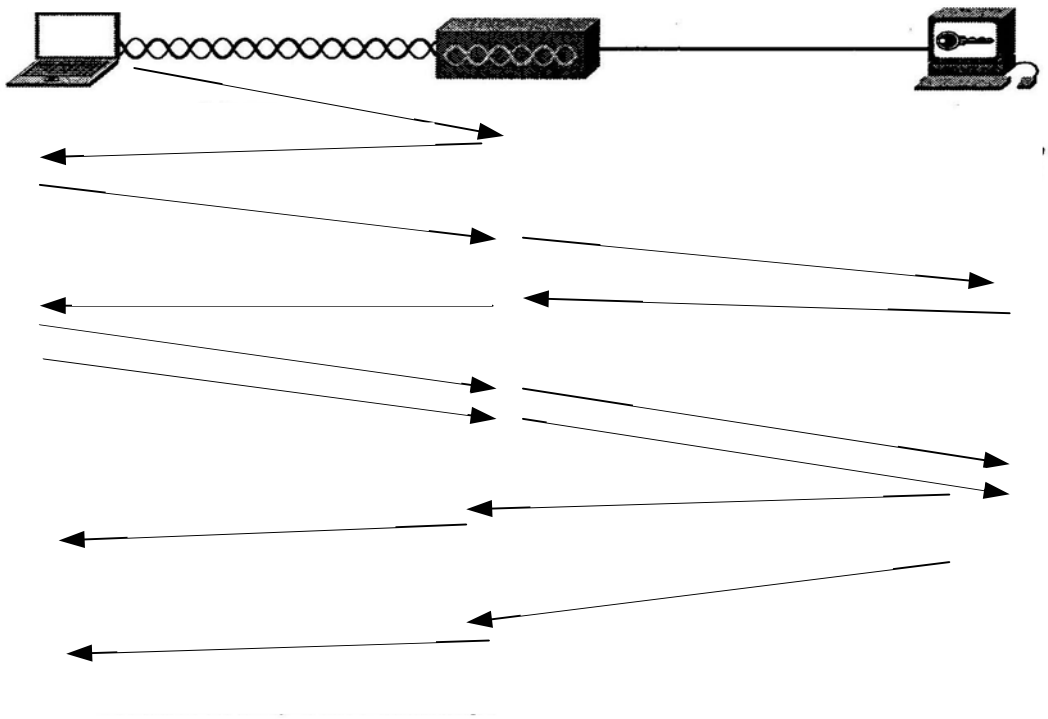
Klien

4.3.2. Otrā komponente: autentifikācijas algoritms.

Standarts 802.11i un WPA nodrošina mehānismus, kuri atbalsta autentifikācijas algoritma darbu ar mērķi nodrošināt saikni starp klientu, pieejas punktu un autentifikācijas serveri, izmantojot standarta 802.1X bāzes autentifikācijas mehānismu. Ne standarts 802.1N, ne WPA nereglamentē īpaša autentifikācijas algoritma pielietošanu, taču abi rekomendē izmantot algoritmu, kurš atbalstītu savstarpējo autentifikāciju, šifrēšanas dinamisko atslēgu ģenerāciju un lietotāja autentifikāciju. Att. 4.12. parādīti ziņojumi, ar kuriem apmainās klients, pieejas punkts un AAA-serveris. Ātrāk orientēties šajā procesā palīdzēs konkrēts piemērs. Dotajā nodaļā aplūkots algoritma EAP-Cisco darbs. Šis algoritms, vairāk pazīstams kā Cisco LEAP, ir vienkāršs un efektīvs algoritms, izstrādāts speciāli izmantošanai bezvadu LAN.

Zīm.4.21 ilustrēts EAP-Cisco darbs. Tālāk sīki aprakstīta katra transakcija:

1. Klients saņem vides pieejamības iespēju un nosūta pieejas punktam pēc standarta 802.1X iekapsulētu ziņojumu EAP-Start.
2. Pieejas punkts bloķē klienta portu, ļaujot pa tīklu pārraidīt tikai standarta 802.1X trafiku.



Att. 4.12. Autentifikacijas process saskaņā ar algoritmu EAP-Cisco.

3. Pieejas punkts nosūta klientam ziņojumu ar identifikācijas EAP – pieprasījumu (EAP-Request Identity), pēc standarta 802.1X iekapsulētu.
4. Klients atbild ar EAP – atbildi (EAP-Response), kura iekapsulēta pēc standarta 802.1X un satur klienta lietotāja vārdu.
5. Pieejas punkts pārraida šo lietotāja vārdu, iekapsulētu servera RADIUS pakotnē pieejas pieprasījumam (RADIUS ACCESS-REQUEST), uz autentifikācijas serveri.
6. Serveris RADIUS izveido algoritmam atbilstošu EAP – Cisco izsaukuma ziņojumu (challenge message) un nosūta to, iekapsulētu servera RADIUS pakotnē par pieejas lūgumu (RADIUS ACCESS-RESPONSE), klientam (caur pieejas punktu).
7. Pieejas punkts EAP-Cisco izsaukumu pārsūta klientam, iekapsulētu standarta 802.1X freimā.
8. Klients apstrādā izsaukumu saskaņā ar EAP-Cisco algoritmu un nosūta izsaukuma atbildi atpakaļ serverim RADIUS caur pieejas punktu.

9. Pieejas punkts izsaukuma atbildi iekapsulē servera RADIUS pieprasījuma pakotnē pēc pieejas (RADIUS ACCESS-REQUEST) un pārvirza to uz serveri RADIUS.
10. Klients atbildi saskaņā ar EAP-Cisco algoritmu sūta uz serveri RADIUS (caur pieejas punktu), lai autentificētu tīklu. Šis izsaukums iekapsulējas standarta 802.1X freimā.
11. Pieejas punkts EAP-Cisco izsaukumu iekapsulē servera RADIUS atbildes pakotnē par pieejas lūgumu (RADIUS ACCESS-RESPONSE).
12. Serveris RADIUS izsaukuma atbildi saskaņā ar EAP-Cisco algoritmu nosūta atpakaļ klientam (caur pieejas punktu), iekapsulētu servera RADIUS atbildes pakotnē par pieejas lūgumu (RADIUS ACCESS-RESPONS).
13. Pieejas punkts iekapsulē ar EAP-Cisco izsaukuma atbildi standarta 802.1X freimā un nosūta to klientam.
14. Serveris RADIUS ģenerē šifrēšanas dinamisko atslēgu (dynamic encryption key) pamatojoties uz lietotāja paroli un specifisku apmaiņas sesijas informāciju.
15. Klients ģenerē tādu pašu šifrēšanas dinamisko atslēgu. Klients lokāli spēj ģenerēt tādu pašu šifrēšanas dinamisko atslēgu, jo viņam ir pieeja pie tās pašas informācijas.
16. Serveris RADIUS šo atslēgu nosūta piekļuves punktam, iekapsulētu RADIUS ACCEPT pakontē (uztverts ar serveri RADIUS). RADIUS ACCEPT pakotne pieejas punktam norāda, ka autentifikācijas process ir beidzies veiksmīgi.
17. Piekļuves punkts iestata dotā klienta dinamisko atslēgu, iekapsulē ziņojumu "EAP-autentifikācija pabeigta veiksmīgi" (EAP-Success) standarta 802.1X freimā un nosūta šo ziņojumu klientam.
18. Piekļuves punkts klienta portu pārved stāvoklī, kurš pieļauj trafika pārvirzīšanu.
19. Klients atver savu portu (pie nosacījuma, ka vairākkārtējā autentifikācija ir veiksmīgi pabeigta).

Algoritms EAP-Cisco ir patentēts algoritms, kurš strādā virs bāzes atklātās autentifikācijas algoritma. Šī iemesla dēļ EAP-Cisco algoritma detaļas, kuras skar izsaukuma ģenerējamo saturu un izsaukuma atbildi, kā arī šifrēšanas atslēgu sadalījumus, nedrīkst izpaust. Algoritms EAP-Cisco pārsniedz prasības, kuras izvirzītas lietotāja atklātajai autentifikācijai bezvadu LAN, pielietojot sekojošus mērus:

- Autentifikācija, orientēta uz lietotāju.
- Savstarpējā autentifikācija.
- Šifrēšanas dinamiskās atslēgas.

Ja kādam lietotājam ir nepieciešams liegt tīkla pieejamību, pietiek viņu izslēgt no uzskaites pieraksta autentifikācijas centralizētajā serverī. Rezultātā lietotājs nevarēs veiksmīgi

iziet autentifikācijas procesu, bet viņa iekārta – noģenerēt pareizu šifrēšanas dinamisko atslēgu.

4.3.3. Trešā komponente: datu aizsardzības algoritms.

WEP šifrēšanas ievainojamība standarta 802.11 tīklu ražotājus un IEEE pētniekus nostādīja apgrūtinošā situācijā. Kā var uzlabot standarta 802.11 šifrēšanas sistēmu, neizmantojot visu pieejas punktu un klientu tīkla karšu nomaiņu?

IEEE uz šo jautājumu atbildēja, piedāvājot standarta 802.11 (un WPA) daļai *atslēgas integritātes pagaidu protokolu* (temporal key integrity protocol, TKIP).

Šis protokols izmanto daudzas WEP pamata funkcijas, lai attaisnotu klientu veiktās iekārtu un standarta infrastruktūras investīcijas, bet likvidē dažas pēdējā vājās vietas, nodrošinot efektīvu datu freimu šifrēšanu. Protokola TKIP ievestie galvenie uzlabojumi ir sekojoši:

- **Šifrēšanas atslēgas izmainīšana pēc freima.** WEP-atslēga ātri mainās un katram freimam tā ir savādāka.
- **Ziņojuma integritātes kontrole** (message integrity check, MIC). Nodrošina efektīvu datu freimu integritātes kontroli ar mērķi novērst slepenas manipulācijas ar freimiem un freimu reproducēšanu (sīkāk par to - zemāk) .

Flurera, Mantina un Šamira rakstā apspriesta algoritma RC4 (pielieto WEP) ievainojamība. Uzbrukumi, kuri izmanto vājo IV ievainojamību un tiek pielietoti AirSnort pielikumā, balstīti uz dažu datu freimu uzkrāšanu, kuri satur informāciju, nošifrētu izmantojot vājos IV. Vienkāršākais veids, lai atturētu tādus uzbrukumus, ir WEP-atslēgas, kuru izmanto pie freimu apmaiņas starp klientu un pieejas punktu, izmainīšana. Šī izmaiņa jāveic pirms vēl uzbrucējs nav paspējis freimus uzkrāt tādā daudzumā, lai varētu izvest atslēgas bitus.

IEEE adaptēja shēmu, zināmu kā *atslēgas izmainīšana pēc freima* (per-frairu keying). (To sauc arī par *atslēgas izmainīšana katrai pakotnei* (per-packet keying) un *bieža pakotnes atslēgas izmainīšana* (fast packet keying).) Galvenais princips, uz kura balstās atslēgas izmainīšana pēc freima, ir tas, ka IV, raidītāja MAC-adrese un WEP-atslēga apstrādājas kopā ar divpakāpju sajaukšanas funkcijas palīdzību. Šīs funkcijas pielietošanas rezultāts atbilst standarta 104-kārtu atslēgai un 24-kārtu IV.

Tāpat IEEE piedāvāja palielināt 24-kārtu inicializācijas vektoru līdz 48-kārtu IV. Nākošajās nodaļās paskaidrots, kāpēc tāds IV paplašinājums ir nepieciešams. Atslēgas izmainīšanas pēc freima procesu var sadalīt sekojošos etapos:

1. Bāzes WEP-atslēga (iegūta autentifikācijas procesā pēc standarta 802.1X) sajaucas ar 48-kārtu IV vecākajām 32 kārtām (32-kārtu skaitļi var pieņemt vērtības 0-4 294 967 295) un raidītāja MAC-adresi. Šīs darbības rezultāts tiek saukts par *1-ās fāzes atslēgu* (phase 1 key). Šis process ļauj 1-ās kārtas fāzes atslēgu ienest kešatmiņā, kā arī ievietot tieši atslēgā .
2. 1-ās fāzes atslēga sajaucas ar IV un raidītāja (TA) MAC-adresi, lai varētu izstrādāt zemfreima atslēgas vērtību.
3. Inicializācijas vektora (IV), kuru izmanto freima pārraidei, garums ir tikai 16 biti (16-kārtu skaitļi var pieņemt vērtības 0-65 535). Atlikušie 8 biti pārstāv fiksētu vērtību, kuru izmanto kā pildītāju.
4. Pēcfreima atslēgu izmanto datu freima WEP-šifrēšanai.
5. Kad IV 16-bitu telpa ir izsmelta, 1-ās fāzes atslēga tiek nomesta un 32 vecākās kārtas palielinās par 1. (Ja IV pirmās fāzes vērtība bija vienāda ar 12, tā palielinājās par 1 un kļuva vienāda ar 13).
6. Pēcfreima atslēgas vērtība tiek aprēķināta no jauna, kā 2 etapā.

Pēc freima maināmai atslēgai spēks ir tikai tad, kad 16-kārtu IV vērtības netiek izmantotas atkārtoti. Ja 16-kartu IV vērtības tiek izmantotas divreiz, notiek kolīzija, kuras rezultātā parādās iespēja veikt uzbrukumu un izvest atslēgas plūsmu. Lai izvairītos no IV kolīzijām, 1-ās fāzes atslēgas vērtība aprēķina par jaunu, palielinot IV vecākās 32 kārtas par 1 un atkārtoti aprēķina pēc freima atslēgu.

4.3.4. Ceturtā komponente: datu integritāte.

Nākotnē, lai pastiprinātu mazas efektivitātes mehānismu, balstītu uz standarta 802.11 integritātes kontroles pazīmes (ICV) izmantošanu, tiks pielietota ziņojuma integritātes kontrole (MIC). Pateicoties MIC var tikt likvidētas aizsardzības vājās vietas, kuras veicina uzbrukumus izmantojot viltotus freimus un bitu žonglēšanu, izskatītus iepriekš šajā nodaļā. IEEE piedāvāja speciālu algoritmu, kurš ieguva nosaukumu *Michael* (Maikls), lai pastiprinātu ICV lomu standarta 802.11 datu freimu šifrēšanā.

MIC pieder unikāla atslēga, kura atšķiras no datu freimu šifrēšanai izmantojamās atslēgas. Šī unikālā atslēga sajaucas ar paredzēto MAC-adresi un freima izejas MAC-adresi, kā arī ar visu nenošifrēto freima daļu, kura nes lietderīgo slodzi.

Kopumā TKIP šifrēšanas mehānisms realizējas sekojošā veidā.

1. Ar pēc freimu atslēgu noteikšanas algoritma palīdzību ģenerējas pēc freima atslēga Algoritms MIC ģenerē MIC freimam kopumā.

2. Freims fragmentējas saskaņā ar MAC iestatījumiem pēc freima.
3. Freima fragmenti šifrējas ar pēc freima atslēgas palīdzību.
4. Īstenojas nošifrēto fragmentu pārraide.

Pretdarbības MIC mēri sastāv no tā, ka uztvērējs izpilda sekojošus uzdevumus:

1. Uztvērējs izņem esošo asociācijas atslēgu.
2. Uztvērējs reģistrē problēmu kā tīkla drošības problēmu.
3. Asociētais klients, no kura tika saņemts viltus freims, nevar tikt asociēts un autentificēts 60 sekunžu laikā, lai palēninātu uzbrukumu.
4. Ja klients ir saņēmis viltus freimu, tad viņš atmet visus freimus, kuri neatbilst standartam 802.1X.
5. Tāds klients tāpat pieprasa jaunu atslēgu.

Izskatītā atslēgu pēc freima noteikšana un MIC skāra galvenokārt šifrēšanas atslēgu un MIC atslēgu. Taču mēs neko nerunājām par to, kā atslēgas ģenerējas un tiek pārsūtītas no klienta uz pieejas punktu un otrādi. Nākošajā nodaļā mēs tad arī apskatīsim standarta 802.11 piedāvāto atslēgu vadības mehānismu.

1997. gadā izstrādātajā standartā 802.11 noteiktajiem autentifikācijas un šifrēšanas algoritmiem ir daudz trūkumu. Autentifikācijas sistēma, tāpat kā WEP-šifrēšanas algoritms, var tikt uzlauzts īsā laikā. Protokols TKIP apsola likvidēt WEP-šifrēšanas un autentifikācijas sistēmas trūkumus īstermiņa perspektīvā, bet standarts 802.1X un AES piedāvās ilglaicīgu bezvadu tīklu drošības problēmas risinājumu.

Šajā nodaļā tika stāstīts par to, kā var aizsargāt bezvadu lokālo tīklu, un tika aprakstīti bezvadu tīklu aizsardzības jautājumi. Pie bezvadu LAN izvēršanas ir svarīgi nodrošināt maksimālu to aizsardzību un lietotāju ērtības.

5. INSTRUKCIJA PAR DARBU TĪKLĀ.

5.1.Ieslēgšana un darbs tīklā.

TCIS tīklā bezvadu maģistrāle izveidota ar 3 bāzes pieejas punktiem: R6, R5 un R2 (skat. shēmu). Pieejas punkti R1, R3, R4 un R7 izpilda individuālo darba staciju bezvadu interfeisu funkcijas, tāpēc tos var iekļaut tajos gadījumos, kad ir nepieciešama izeja atbilstošā termināla tīklā. Jāatzīmē, ka R2 vajadzīgs, lai pie pārējā tīkla pieslēgtu segmentu Fast Ethernet, kurš satur mezglus Aud320-1, Aud320-2, Aud320-3 un Aud320-4, kā arī laboranta darba staciju ar bezvadu interfeisu, ko pārstāv R1. Atkarībā no situācijas (darbs konkrētās auditorijās un noteiktu tīkla resursu izmantošana) bezvadu savienojumi būvējas uz TCIS kopējās shēmas bāzes, ņemot vērā nepieciešamo bezvada tilta starpkomponenšu funkcionēšanas.

Barošana pieejas punktam A032 tiek padota uzreiz pēc elektriskā adaptera ieslēgšanas 220V tīklā. Pēc palaišanas jāgaida 10-30ms, līdz pieejas punkta aparatūras nodrošinājums ielādēsies un tiks izveidota tīkla iekārtu pieejamības maršrutu dinamiskā bāze.

Sakaru nodibināšanu LAN starp divām iekārtām var pārbaudīt ar atbalss-pieprasījuma ping *ip_address* palīdzību (apkopojas komandrindas režīmā: Start→Run→Open: *command*), ko realizē uz protokola ICMP bāzes. Šī komanda nosūta pieprasījumu uz norādīto IP adresi un uz ekrāna izdod pienākošās atbildes gaidīšanas laiku.

Piezīme. Dažos gadījumos bezvadu savienojumi var neierosināties, kam ir noteikti iemesli. Piemēram, pagaidu šķēršļi, caur kuriem nepārraidās radiosignāls (atvērtās durvis un intensīva mobilo objektu pārvietošana, kuri absorbē radioviļņus). Tādās situācijās nepieciešams kādu laiku nogaidīt, līdz tiks veikti atkārtoti savienojuma identifikācijas mēģinājumi faktoru skaita samazināšanās apstākļos, kuri traucē bezvadu saites organizācijai. Tāpat savienojumu reģistrācija dažreiz nobrūk programmatūras kļūmes rezultātā. Šajās situācijās palīdz pieejas punktu, kuri veido bezvadu savienojumu, pārlāde ar speciālas komandas programmas interfeisā A032 izslēgšanu un atkārtotu ieslēgšanu vai inicializāciju. Iekārtas pārlāde rekomendējas pie jebkurām tīklu mezglu konfigurācijas izmaiņām.

Pēc tam, kad saikne WLAN ir uzstādīta, var lietot tīkla klientu MS Windows, lai piekļūtu citu darba staciju resursiem. Lai darba stacijas faili būtu pieejami lokālajā tīklā, nepieciešams operētājsistēmas slānī iestatīt tīkla pieejamības atļauju. Windows 9x objekta (faila vai pakotnes) Properties izvēlnē izvēlas pielikumu Sharing→Shared As un norāda Access Type:

1) Read Only (tikai lasīšana).

2) Full (pilnvērtīga resursu pieejamība – bez pārlūkošanas ir iespējama jebkura to izmainīšana un dzēšana).

3) Depend on Password (nosaka Read Only и Full paroles). Šajā gadījumā resursa pieejamību var saņemt tikai pēc paroles ievadīšanas autentifikācijas logā.

Ja pie LAN pieslēgtajās darba stacijās ir resursi ar noteiktu tīkla pieejamību, tad tos var apskatīties Network Neighbourhood. Tur arī notiek visas atļautās operācijas saistītas ar šiem resursiem.

Salīdzinājumā ar Windows iebūvētajiem failu apmaiņas dienestiem, failu pārraides protokols FTP (File Transfer Protocol) nodrošina lielu datu piegādes drošību un ātrumu tīklā. Galvenā tā priekšrocība ir iespēja izmantot speciālas lejupielādes pārvaldnieku programmas, kuras ļauj atsākt faila pārraidi pēc nobrukušā savienojuma atjaunošanas, kas ir īpaši aktuāli bezvadu tīkliem, kur laiku pa laikam var novērot uztverošā signāla pazušanu traucējošu faktoru ietekmē. lejupielādes pārvaldnieks strādā tādā veidā, ka faila pārraide turpinās no tās vietas, kur notika sakara pārtrūkums. Pēc lejupielādes pārvaldnieka instalācijas, tas parasti integrējas Web-pārlūks un, vēršoties pie faila, automātiski palaižas.

Izmantot FTP dienestu uz klienta mašīnas operētājsistēmas Windows vadībā var divos populāros veidos:

1) ar Web-pārlūka starpniecību (Internet Explorer, Opera u.t.t.);

2) ar faila-pārvaldnieka palīdzību (Norton Commander, Windows Commander u.c.).

1) *FTP-servera pieejamība caur Internet Explorer interfeisu uz klienta darba stacijas*

- Palaist IE
- Adreses virknē ievadīt *ftp://ftp_address/*,

kur *ftp_address* – FTP-servera adrese.

Ja anonīma FTP-servera resursu pieejamība ir aizliegta, tad IE izvēlnē jāizvēlas File->Login As..., pēc tam parādītajā logā jāievada lietotāja vārds un parole.

Analoģiski identifikācijas datus var ievadīt tieši adreses virknē (jebkurā pārlūkā): *ftp://user_login:user_password@ftp-address/*,

kur *user_login* – lietotāja vārds;

user_password – viņa parole;

ftp_address – FTP-servera IP adrese.

2) *FTP pieejamība no Windows Commander*

- Palaist Windows Commander
- Atvērt Net–>FTP Connect…

- Izvēlēties vajadzīgo savienojumu no saraksta un nospiest Connect
- Ja FTP-savienojuma sarakstā nav, tad to nepieciešams izveidot, izvēloties New Connection un aizpildot pamata laukus parādītajā iestatījumu logā:

Session – nosaukums, kuru Jūs vēlaties piešķirt FTP-savienojumam (tas tiks parādīts sarakstā);

Hostname – FTP-servera IP adrese;

User_name – lietotāja vārds;

Password – parole.

Ja uz FTP-servera ir atļauta anonīma piekļuve, tad jāieslēdz Anonymous login.

- Pēc savienojuma ar FTP-serveri iestatījuma kreisajā programmas pamata loga daļā tiks parādītas pieejamās tīkla direktorijas un faili. Tai pašā laikā loga labajā daļā var izvēlēties klienta diska vietu, kur tiks novietoti lejupielādētie dati. Kopēšanas procedūra realizējas tāpat, kā Windows standarta līdzekļos.
- Pirms pārraides sākšanas, parādītajā apstiprinājumu logā var izvēlēties ātruma atrādīšanu: Show in the background.

Analoģiskā veidā notiek failu lejupielāde uz FTP-servera.

TCIS tīklā internet resursu pieejamība uz klienta stacijas realizējas caur jebkuru iestatīto Web-pārlūku un neprasa proxy-servera konfigurāciju.

5.2.TCIS tīkla iekārtu iestatīšana.

Bezvadu LAN konfigurācija sastāv no sekojošiem trīs pamata etapiem:

1. Bezvadu savienojuma parametru uzstādīšana;
2. IP-adresācijas organizācija iekšējā LAN;
3. Vārtejas uzstādīšana, kura nodrošina izeju no iekšējā tīkla uz ārējo.

Bezvadu sadales sistēma TCIS sīki aprakstīta projekta 2 nodaļā "Lokālais tīkls ar bezvadu sadales sistēmu". Dotajā instrukcijā aprakstīti tikai galvenie uzstādījuma momenti.

1. Pieejas punktu A032 uzstādīšana. Pieejas punkts – tā ir vadāma komutatīva stacija ar ražotāja uzstādītu programmatūras nodrošinājumu (sīkāk skat. projekta 1 un 2 nodaļu).

A032 uzstādījumu piekļuve ir iespējama trīs veidos:

1. Caur Web-interfeisu (LAN-savienojums);
2. Caur COM-porta sakaru līdzekļiem;

3. Termināla Telnet režīmā (LAN-savienojums).

Tālāk tiks aprakstīti pirmie divi veidi.

Ja pieejas punkts pieslēgts LAN caur vadu vai bezvadu savienojumu, tad pats ērtākais piekļuves veids to uzstādījumiem – caur pārlūka interfeisu. Tāpēc adreses virknē uzraksta: *http://AP_address/*, kur AP address – pieejas punkta IP.

Pēc komandas interfeisa A032 uzaicinājuma ielādes izvēlamies Setup. Parādītājā laukā jāievada iepriekš uzstādītā parole un jānospiež Enter setup. Pēc veiksmīgas autentifikācijas atveras uzstādījumu interfeiss, kurā navigācija realizējas ar vajadzīgo norāžu starpniecību zilajā laukā lapas kreisajā daļā.

Bezvadu savienojuma bāzes parametri:

1. Radio Channel (Basic Setup: Access Point) – frekvences kanāla izvēle. Visiem sadales sistēmas piekļuves punktiem jāstrādā vienā un tai pašā radio kanālā (TCIS tīklā, tas ir kanāls 1). Ja šī parametra vērtību uz vienu no pieejas punktiem izmaina, tad citu bezvadu mezglu pieslēgums tai ir neiespējams līdz atbilstošai to uzstādījumu mainīšanai.
2. Network Name (Basic Setup: Access Point) – BSS identifikators. Priekš A032 šim parametram rekomendējas piešķirt unikālu vērtību, lai novērstu neatbalstāmu mobilo staciju atmiņu (TCIS tīklā Network Name – TCISx, kur x=1...7).

Pēc norādīto uzstādījumu nomaiņas nepieciešams nospiest pogu Enter Web-lappusē, lai jaunās vērtības tiktu ienestas iekārtas atmiņā. Lai izmainītie uzstādījumi sāktu darboties, nepieciešams pārlādēt A032, nospiežot pogu Save interfeisa kreisajā daļā. (Dotie noteikumi ir patiesi visiem piekļuves punktu uzstādījumiem).

Tīkla iestatījumi A032 satur TCP/IP uzstādījumus (Advanced Setup: Access Point):

1. (Mgmt) IP address – piekļuves punkta IP adrese;
2. Subnet Mask – apakštīkla maska;
3. IP Gateway – vārtejas pieejamības iekšējam tīklam IP adrese.

Apakštīkla TCIS maskas vērtība: 255.255.255.0. Tas nozīmē, ka dotajā tīklā var ieiet stacijas ar IP adresēm 192.168.0.X, kur X=1...254. Tās ir iekšējo tīklu mezglu standarta adreses. IP adrešu sadalījums starp TCIS stacijām parādīts tīkla shēmā.

Vārtejas iekšējā adrese, kura bāzējas uz R6, - 192.168.0.206. Šī vērtība tiek norādīta IP Gateway laukā uz visiem pārējiem piekļuves punktiem. Vārteja satur tīkla ekrānu (Firewall), kurš neizlaiž ārējā tīkla pieprasījumus uz iekšējo, un translē darba stacijas IP adresi TCIS iekšienē Internet-adresē tīkla ekrāna ārējā pusē, kad notiek mēģinājums iziet uz iekšējo tīklu. Tāpēc bez iekšējās IP adreses piekļuves punktā R6 pieslēgta Internet piekļuve caur Ethernet-interfeisu (Advanced Setup: Access Point -> Nat Port -> LAN). Pēc tam atsauksmju

sarakstā parādās rinda Internet Access, kura uz TCP/IP ekrāna izsauc provaidera nodotos tīkla ekrāna uzstādījumus: ārējā IP adrese, maska, vārtejas un DNS-servera adrese.

Laiku pa laikam pēc drošības apsvērumiem nepieciešams mainīt piekļuves punktu adreses. To var izdarīt izvēlnē Advanced Setup: Access Point.

Tīkla konfigurācijas sākuma etapos var izrādīties, ka LAN savienojums ar piekļuves punktu nav iestatīts. Tādā gadījumā izmanto uzstādījumu A032 piekļuvi caur seriālo pieslēgvietu. Tāpēc interfeisam RS232 ir nepieciešams kabelis null-modem. Pēc datora pieslēgšanas piekļuves punktam caur COM-portu, uz to vajag palaist programmu Hyper Terminal (Start -> Programs -> Accessories -> Communications -> Hyper Terminal) ar uzstādījumiem: 9600 baud, 8 bits, no parity. Pēc autentifikācijas pabeigšanas parādās komandrindas aicinājums.

Lai aplūkotu piekļuves punkta konfigurācijas, izmanto komandu *config*. Uzstādījumu mainīšanas pamata komandas sintakse: *set parameter value*,

kur *parameter* – parametra nosaukums,

value – piešķiramā vērtība.

Piemēram,

set ip_address 192.168.0.1

set subnet_mask 255.255.255.0

Lai ieraudzītu pilnu maināmo parametru sarakstu, ievadiet *set help*. Sīkāks komandu un parametru apraksts dots Nokia A032 WLAN Access Point Advanced User Guide.

Jāatzīmē, ka bezvadu sadales sistēmas tiltu konfigurēšana iespējama tikai komandrindas režīmā. Sīkāk par tiltiem skat. projekta 2 nodaļā un Nokia A032 WLAN Access Point Advanced User Guide.

Tilta savienojuma partneru uzdevums realizējas ar komandu:

bridge add bridge_MAC bridge_name;

dzēšana notiek pēc komandas:

bridge delete bridge_MAC,

kur *bridge_name* – vārds, kuru piešķir tilta partnerim,

bridge_MAC – tilta partnera MAC-adrese.

Piemēram,

bridge add 00e003051599 BridgeA

Tilta partneru sarakstu var aplūkot ar komandas *bridge list* palīdzību.

Līdz ar to, tiltu sakaru formēšanās balstās uz radio karšu pieejas punktu MAC-adrešu norādīšanu un nav atkarīga no IP-adresācijas lokālajā tīklā. Tabulā parādīta tīkla TCIS

piekļuves punktu IP adrešu atbilstība to radio karšu adresēm. (Nomainot radio karti, mainās arī MAC-adrese, kas prasa bezvadu tiltu savienojumu rekonfigurāciju).

Tabula 5.1. Access pointu IP un Mac adresu saraksts

Piekļuves punkta vārds	IP adrese	MAC-adrese
R1	192.168.0.201	00E00305A8C7
R2	192.168.0.202	00E0030529DB
R3	192.168.0.203	00E003051981
R4	192.168.0.204	00E00304FA90
R5	192.168.0.205	00E003051599
R6	192.168.0.206	00E0030529E9
R7	192.168.0.207	00E003051597

2. klientu staciju tīklu interfeisu iestatīšana.

Vairumam WLAN mobilo darba staciju programmatūras nodrošinājums ļauj automātiski noteikt bezvadu tīkla iestatījumus. Lai pieslēgtos TCIS tīklam, viss, kas ir jānorāda tādās sistēmās, - tas ir BSSID (Network Name) TCISx, kur x = 2, 5 vai 6 atkarībā no mobilās stacijas atrašanās vietas (skat. shēmu).

Darba stacijas ar vadu interfeisu Ethernet pieslēdzas piekļuves punktiem ar 5 kategorijas UTP kabeļu starpniecību. Bez tam, individuālās stacijas ar A032 savienojas caur kabeli, kuram ir sadales vads crossover (atzīmēti ar melnu etiķeti), bet Fast Ethernet segmanti uz Eusso Nway Switch bāzes – caur parastu patch-kabeli (bez tam, nekādus papildus programmatūras iestatījumus Eusso Nway komutators neprasa). Par to, ka savienojums ir strādāt spējīgs, signalizē tīkla adapteru indikatoru zaļā gaisma. (Lai atļautu piekļuves punkta savienojumu caur Ethernet-interfeisu, A032 iestatījumos Advanced Setup: Access Point –> LAN Interface jānorāda 10baseT).

Kā vadu, tā arī bezvadu darba staciju TCP/IP uzstādījumi tiek nozīmēti, kā parādīts iepriekšējā nodaļā (“Piekļuves punktu A032 iestatījumi”). Windows9x ceļš pie TCP/IP uzstādījumiem: Network Neighbourhood -> Properties Configuration -> TCP/IP -> Properties. Tāpat arī darba staciju (vadu un bezvadu) TCP/IP iestatījumos jānorāda DNS-servera IP adrese (to var uzzināt pie administratora).

3. FTP-servera Serv-U iestatīšana.

Pirms prasīt FTP-servera resursus uz klientu stacijām, nepieciešams noteikt šo resursu piekļuvi ar uz servera uzstādītā Serv-U Administrator palīdzību. Tāpēc ar peles labo taustiņu

ir jānoklikšķina uz zīmi **U** Windows uzdevumu paneļa labajā daļā un jāizvēlas Start Administrator.

Resursu izdalīšana uz FTP-servera ietver sekojošus etapus:

1) Jaunā lietotāja uzskaites ieraksta izveidošana;
2) Lokālo direktoriju norādīšana, pie kurām šim lietotājam tiks atļauta piekļuve.
    - Lai izveidotu lietotāju, izvēles kokā loga kreisajā pusē izvēlieties Serv-U Administrator Domains -> … -> Users. Pēc tam galvenajā (augšējā) izvēlnē jāizvēlas Users -> New User (to var izdarīt arī ar labo peles taustiņu noklikšķinot uz Users izvēlnes kokā).
    - Ievadiet lietotāja vārdu (bez atstarpēm) un nospiediet NEXT. Piemēram, *student*.
    - Ievadiet paroli un password lauku atstājiet tukšu, ja uzskaites ierakstu vēlaties atstāt bez paroles. NEXT.
    - Ievadiet lietotāja mājas direktorijas ceļu. Tā – direktorija, pie kuras satura lietotājs saņem piekļuvi uzreiz pēc veiksmīgas identifikācijas uz servera. Piemēram, *C:/My Documents*.
    - Nākošajā etapā tiks uzdots jautājums: Lock user in home directory? (Yes/No), kas nozīmē, vai vajag ierobežot lietotāja piekļuvi tikai ar mājas direktorijām un tās apakšdirektorijam, pat ja piekļuve pie augstākstāvošajām direktorijām dotajam lietotājam ir atļauta.
    - Pēc tam Users sarakstā parādīsies jauns uzskaites ieraksts. Izvēloties to, Jūs saņemat piekļuvi administratoru iestatījumiem, kurus pielieto konkrēti dotajam lietotājam. Šeit var iestatīt paroli (Account -> Password), failu lejupielādes un augšupielādes ātrumu (General -> Max. download и Max. upload speed), noteikt piekļuves tiesības direktorijām un failiem (Dir Access), staciju IP adreses, no kurām ir atļauta ieeja uz FTP-serveri dotajam uzskaites pierakstam, un brīvā diska telpas kvotu datu ielādei no klienta stacijas uz serveri.
    - Iestatīšanas procedūras beigās jāizvēlas User -> Apply galvenajā izvēlnē visu iestatījumu saglabāšanai un jāiziet no Serv-U Administrator interfeisa.

Lai dzēstu FTP-servera lietotāja uzskaites ierakstu, vienkārši noklikšķiniet ar peles labo taustiņu uz nevajadzīgo lietotāju Users sarakstā un izvēlieties Delete User.

5.3. Mobilas stacijas uzstādīšana un pieslēgšana

Dotajā nodaļa ir aprakstīts Nokia C110/C111 WLAN Card instalacijas process

Nokia C110/C111 ir WLAN adapteri, kam ir Extended Type formāts II PC Card un paredzēti uzstādīšanai portatīvās darba stacijās ar atbilstošajiem slotiem. C110/C111 pilnībā atbilst IEEE specifikācijas 802.11b un aprīkoti ar divām kompaktām iekšantenām.

5.3.1. Nokia C110/C111 kartes instalācijas process un profila uzstādīšanas

1 Sākumā izejiet no visām Windows programmām. Ielieciet CD-ROM jūsu datorā.

2 Izvēlieties CD-ROM valodu un izlasiet un pieņemiet Nokia licenci. Ja jūs nepieņemat licenci, jūs nevarat izmantot CD-ROM.

3 No CD-ROM menu, izvēlēsieties - Nokia C110/C111 instalacija un klikšķēšana Uzstādīšana.

4 Parādīsies sveikuma logs. Klikšķiet Tālāk turpinājumam.

5 Izvēlas valsti, kur jūs - īstā laikā izmantojat karti. Klikšķiet Tālāk.

6 Izvēlēsieties iecelšanas mapi programmas nodrošinājumam. Tipveida mape - C:\ProgramFiles\Nokia C110. Ja jūs gribat instalēt programmas nodrošinājumu citā diskā vai mapē, klikšķiet Caurskatīt. Kad jūs izvēlējāties pareizu iecelšanas mapi, klikšķēt Tālāk.

7 Izvēlas uzstādīšanas tipu. *Tipisks* uzstāda paša standarta programmas nodrošinājuma komponentus. Šī izvēle ir rekomendēta patērētāju vairākumam. *Tipisks ar SIM Service*

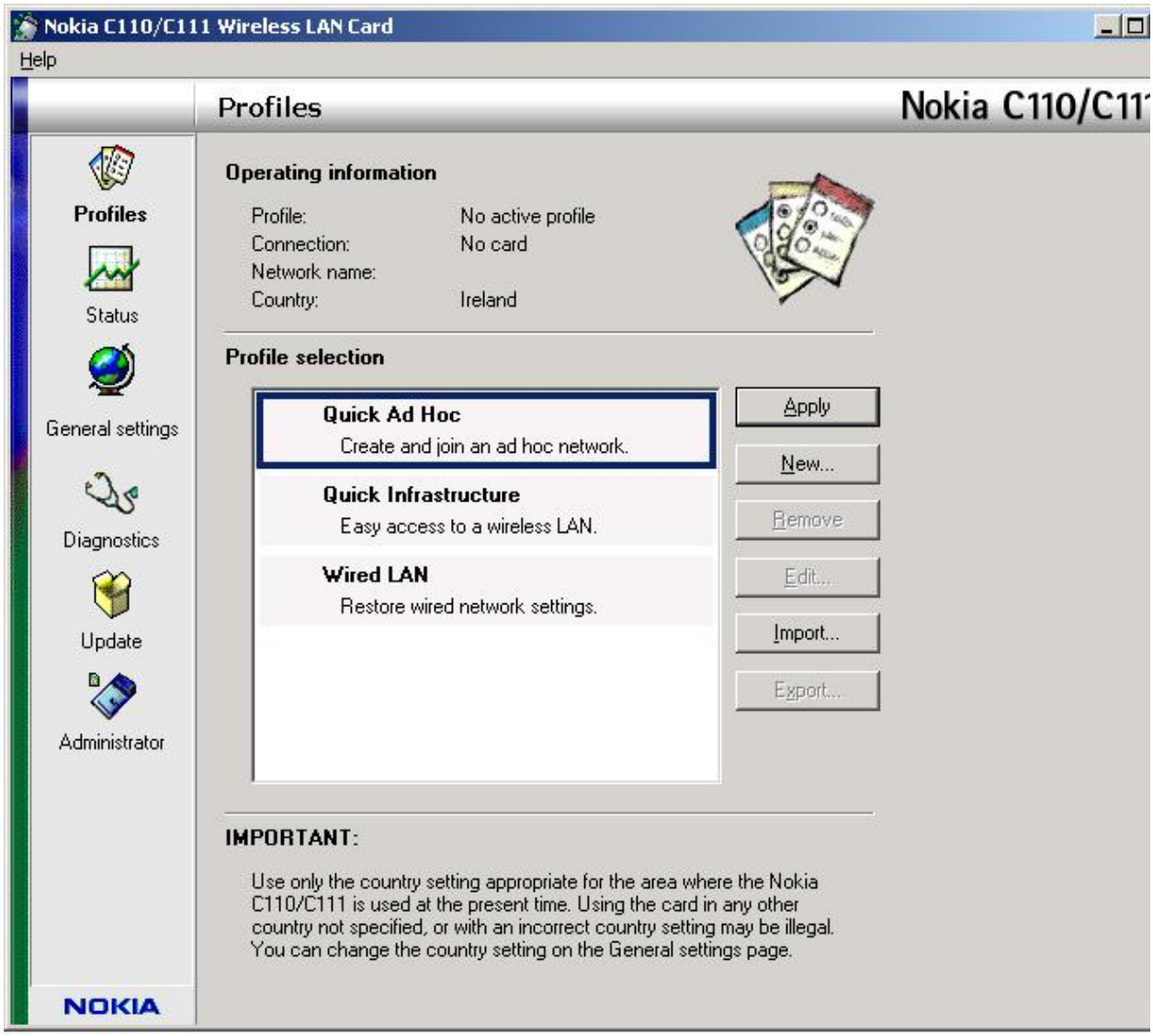
uzstāda paša standarta programmas nodrošinājuma un *SIM Service page* komponentus. Izvēlaties šo uzstādīšanas tipu, ja jūs parakstījāties uz *SIM Service* no pakalpojumu vai tīkla operatora jūsu piegādātāja. Izvelamais tips ļauj jums izvēlēties individuālus programmiskus komponentus, kuri ir uzstādīti, un rekomendēts virzītajiem patērētājiem. *Administratora* izvēle sistēmas administratoriem.
Kad jūs izvēlējāties vēlamu uzstādīšanas tipu, klikšķēt Tālāk.

8 Parbaudiet uzstādīšanas parametri. Lai pieņemtu tos, klikšķiet Tālāk, lai aizstātu uzskaņošanu parametrus, klikšķētu Atpakaļ, ienesiet izmaiņas, bet pēc tam klikšķēt Tālāk. Uzstādīšanas programma palaiž failu kopēšanu.

9 Setup Logs informē jūs, kad uzstādīšana ir pabeigta. Izņemiet CD-ROM un klikšķiet Pabeigt.

10 Parstartejot datoru un ielikot C110 karti(kā parādīts zemāk), instalejiet to, izveloties ceļu pie driveriem uz CD-ROM.

11 Iekļausiet jūsu datoru. Dialoģisks logs prasīs, vai gribat jūs radīt tīkla profilu pašlaik. Atceraties, ka jūs varat radīt un rediģēt jūsu personīgos tīkla profilus jebkurā laikā. Ja jūs negribat radīt profilu, ne klikšķiet Neko un uzstādīšanas procedūra ir pabeigta.(Att.5.1.) Ja jūs gribat radīt profilu, klikšķiet, Jā.



Att.5.1. Dialoga logs tīkla profila izvelej vai uzstadīšnai.

12 Parādīsies Profile Wizard logs. Klikšķiet Tālāk.

13 Piešķir vārdu profilam. Jūs varat tāpat ieiet profila aprakstā. Klikšķiet Tālāk.

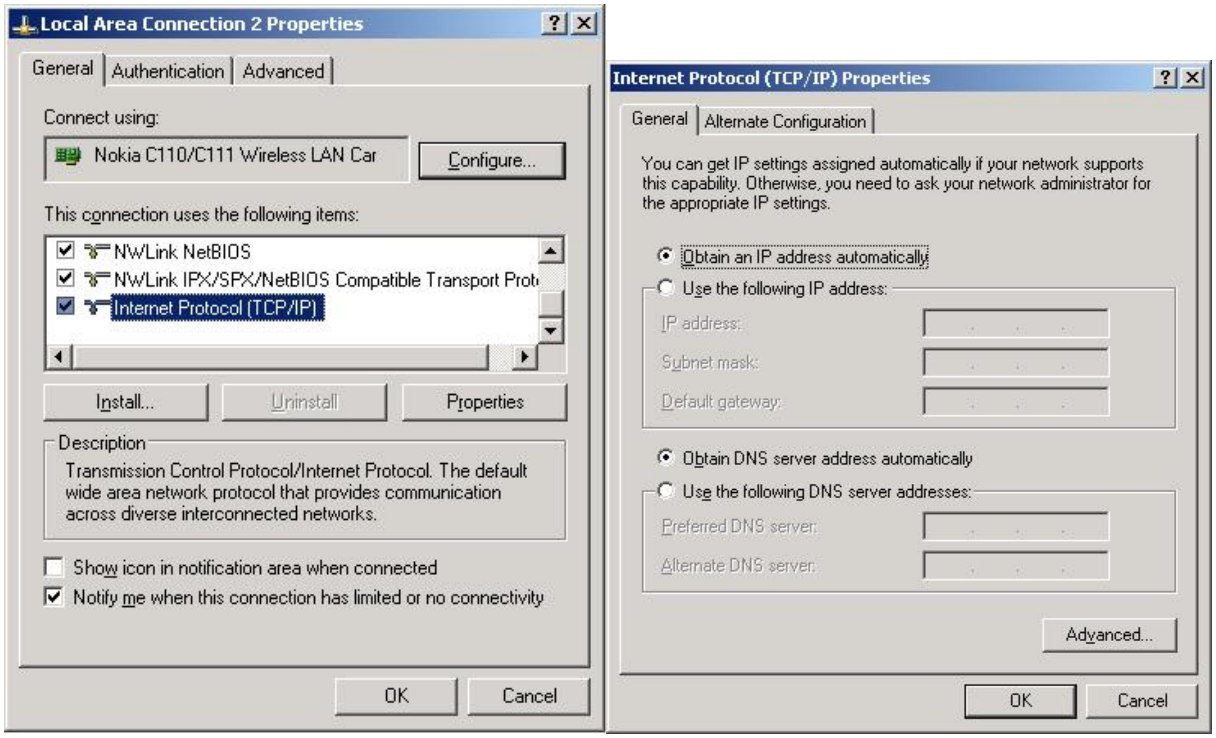
14 Iespiediet tīkla vārdu vai izvēlas vienu no saraksta. Pēc tam izveleties vai *Automatic kanāla izvēle,* vai uzstāda pareizu kanālu ar rokām Klikšķēsiet Tālāk.

15 Izvēleties saņemt *IP adresi no DHCP(Obtain an IP address from bet DHCP server)servera.* Ja vajag, jūs varat saformēt IP adresi, zemtikla maska, kas ir tipveida vārti, un uzskaņošanu TCP/Ip parametrus ar rokām

16 Saformēto uzskaņošanu parametru Īsā atskaite ir parādīta. Lai pieņemtu tos, klikšķiet Nobeigumu. Lai aizstātu uzskaņošanu parametrus, klikšķiet Atpakaļ, ienesiet izmaiņas, bet pēc tam klikšķiet Nobeigumu,

Jauns profils netiks aktivizēts automātiski. Lai aktivizētu profilu, jums ir jāizvēlas viņš no profilu saraksta.

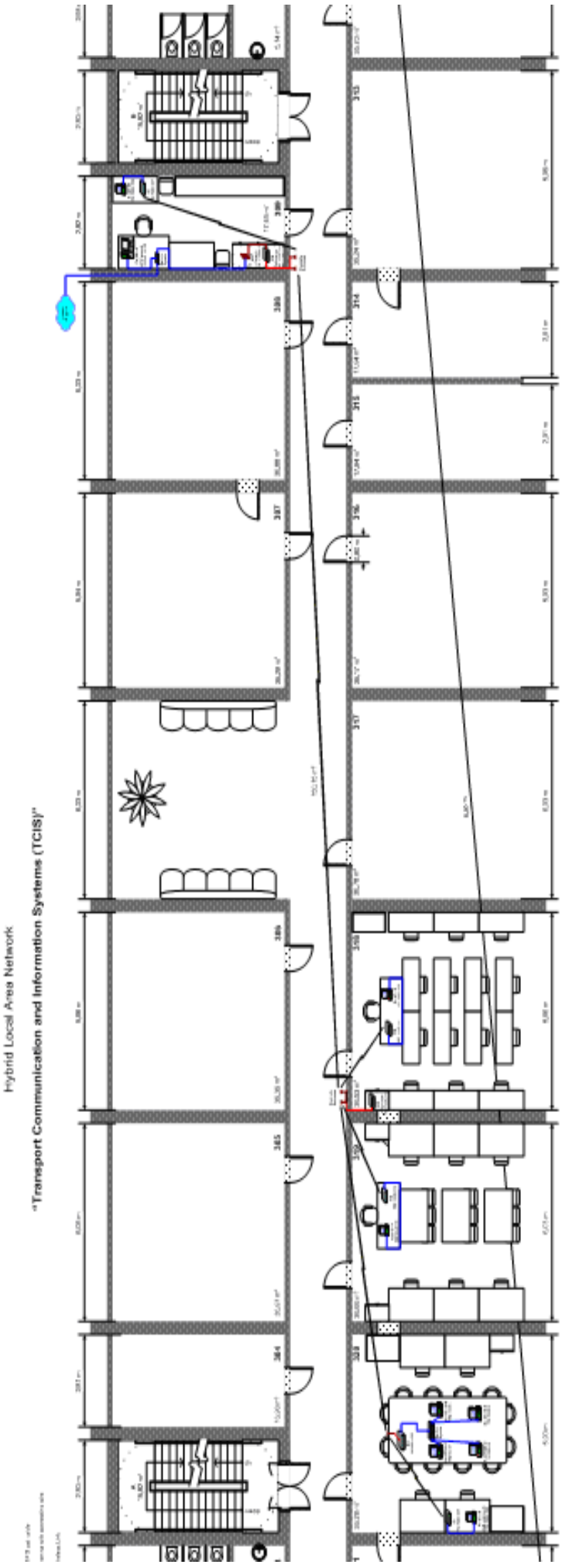
IP adrese var izvēlēties automātiski - mobilas stacijas var saņemt adreses, kuras nav aizņemtas ar stacionārām ierīcēm (vēlamākais diapazonā 192.168.0.210-192.168.0.254) un viņš piesavināsies no šā diapazona.Vai gan ar rokam pierakstīt šo адресс no dotā diapazona.(Att.5.2.)

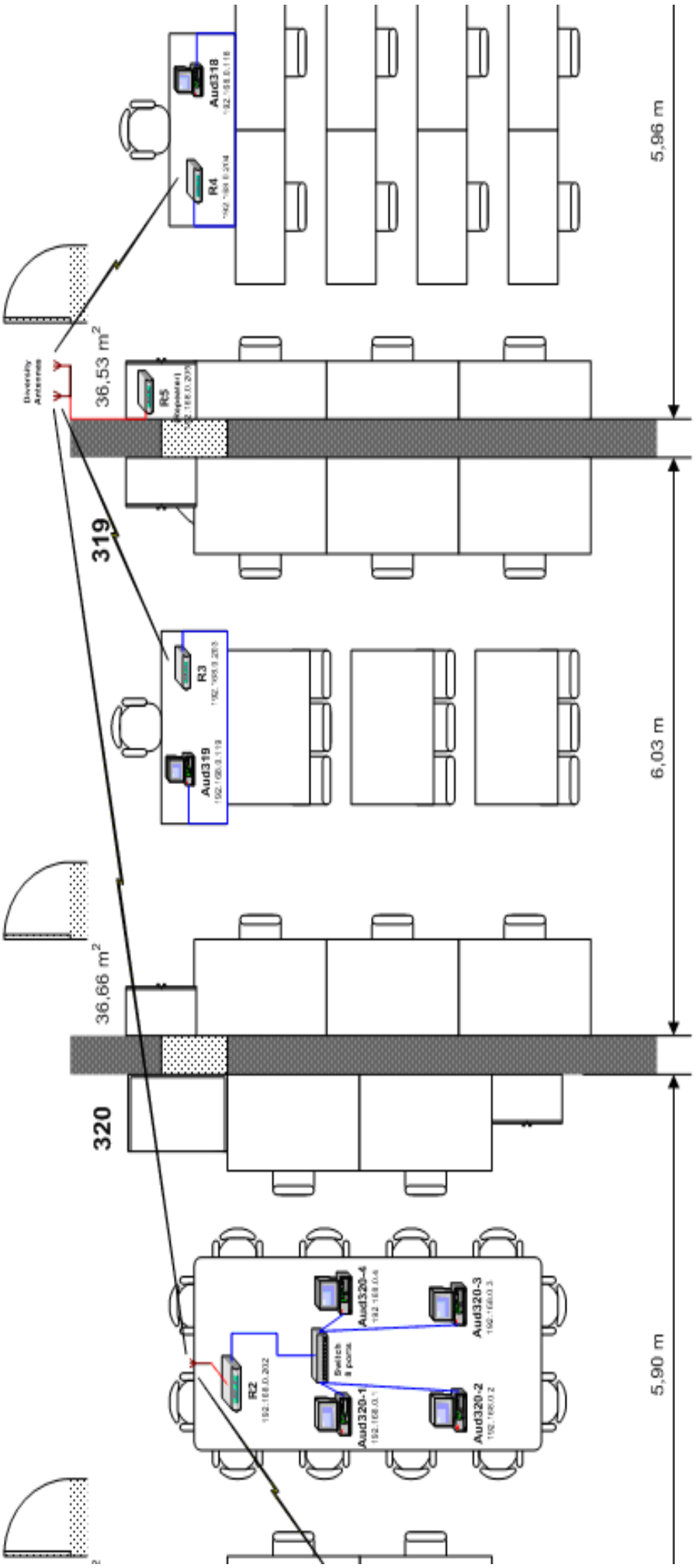


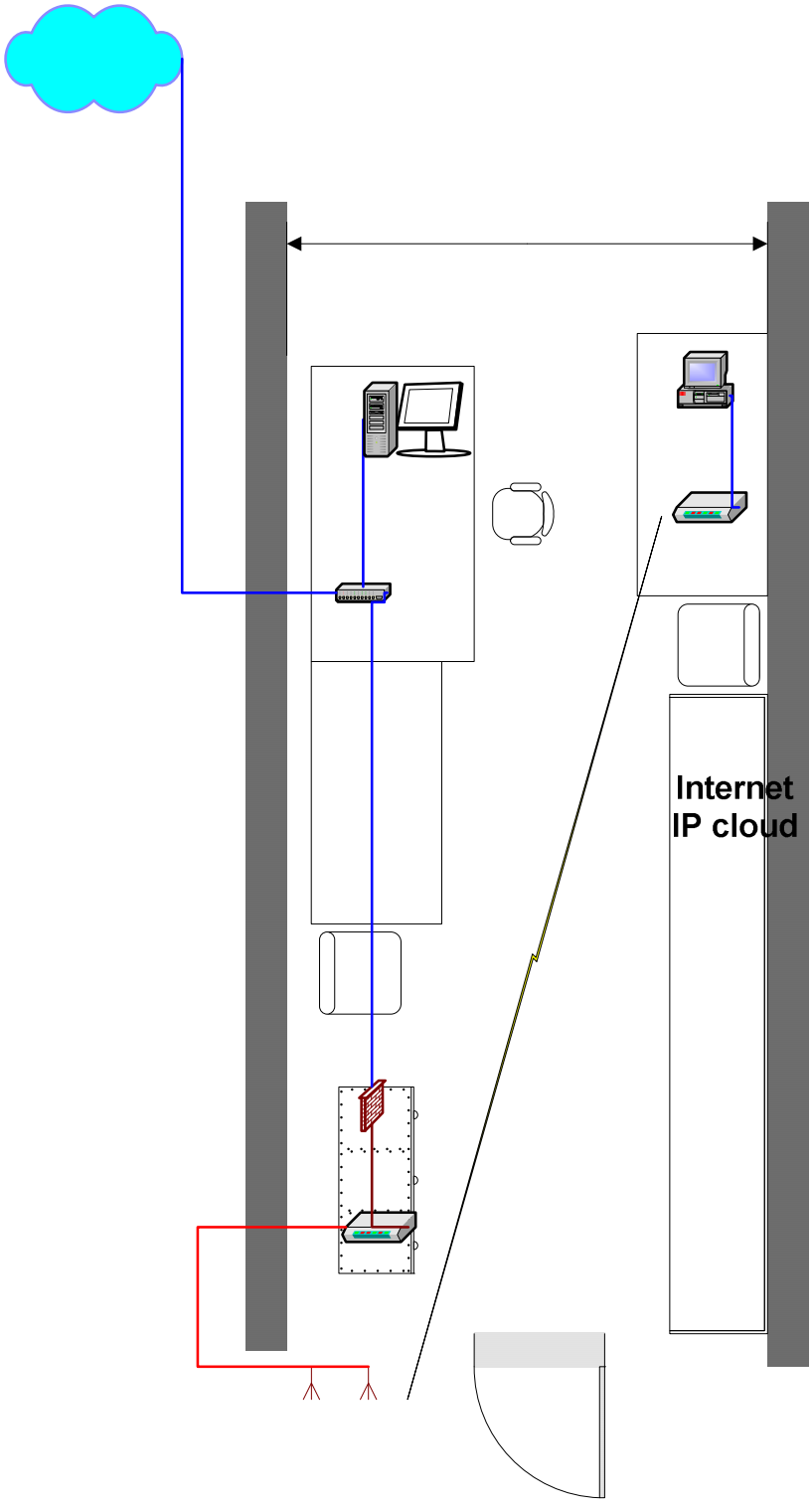
Att.5.2. IP adreses uzstadīšanas logs.

Pielikums

WLAN shēmas:


Hybrid Local Area Network
"Transport Communication and Information Systems (TCIS)"


Aud318
R4
5,96 m
Diversity Antenas
36,53 m²
R5
319
R3
Aud319
6,03 m
36,66 m²
320
R2
Switch 8 ports
Aud320-4
Aud320-3
Aud320-1
Aud320-2
5,90 m


Internet
IP cloud

Literatūra

1. П. Рошан, Дж. Лиэри. Основы построения беспроводных локальных сетей стандарта 802.11. М., СПб: Cisco Press, 2004.

2. Е. Головин. Локальная Сеть с Беспроводной Распределительной Системой: Проект WLAN сети в DzTI. Rīga: RTU DzTI, 2004, 50 с.

3. http://www.nokia.com: Nokia Equipment Support and Software.

4. http://www.wi-fi.org: Nonprofit international association certifying interoperability of wireless localarea network products based on IEEE 802.11 specification

5. Л. Невдяев Стандарты 802.11 и - Bluetooth- технология будущего. М.: Мобильный мир, №4, 2002, с.36-43.

6. Popovs V. GSM standarta šūnu mobilo sakaru sistēma. Projektēšanas problēmas. Rīga: RTU DzTI, 2003, 362.lpp.

7. Попов В.И. Многолучевое распространение радиоволн в WLAN (рукопись, CD-ROM). Рига: РТУ ИЖТ, 2005, 10 с.

8. Попов В.И. Основы сотовой связи стандарта GSM. М.: Эко-Трендз, 2005, 296 с.