LATVIJAS UNIVERSITĀTE

KVALIFIKĀCIJAS DARBS

RĪGA 2007

LATVIJAS UNIVERSITĀTE
FIZIKAS UN MATEMĀTIKAS FAKULTĀTE
DATORIKAS NODAĻA

RĪGAS VALSTS 1. ĢIMNĀZIJAS DATORTĪKLA MODERNIZĀCIJA

KVALIFIKĀCIJAS DARBS

Autors: **Kirils Solovjovs**
Stud. apl. ks05020
Darba vadītājs: pasn. B.dat. Leo Trukšāns

RĪGA 2007

ANOTĀCIJA

Savā kvalifikācijas darbā "Rīgas Valsts 1. ģimnāzijas datortīkla modernizācija" es tiecos modernizēt Rīgas Valsts 1. ģimnāzijas informācijas sistēmu, sasniedzot šādu uzdevumu izpildi: nodrošināt tīkla aizsardzību pret nesankcionētu piekļūšanu, izveidot uzticamu datu rezerves kopēšanas sistēmu, ieviest aizsardzību pret surogātpastu, izplānot un ieviest aizsargātu un ātru bezvadu tīklu, uzsākt sekundārā Interneta pieslēguma izmantošanu, nodrošināt rīkus darbstaciju vieglai atjaunošanai uz sākotnējo stāvokli, uzlabot lokālā tīkla ātrdarbību u.c., kā arī dokumentēt informācijas sistēmu un ieviest rīkus turpmākas administrēšanas atvieglošanai.

Kvalifikācijas darbā ir iekļauts sākotnējais situācijas apraksts un analīze, darba rezultātu apraksts, kā arī salīdzinājums starp sākotnējo situāciju un situāciju pēc darba pabeigšanas.

Atslēgvārdi: Rīgas Valsts 1. ģimnāzija, informācijas sistēma, datortīkls, modernizācija.

ABSTRACT

In my dissertation “Modernisation of the computer network at Riga State Gymnasium No. 1” I strive to modernise the information system of Riga State Gymnasium No. 1. by reaching the completion of the following tasks: ensuring the protection of the network against unauthorized access, creating a reliable data backup system, implementing the protection against e-mail spam, designing and implementing a protected high-speed wireless network, taking up the usage of the secondary Internet connection, providing facilities for restoring workstations to their original state, improving the speed of the LAN, etc., while documenting the information system and creating the tools for easing further administration of the system.

Dissertation includes description of the initial situation and the results of my work, and a comparison between the two.

Keywords: Riga State Gymnasium No. 1, information system, computer network, modernisation.

SATURS

APZĪMĒJUMU SARAKSTS

EIRP (Effective Isotropic Radiated Power) – efektīvā izotropiskā izstarotā jauda

IS – informācijas sistēma

MiB(5) – mebibaits – 1048576 baiti

MB(5) – megabaits – 1000000 baiti

Zeroconf – tehnoloģija, kas atļauj datoru kopai sazināties savā starpā bez papildus konfigurēšanas, tā sevī iekļauj, piemēram, DHCP

ēnotās paroles (shadow passwords) – paroļu glabāšanas sistēma, kas izplatīta Linux distributīvos

vienrežīms (singlemode) – pārraides režīms vienā optiskajā šķiedrā laižot vienu staru.

FX-TX – vides pārveidotājs, kas pārveido optiskās šķiedras signālu par vītā pāra (un otrādi)

IPS – Interneta pakalpojumu sniedzējs

CAM tabula (Content-addressable memory table) – tabula, kurā tiek uzglabātas MAC adreses; tā raksturīga komutatoriem

LVS - Latvijas Valsts standarts

ICS - International Classification for Standarts

IEC - International Electrotechnical Commission

ERC - European Radio Communications Committee

TIA - Telecommunication Industry Association

EIA - Electronic Industries Alliance

automātiskā saskaņošana (auto-negotiation) – datortehnikas spēja automātiski noteikt datortīkla, kurā tā atrodas, ātrumu

IKARUSS, *BETONS, RIEXC, RR* – Rīgas Valsts 1. ģimnāzijas serveri

maršrutētājs (router) – tīkla iekārta, kuras uzdevums ir nodrošināt datu pārraides maršruta izvēli

centrmezgls (hub) – tīkla iekārta, kas atkārto saņemto signālu uz visām tās pieslēgvietām

komutators (switch) – tīkla iekārta, līdzīga centrmezglam, bet kas atceras, pie kuras pieslēgtvietas pieslēgts, kurš saņēmējs

vides pārveidotājs – tīkla iekārta, kas pārveido vienas vides signālus par citas

cilvēkstunda – viena cilvēka vienā stundā patērētais laiks

sekundārais tīkls – *šajā gadījumā* tīkls, kas savienots ar otru IPS un netiek izmantots

pakalpojuma noraidījuma uzbrukums (DoS) – uzbrukums, kura mērķis ir liegt pakalpojumu izmantot citiem pakalpojuma lietotājiem

okšķeris – programmatūra vai iekārta, kas noklausās datu plūsmu tīklā

dēmons – programmatūra, kas atrodas servera atmiņā un izpilda lietotāju pieprasījumus

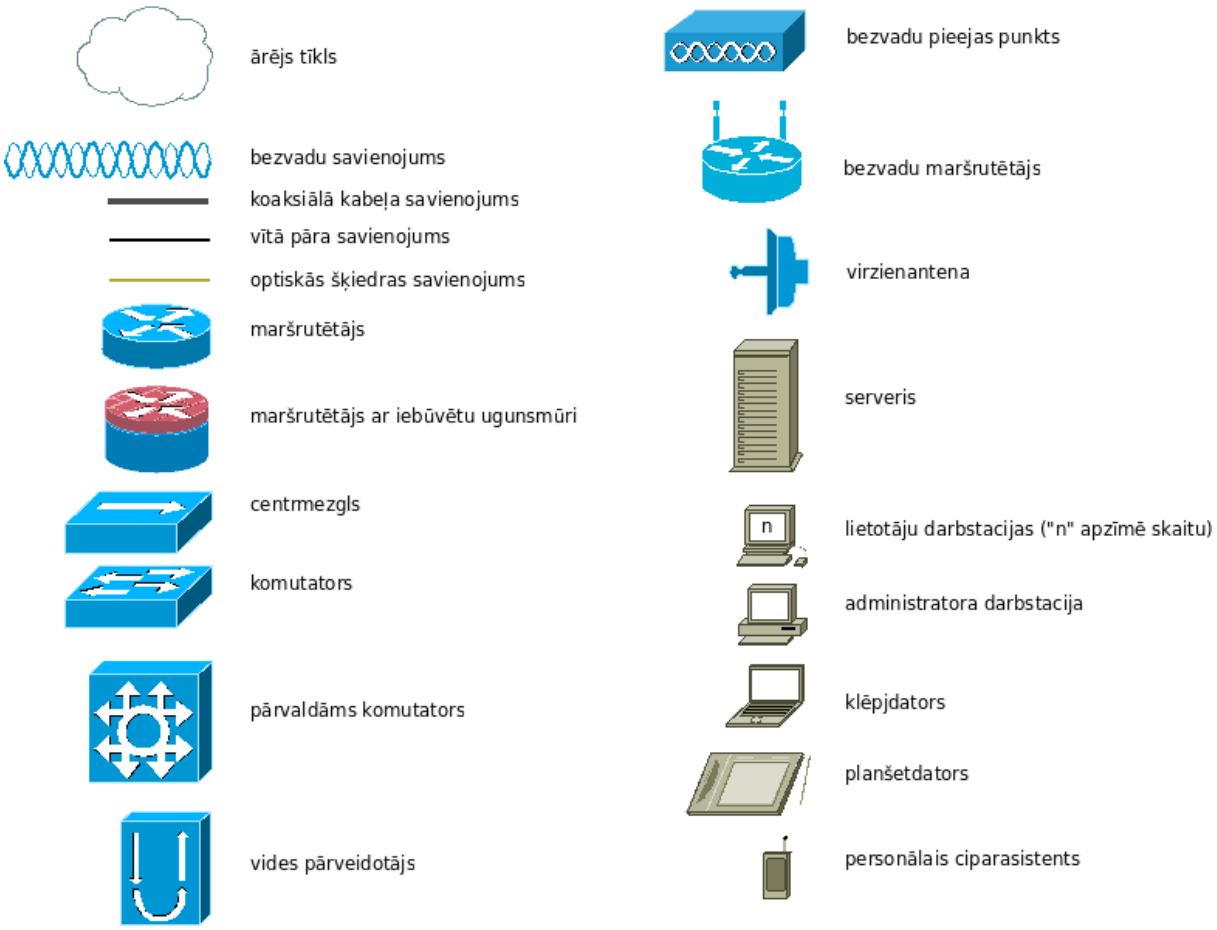
Teksta faila vai skripta saturs darbā tiks apzīmēts šādi. Fails *dati.txt:*

```
Hello, world!
```

Komandu izpilde darbā tiks apzīmēta sekojoši:

```
root@none:~# echo hello
hello
root@none:~# echo welcome
welcome
```

Datortīkla fiziskā slēguma shēmās tiek izmantoti sekojoši apzīmējumi:



A.1. att. **Shēmās izmantoto simbolu atšifrējums**

IEVADS

Kļūstot pieejamām ar vien jaunām tehnoloģijām, aug arī lietotāju prasības pret IS. Tāpēc līdzās ikdienišķiem administrēšanas uzdevumiem kā datu un IS drošības un integritātes nodrošināšana, ir svarīgi pievērst uzmanību arī sistēmas modernizācijai.

Kvalifikācijas darbā "Rīgas Valsts 1. ģimnāzijas datortīkla modernizācija" tiek strādāts ar Rīgas Valsts. 1. ģimnāzijas datortīklu, kas sastāv no vairāk kā 10 centrmezgliem un komutatoriem, 1 centrālā maršrutētāja un vairāk kā 100 darbstacijām. Datortīklam ir divi autonomi Interneta pieslēgumi un tajā funkcionē datubāzes, tīmekļa, failu, pasta u.c. serveri.

Veicot šo darbu, ir būtiski atcerēties, kas būs IS lietotāji, jo tas nosaka IS attīstības un uzturēšanas specifiku. Lielāko daļu no cilvēkstundām, kas tiek pavadītas lietojot Rīgas Valsts 1. ģimnāzijas IS, veido skolēni. Tā kā Rīgas Valsts 1. ģimnāzija nodrošina pamatizglītības programmu sākot ar 7. klasi un pilnu vidējās izglītības programmu, tad, ņemot vērā, ka iet 1. klasē bērns uzsāk ne ātrāk kā 5 gadu vecumā, bet iestāties 10. klasē var jebkurā vecumā, ja vien ir saņemts sertifikāts par pamatizglītību(6, 41. panta 1. daļa), varu secināt, ka skolēni ir personas vecumā no 12 gadiem. Izmērā mazāka, taču ne mazāk svarīga lietotāju grupa, ir akadēmiskais personāls (skolotāji u.c.) Gandrīz neviens no administratīvais personāla pārstāvjiem IS nelieto, tomēr izpētot situāciju, var redzēt, ka visas trīs personas, kas darbojas ar grāmatvedību, aktīvi izmanto IS. Līdz ar to secinu, ka IS attīstība ir jācentrē uz šo trīs lietotāju grupu darba atvieglošanu un iespēju palielināšanu, paturot prātā, ka lielākā lietotāju grupa ir skolēni.

Ne mazāk svarīgi ir arī ņemt vēra, ka darbs tiek veikts pašvaldības iestādē, kuras pamatuzdevums nav saistīts ar informācijas sistēmām vai datortīkliem, kas nozīmē, ka iekārtu iegādei un uzlabošanai netiks atvēlēts pārāk daudz naudas; tātad iekārtas būs jāizvēlas optimāli sabalansējot to cenu un gaidīto efektivitāti.

Šī darba mērķis ir modernizēt, uzturēt un attīstīt Rīgas Valsts 1. ģimnāzijas IS, kā arī dokumentēt šo procesu un tā rezultātu. Šajā darbā es izmantoju sekojošas metodes mērķa sasniegšanai:

- attīstības plānošana;
- iekārtu uzstādīšana, uzlabošana un nomaiņa;
- iekārtu konfigurēšana;
- sīku programmatūras vienību (skriptu un administrācijas saskarņu) izstrāde

- IS testēšana pirms un pēc uzlabojumiem.

Darbā izmantoti šādi faktoloģiskā materiāla avoti:

- datu pārraides ātruma mērījumi lokālajā tīklā (ar rīkiem *nc* un *dd*);
- tīkla un Interneta ātruma novērošana (ar rīku *iptraf*);
- vadu slēguma pareizības mērījumi (ar iekārtu *Multi-Network Cable Tester*);
- tīkla iekārtu TCP un UDP portu stāvokļa pārbaude (ar programmatūru *nmap*);
- tīkla iekārtu pārbaude uz zināmajām ievainojamībām (ar programmatūru *nessus*);
- bezvadu tīklu atklāšana (ar programmatūru *kismet*).
- tīkla plūsmas novērošana (ar okšķeriem *tcpflow, tcpdump,* u.c.).

Kvalifikācijas darbs ir sadalīts nodaļās. Darba sākumā tiek apskatīta sākotnējā IS struktūra, tad seko uzdevumu un programmu uzskaitījumus, katru no tām izdalot savā apakšnodaļā. Tam seko iespējamie risinājumi, to plānošanas un ieviešanas apraksts, kā arī dokumentācija, bet kvalifikācijas darbs noslēdzas ar rezultātiem un secinājumiem.

1. ESOŠĀ INFORMĀCIJAS SISTĒMAS STRUKTŪRA

1.1. Apraksts

1.1.1. Datortīkla apraksts

Līdz darba uzsākšanai tīkls sastāvēja no apmēram 100 darbstacijām, diviem serveriem – ārējās lietošanas servera *IKARUSS* un iekšējās lietošanas servera *BETONS*, kā arī maršrutētāja *ROUTER*. Tīkls saslēgšanai izmantoti komutatori un centrmezgli. Viss augstākminētais, izņemot pusi no darbstacijām kā arī 5 centrmezglus, atradās ēkas trešajā stāvā.

No maršrutētāja vairāku metru garumā stiepās koaksiālais kabelis, kas savienoja to ar virzienantenu uz ēkas jumta. Caur antenu Rīgas Valsts 1. ģimnāzija bija savienota ar Internetu. Otrā galā – citā ēkā – atradās aparatūra, ko pārvaldu nevis es, bet gan IPS. Fiziskā slēguma shēma (1.1. att.) ir iekļauta arī antena un maršrutētājs, kas atrodas citā ēkā.

Tīklā izmantoti šādi centrmezgli (slēguma shēma redzama 1.1. att.):

- 2 gab. *EtherPerfect ShureCom 505ST* – 5 pieslēgumvietas, 10BASE-T;
- 2. gab. *3Com 3C16701* – 8 pieslēgumvietas, 10BASE-T;
- 1. gab. *3Com HUB 8/TPO* – 8 pieslēgumvietas, 10BASE-T;
- 1. gab. *IBM 8222-008* – 8 pieslēgumvietas, 10BASE-T;
- 1. gab. *3Com 3C16592B* – 12 pieslēgumvietas, 100BASE-T.
- 5. gab. *3Com 3C16593B* – 24 pieslēgumvietas, 100BASE-T.

un šādi komutatori:

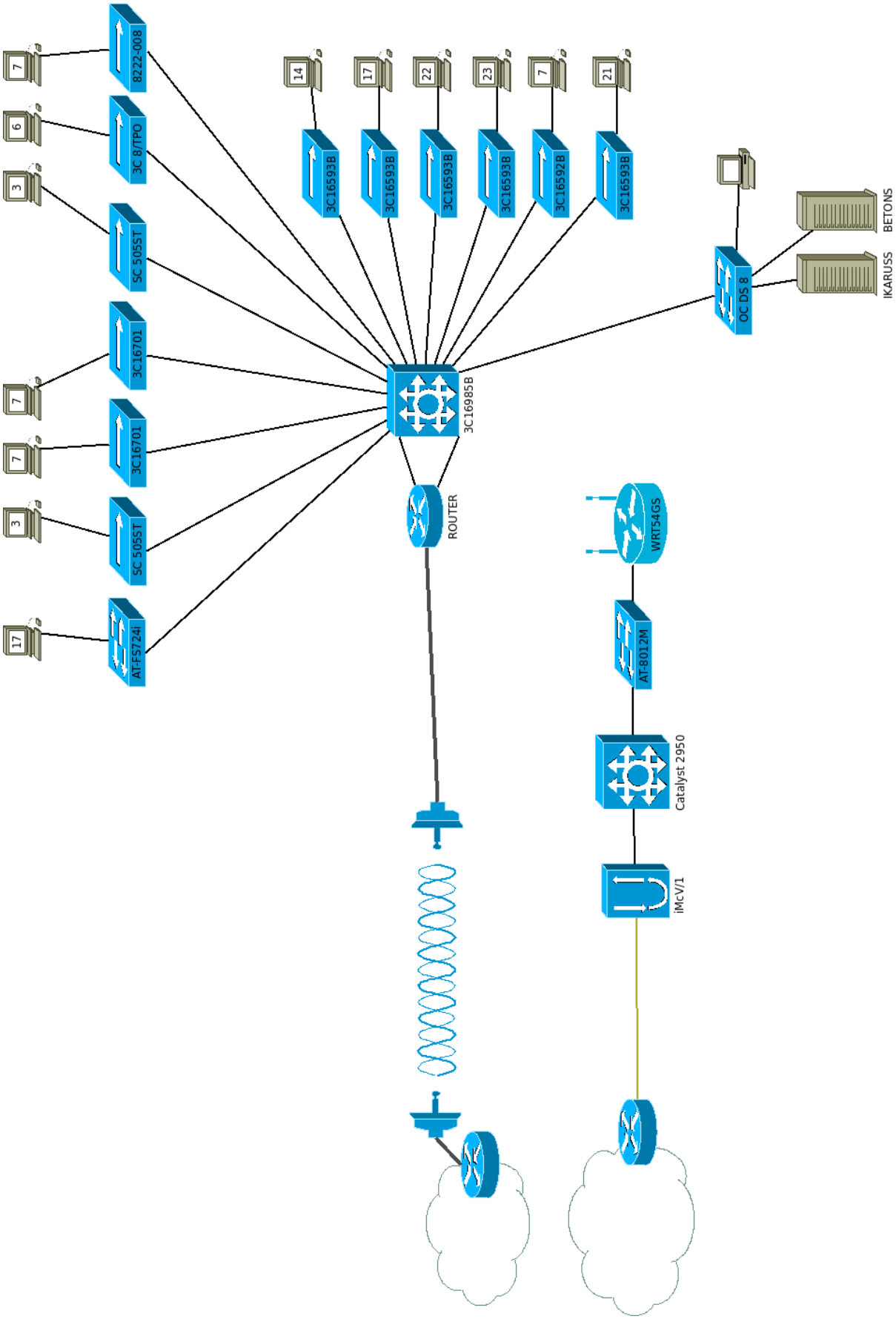
- 1. gab. *3Com 3C16985B* – 24 pieslēgumvietas, 100BASE-TX, pārvaldāms.
- 1. gab. *3Com OfficeConnect Dual Speed Switch 8* – 8 pieslēgumvietas, 100BASE-TX;
- 1. gab. *Allied Telesyn AT-FS724i* – 24 pieslēgumvietas, 100BASE-TX;

Paralēli šim pieslēgumam pirms pāris gadiem ēkai tika pievilkts arī optiskā kabeļa pieslēgums (sekundārais pieslēgums), kas netiek izmantots. Pieslēgums veikts ēkas otrajā stāvā, kur šim mērķim uzstādīts datortehnikas skapis, kurā atrodas četras tālākminētās iekārtas. Optiskais kabelis sastāv no divām vienrežīma šķiedrām (katra savā virzienā) ar optiskā viļņa garumu 1300 nm. Tas ir atsevišķs tīkls, ko es nepārvaldu. Tīkls sastāv no vides pārveidotāja (*IMC iMcV/1,* FX-TX), pārvaldāma komutatora *Cisco Catalyst 2950* (12 pieslēgumvietas, 100BASE-TX), komutatora *Allied Telesyn AT-8012M* (12 pieslēgumvietas, 100BASE-TX) un bezvadu maršrutētāja *Linksys WRT54GS* (5 pieslēgumvietas, 100BASE-TX, 802.11b/g). Šī pieslēguma elementus pārvalda IPS, tāpēc tam turpmākajā darbā tiks pievērsta maza uzmanība.

1.1.2. Pārējās IS apraksts

Rīgas Valsts 1. ģimnāzijas IS sastāv ne tikai no datortīkla. IS sastāvā ir arī vairākas lāzera drukas iekārtas, trīs skeneri. Taču tā kā pašreizējā politika nepieļauj šo un tml. iekārtu izmantošanu caur datortīklu, bet gan tikai lokāli – no attiecīgās darbstacijas, pie kuras iekārta pieslēgta –, tās nav vērts apskatīt.

IS sastāvā šobrīd ietilpst arī divas UPS iekārtās: maršrutētājs *ROUTER* un serveri *IKARUSS* un *BETONS* ir pieslēgti pie *APC Back-UPS 300VA*, bet visas četras sekundāra pieslēguma tīkla iekārtas ir pieslēgtas pie *APC Smart-UPS 450*.



1.1. att. **Rīgas Valsts 1. ģimnāzijas datortīkla fiziskā slēguma shēma pirms darba uzsākšanas**

1.2. Analīze

Lai sīkāk apskatītu IS uzbūvi, iedalīšu analīzi vairākās daļās, atsevišķi apskatot maršrutētāju, komutatorus, centrmezglus, kabeļus, darbstacijas, maršrutētāju, UPS un katru serveri.

1.2.1. Maršrutētājs

Maršrutētājs *ROUTER* atrodas servertelpā un ir būvēts uz PC arhitektūras bāzes. Tas darbojas uz OS *Slackware 10 Linux 2.4.31*. Tas sastāv no korpusa, barošanas bloka, mātesplates, 100 MHz procesora ar pasīvo dzesēšanu, videokartes, diskešu diskdziņa, 500MB IDE PATA cietā diska, 16MiB operatīvās atmiņas un trim tīkla kartēm:

- 2 gab. *3Com ISA EtherLink II* (ISA, 10BASE-T, draiveris *3c503*)
  - viena tīkla karte ir savienota ar komutatoru *3Com 3C16985B* un nodrošina, ka maršrutētājs ir sasniedzams no lokālā tīkla;
  - otra tīkla karte ir savienota ar komutatoru *3Com 3C16985B*, taču pieslēgumvieta, kurā tīkla karte savienota, ir atspējota. Tas, acīmredzot, darīts ar mērķi radīt iespēju attālināti pārslēgt savienojumu no vienas tīkla kartes uz otru avārijas gadījumā. Jāpiezīmē, ka automātiska pārslēgšana šajā konfigurācijā nebija paredzēta.
- 1 gab. *Aironet ISA4500* (ISA, 2 Mbps, 802.11b, draiveris *airo*)
  - tīkla karte ir savienota ar antenu izmantojot 9.5 mm 50 Ω koaksiālo kabeli.

Maršrutētāja uzdevums ir sazināties ar maršrutētāju, kas atrodas bezvadu savienojuma otrā galā, pārraidot datus caur virzienantenu. Uz tā ir uzstādīts primitīvs ugunsmūris, kas ierobežo visu ārvalstu datu plūsmu, izmantojot Latvijas IP adrešu sarakstu, kas pieejams tīmekļa vietnē http://nic.lv/local.net. Šim nolūkam tiek izmantota programmatūra *ipchains.* Maršrutētājs sinhronizē Latvijas IP adrešu sarakstu reizi nedēļā, reizē arī sinhronizējot savu iekšējo pulksteni ar NTP serveri ntp.latnet.lv. Šim nolūkam uz maršrutētāja strādā dēmons *crond*, kas noteiktajā laika aktivizē vajadzīgo programmu. Maršrutētājs nepielieto NAT.

Lēmums ierobežot ārvalstu datu plūsmu tika pieņemts, jo IPS pieprasīja atsevišķu samaksu par katru MB, kas tiek pārraidīts vienā vai otrā virzienā.(7) Lai gan tagad tā vairs nav, vadība joprojām uzstāj, ka ārvalstu datu plūsma tiek ierobežota.

Lai atsevišķi lietotāji varētu piekļūt ārvalstu tīmekļa vietnēm, uz maršrutētāja *ROUTER* ir uzstādīts arī starpniekserveris *squid,* kas pieprasa lietotājiem autentificēties. Lietotāju saraksts tiek mainīts no komandrindas, izmantojot rīku *htpasswd*.

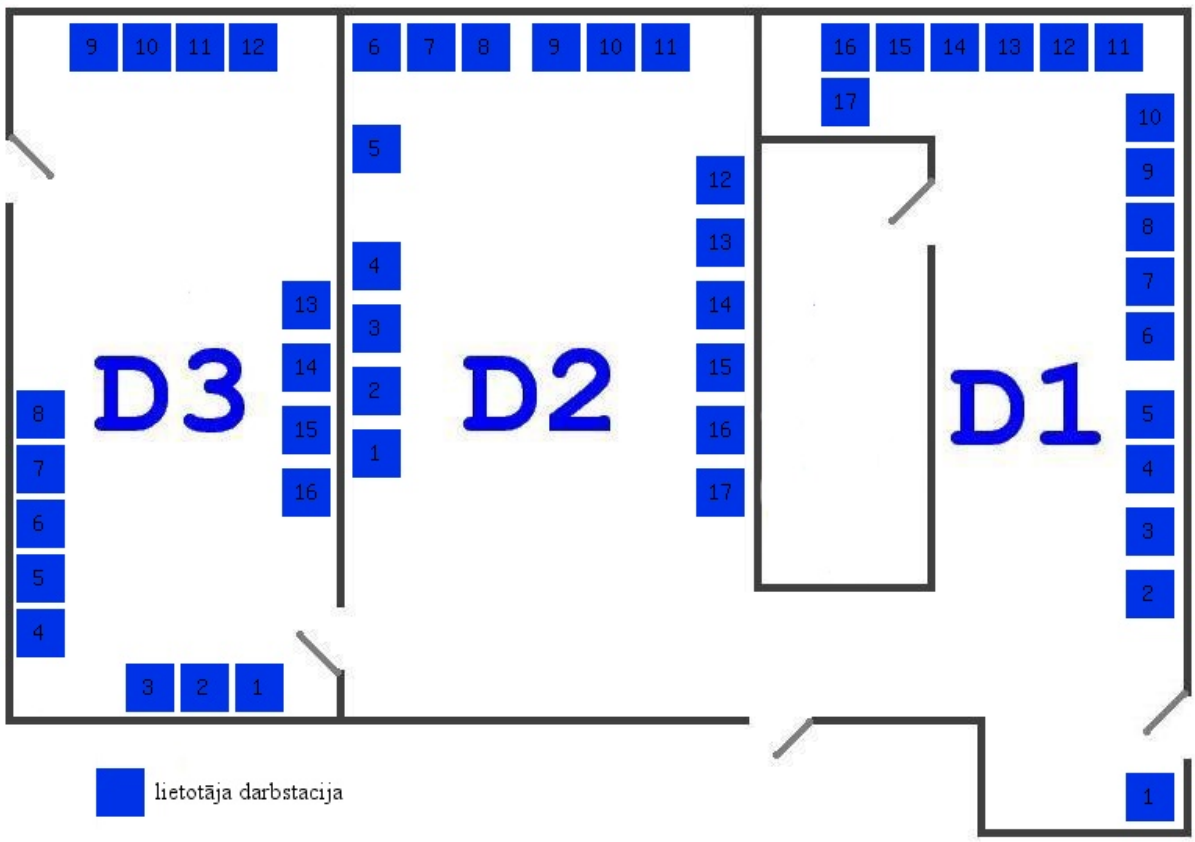
Administrēšanas nolūkiem uz maršrutētāja darbojas dēmons *sshd*.

1.2.2. Komutatori

Pārvaldāmais komutators *3Com 3C16985B* atrodas blakus maršrutētājam *ROUTER* un tā uzdevums ir strādāt kā parastam komutatoram, kas atceras MAC adrešu un pieslēgumvietu portus CAM tabulā. Tā pārvaldības funkcijas netiek izmantotas un paroles ir uzstādītas uz rūpnīcas noklusētajām vērtībām(13). Komutatoram ir 24 pieslēgumvietas, no kurām 16 ir aizņemtas.

Komutatora *3Com OfficeConnect Dual Speed Switch 8* uzdevums ir sadalīt tīklu plūsmu starp abiem serveriem un administratora darbstaciju un arī tas atrodas servertelpā. Komutators ar šo uzdevumu tiek galā pieņemami, ņemot vērā, ka Interneta pieslēguma ātrums ir tikai 2 Mbps un abu serveru tīkla spēj darboties tikai 10BASE-T standartā. Komutatoram ir 8 pieslēgumvietas, no kurām 4 ir aizņemtas.

Datorklasē D1 atrodas komutators *Allied Telesyn AT-FS724i*. (Skat. 1.2. att.) Tas darbojas 100BASE-TX standartā un tam ir 24 pieslēgumvietas, no kurām 18 ir aizņemtas.



1.2. att. **Datorcentra lietotāju darbstaciju izvietojums pa datorklasēm**

1.2.3. Centrmezgli

Datorklasēs D2 un D3 atrodas pa trim centrmezliem katrā. To standarti un pieslēgumvietu skaits ir redzams 1.1.1. apakšnodaļā, bet aizņemto pieslēgumvietu skaits – 1.1. att. Šo centrmezglu uzdevums ir sadalīt tīklu darbstacijām.

Centrmezgli *3Com 3C16592B* un *3Com 3C16593B* ir izvietoti dažādās ēkas vietās un nodrošina tīklu darbstacijām, kas atrodas ārpus datorcentra. Centrmezgli *3Com 3C16592B* izvietoti servertelpā (1 gab.), 2. stāvā (2 gab. vienā telpā un 1 gab. citā) un 1. stāvā (1 gab.); centrmezgls *3Com 3C16593B* izvietots 2. stāvā kopā ar centrmezglu *3Com 3C16592B*. (14)

1.2.4. Kabeļi

Izlases veidā pārbaudot Rīgas Valsts 1. ģimnāzijas ēkā esošos vītā pāra kabeļus ar nedārgu kabeļu testeri *Multi-Network Cable Tester*, noskaidroju, ka datorcentra klasē D1 (skat. 1.2. att.) izvietotie kabeļi neatbilst TIA/EIA-568-B standartam(1, 8), tamdēļ datorklases D1 tīkla ātrums ir lēnāks, nekā tas ir pārējās datorklasēs.

1.2.5. Darbstacijas

Rīgas Valsts 1. ģimnāzijas IS sastāvā ietilpstošās darbstacijas ir dažādi datori, ko vidēji raksturo šādi parametri ar pāris izņēmumiem:

- procesora takts frekvence: 250 MHz – 2 Ghz;
- operatīvās atmiņas apjoms: 32MiB – 512MiB;
- cietā diska apjoms: 2GB – 100GB;
- operētājsistēma:
  - *Windows 98SE* – apm. 60 darbstacijas;
  - *Windows ME* – apm. 10 darbstacijas;
  - *Windows XP* – apm. 30 darbstacijas;
- biroja programmatūra:
  - *Microsoft Office 97* – apm. 70 darbstacijas;
  - jaunāka *Microsoft Office* versija – apm. 30 darbstacijas;
- pretvīrusu programmatūra;
- cita programmatūra.

Darbstacijas ar zemākiem rādītājiem un vecāku operētājsistēmu (*Windows 3.11*, *DOS*) un programmatūru ēkā ir atrodami, taču saglabāti nostaļģijas dēļ un kā vēsturiska vērtība, tīklam nav pieslēgti un ikdienas darbiem netiek lietoti, kā arī nekādu svarīgu vai derīgu informāciju neglabā.

Lai gan daudzas Rīgas Valsts 1. ģimnāzijas lietotāju darbstacijas ir pēc savas aparatūras uzbūves identiskas, datori tiek pārinstalēti manuāli vismaz divas reizes gadā, ja darbstacijas atrodas datorklasē, vai ne biežāk kā reizi divos gados, ja darbstacijas atrodas ārpus tās.

Manuālā pārinstalēšana sevī ietver:

- licenzētas *Windows* OS uzstādīšanu un konfigurēšanu;
- draiveru uzstādīšanu un konfigurēšanu;
- datora konfigurēšanu darbam tīklā (IP parametri, u.c.);
- licenzētas programmatūras *Microsoft Office* uzstādīšanu;
- licenzētas programmatūras *Tildes Birojs* uzstādīšanu un konfigurēšanu;
- programmatūras izstrādes vižu un citu programmatūras pakešu uzstādīšanu.

1.2.6. UPS

Pārbaudot *APC Back-UPS 300VA* darbspēju, tika noskaidrots, ka tas maiņstrāvas zuduma gadījumā spēj noturēt maršrutētāju un abus serverus ieslēgtus 3 sekundes, bet, ja noslogots tikai ar maršrutētāju – 10 sekundes. Līdz ar to UPS atzīts par nederīgu akumulatora vainas dēļ.

1.2.7. Serveris *BETONS*

BETONS ir cienījama vecuma serveris – tas Rīgas Valsts 1. ģimnāzijas tīklā darbojas jau vairāk kā 10 gadus. Servera OS ir *Novell Netware 4.11*, tam ir 2GB SCSI cietais disks un 32MiB operatīvā atmiņa. Tas darbojas tikai un vienīgi kā lokālā tīkla failu serveris, kas veic lietotāju pilnvarošanu, izmantojot iekšēju lietotāju vārdu, paroļu un atļauju datubāzi. Šī datubāze ir administrējama,

a) izmantojot *Netware* administrēšanas konsoles rīkus;

b) piesakoties sistēmā ar administratora atļaujām un izmantojot DOS izpildāmos failus.

Serveris tiek izmantots tikai mācību procesa nodrošināšanai – mācību materiālu un pārbaudes darbu glabāšanai, taču šī izmantošana ir ļoti bieža – serveris tiek izmantots ikdienā. Avoti liecina, ka serveris kādreiz ticis izmantots arī e-pastu sūtīšanai un saņemšanai(15), tātad bez IPX/SPX protokola atbalstījis arī IP un TCP protokolu, taču vairs tādam mērķim izmantots netiek.

1.2.8. Serveris *IKARUSS*

Servera *IKARUSS* darbību nodrošina OS *Lingo 1.3 Linux 2.4.18*. Nekādu informāciju par šo distributīvu vai tā eksistenci man neizdevās atrast(16), kas varētu nozīmēt, ka distributīvs ir būvēts speciāli šī servera vajadzībām. Serveris ir būvēts uz *DELL TowerEdge 2200* bāzes un tā sastāvā ietilpst 265 MHz procesors, 64 MiB operatīvā atmiņa un 3 SCSI cietie diski ar 4GB ietilpību katrs. Serveri joprojām administrē cits cilvēks, kā rezultātā, man nav pieejama likumiska piekļuve tam, taču tā kā serveris atrodas manis pārvaldītās IS struktūrā, varu to pārbaudīt ārēji, kā arī vadoties pēc dokumentācijas(15).

Serveris nodrošina sekojošus pakalpojumus:

- tīmekļa serveris *Apache 1.3.24*;
- failu serveris *Samba 2.2.3a*;

- SSH servera programmatūra *OpenSSH 3.0p1*;
- SMTP servera programmatūra qmail 1.03;
- IMAP servera programmatūra *Courier-IMAP*;
- DB servera programmatūra *MySQL 4.0.1*.

1.2.9. Sekundāra tīkla analīze

Tā kā sekundārais tīkls netiek izmantots, kā arī iekārtas ir IPS, nevis manā pārvaldība, tad tīkla analīze būtu lieka, taču manu uzmanību pievērsa bezvadu maršrutētāja esamība tīklā, kas teorētiski var radīt draudus citu bezvadu tīklu drošībai, kā arī radīt iespēju apiet Rīgas Valsts 1. ģimnāzijas drošības politiku, piekļūstot Internetam caur šo bezvadu maršrutētāju.

1.2.10. Kopsavilkums

Analīze parāda, ka esošajā IS ir nopietnas problēmas, kas ir jārisina, taču darba laikā radās arī citas problēmas un uzdevumi, kas neizriet no esošās IS struktūras. Tie iedalāmi divās kategorijās:

- tādas problēmas un uzdevumi, ko iepriekš paredzēt nebija iespējams, bet kuru risināšana neizbēgami ir datortīkla administratora darba sastāvdaļa;
- tādi uzdevumi, kam par pamatu ir lietotāju prasību paaugstināšanās pret IS (šo pieminēju jau kvalifikācijas darba ievadā).

Visus uzdevumus uzskatīšu nākamajā nodaļā.

2. PROBLĒMAS UN UZDEVUMI

2.1. Maršrutētāja *ROUTER* problēmas

2.1.1. Aparatūra un caurlaidība

Veicot maršrutētāja analīzi, atklājās, ka maršrutētāja aparatūra ir novecojusi un mazjaudīga, maksimālais teorētiskais Interneta ātrums, ko tas var nodrošināt ir 2 Mbps, kas ir vienāds ar 250 kB sekundē uz visu tīklu. Šī problēma attiecas uz Rīgas Valsts 1. ģimnāzijas IS daļu, kas pieslēgta Internetam. Maksimuma laikā Internetu lietojošo darbstaciju skaits sasniedz 50, kas realitātē nozīmē Interneta piekļuves ātrumu ne vairāk kā 5 kB sekundē uz katru darbstaciju. Šāds Interneta piekļuves ātrums mūsdienās lietotājiem nav pieņemas.

Tamdēļ ir jāuzlabo maršrutētāja aparatūra un jāpalielina maršrutētāja caurlaidība ar mērķi celt maksimālo Interneta ātrumu.

2.1.2. Latvijas IP adrešu saraksts

Latvijas Interneta adrešu saraksts, kas atrodas tīmekļa vietnē http://www.nic.lv/local.net, nav korekts (apakštīkli pārklājas). Tas rada lieku slodzi uz programmatūru *ipchains* un *squid*, kā arī palielina maršrutētāja žurnāla aizpildīšanās ātrumu. Pagātnē ir bijuši gadījumi, kad dēļ maršrutētāja nelielā cietā diska pārpildes, atsakās darboties *squid*. Tas efektīvi nobloķē pieeju ārvalstu Interneta resursiem.

Ir nepieciešams dinamiski izveidot tādu sarakstu, kas ir korekts.

Pārbaudot, kā darbojas primitīvie ierobežojumi, kas neļauj piekļūt ārvalstu Interneta adresēm, noskaidroju, ka pat serveris *IKARUSS* nevar tām piekļūt. Manī tas radīja aizdomas, ka *IKARUSS,* serveris, kas šobrīd uztur Rīgas Valsts 1. ģimnāzijas mājaslapu un e-pastu sistēmu, nav sasniedzams no ārzemēm. Tas tika pārbaudīts un izrādījās taisnība.

Plānojot jauno ugunsmūri un maršrutētāju, ir jānodrošina, ka serveri ir sasniedzami no visa Interneta.

2.2. Ugunsmūris

Zemāk esošajā termināļa izdrukā redzama pārbaude, kas pierāda, ka viens no Rīgas Valsts 1. ģimnāzijas *Windows 98SE* datoriem nav aizsargāts no ārpasaules.

```
root@ps:~# nmap -A -sS 85.254.197.241
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-10-20 21:23 EEST
```

```
Interesting ports on 85.254.197.241
Not shown: 1679 closed ports
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn
Device type: general purpose|media device
Running: Microsoft Windows 95/98/ME|NT/2K/XP, Turtle Beach embedded
OS details: Microsoft Windows NT 3.51 SP5, NT 4.0 or 95/98/98SE, Turtle Beach AudioTron
network MP3 player

Nmap finished: 1 IP address (1 host up) scanned in 13.948 seconds
```

Komanda *nmap* veic dotās IP adreses portu pārbaudi, izmantojot SYN skanēšanas metodi (*-sS*) un veicot OS un programmatūras versiju noteikšanu (*-A*).

Lai gan atvērts ports vēl pats par sevi nekādus draudus nerada, tas var būt par pamatu visu Rīgas Valsts 1. ģimnāzijas IS glabāto datu drošības apdraudējumam. Var tikt apdraudēta:

- datu integritāte (informācijai jābūt pilnīgai un precīzai);
- datu konfidencialitāte (informācijai būtu jābūt pieejamai tikai tām personām, kas ir pilnvarotas darbam ar šiem datiem);
- datu pieejamība (informācijai nepieciešamības gadījumā jābūt pieejamai).

Windows 98SE sistēma standarta komplektācijā ir samērā aizsargāta pret vīrusu un hakeru uzbrukumiem, taču Windows XP operētājsistēma, kura arī ir pārstāvēta Rīgas Valsts 1. ģimnāzijas datortīklā, "nāk jau komplektā" ar programmatūras kļūdu, kas ļauj ļaundarim pilnībā pārņemt svaigi instalētu datoru dažu sekunžu laikā.

```
root@ps:~# nmap -A -sS 85.254.197.243
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-10-20 21:35 EEST
Interesting ports on 85.254.197.243:
Not shown: 1678 closed ports
PORT    STATE SERVICE     VERSION
135/tcp open  msrpc       Microsoft Windows RPC
139/tcp open  netbios-ssn
Device type: general purpose
Running: Microsoft Windows 2000|XP|2003
OS details: Microsoft Windows 2000 Server SP4, Microsoft Windows XP SP2 (firewall
disabled), Microsoft Windows 2000 SP4, Microsoft Windows XP SP2, Microsoft Windows 2000
SP3, Microsoft Windows 2003 Server SP1, Microsoft Windows 2000, SP0, SP1, or SP2

Nmap finished: 1 IP address (1 host up) scanned in 17.550 seconds
```

Ir jāizstrādā un jāuzstāda kvalitatīva ugunsmūra konfigurācija, kas bāzēta uz modernas ugunsmūra programmatūras.

2.3. Neautorizēta pieslēgšanās no tīkla iekšienes

Šobrīd jebkurš var pieslēgties IS un piekļūt tajā izvietotajiem serveriem. Tas arī var apdraudēt IS.

Datortīkls jāpārkonfigurē tā, lai darbstacijas būtu nodalītas no serveriem, kā arī jāievieš datortīkla aparatūras obligātu reģistrāciju pirms tā tiek atpazīta tīklā.

2.4. Pārvaldāmā komutatora drošība

Tas, ka komutatora *3Com 3C16985B*, administratīvie autentifikācijas parametri ir uzstādītas uz rūpnīcas noklusētajām vērtībām, rada draudus datortīkla darbībai. Šis ir vienīgais komutators, pie kura ir pieslēgts maršrutētājs *ROUTER*, kas nozīmē, ka šī komutatora darbnespējas gadījumā, zustu tīkla savienojums ar Internetu.

2.5. Servera *IKARUSS* drošība

Kā parāda pielikums nr. 1 "Servera *IKARUSS* drošības audits", servera programmatūra ir morāli novecojusi un satur ļoti daudz drošības kļūdas. Tas, ka līdz šim nav notikusi IS katastrofa, ir tikai laimes jautājums.

Serveris ir nekavējoties jāizolē no tīkla.

2.6. Jauna servera izveide

Tā kā serveris *IKARUSS* vairs nespēj uzticami veikt savas funkcijas, ir steidzami jāizveido jauns serveris, kas varētu apvienot gan servera *IKARUSS*, gan *BETONS* funkcijas, jo *BETONS* ir mazjaudīgs un ar nelielu ietilpību.

2.7. Bezvadu tīkls

Lietotāji lūdz izveidot bezvadu tīklu, jo pašreiz pieslēgties tīklam ar personīgajiem klēpjdatoriem ir neērti un apgrūtinoši. Bezvadu tīkla ieviešana un klēpjdatoru un citu mobilo ierīču izplatība ļaus Rīgas Valsts 1. ģimnāzijas ikdienā sekmīgāk ieviest e-pārvaldi, jaunas mācību formas un e-sadarbības rīkus.

Ir jāizpēta, vai klēpjdatoru lietošanas tīklā oficiāla atļaušana neradīs draudus IS drošībai, jāizpēta likumiskais regulējums saistībā ar bezvadu pieejas punktiem, iespēja uzstādīt bezvadu pieejas punktus ar centralizētu lietotāju vadību ēkas teritorijā, un jānodrošina sistēma, kā tiek reģistrētas personas, kas lietos bezvadu tīklu, kā arī viņu aparatūra.

2.8. Sekundārā tīkla draudu novēršana

Bezvadu maršrutētāja esamība sekundārajā tīkla rada potenciālus draudus plānotajam Rīgas Valsts 1. ģimnāzijas bezvadu tīklam. Reālākie iespējamie draudi ir pakalpojuma noraidījuma uzbrukums, kas var novest pie tā, ka leģitīmi lietotāji nespēj izmantot bezvadu tīklu. Šis faktors apdraud tikai vienu IS daļu – bezvadu tīklu – un citās IS daļās nekādus draudus nerada.

Ir jāatslēdz strāvas padeve bezvadu maršrutētājam.

2.9. Sekundārā tīkla izmantošana

Rīgas Valsts 1. ģimnāzijai ir veikts pieslēgums ar optisko kabeli (sekundārais tīkls), taču tas šobrīd netiek izmantots.

Ir jāizpēta iespējas novilkt stāvvadu no 2. stāva servertelpas, kur atrodas sekundārais tīkls, uz 3. stāva servertelpu.

2.10. Datu rezerves kopēšana

Šobrīd datu rezerves kopēšana netiek veikta un tas rada draudus IS informācijas pieejamībai un integritātei.

Vajadzētu izveidot uzticamu datu rezerves kopēšanas sistēmu.

2.11. Surogātpasts

Liela daļa lietotāju laika tiek patērēta apskatot un dzēšot surogātpastu. Tas aizņem arī vietu uz servera un noslogo datu pārraides kanālus. Šī problēma ietekmē visu IS, ieskaitot tās lietotājus, administratorus un datortīklu.

Ir nepieciešams izveidot risinājumu aizsardzībai pret surogātpastu.

2.12. Darbstaciju administrēšana

2.12.1. Darbstaciju individuālā drošība

Datoru ar Windows XP operētājsistēmu (bez servisa pakām) esamība tīkla rada draudus IS.

Jāapzina Windows XP datoru esamība vai neesamība tīklā un

a) jāuzinstalē 2. servisa paka

vai

b) jāuzinstalē cita OS.

2.12.2. Pārinstalēšanas atvieglošana

Datoru pārinstalēšana aizņem ļoti daudz laika, turklāt apm. 50 datoriem to ir jāveic ļoti bieži (skat. esošās informācijas sistēmas struktūras analīzi). Tā ir neefektīva informātikas pasniedzēju, kas parasti ir šī procesa veicēji, laika tērēšana.

Tāpēc ir jāievieš DHCP serveris un jāizveido vienota pakete, kas atvieglos datoru instalēšanu un samazinās instalēšanai nepieciešamo laiku.

2.13. Lokālā tīkla ātrums

Veicot lokālā tīkla ātruma mērījumus, kuru sīkāka norise apskatāma pielikumā nr. 4 "Lokālā tīkla ātruma mērījumi", secināju, ka lokālā tīkla ātrums datorcentra ietvaros nav apmierinošs, kam par iemeslu ir nekvalitatīvi kabeļi (datorklasē D1) un 10BASE-T tīkla iekārtas (datorklasēs D2 un D3).

Lasot literatūru, secināju, ka tam par iemeslu var būt arī neatbilstība starp tīkla iekārtu automātisko ātrumu saskaņošanu(17). Ja vienai (vai vairāk) no iekārtām būs manuāli iestādīts pilns duplekss, bet pārējām – automātiskā ātrumu saskaņošana, tad šī viena (vai vairākas) iekārtas tīklā nefunkcionēs korekti.

Līdz ar to ir nepieciešams:

- pārvilkt kabeļus datorklasē D1;
- aizvietot visas 10BASE-T iekārtas un, ja finanses to atļauj, arī 100BASE-T iekārtas ar 100BASE-TX iekārtām;
- pārliecināties, ka visām tīkla iekārtām ir ieslēgta automātiskā ātrumu saskaņošana.

2.14. UPS iegāde

Šī darba analīzes daļā noskaidroju, ka *APC Back-UPS 300VA* ir nederīgs, jo maiņstrāvas pazušanas gadījumā nespēj pildīt savu uzdevumu ilgāk par dažām sekundēm. Šādā gadījumā būs paralizēta praktiski visas IS darbība: nedarbosies maršrutētājs un abi serveri.

Nepieciešams iegādāties jaunu UPS.

2.15. Brīvā izpēte

Lai gan šobrīd pēc sekojoša veida uzlabojumiem IS nav vajadzības, tomēr, izrādot pašiniciatīvu, nolēmu pētīt iespējas Rīgas Valsts 1. ģimnāzijas IS ieviest IPv6 adresāciju (paralēli esošajai), kā arī atrast pielietojumu jaunajam *IBM @server xSeries 205* serverim.

2.16. Administrēšanas atvieglošana

Zemāk uzskaitītos uzdevumus vajadzētu veikt, lai paātrinātu un atvieglotu administrēšanas darbu. Tiem nav tiešas ietekmes uz IS struktūru, kā vien uz administratoru laika patēriņu. Varētu domāt, ka administratora laika patēriņa samazinājums ļaus pievērst vairāk uzmanības citām aktualitātēm.

Tātad, lai panāktu augšminēto, jāizveido administrēšanas rīki lietotāju veidošanai (šobrīd lietotāju pievienošana starpniekserverim *squid* nav ērta) u.c., jāpārnes vārdu serveris uz kāda servera, ko pārvaldu es pats.

Mācību kvalitātes celšanas nolūkos pēc akadēmiskā personāla pieprasījuma ir jāizveido rīks, kas ļauj vienkārši atslēgt vai pieslēgt Internetu katrā no trijām datorklasēm atsevišķi (skat. 1.2. att.)

2.16.1. Dokumentācija

Nepieciešams apzināt, kurā telpā un vietā atrodas kurš stacionārais dators. Tas ļaus, piemēram, vīrusa uzbrukuma gadījumā no iekštīkla, ātri identificēt vainīgo datoru un telefoniski informēt lietotāju vai kādu, kurš dotajā brīdi ir attiecīgajā telpā.

2.17. Servera *BETONS* diska nobrukšana

Pie neparedzētajiem darbiem pieskaitāma servera *BETONS* vairākkārtēja attiekšanās strādāt diska bojājuma dēļ. Tiklīdz kļuva skaidrs, ka disks nu pat neatgriezeniski sabojāsies, nācās glābt situāciju, jo pretējā gadījumā tiktu pazaudēti visi uz servera esošie dati, t.i. tiktu apdraudēta informācijas pieejamība. Tā kā tobrīd rezerves kopijas netika veidotas, tas atstātu tiešāko iespaidu uz IS un tās lietotājiem – skolēniem būtu jāpārraksta neizlabotie kontroldarbi, skolotājiem būtu jāsāk pilnīgi no jauna veidot daudzu gadu gaitā uzkrātā un izveidotā metodisko materiālu bāze.

Tāpēc bija vitāli svarīgi maksimāli pilnīgi un precīzi atjaunot piekļuvi datiem un nodrošināt, ka tie tuvākajā nākotnē šādā veidā vairs netiks apdraudēti.

2.18. Informātikas ieskaite

Nedēļu pirms Rīgas Valsts 1. ģimnāzijā bija jānotiek informātikas ieskaitei, informātikas skolotāji man lūdza, vai nevaru atvieglot darbu savākšanu no datoriem, jo šogad ieskaite notikšot 4 daļās, no kurām 3 būšot pildāmas pie datora. Rīgas Valsts 1. ģimnāzijā šo ieskaiti kārto apmēram 200 skolēnu. Kopā tas veido vismaz 600 darbus.

Tāpēc ir nepieciešams izveidot nelielu skriptu, kas automātiski vai pusautomātiski savāks katru darbu no datora un novietos to uz servera, kur to vēlāk būs iespējams novērtēt skolotājam.

3. RISINĀJUMI

3.1. Plānošana

Pirmais plānošanā veicamais darbs ir uzdevumu prioritāšu noteikšana. Steidzamākās problēmas, pie kurām jāsāk darbs nekavējoties, ir:

- servera *IKARUSS* drošība;
- ugunsmūris;
- pārvaldāmā komutatora drošība un efektīva izmantošana.

Tiklīdz šie darbi ir izplānoti un padarīti, jāturpina ar šo problēmu izpēti:

- UPS iegāde;
- neautorizēta pieslēgšanās no tīkla iekšienes;
- maršrutētāja *ROUTER* problēmas;
- sekundārā tīkla draudu novēršana;
- surogātpasts.

Tikai pēc tam jāķeras pie pārējām lietām. Šādu secību izvēlējos, jo, manuprāt, IS sākumā jānovērš draudi informācijas drošībai, tad jebkāda cita veida drošībai, pēc tam jāķeras pie kļūdu labošanas. Pašās beigās (neizceļot kādu kategoriju virs citas) seko uzlabojumi, paša darba atvieglošana, brīvā izpēte un dokumentācijas sagatavošana.

Pēc tam, kad darbu prioritātes ir noteiktas, var sākt darbu pie plānošanas.

3.1.1. Ugunsmūris (iesk. pieslēgumu no tīkla iekšienes reģistrāciju) un maršrutētājs

Stratēģiski izdevīga vieta, kur izvietot ugunsmūri, būtu maršrutētājs. Tamdēļ sākumā jānomaina maršrutētāja aparatūra – jāuzstāda vismaz 300 MHz procesors, vismaz 256 MiB operatīvās atmiņas un vismaz 10 GB liels cietais disks, kā arī abas 10BASE-T tīkla kartes jānomaina ar 100BASE-TX tīkla kartēm, bet *Aironet ISA4500* 2 Mbps tīkla karti pret 11 Mbps, jo tas ir maksimālais, ko nodrošina 802.11b standarts, tātad maksimālais, ko var sasniegt, nelūdzot aparatūras maiņu otrā galā. Neviens no šiem uzlabojumiem, izņemot cieto disku un radiotīkla karti, nav saderīgi ar esošo mātesplati(2), tāpēc būs nepieciešama arī jauna mātesplate.

Šiem maršrutētāja parametriem vajadzētu pietikt plānotajai attīstībai un ļaut uz tā uzstādīt ugunsmūri. Lielāku parametru izmaksās dārgāk, un, ņemot vērā Rīgas Valsts 1. ģimnāzijas specifiku, lietotāji pagaidām nenovērtu to, tāpēc arī finansējums dārgākai aparatūrai piešķirts netiktu. Alternatīvi varētu uzstādīt arī aparatūras maršrutētāju (piemēram, *Cisco* maršrutētāju), taču, zinot, cik tas izmaksātu, šo domu es uzreiz atmetu, jo neatkarīgi no labumiem vadība nepiekristu tādai cenai.

Plānojot, kādu programmatūru lai uzstāda uz maršrutētāja, sāku ar OS izvēli. Iespējamie varianti ir Slackware Linux, kāds cits Linux distributīvs vai kāda BSD OS. Nolēmu pieturēties pie *Slackware Linux,* kas jau vēsturiski "darbinājis" Rīgas Valsts 1. ģimnāzijas IS(15), jo tas atļauj brīvību atstāt konfigurāciju noklusētu vai veidot to pēc sirds patikas sarežģītu, kā arī izmantot pakotņu sistēmu vai kompilēt programmatūru un pat kodolu no pirmkoda. Ir redzētas arī lietotājam (šajā gadījumā – administratoram) draudzīgākas pakotņu sistēmas par *Slackware Linux* esošo, bet tik un tā visu iespējams paveikt bez problēmām. Izvēlējos, ka uz maršrutētāja kā OS jāuzstāda *Slackware 11.1 Linux 2.6.21.1* versija, jo tā ir jaunākā, kas ir pieejama. Ar šo versiju lieliski darbotos ugunsmūris *iptables*, kas varētu aizvietot *ipchains.* Izvēlējos iptables, jo tas šobrīd ir līderis starp ugunsmūriem, kas pieejami uz šīs OS, turklāt pieejams kā *Slackware Linux* pakotne. Jāuzliek arī starpniekservera *squid* jaunāka versija, jo vadības politika ir neļaut neierobežotu piekļuvi ārvalstu Interneta resursiem ir vēsturiski saglabājusies, neskatoties uz to, ka par ārvalstu Interneta datu pārraidi vairs nav jāmaksā. Starpniekserveris *squid* gan diemžēl šobrīd nav pieejams kā *Linux Slackware* pakotne(18),

Lai novērstu lietotāju iespēju nesankcionēti pieslēgties tīklam no iekšienes maršrutētāja katra 100BASE-TX tīkla karte jākonfigurē atsevišķā apakštīklā (nodalīti – serveriem un darbstacijām) un maršrutētājs jākonfigurē tā, lai caur to izietu tikai paketes no reģistrētām MAC adresēm. Jāizveido skriptu komplekts, kas ļauj šīs adreses reģistrēt.

Papildus tam uz maršrutētāja jāuzstāda DHCP serveris, kas ļoti atvieglos datoru IP adrešu pārvaldību.

Tā kā Latvijas IP adrešu saraksts, kas atrodas tīmekļa vietnē http://www.nic.lv/local.net, nav korekts, jo tā vairāki apakštīkli pārklājas, un jau ilgi ir gaidīts, kamēr nic.lv šo sarakstu izlabos paši, esmu nolēmis izveidot korektu sarakstu, kas automātiski atjaunināsno oriģinālā saraksta reālajā laikā un izlikt šo sarakstu publiskai lietošanai, jo arī citiem kas tāds var noderēt. Kad IP adrešu saraksts būs izveidots un stabili funkcionējošs, tas uz maršrutētāja aizvietos nic.lv piedāvāto sarakstu.

Maršrutētāja vārds būs *WATERFALL*.

3.1.2. Servera *IKARUSS* drošība

Tā kā serveri nepārvaldu es, man nav iespēju mainīt tā konfigurāciju, atjauninot programmatūru. Vienīgais risinājums ir ierobežot tam piekļuvi. Tāpēc uz ugunsmūra tiks izvietoti noteikumi, kas bloķēs visus servera *IKARUSS* piedāvātos pakalpojumus, izņemot SMTP.

3.1.3. Pārvaldāmā komutatora drošība

Komutatora *3Com 3C16985B* administratīvie autentifikācijas parametri nekavējoties tiks nomainīti un piekļūšana komutatora uzstādījumiem ierobežota ar ugunsmūra palīdzību.

3.1.4. Jauna servera izveide

Tā kā serveris *IKARUSS* nu spēs tikai pieņemt e-pastus, tiks veidots jauns serveris, būtiskāko lietotāju informāciju kopējot no servera *IKARUSS* un veicot aptauju starp akadēmisko personālu un skolēniem par servera nosaukumu.

Serverim būs jānodrošina sekojoši pakalpojumi:

- tīmekļa serveris *Apache 2.2.4* ar *PHP 5.2.2*;
- failu serveris *Samba 2.2.8a*;
- failu serveris *ProFTPD 1.3.0a*;
- SSH servera programmatūra *OpenSSH 4.6*;
- SMTP servera programmatūra *qmail 1.03*;
- POP3 dēmons *popa3d*;
- DB servera programmatūra *MySQL 5.0.37*.

Šāda programmatūra izvēlēta primāri tāpēc, ka tā ir bez maksas. Otrkārt, izvēlēti industrijas līderi – tas ļaus, gadījumā, ja nespēšu kādu problēmu, kas radīsies ar uzstādīšanu vai ekspluatāciju, atrisināt saviem spēkiem, vieglāk palūgt un ātrāk saņemt palīdzību no citiem amata brāļiem.

Iespējams, ka *qmail* vietā varētu lietot *Postfix,* taču es neparedzu tik plašu e-pasta pakalpojuma izmantošanu, lai *Postfix* sarežģītība un smalkās konfigurācijas iespējas atmaksātos.

Uz servera jāuzstāda arī *phpMyAdmin 2.10.1*, lai lietotājiem un administratoriem atvieglotu darbu ar DB. Tas ir plaši izplatīts

Balsojumā visvairāk balsu ieguva servera nosaukums *RIEXC*, tāpēc jaunais serveris tā arī tiks dēvets.

3.1.5. Bezvadu tīkls

Bezvadu tīkls ir jāveido tāds, ka tajā drīkst pieslēgties tikai reģistrēti datori (to var panākt ar to pašu skriptu, kas nodrošinās tikai reģistrēto datoru pieslēgšanos visam datortīklam).

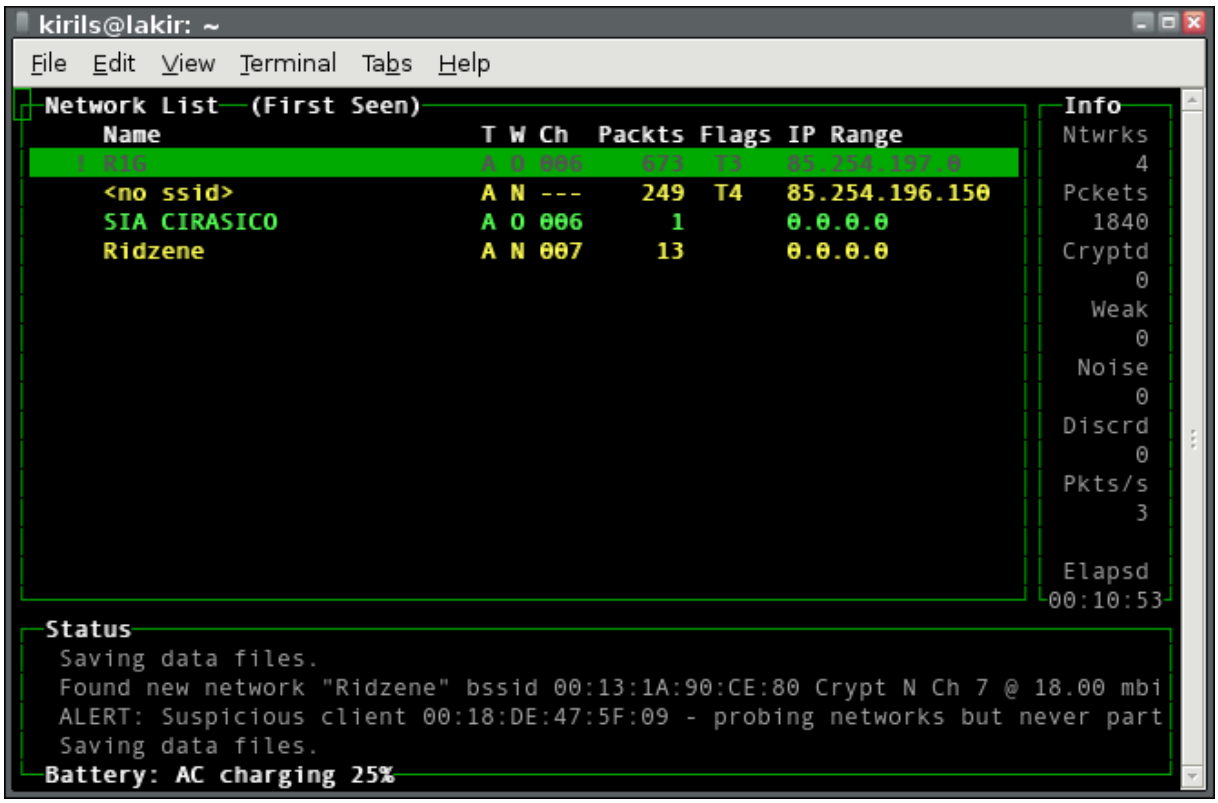
Apspriežoties ar potenciālajām lietotāju grupām, noskaidroju, ka bezvadu tīkls būtu ieviešams datorcentrā, aulā, 2. stāva vestibilā un kafejnīcā. Tam būtu nepieciešami 3 bezvadu pieejas punkti (aula un 2. stāva vestibils viegli nosedzami ar vienu).

Lai nodrošinātu, ka tīklam pieslēgties var tikai pilnvarotie lietotāji, nolēmu lietot WPA2 RADIUS autentifikāciju. Šim nolūkam uz maršrutētāja *WATERFALL* tiks uzstādīts RADIUS serveris, lai lietotājus varētu pārvaldīt centralizēti. WPA2 nodrošinās, ka bezvadu savienojums tiek gana droši šifrēts, lai mazinātu draudus informācijas konfidencialitātei.

Lai iegūtu pēc iespējas pielāgojamāku risinājumu, es nolēmu pasūtīt bezvadu maršrutētājus *Linksys WRT54GL*, kura sastāvā ietilpst 216 MHz procesors, 16 MiB operatīvā atmiņa un 4 MiB zibatmiņa(19), un iešūt tajā programmaparatūra *DD-WRT v23 SP2*. Šāds risinājums dos vislielāko labumu par viszemāko cenu. Lētākie bezvadu maršrutētāji, kas spēj strādāt kā parasti pieejas punkti (neveicot maršrutēšanu) un atbalsta RADIUS autentifikāciju maksā apmēram 3 reizes dārgāk.

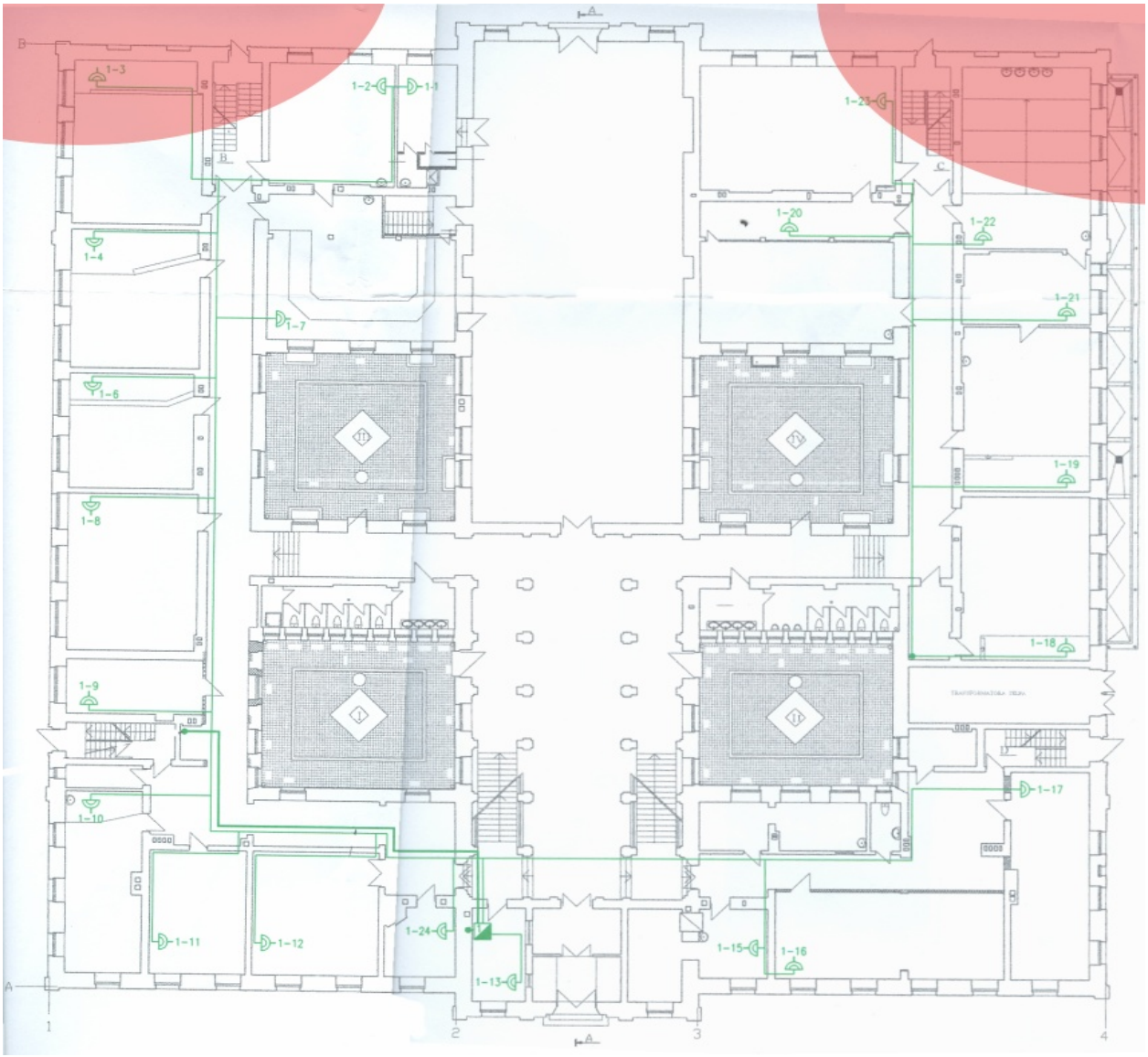
Ar mērķi noskaidrot, kādas frekvences ir izdevīgāk izmantot pieejas punktiem (tādā veidā, lai nepārklātos ar jau esošajiem), veicu Rīgas Valsts 1. ģimnāzijas apgaitu, izmantojot klēpjdatoru *HP Compaq nc6120* ar iebūvētu Intel PRO/Wireless 2915ABG tīkla karti un programmatūru *kismet*.

Noskaidroju, ka šobrīd aizņemti ir tikai 6. un 7. kanāls (skat. 3.1. att.).



3.1. att. **Programma *kismet* pēc visas ēkas apgaitas uzrāda divus citus tīklus ēkas teritorijā**

6. kanālu (2437 MHz) aizņem tīkls ar nosaukumu "SIA CIRACISO" un tas uztverams tikai ēkas labajā aizmugurējā spārnā, bet 7. kanālu (2442 MHz) aizņem tīkls ar nosaukumu "Ridzene" un tas uztverams tika ēkas kreisajā aizmugurējā spārnā(20). (skat. 3.2. att.)



3.2. att. **Eksistējošo 802.11b/g tīklu atrašanās vieta Rīgas Valsts 1. ģimnāzijas teritorijā**

Līdz ar to, es izvēlējos izvietot bezvadu pieejas punktus 1., 3. un 5. kanālā (attiecīgi 2412, 2422 un 2432 MHz).

Tālākā plānošana turpinājās izvēloties vajadzīgo jaudu. *Linksys WRT54GL* standarta antenu pastiprinājums ir 2.2 dBi(21).

Saistošie normatīvie akti un rekomendācijas nosaka, ka 2400-2483.5 MHz radiofrekvenču joslā izstarotā EIRP nedrīkst pārsniegt 100 mW(9, 10, 11).

Lai noskaidrotu kādu maksimālo raidītāja jaudu ir likumīgi uzstādīt šādā konfigurācijā, lietoju izteiksmi **EIRP = TPO + AG**(3), kur TPO (Transmmiter Power Output) ir radītāja jauda dBW un AG (Antenna Gain) ir antenas pastiprinājums dBi. Tā kā antenas pastiprinājums mums ir zināms (2.2 dBi) un maksimālais EIRP arī (100 mW), varam sarēķināt maksimālo TPO. Bet vispirms jāpārveido EIRP uz dBW. to var izdarīt ar vienkāršu formulu **1 dBW = 10 log(1 W)**.

AG = 100 mW = 0.1 W; 10 * log (0.1 W) = -10 dBW.

EIRP = TPO + AG => -10 dBW = TPO + 2.2 dBi => TPO = -12.2 dBW

Atliek pārveidot dBW atpakaļ uz W pēc formulas $1W = 10^{0.1* 1\ dBW}$

$10^{0.1* -12.2dBW} = 10^{-1.22dBW} = 0.060$ W = **60 mW**

Tātad, bezvadu pieejas punkti tiks uzstādīti norādītajās vietās ar TPO ne lielāku par 60 mW.

3.1.6. Sekundārais tīkls

Kā jau plānots, bezvadu maršrutētājam, kas atrodas sekundārajā tīklā "bez liekām ceremonijām" tiks atslēgta strāvas padeve.

Izpētot iespējas savienot 2. stāva servertelpu ar 3. stāva servertelpu, lai izveidotu savienojumu starp sekundāro tīklu un esošo tīklu, kas tiek aktīvi izmantots, secināju, ka šāds savienojums teorētiski ir iespējams. Nolēmu, ka iesākumā šis savienojums tiks izmantots, kā rezerves savienojums, gadījumam, ja pārtrauc darboties savienojums ar primāro IPS. Šim mērķim ir ar kabeli jāsavieno komutators *Cisco Catalyst 2950* un maršrutētājs *WATERFALL*, ievietojot tajā papildus tīkla karti, jo tas ir lētākais variants.

3.1.7. Brīvā izpēte

Jaunajam serverim *IBM @server xSeries 205* pielietojums ilgi nebija jāmeklē – to esmu ieplānojis kā rezerves kopiju serveri un nosaucis par *RR (*no *Re-RIEXC*), jo rezerves kopiju risinājums Rīgas Valsts 1. ģimnāzijas IS jau sen ir nepieciešams.

Eksperimentējot ar IPv6, piereģistrēju 6in4 tuneli vietnē sixxs.net. Izmantojot literatūru(4), iemācījos daudz jauna un pārbaudīju dažādas iespējamās konfigurācijas. Secināju, ka Rīgas Valsts 1. ģimnāzijas datortīklā IPv6 pagaidām nav pielietojams.

3.1.8. Datu rezerves kopēšana

Sākotnējā datu rezerves kopēšanas shēma attieksies tikai uz jauno serveri *RIEXC,* jo uz no servera *BETONS* nav iespējams nokopēt datus, neizmantojot IPX/SPX protokolu, bet mūsdienās tas reti tiek atbalstīts, un servera *IKARUSS* būtiskākais saturs tiks dublēts uz servera *RIEXC.*

Datu rezerves kopēšanas shēma būs šāda: katra mēneša 1., 3., 7., 11., 15., 21., 25., 27. un 31. (ja tāds ir) datumā tiek saglabāts mapju /etc, /root, /home, /www, /var/lib/mysql, /var/log un faila /quota.user saturs. Tiek izveidots arhīvs, kurš tiek caur tīklu noglabāts uz jaunā servera *IBM @server xSeries* 205 (kuru es nodēvēju par *RR*, no *Re-RIEXC).* Jaunākā arhīva kopija tiek saglabāta arī uz servera *RIEXC*, bet serveris *RR* uztur visas šī mēneša kopijas, trīs iepriekšējā mēneša (1., 11. un 21. datuma) un vēl iepriekšējo 11 mēnešu 1. datuma kopijas.

3.1.9. Surogātpasts

Aizsardzībai pret surogātpastu tiks izmantota bezmaksas programmatūra *SpamAssassin* kas automātiski dzēsis visu acīmredzamo surogātpastu, bet šaubīgās vēstules marķēs, mainot to tēmu. Šī programmatūra aizsargās e-pasta serveri *RIEXC* un atradīsies uz tā, jo tas ir vienīgais serveris, kas atbalsta SMTP protokolu (izņemot serveri *IKARUSS*). Programmatūra *SpamAssasin* izvēlēta, tāpēc ka tas ir populārs un kvalitatīvs bezmaksas risinājums.

3.1.10. Darbstaciju administrēšana

Apstaigājot Rīgas Valsts 1. ģimnāzijas IS, tika secināts, ka tīklā ir četras *Windows XP* darbstacijas bez 2. servisa pakas. Tām šī paka tiks uzlikta, jo lietotāji šobrīd nav gatavi pāriet uz vecāku *Windows* versiju vai alternatīvu OS (pēc lietotāju izvēles).

Lai cīnītos ar datoru pārinstalēšanas problēmu, ar programmas palīdzību tiks izveidots datoru klonēšanas disks, ko būs iespējams lietot, lai klonētu visas darbstacijas, kas nav principiāli atšķirīgas. Prātā nāk divas dažādas programmas, ar ko to iespējams izdarīt: *dd* un *Norton Ghost*. Tā kā *dd* kopēs visu disku vai partīciju, rezultējošais attēls būs liels un, lai tas ietilptu diskā vēl būs jāapstrādā ar kādu arhivēšanas programmu, kas bez īpaša kompresēšanas algoritma būs ilgi, tāpēc izvēlējos *Norton Ghost,* kas nav pārlieku dārgs risinājums(22), īpaši, ja tiek lietota kāda vecāka versija.

3.1.11. Lokālā tīkla ātrums

Lai uzlabotu lokālā tīkla ātrumu, 6 koncentratori, kas atrodas datorklasēs, tiks aizvietoti ar 4 komutatoriem (ar lielāku pieslēgumvietu skaitu). Ja rastos finansiāla iespēja aizvietot pārējos Rīgas Valsts 1. ģimnāzijas tīklā esošos koncentratorus, arī tas noteikti būtu jādara.

Izvērtējot cenu un kvalitātes attiecību, kā arī ņemot vērā *Linksys* reputāciju, nolēmu iegādāties *Linksys* komutatorus, lai arī izpētīju dārgākos *Cisco* modeļus. Tā kā ir nepieciešami divi komutatori ar 8 pieslēgumvietām un divi – ar 16, kuru izmēri nedrīkstētu būt pārāk lieli, jo tie novietojami datorklasēs, tad derīgi šķita šādi modeļi:

a) *EZXS88W* un *EZXS16W*

b) *SD208* un *SD216*

Mana izvēle krita uz b variantu, jo komutatoriem ir metāla korpuss, kam vajadzētu nodrošināt izturību, un tie ir ļoti kompakti, kā arī atsauksmes dažādās tīmekļa lapās saka, ka to ātrums pie lielas slodzes ir nedaudz lielāks.

Tiks arī pārvilkti datortīkla kabeļi datorklasē D1. Kabeļi atrodas virsapmetuma tuneļos, kas piestiprināti pie sienas. Šie tuneļi ir viegli atverami un tajos esošie vadi – nomaināmi.

Lai pārbaudītu, vai pieņēmums par to, ka lokālā tīkla darbību, iespējams, ietekmē arī neatbilstība starp tīkla iekārtu automātisko ātrumu saskaņošanu, tika veikta tīkla iekārtu apsekošana un konstatēts, ka 4 darbstacijām tīkla karte manuāli iestatīta uz pilnu dupleksu. Šīs kartes tiks pārstatītas uz automātisko ātrumu saskaņošanu.

3.1.12. UPS iegāde

Tā kā Rīgas Valsts 1. ģimnāzijas IS shēma šī darba rezultātā mainās, tad es pieņēmu lēmum, ka nefunkcionējošā *APC Back-UPS 300VA* vietā tiks iegādāti divi nedārgi UPS – *Mustek PowerMust 600VA*, kuri tiks izvietoti tā, lai nodrošinātu nepārtrauktu barošanu maršrutētājam *WATERFALL* un visiem serveriem. Šobrīd šis ir lētākais UPS, kas ir pieejams un, lai arī viennozīmīgi būtu nepieciešams labāks risinājums, tam nav pieejams attiecīgā apjoma finansējums.

3.1.13. Administrēšanas atvieglošana

Plānojot šo darbu, es apzināju, kurā telpā un vietā atrodas kurš stacionārais dators un tagad no tā izveidošu elektronisku datubāzi. Datu bāzei es izstrādāšu tīmekļa saskarni.

Vārdu serveris tiks pārnests uz maršrutētāju *WATERFALL,* kā rezultātā es varēšu veikt izmaiņas domēnu vārdos, kas pieder Rīgas Valsts 1. ģimnāzijai. Tiks arī pieprasīts, lai IPS deleģē man tiesības veidot atgriezeniskos ierakstus IP adresēm un šādi ieraksti tiks izveidoti visām lietotāju darbstacijām un lielākajai daļai tīkla iekārtu. Lietotāju darbstaciju nosaukumi būs konsekventa garuma un ne garāki kā 5 simboli.

Tiks izstrādāta tīmekļa saskarnes pārvaldība maršrutētājam *WATERFALL,* kas pamatā domāta, lai administrētu *squid* dēmonu, kā arī pieslēgtu vai atslēgtu Internetu konkrētā datorklasē.

3.1.14. Servera *BETONS* diska atjaunošana

Tiklīdz par šo uzzināju, tā, protams, uzreiz vajadzēja "ķerties vērsim pie ragiem". Nebija daudz laika plānot – SCSI disks tika pieslēgts pie kontroliera un tā attēls veiksmīgi nokopēts, izmantojot programmu *dd* (tas tika darīts, lai cilvēka kļūdas gadījumā nesabojātu diskā esošo informāciju vēl vairāk). Pēc šādas veiksmīgas kopijas izveidošanas, radās ideja izmantot šo pašu programmu *dd, "*iepūst dzīvību citā diskā". Tā kā *BETONS* ir mācību un metodiskā darba failu serveris, tas nedrīkst ilgi nebūt pieejams. Tāpēc tika paņemts jebkāds disku, kas bija pa rokai – tas gadījās 10GB liels IDE PATA disks, kurā tika iekopēts oriģinālā diska saturs.

3.1.15. Informātikas ieskaite

Nedēļu pirms Rīgas Valsts 1. ģimnāzijā bija jānotiek informātikas ieskaitei, informātikas skolotāji man lūdza, vai nevaru atvieglot darbu savākšanu no datoriem, jo šogad ieskaite notikšot 4 daļās, no kurām 3 būšot pildāmas pie datora. Rīgas Valsts 1. ģimnāzijā šo ieskaiti kārto apmēram 200 skolēnu. Kopā tas ir 600 darbu.

Tāpēc ir nepieciešams izveidot nelielu skriptu, kas automātiski vai pusautomātiski savāks katru darbu no datora un novietos to uz servera, kur to vēlāk būs iespējams novērtēt skolotājam.

3.2. Ieviešana

Pirms risinājumu ieviešanas dzīvē, tie vēl jāsakārto loģiskā secībā (piemēram, ja vien nevēlos serveri *IKARUSS* permanenti atslēgt no Interneta, tad steidzami vajadzētu ieviest labu ugunsmūri un pēc tam nobloķēt visus nedrošos servera *IKARUSS* pakalpojumus), bet kad secība skaidra – jāsāk darbs pie konkrētu risinājumu ieviešanas.

3.2.1. Maršrutētājs ar ugunsmūri (*ROUTER* aizvietošana ar *WATERFALL)*

Tā kā gandrīz neviens no plānotajiem uzlabojumiem nav saderīgi ar esošo mātesplati, tiek mainīta visa iekārta. Jaunā korpusā tiek salikts kopā dators ar 435 MHz procesoru, 320 MiB operatīvo atmiņu un 13 GB cieto disku. Tā kā jaunā mātesplate atbalsta PCI, ne tikai ISA, paveras iespēja 10BASE-T tīkla karšu vietā uzstādīt 100BASE-TX tīkla kartes. Tā arī tiek darīts – tiek uzstādītas divas tīkla kartes *RealTek RTL8139* (PCI, 100BASE-TX, draiveris *8139too*) un viena tīkla karte *3Com PCI 3c905 Boomerang* (PCI, 100BASE-TX, draiveris *3c59x*).

Radiokarte tiek uzlabota no 2 Mbps uz 11 Mbps, kas ir maksimālais 802.11b standarta pieļaujamais ātrums. Tiek uzstādīta karte *Aironet ISA4800 11Mbps ISA adapter* (ISA, 11 Mbps, 802.11b, draiveris *airo*).

Kad maršrutētājs salikts, izmantojot no Interneta lejupielādētu *Slackware 11.1 Linux 2.4.33.3* diska attēlu, kas ierakstīts kompaktdiskā, tas tiek uzinstalēts, atjaunināts uz *Slackware-current Linux 2.6.21.1*. Šis process sīkāk ir aprakstīts nodaļā "Iekārtu *WATERFALL* un *RIEXC* programmatūras atjaunināšana".

Tālāk notiek darbs pie maršrutētāja konfigurācijas. Šobrīd par Interneta nodrošināšanu vēl atbild vecais maršrutētājs *ROUTER,* no kura aizņemos dažus konfigurācijas aspektus.

Izmantojot komandu *modinfo airo* tiek noskaidroti draivera iespējamie parametri un pārbaudot dažādus *io=* un *irq=* parametrus, tiek iegūta strādājoša kombinācija *irq=5 io=0x300*. Lai tīkla kartes darbotos katru reizi ieslēdzot maršrutētāju, failā */etc/rc.d/rc.netdevice* tiek ierakstīts:

```
/sbin/modprobe airo irq=5 io=0x300
iwconfig eth0 essid ISPname nick myname ap 00:0C:30:24:10:42
/sbin/modprobe 8139too
/sbin/modprobe 3c59x
/sbin/insmod -o isp2 8139too
```

Rinda, kas sākas ar *iwconfig,* norāda, ka *Aironet* tīkla kartei jāpieslēdzas bezvadu tīklam "ISPname", sevi nosaucot "myname" un pieslēdzoties tieši pieejas punktam ar MAC adresi 00:0C:30:24:10:42 un nekam citam. Pēdējā rinda vēlreiz ielādē draiveri *8139too*, bet nu jau priekš otrās tīkla kartes; tā kā draiveriem nedrīkst būt vienādi nosaukumi, tiek izmantota komanda *insmod -o cits_nosaukums draiveris*. Vēlāk, kad tīkla kartēm tiks pievienoti vadi, tiks empīriski noteikts, kura no *RTL8139* kartēm ir *eth1,* bet kura *eth3*.

Tālāk tiek nokonfigurēta IP adresācija, ierakstot failā */etc/rc.d/rc.inet1* šādas rindas:

```
#! /bin/sh

if [ "$1" == "stop" ]; then
```

```
 return 2> /dev/null
 exit
fi

ifconfig lo 127.0.0.1
route add -net 127.0.0.0 netmask 255.0.0.0 lo

ifconfig eth0 192.168.19.15 netmask 255.255.255.224
ifconfig eth0:0 85.254.197.1 netmask 255.255.255.255
ifconfig eth0:1 85.254.196.129 netmask 255.255.255.255
ifconfig eth0:2 85.254.196.130 netmask 255.255.255.255
ifconfig eth0:3 85.254.197.3 netmask 255.255.255.255

ifconfig eth1 85.254.196.129 netmask 255.255.255.224
ifconfig eth1:1 85.254.196.130 netmask 255.255.255.224

ifconfig eth2 85.254.197.1 netmask 255.255.255.0
ifconfig eth2:1 85.254.197.3 netmask 255.255.255.0

#ifconfig eth3 213.175.126.20 netmask 255.255.255.0

route add default gw 192.168.19.34 eth0:0
```

Tīkla kartes, kas savienota ar antenu, saskarne tiek konfigurēta četrām IP adresēm, serveriem iedalu apakštīklu 85.254.196.128/27 un maršrutētājam piešķiru adreses 85.254.196.129 un 85.254.196.130, bet darbstacijām iedalu apakštīklu 85.254.197.0/24, maršrutētājam piešķirot adreses 85.254.197.1 un 85.254.197.3. Uz katras saskarnes maršrutētājam tiek piešķirtas divas IP adreses – viena, caur kuru tiks maršrutētas paketes, bet otra, uz kuras atradīsies starpniekserveris *squid.* Uz ārējā tīkla saskarnes ir visas šīs 4 adreses (lai gan ārtīklā, gan iekštīklā iekārta būtu sasniedzama ar vienādām IP adresēm un nebūtu jāievieš "split DNS") un viena adrese, kas atrodas IPS noteiktajā apakštīklā. Adrese 213.175.126.20 tiek piešķirta pēdējai saskarnei (rindiņas sākumā ir simbols "#", kas nozīmē, ka tā netiek izpildīta). Fails beidzas ar rindu, kas nosaka, ka visas paketes, kuras nevar maršrutēt savādāk (pa tiešo), jāmaršrutē caur nākamo maršrutētāju 192.168.19.34.

Tālāk tiek konfigurēti pakalpojumi. *OpenSSH* konfigurācijā tiek veiktas izmaiņas, kas neļauj pieslēgties serverim savādāk kā vien izmantojot 2. protokola versiju, tiek nokonfigurēts *MySQL,* pielāgojot atvēlētās atmiņas apjomu paredzamajai situācijai un ierakstot konfigurācijas failā "skip-bdb " un "skip-innodb", kas atļaus ietaupīt vietu uz diska, jo šie datu bāzes dziņi netiks izmantoti . Pieslēdzos *MySQL* serverim un uzstādu administratora paroli, jo konts šobrīd vēl ir bez tās.

Pienākusi kārta konfigurēt domēnu vārdu serveri. Tas ir *BIND 9.3.4.* Konfigurācijas failu */etc/named.conf* aizpildu ar sekojošo:

```
options {
        directory "/var/named";
        pid-file "named.pid";
        allow-recursion {85.254.197.0/24; 85.254.196.128/27; };
        allow-query { 85.254.197.0/24; 85.254.196.128/27; };
```

```
        allow-transfer { 159.148.108.0/24; 89.248.84.150; };
        allow-notify { 85.254.196.130; };
        notify-source 85.254.196.130;
        transfer-source 85.254.196.130;
        version "standart";
};

logging {
        channel def {
                file "/var/log/named.log";
                severity info;
                print-time yes;
                print-severity yes;
        };
        channel err {
                file "/var/log/named-error.log";
                severity error;
                print-time yes;
        };
        category lame-servers { null; };
        category default { def; err; };
        category queries { err; };
};

zone "r1g.edu.lv.196.254.85.in-addr.arpa" IN {
        type master;
        file "pri/85.254.196.ptr.zone";
        allow-query { any; };
        allow-update { none; };
};

zone "197.254.85.in-addr.arpa" IN {
        type master;
        file "pri/85.254.197.ptr.zone";
        allow-query { any; };
        allow-update { none; };
};

zone "r1g.edu.lv" IN {
        type master;
        file "pri/r1g.edu.lv.zone";
        allow-query { any; };
        allow-update { none; };
};
```

Manis administrētajam domēnu vārdu serverim būs sekundārie serveri, kā to prasa pieņemtie Interneta standarti(12). Šie serveri būs 159.148.108.2 un 89.248.84.150, tāpēc ievietoju failā rindu, kas sākas ar *allow-transfer.* Rinda *allow-query* atļauj izmantot šo vārdu serveri tikai Rīgas Valsts 1. ģimnāzijas IP adresēm, bet rindas *allow-query* katras zonas definīcijā norāda, ka par šo zonu drīkst prasīt visi, jo kur gan citur, tad šo informāciju viņi varētu iegūt!

Šeit ir **neliels sākuma fragments** no faila */var/named/pri/85.254.197.ptr.zone*:

```
$TTL 1W
@                       IN SOA  ns.r1g.edu.lv. root.ps.id.lv. (
                                2007041002 ; serial
                                1D         ; refresh
                                15M        ; retry
                                1W         ; expire
                                1D         ; minimum
```

```
                                )

    IN NS   ns.r1g.edu.lv.
    IN NS   nsz2.latnet.lv.
    IN NS   ns.02.lv.


1                       PTR     router.r1g.edu.lv.
3                       PTR     proxy.r1g.edu.lv.
                        PTR     waterfall.r1g.edu.lv.

100  PTR  add.r1g.edu.lv.
101  PTR  age.r1g.edu.lv.
102  PTR  aid.r1g.edu.lv.
103  PTR  aim.r1g.edu.lv.
104  PTR  air.r1g.edu.lv.
105  PTR  ale.r1g.edu.lv.
106  PTR  all.r1g.edu.lv.
107  PTR  and.r1g.edu.lv.
108  PTR  ant.r1g.edu.lv.
109  PTR  any.r1g.edu.lv.
110  PTR  apt.r1g.edu.lv.
111  PTR  art.r1g.edu.lv.
```

Darbstaciju nosaukumi, kā plānots ir konsekventa garuma. Fails sākas ar SOA (Start of Authority) ierakstu, kas norāda zonas tehnisko informāciju, tam seko vārdu serveru nosaukumi un tad paši zonas ieraksti. Jāpievērš uzmanība, lai neizmirstu punktu pēc domēnu vārdiem. Pretējā gadījumā *BIND* to neuzskata par FQDN (Fully Qualified Domain Name) un automātiski pievieno galā zonas nosaukumu.

Turpinu ar DHCP konfigurāciju, sastādot failu */etc/dhcpd.conf* šādi:

```
subnet 85.254.197.0 netmask 255.255.255.0 {
range 85.254.197.100 85.254.197.249;
 option domain-name "r1g.edu.lv";
 option domain-name-servers 85.254.196.130, 159.148.60.2, 159.148.60.20;
 option routers 85.254.197.1;
 default-lease-time 8640000;
 max-lease-time 8640000;
}

ddns-update-style none;
```

Tālāk ķeros pie *Apache* un *PHP* konfigurācijas. Šie pakalpojumi uz maršrutētāja vajadzīgi, lai varētu nodrošināt administrēšanu caur tīmekļa saskarni. Nokonfigurēju *Apache* uz nestandarta porta, izmantojot *Listen* direktīvu. Pārliecinos, ka tai nav administratora privilēģiju, bet gan *nobody:nogroup* privilēģijas. Tad nokonfigurēju HTTPS un izveidoju pašparakstītu SSL sertifikātu(23).

```
root@waterfall:/etc/httpd/ssl# openssl genrsa -des3 -out ca.key 4096
root@waterfall:/etc/httpd/ssl# openssl req -new -x509 -days 365 -key ca.key -out ca.crt
root@waterfall:/etc/httpd/ssl# openssl genrsa -des3 -out server.key 4096
root@waterfall:/etc/httpd/ssl# openssl req -new -key server.key -out server.csr
root@waterfall:/etc/httpd/ssl# openssl x509 -req -days 365 -in server.csr -CA ca.crt
-CAkey ca.key -set_serial 01 -out server.crt
root@waterfall:/etc/httpd/ssl# openssl rsa -in server.key -out server2.key
```

Augstākminētajā fragmentā komandu izvads ir izlaists. Pirmā rinda izveido CA (sertifikātu autoritātes) atslēgtu, otrā rinda – sertifikātu. Trešā rinda izveidot servera atslēgu, nākamā – CSR (sertifikāta parakstīšanas pieprasījumu) –, ko piektajā rindā paraksta CA, veidojot servera sertifikātu. Pēdējā rinda izveido servera atslēgu, kas nav aizsargāta ar paroli. Tas nepieciešams, lai *Apache* varētu pārstartēt un palaist, neievadot paroli katru reizi. Jāpiezīmē, ka ir jābūt ļoti uzmanīgam, lai pārbaudītu, vai šiem failiem nevar piekļūt neviens cits kā vien administrators, jo ar to palīdzību iespējams atšifrēt SSL savienojumus.

Tā kā *Slackware Linux* nepiedāvā programmatūru *squid* un RADIUS serveri, tad nokopēju to no tīmekļa vietnēm www.squid-cache.org un www.freeradius.org attiecīgi.

Kā vienu tā otru uzinstalēt ir samēra vienkārši, izmantojot pamācības, kas nāk līdzi.

```
./configure
make
make install
```

Tālāk ķeros pie pakalpojumu konfigurēšanas. Lai panāktu, ka FreeRADIUS strādās ar MS-CHAPv2 un spēs uzglabāt datus MySQL datubāzē noņemu komentārus no vajadzīgajām rindām *radiusd.conf* konfigurācijas failā (*sql, pap,* utt.). Izveidoju SSL sertifikātus līdzīgi kā to darīju iepriekš un norādu uz tiem no faila *eap.conf,* kurā arī veicu nelielas izmaiņas.

Lai *radiusd* nestrādātu ar administratora privilēģijām, izveidoju lietotāju "radius", pārliecinoties, ka tam nav uzstādīta parole (taču nav arī tukša) un čaula, lai lietotājs nevarētu pieteikties sistēmā un norādu šo lietotāju iekš *radiusd.conf*. Izveidoju arī tādu pašu *MySQL* lietotāju un datubāzi ar tādu nosaukumu. To visu (arī *MySQL* lietotāja paroli) ierakstu *sql.conf*. Tad izveidoju datubāzes struktūru, izmantojot failu /doc/examples/mysql.sql.

Pārliecinos, ka visi pakalpojumi startējas, un ķeros pie ugunsmūra *iptables* un *squid* konfigurācijas izstrādes. Tā kā tiem abiem ir jāmāk dinamiski atjaunināt Latvijas IP adrešu sarakstu, sākumā jāatrisina problēma ar sarakstu un tad jāturpina skatīties uz abiem kopskatā.

Par pamatu ņemot http://www.nic.lv/local.net, izveidoju korektu sarakstu http://net.02.lv/lvnet, kas visiem ir publiski pieejams, un izmantošu to skriptu rakstīšanā. Šeit iekļauju arī servera *IKARUSS,* komutatora *3Com 3C16985B* pieejas ierobežošanu un iespēju atslēgt Internetu datorklasēs. Tā kā risinājums ir apjomīgs, izvietoju to pielikumā nr. 5 "*WATEFALL* skripti". Starpniekservera *squid* konfigurācijas darbs sastāvēja no failu *squid.conf.pre* un *squid.conf.post* sastādīšanas, kā arī pielāgotu lietotāju kļūdu paziņojumu izstrādes.

Kad pārbaudu, ka visi pakalpojumi veiksmīgi palaižas, vecais maršrutētājs *ROUTER* tiek atslēgts no tīkla un novietots nomalē, lai no tā varētu smelties padomu, gadījumā, ja rodas kāda aizķeršanās jaunā maršrutētāja darbībā.

3.2.2. Pārvaldāmais komutatora drošība

Nomainu komutatora *3Com 3C16985B* administratīvos autentifikācijas parametrus.

3.2.3. Servera *IKARUSS* aizvietošana ar *RIEXC* un *RR.*

Tā kā serveris *IKARUSS* nu spēj tikai pieņemt e-pastus, izveidoju serveri RIEXC. Instalācija un konfigurācija notiek analoģiski maršrutētājam *WATERFALL,* vien instalācijas gaitā neizvēloties dažus un izvēloties citus pakalpojumus – *Samba, ProFTPD, popa3d,* un vēlāk uzliekot un konfigurējot *qmail* un *phpMyAdmin.*

(Servera RR konfigurācija notiek analoģiski WATERFALL, bet izlaižot lielāko daļu pakalpojumu.)

Sambas konfigurēšana notiek ļoti vienkārši. Te ir **sākuma fragments** no faila */etc/samba/smb.conf*:

```
[global]
        workgroup = RIEXC
        server string = Jaunais RIEXC
        netbios name = rieksts
        bind interfaces only = Yes
        encrypt passwords = Yes
        log level = 1
        log file = /var/log/samba.log
        name resolve order = lmhosts host bcast
        getwd cache = No
        socket options = TCP_NODELAY IPTOS_LOWDELAY
        logon script = login.bat
        domain logons = Yes
        os level = 64
        preferred master = False
        domain master = True
        dns proxy = No
        wins support = Yes
        hosts allow = 127.0.0.1 85.254.197.0/255.255.255.0
85.254.196.128/255.255.255.244
        follow symlinks = no

[netlogon]
        comment = Network Logon Service
        path = /samba/netlogon
        read only = Yes
        browseable = No

[home]
        comment = Home Directory
        path = /home/%u
        writeable = Yes
```

Lai atvieglotu lietotājiem dzīvi tiek izveidots fails login.bat, kas uz OS *Windows* piesaistīs viņu mapes disku nosaukumiem:

```
@echo off
net use h: \\rieksts\home>nul
net use p: \\rieksts\public>nul
net use w: \\rieksts\web>nul
```

ProfFTP tiek nokonfigurēts tā, lai tas neaizņemtu pārāk daudz vietas atmiņā un būtu maksimāli drošs, cik nu FTP serveris var būt drošs.

DB pārvaldes rīka *phpMyAdmin* uzstādīšana ir vienkārša. To uzstāda, atarhivējot un izveidojot *config.inc.php* failu:

```
<?
 $cfg['PmaAbsoluteUri'] = 'https://admin.r1g.edu.lv/phpMyAdmin/';
 $cfg['Servers'][1]['controluser']   = 'neiistais lietotaajs';
 $cfg['Servers'][1]['controlpass']   = 'shi nav iistaa parole';
 $cfg['Servers'][1]['auth_type']     = 'http';
 $cfg['Servers'][1]['user']          = '';
 $cfg['Servers'][1]['verbose']       = 'RIEXC';
 $cfg['Servers'][1]['pmadb']         = 'pma';
 $cfg['Servers'][1]['bookmarktable'] = 'bookmark';
 $cfg['Servers'][1]['relation']      = 'relation';
 $cfg['Servers'][1]['table_info']    = 'table_info';
 $cfg['Servers'][1]['table_coords']  = 'table_coords';
 $cfg['Servers'][1]['pdf_pages']     = 'pdf_pages';
 $cfg['Servers'][1]['column_info']   = 'column_info';
 $cfg['Servers'][1]['history']       = 'history';
 $cfg['ShowChgPassword']       = TRUE;  // simple users or not
 $cfg['MaxRows']               = 80;
 $cfg['InsertRows']            = 1;
 $cfg['DefaultLang'] = 'lv-utf-8';
 $cfg['RepeatCells']         = 0;
?>
```

Atliek uzstādīt *qmail.* Šim mērķim sākumā izveidoju lietotājus “alias” , “qmaild ”, “qmaill ”, “qmailp” , “qmailq” , “qmailr” un “qmails” , lai dēmoni nestrādā ar administratora atļaujām un tad, sekojot instalācijas instrukcijām, izpildu:

```
root@riexc:~/setup/soft/qmail-1.03# mkdir /var/qmail
root@riexc:~/setup/soft/qmail-1.03# make setup check
root@riexc:~/setup/soft/qmail-1.03# ./config
root@riexc:~/setup/soft/qmail-1.03# (cd ~alias; touch .qmail-postmaster .qmail-mailer-
daemon .qmail-root)
root@riexc:~/setup/soft/qmail-1.03# chmod 644 ~alias/.qmail*
```

Komandu izvads izlaists, jo ir neatbilstoši garš.

Lai lietotāji neaizņemtu visu vietu, kas pieejama uz servera, es ieviesu kvotu sistēmu. Katram lietotājam normāli ir pieejami 50 MiB vietas. Ieviešana bija elemetāra – failu */etc/fstab* vajadzēja papildināt ar tekstu “usrquota” pie tām failu sistēmām, kurām vajag iespējot kvotu. Viena no faila */etc/fstab* rindiņām tagad izskatās šādi:

```
/dev/hda1       /               ext2        defaults,usrquota         1   1
```

Pēc noklusējuma lietotājiem kvota nav uzstādīta un tie var aizņemt cik vietas vien vēlas. Lai uzstādītu lietotāja kvotu var lietot komandu *edquota* vai *setquota.* Piemēram:

```
root@riexc:~# setquota kirils 51200 60000 1024 2048
```

Šī komanda uzstāda lietotāja "kirils" maksimāli izveidojamo failu skaitu uz 1024 un atvēlēto vietu uz 50 MiB. Taču šo kvotu ir pārsniegt (ne ilgāk kā uz nedēļu) līdz 2048 failiem un 58.5 MiB. Ja kvota ir pārsniegta ilgāk par nedēļu, jaunu rakstīšana failos tiek aizliegta.

3.2.4. Iekārtu WATERFALL un RIEXC programmatūras atjaunināšana

Lai atjauninātu programmatūru uz jaunāku, nokopēju Slackware-current failus no ftp://ftp.linux.edu.lv/mirrors/ftp.slackware.com/slackware-current/slackware/ uz katras iekārtas (servera *RIEXC* un maršrutētāja *RR*). Tālāk uzmanīgi izpētiju nepieciešamo darbību secību(24) un tad, izmantojot *installpkg,* uzinstalēju jaunāko kodolu ar moduļiem (arī draiveriem), pārrakstīju diska ielādes sektoru, palaižot LILO. Pārbaudot, kodols funkcionē, noņēmu veco (izmantojot *removepkg*) un iegāju 1. sistēmas līmenī (runlevel 1), pazīstamā arī kā viena lietotāja režīms. Tad ar komandas *upgradepkg* palīdzību uzinstalēju jaunākos *solibs (*shared object libraries), *pkgtools, sed* un *aaa_base.* Tālāk veicu *expat* instalāciju, rakstot:

```
root@riexc:~/slackware/l1# upgradepkg –install-new expat
```

Atlika vien uzinstalēt visu paku jaunākās versijas, izmantojot to pašu *upgradepkg,* un pievērst pastiprinātu uzmanību pakām, kurām mainījušies nosaukumi(25):

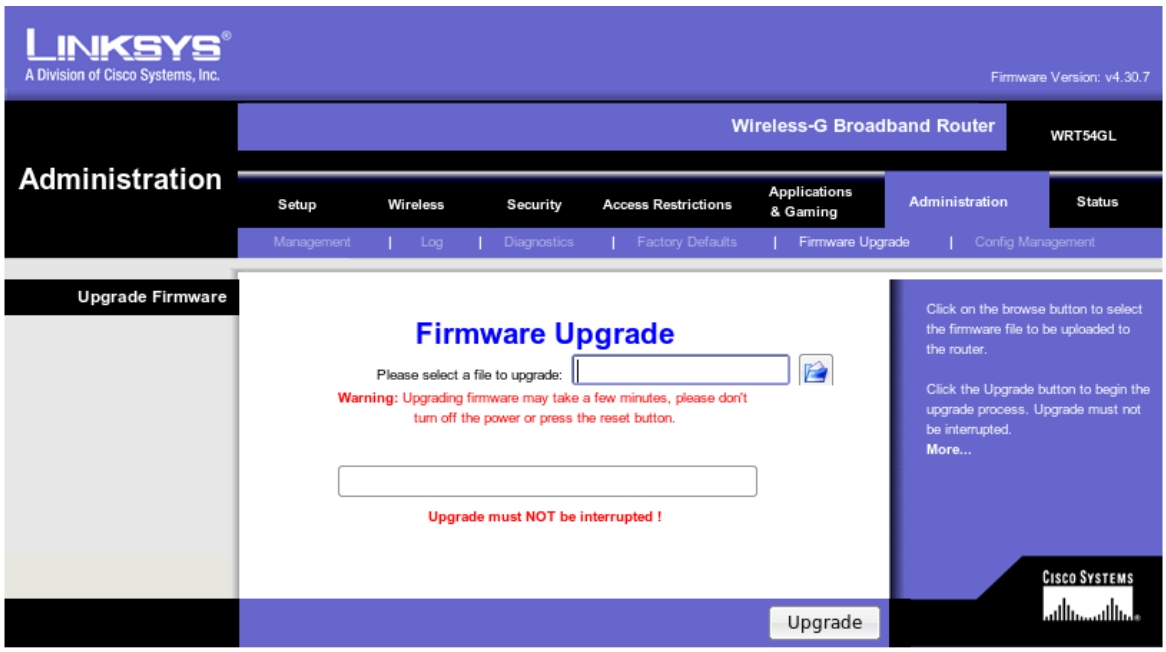
```
root@riexc:~/slackware/a# upgradepkg modutils%module-init-tools
root@riexc:~/slackware/n# upgradepkg apache%httpd
```

un kuras nākušas klāt kā svarīgas sistēmas pakotnes. Otrās es uzinstlāju ar komandu *upgradepkg -install-new*, pārliecinoties, ka viss joprojām strādā.

Pēc instalācijas pabeigšanas, protams, pārlādēju iekārtu, lai nokļūtu atpakaļ daudzu lietotāju režīmā.

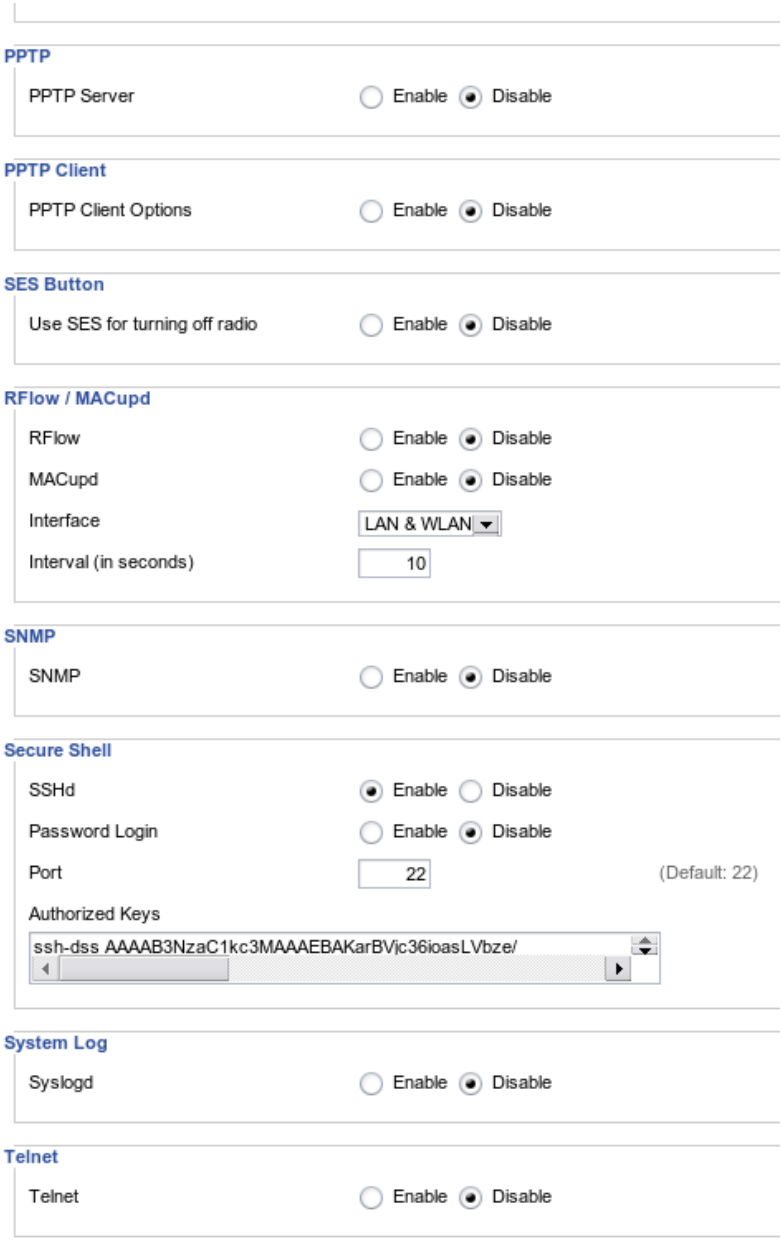
3.2.5. Bezvadu tīkls

Bezvadu tīkla ieviešanu sāku, iegūstot *DD-WRT v23 SP2* attēla failu *dd-wrt.v23_generic.bin*(19) no tīmekļa vietnes *www.dd-wrt.com*. Tad to ielādēju maršrutētājos *Linksys WRT54GL*, izmantojot tīmekļa saskarni (skat. 3.3. att.)



3.3. att. Linksys programmaparatūras aizvietošana ar DD-WRT.

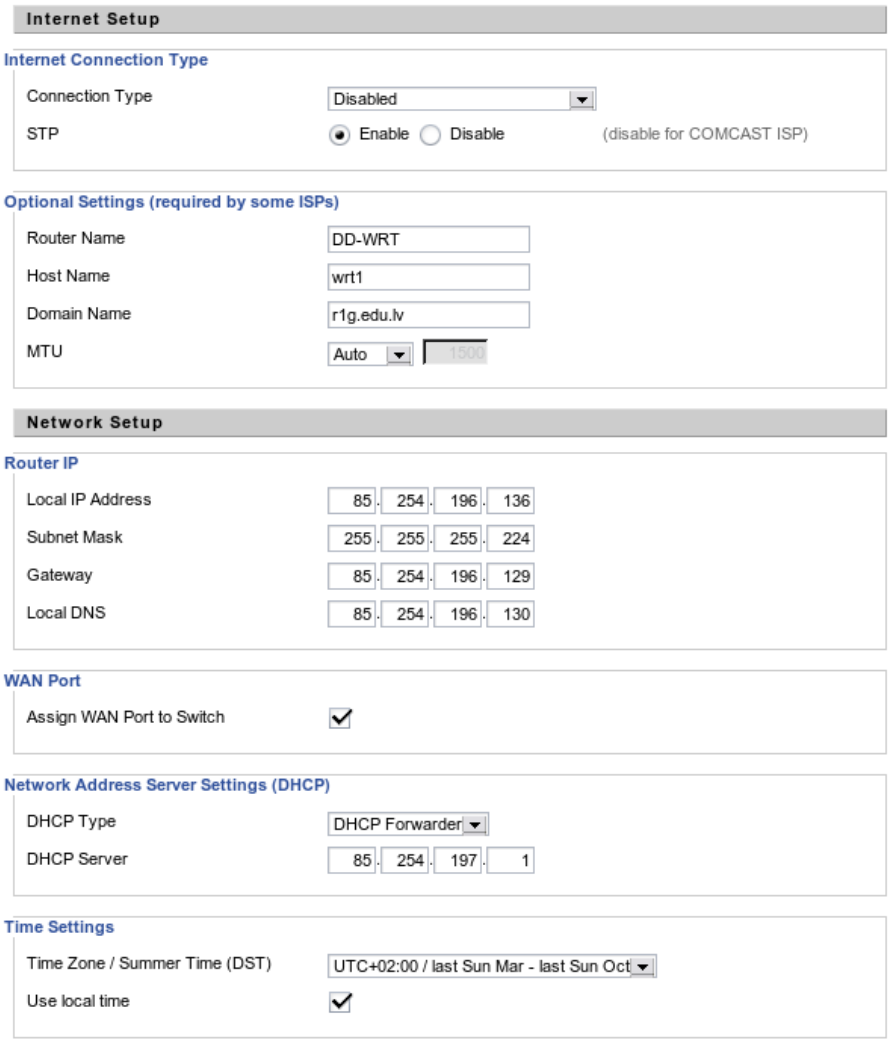
Veicu iekārtas konfigurēšanu, atslēdzot lielāko daļu tās pakalpojumu (skat. 3.4. att.), bet atstājot SSH un HTTP, HTTPS administrēšanas nolūkiem un NTP klientu laika sinhronizācijas nolūkiem. HTTP biju spiests atstāt, jo caur HTTPS nav iespējams izveidot konfigurācijas uzstādījumu rezerves kopiju, kas man būs vajadzīga vēlāk.



3.4. att. ***DD-WRT*** **pakalpojumu konfigurācijas logs**

NTP nokonfigurēju uz serveri ntp.latnet.lv un SSH atslēdzu iespēju pieteikties sistēmā ar paroli, taču iekopēju savu publisko SSH atslēgu.

Lai WRT54GL, kas pēc savas būtības ir bezvadu **maršrutētājs,** darbotos kā vienkāršs bezvadu pieejas punkts, uzstādīju tā Interneta savienojuma veidu uz "atslēgts". Turpināju ar to, ka uzstādīju laika joslu, bezvadu pieejas punkta vārdu, IP uzstādījumu konfigurāciju. Liku tam padot visus DHCP pieprasījumus tālāk uz DHCP serveri, ko uzstādīju uz maršrutētāja WATERFALL. (skat 3.5. att.)



3.5. att. ***DD-WRT*** **laika zonas un IP uzstādījumu konfigurācijas logs**

Šo konfigurēšanas fāzi pabeidzu ar to, ka iestatīju tīkla nosaukumu – "r1g" –, raidīšanas kanālu – 1, ieslēdzu tīkla nosaukuma apraides režīmu, uzstādīju, lai bezvadu tīkls automātiski izslēdzas laikā no plkst. 23.00 līdz plkst. 05.00, pacēlu raidīšanas jaudu uz 60 mW un nokonfigurēju maršrutētāju darbam WPA2 režīmā, izmantojot AES algoritmu, autentificējot lietotājus pret RADIUS serveri *WATERFALL*. Kā bezvadu maršrutētāja, tā maršrutētājā *WATEFALL* ievadīju kopējo atslēgu, ar ko šifrēt RAIDUS saziņu starp abiem maršrutētājiem.

Pirmais bezvadu pieejas punkts bija pabeigts. Izveidoju konfigurācijas rezerves kopiju un ielādēju to pārējos divos bezvadu pieejas punktos. Atlika nomainīt IP uzstādījumu konfigurāciju un raidīšanas kanālu (vienā kanālā esoši pieejas punkti, arī ja kopā veido vienu tīklu, traucēs viens otram).

3.2.6. Sekundārais tīkls

Maršrutētāju *Linksys WRT54GS* atslēdzu, taču drīzumā saņēmu zvanu ar lūgumu pievienot to atpakaļ. Sākumā nespējām vienoties par kompromisu, jo katrs pastāvēja uz sava: IPS vēlējās, lai maršrutētājs tur paliek, taču es, rūpējoties par tīkla drošību un caurspīdīgumu, pret to iebildu.

Galu galā vienojāmies par pagaidu risinājumu. Noņēmu bezvadu maršrutētāja antenas, samazinot tā potenciālo darbības rādiusu. Lai gan IPS solīja drīzumā nomainīt maršrutētāju ar kādu ierīci, kam nav bezvadu iespējas, tas joprojām nav izdarīts.

Lai nodrošinātu sekundārā tīkla savienošanu ar esošo datortīklu, biju nolēmis savienot komutatoru *Cisco Catalyst 2950* un maršrutētāju *WATERFALL*, ievietojot tajā papildus tīkla karti. Tā kā urbt stāvvadu starp Rīgas Valsts 1. ģimnāzijas ēkās stāviem man nav tiesību, nolēmu izmantot kādu no esošajiem slēgumiem, kas savieno 2. stāva servertelpu ar 3. stāva servertelpu. Man par lielu izbrīnu, lai gan ar vadu viss ir kārtība, saklausīt jebkāda veida aktivitāti, izmantojot zema līmeņa oskšķerus, šajā tīkla neizdodas. Esmu izmēģinājis arī aktīvo metodi, izsūtot Zeroconf pieprasījumus, taču arī tas rezultātus nedeva. Šobrīd ceru saņemt kādu papildus informāciju no IPS.

3.2.7. Datu rezerves kopēšana

Kopēšana norisinās pateicoties uz servera *RIEXC* esošajam *cron* dēmonam, kas noteiktās dienās (skat. plānošanas daļu) nakts vidū izpilda nelielu skriptu. Šī skripta izpildīšanai ir izveidots īpašs lietotājs "remback", kuram ir izveidots SSH atslēgu pāris (privāta un publiskā). Publiskā atslēgta atrodas uz servera RR un autorizē šī lietotāja pieslēgšanos.

Arhivēšana tiek veikta uz servera *RIEXC,* kas patērē noteiktus resursus. Tieši tāpēc izvēlētais laiks darbam ir nakts vidus. Arhivēšana tiek veikta ar komandas *tar* palīdzību, kas pārraksta iepriekšējo rezerves kopijas failu uz servera *RIEXC*. Tas tiek veikts ar administratora privilēģijām, jo lietotājam "remback" nav pieejas visiem vajadzīgajiem failiem. Kad jaunā rezerves kopija ir izveidota, tā ar komandas *sftp* un augšminētās SSH atslēgas palīdzību nokļūst uz servera *RR*. Pirms veidot rezerves kopiju, skripts vēlreiz pārliecinās, ka faila atļaujas nodrošina faila nepieejamību nevienam kā vien administratoram.

Uz servera RR arī ir *cron* dēmons, kurš reizi mēnesī iznīcina vecās rezerves kopijas atbilstoši rezerves kopēšanas plānam (skat. plānošanas daļu).

permisijas

3.2.8. Surogātpasts

Aizsardzībai pret surogātpastu, sekojot uzstādīšanas instrukcijai, uzstādīju *SpamAssassin*, ko lejupielādēju tīmekļa vietnē spamassassin.apache.org. Tā noklusētie uzstādījumi mani pagaidām apmierina, tāpēc tā uzstādījumiem tika veiktas tikai nelielas izmaiņas. Kad būs pagājis kāds laiks un saņemtas atsauksmes no lietotājiem, tad, iespējams, uzstādījumi tiks pielāgoti.

Lai savienotu *qmail* ar *SpamAssasin*, es izmantoju nelielu skriptu ar nosaukumu *ifspamh*(26). E-pasti tiek padoti uz šo skriptu izmantojot aizstājvārdu failus.

3.2.9. Darbstaciju administrēšana

Apstaigājot Rīgas Valsts 1. ģimnāzijas IS, tika secināts, ka tīklā ir četras *Windows XP* darbstacijas bez 2. servisa pakas. Tām šī paka tika veiksmīgi uzlikta.

Lai cīnītos ar datoru pārinstalēšanas problēmu, ar programmas *Norton Ghost* palīdzību tika izveidoti datoru klonēšanas diski. Viens disks ir derīgs visām darbstacijām, kas nav principiāli atšķirīgas.

Tā izveidošanas secība bija sekojoša:

1. uz bāzes datora tiek veikta pilna manuālā instalācija, kā tas aprakstīts šajā darbā pie esošās IS struktūras analīzes;
2. OS tiek iztīrīta no darbību vēstures, pagaidu failiem, utt.;
3. disks tiek defragmentēts;
4. datora cietais disks tiek izņemts un ievietots **otrā datorā,** kuram ir ierakstāmā kompaktdiska diskdzinis.
5. ar programmu *Norton Ghost*, kas palaista, izmantojot, **otra datora** OS, izveidojam diska attēlu un noglabājam otra datora diskā.
6. izmantojot *Windows 98SE* starta disketi un nelielu skriptu, izveidojam startējamu kompaktdisku, kurā iekopējam programmu *Norton Ghost* un diska attēlu.

Lai izveidotu šādu disku principiāli atšķirīgai darbstaciju grupai, izmantoju tikko izveidotu disku, lai klonētu vienu no principiāli atšķirīgajām darbstacijām. Pēc tam pārinstalēju draiverus un turpinu ar augstāk esošās izveidošanas secības 2. punktu.

Ja draiverus pārinstalēt neizdodas, jo sistēma ir nestabila, tad atsāku ar augstāk esošās izveidošanas secības 1. punktu.

3.2.10. Lokālā tīkla ātrums

Visi 6 datorcentrā esošie koncentratori tika aizvietoti ar diviem *Linksys SD208* un diviem *Linksys SD216* komutatoriem. Diemžēl finansiālas iespēja aizvietot pārējos Rīgas Valsts 1. ģimnāzijas tīklā esošos koncentratorus šobrīd nav.

Visi datortīkla kabeļi, kas neatbilda standartam, datorklasē D1 ir pārvilkti no jauna(1, 8).

Tām 4 darbstacijām, kurām tika konstatēts, ka tīkla karte manuāli iestatīta uz pilnu dupleksu, kartes pārstatītas uz automātisko ātrumu saskaņošanas režīmu.

3.2.11. UPS iegāde

Ir nopirkti divi *Mustek PowerMust 600VA*.

Viens no tiem izvietots 3. stāva servertelpā, kur uztur serveri RIEXC, maršrutētāju WATERFALL un pārvaldāmo komutatoru *3Com 3C16985B*. Otrs izvietots 2. stāva datortelpā, kur uztur trīs serverus ar nosaukumiem *BETONS, IKARUSS* un *RR*.

3.2.12. Administrēšanas atvieglošana

Šajā nodaļā veiktās darbības ir vairāk raksturīgas programmētājam nekā datortīkla administratoram, tāpēc procesā neiedziļināšos, bet tikai pastāstīšu, ko esmu izveidojis.

Ir izveidota datu bāze, kurā tīklā esošo iekārtu MAC adreses ir saistītas ar kabineta numuru (atrašanās vietu) un atbildīgo personu. Šī datubāze ir pieejama caur tīmekļa saskarni.

Vārdu serveris ir pārnests uz maršrutētāju *WATERFALL* (tā konfigurēšanas process aprakstīts augstāk).

Pieprasīju tiesības veidot atgriezeniskos ierakstus Rīgas Valsts 1. ģimnāzijas IP adresēm un šādi ieraksti izveidoti visām lietotāju darbstacijām un lielākajai daļai tīkla iekārtu. Lietotāju darbstaciju vārdi ir uzstādīti gan atgriezeniskajos, gan tiešajos vārdu ierakstos. Katrs no tiem ir tieši 3 simbolu garš.

Ir izstrādāta tīmekļa saskarnes pārvaldība maršrutētājam WATERFALL. Caur to iespējams administrēt starpniekservera *squid* lietotāju sarakstu, bezvadu lietotāju sarakstu, kā arī pieslēgt un atslēgt Internetu konkrētā datorklasē.

Visi administrēšanas rīki, kas darbojas caur tīmekļa saskarni, ir pieejami caur vienotu vietni admin.r1g.edu.lv, izmantojot HTTPS protokolu, un ir aizsargāti ar paroli.

3.2.13. Servera *BETONS* diska atjaunošana

Par rīcību šajā situācija daudz jau pastāstīju, kad runāju par plānošanu. Kā tad reāli tika veikta atjaunošana? Kā jau rakstīju, startēju datoru, izmantojot *Linux* distributīvu un izveidoju diska pilnu rezerves kopiju:

```
root@nut:~# dd if=/dev/sda of=~/backup
```

Kā par brīnumu tas lieliski izdevās, tāpēc nolēmu pamēģināt šo kopiju 1:1 ievadīt citā diskā. Brīvi 2 GB diski nebija pieejami. Paņēmu 10 GB IDE PATA disku, kas tajā brīdī bija brīvs un ievadīju rezerves kopiju tajā:

```
dd if=~/back of=/dev/hdb
```

Ievietojot šo disku atpakaļ serverī *BETONS*, tas atdzīvojās. Atlika tikai mainīt tā draiveru konfigurāciju, lai tiktu ielādēts, nevis SCSI, bet gan IDE draiveris. Protams, ka BETONS disku joprojām redzēja kā 2 GB lielu, jo nodalījumu tabula nebija mainījusies, un nevarēja izmantot brīvo vietu, bet visi bija apmierināti un laimīgi arī par šādu iznākumu.

3.2.14. Informātikas ieskaite

Manis izveidoto skriptu šeit detalizēti neiztirzāšu jau vairākkārt pieminētā iemesla dēļ – tas ir vairāk programmētāja, nekā administratora uzdevums. Taču šoreiz uzrakstīšu par, manuprāt, ģeniālo (“viss ģeniālais ir vienkāršs”) metodi, kas tika izmantota, lai ieskaites materiālus transportētu tīklā. Uz katra datora tika uzstādīts neliels GNU programmu komplekts (*tar, gzip, gpg*, utml.) un *scp*. Uz katra datora arī atradās divi sertifikāti – privāts sertifikāts S_{priv} un publisks sertifikāts K_{pub}. Skripts, kad izsaukts, pieslēdzās serverim, uz kura atradās sertifikāts S_{pub}. Savienojums notika automatiski, jo S šajā gadījumā ir domāts savienojuma sertifikāts. Pirms pieslēgties, skripts nošifrēja arhīvu ar šifrēšanas atslēgu K_{pub}, un drošības labad atstāja to uz datora, kā arī uzkopēja uz serveri.

Pat, ja skolēns būtu atradis skriptu, viņš varētu pieslēgties serverim vai sameklēt šifrēto arhīvu, taču atšifrēt nevarētu. Privāta atslēga K_{priv} atradās uz servera, citā lietotāja, uz kuru visi darbi tika pārkopēti pēc ieskaites beigām.

3.3. Dokumentācija

Zemāk iekļauju savu risinājumu dokumentāciju.

3.3.1. Konfigurācijas apraksts

Tagad, kad darbs ir pabeigts, Rīgas Valsts 1. ģimnāzijas ēkas uzbūve nav mainījusies, taču IS struktūra gan.

Tagad Rīgas Valsts 1. ģimnāzijai ir 2 servertelpas – 3. stāva un 2. stāvā.

Uz jumta atrodas virzienantena, 3. stāva servertelpā stāv maršrutētājs *WATERFALL,* pārvaldāms komutators *3Com 3C16985B*, serveris RIEXC, komutators *3Com OfficeConnect Dual Speed Switch 8*, komutators *3Com 3C16593B*, UPS *Mustek PowerMust 600VA* un viena lietotāja, viena administratora darbstacija.

2. stāva servertelpā atrodas komutators *3Com 3C16593B*, komutators *3Com 3C16592B*, serveri *RR*, *IKARUSS* un *BETONS*, administratora darbstacija un sekundārais tīkls (tā sastāvā ietilpst vides pārveidotājs *IMC iMcV/1* (FX-TX), pārvaldāms komutators *Cisco Catalyst 2950*, komutators *Allied Telesyn AT-8012M,* maršrutētājs *Linksys WRT54GS* (bez antenām)).

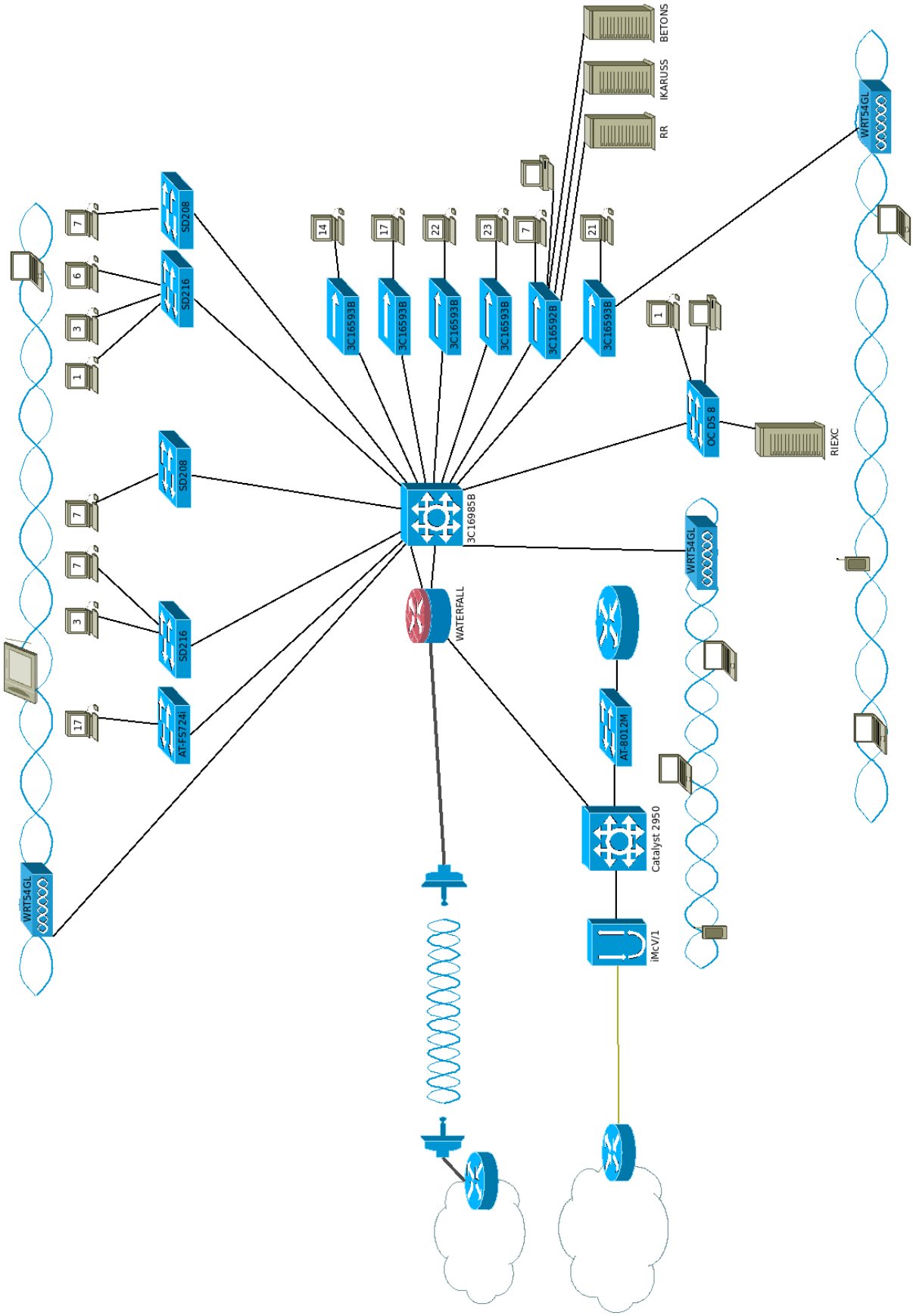
Rīgas Valsts 1. ģimnāzijā ir 3 datorklases. Tajās ir izvietotas apmēram 50 darbstacijas un sekojoši komutatori:

- 1. gab. *Allied Telesyn AT-FS724i* – 24 pieslēgumvietas, 100BASE-TX;
- 2 gab. *Linksys SD216* – 16 pieslēgumvietas;
- 2. gab. *Linksys SD208* – 8 pieslēgumvietas;

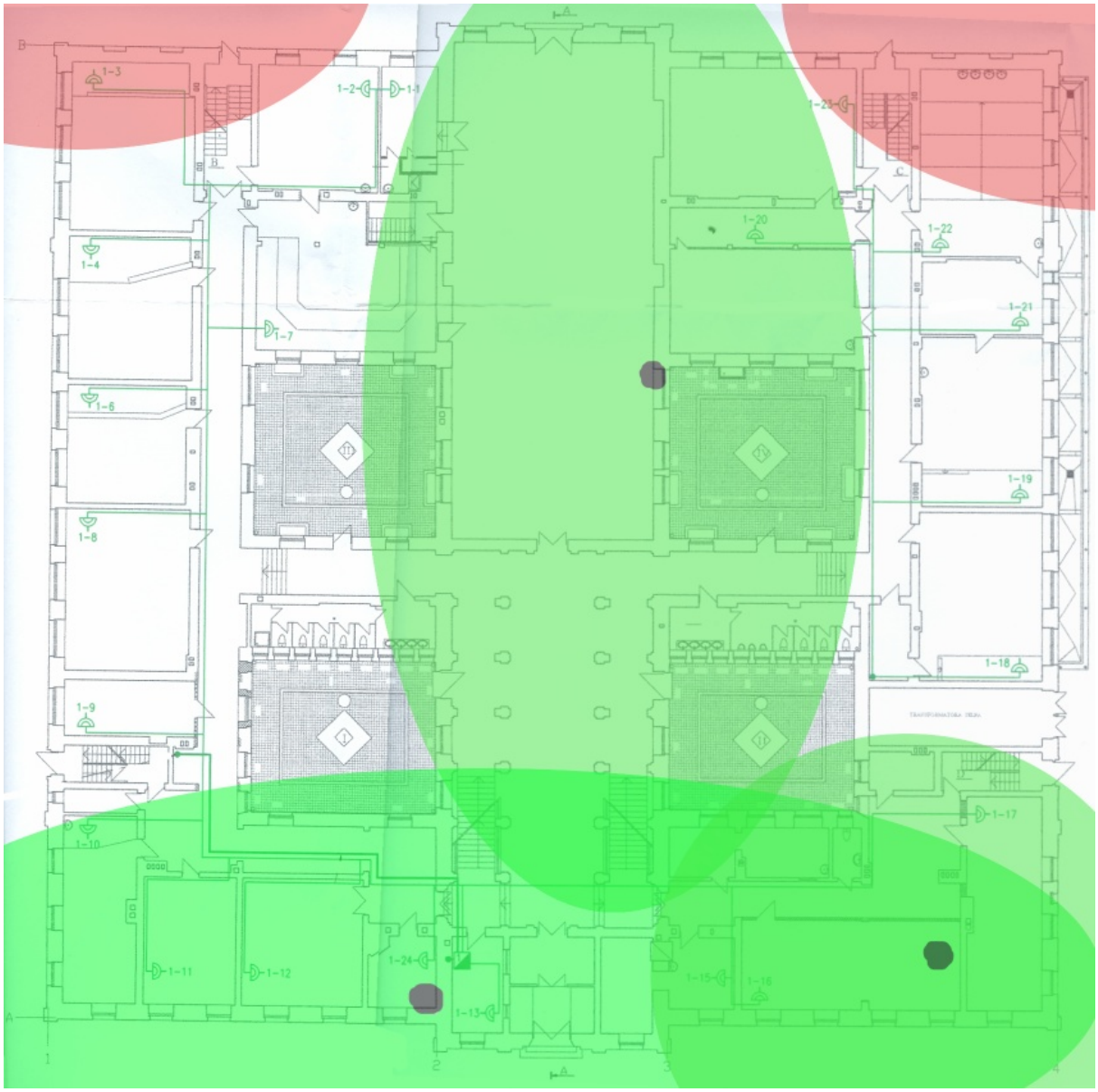
Bez augstāk nosauktajiem elementiem, citās ēkas vietās vēl ir izvietoti 5 komutatori *3Com 3C16593B* un 3 bezvadu pieejas punkti *Linksys WRT54GL* ar *DD-WRT* programmaparatūru, kā arī apmēram 50 datori.

Tīklā tiek periodiski lietoti arī 10-20 klēpjdatori, taču to skaitam ir tendence augt.

Datortīkla elementu fiziskais slēgums ir redzams 3.6. att.



3.6. att. **Rīgas Valsts 1. ģimnāzijas datortīkla fiziskā slēguma shēma pēc darba pabeigšanas**



3.7. att. **Bezvadu pieejas punktu izvietojums un bezvadu tīkla darbības rādiusi**

Bezvadu tīkls ir pieejams aulā, bibliotēkā, 1. un 2. stāva vestibilā, divos no četriem gaismas dārziem, datorcentrā, kafejnīcā un skolotāju istabā (skat. 3.7. att.) Ar punktiem apzīmēta bezvadu punktu atrašanās vieta, ar sarkano krāsu – svešie bezvadu tīkli, bet ar zaļo - Rīgas Valsts 1. ģimnāzijas bezvadu tīkls. Tīkla darbības rādiusi ir elipses formas, dēļ dažādos virzienos atšķirīgā sienu skaita, vērsuma un biezuma.

Rīgas Valsts 1. ģimnāzijas datortīklā tiek lietoti divi apakštīkli: 85.254.197.0/24, kas domāts lietotāju iekārtām un visām darbstacijām, un 85.254.196.128/27, kas atvēlēts serveru, tīkla iekārtu un citām vajadzībām. Tīklam ir arī divi IPS, taču šobrīd IP protokols darbojas tikai vienā tīklā. Lai gan sekundārā tīkla (otrs tīkls) iekārtas funkcionē, tajā neizdodas saklausīt nekāda veida aktivitāti.

Visi savienojumi starp apakštīkliem tiek maršrutēti caur maršrutētāju *WATERFALL,* kur tos iespējams kontrolēt. Visas MAC adreses tiek reģistrētas speciālā reģistrā, pirms tiek atļauta to lietošana tīklā. Iekārta ar nereģistrētu MAC adresi tīklā nedarbosies.

Tīklā darbojas sekojoši pakalpojumi:

- SMTP
- POP3
- HTTP
- HTTPS
- SSH
- FTP
- RADIUS
- *MySQL*

3.3.2. Kvalitātes nodrošināšanas pasākumi

Brīdi, kad kvalifikācijas darba tika pabeigts, Rīgas Valsts 1. ģimnāzijas IS tika veikti šādi kvalitātes nodrošināšanas pasākumi:

- Lietotāju apakštīkla drošības audits

  » Veicu pārbaudījums manis uzstādītā ugunsmūra kvalitātei no ārēja tīkla – tika mēģināts uzzināt, kuri datori ir ieslēgti, kādi porti tiem ir atvērti, kas darbojas uz šiem portiem, kā arī tika izmēģināti simtiem uzbrukumu ar mērķi iegūt piekļuvi darbstacijām vai izraisīt to avāriju. Audits neuzrādīja nevienu pašu darbstaciju. Tas šajā apakštīkla spēja atrast tikai maršrutētāju. Audits pieejams pielikumā nr. 2: "Lietotāju apakštīkla drošības audits".

- Serveru apakštīkla drošības audits

  » Šis ir pārbaudījums ne tikai ugunsmūra kvalitātei, bet arī programmatūrai, kas nodrošina serveru piedāvātos pakalpojumus. Audits parādīja, ka viss ir labākajā kārtībā. Audits pieejams pielikuma nr. 3: "Serveru apakštīkla drošības audits".

- Datorklases D1 vītā pāra kabeļu tests

  » Izmantojot nedārgo iekārtu *Multi-Network Cable Tester*, pārbaudīju katru vītā pāra kabeli. Pārbaude parādīja, ka nu vadi ir standartam atbilstoši.

- Bezvadu tīkla diapazona tests

» Ar klēpjdatoru *HP Compaq nc6120* pārliecinājos, ka bezvadu tīkls darbojas kvalitatīvi un tā pārklātā teritorija dažviet ir nedaudz plašāka kā cerēts. (skat. 3.7. att.) Signāls viegli izspraucas starp stāviem, piemēram, 3. stāva bezvadu punkts ir bez problēmām lietojams 2. stāvā. Tam par iemeslu kalpo tas, ka grīdas nesatur lielas metāla konstrukcijas, bet ir veidotas uz koka pamata.

- Bezvadu pieejas punktu temperatūras tests

» Tā kā es palielināju bezvadu pieejas punktu jaudu uz 60 mW, tad pirms tos uzstādīt, es vienu no tiem pārbaudīju, divas diennaktis atstājot ieslēgtā stāvoklī un pēc tam pārbaudot tā temperatūru.

- UPS pārbaude

» Pirms jauno UPS pielietošanas praksē, to maksimālais darbības laiks bez maiņstrāvas padeves tika pārbaudīts kontrolētos apstākļos. UPS izdevās noturēt plānoto slodzi 5-10 minūtes, kas attiecīgajā cenu kategorijā ir pieņemami un daudz labāk, nekā tas bija pirms uzlabojumu veikšanas.

- Lokālā tīkla ātruma pārbaude

» Lai pārliecinātos, ka un kāds ir uzlabojums pēc Lokālā tīkla iekārtu nomaiņas, veicu testu, kas sīkāk aprakstīts pielikumā nr. 4: "Lokālā tīkla ātruma mērījumi". Ātruma uzlabojums bija vairāk kā desmitkārtīgs, bet pakešu zudumi tīklā dramatiski mazinājās.

- Klona diska tests

» Pēc klonēšanas diska izveides, pārbaudīju to uz vairākiem datoriem izlases veidā un pārliecinājos, ka klonēšanas process norit bez kļūdām un ka klonētā sistēma pēc tam funkcionē normāli.

Lai arī turpmāk nodrošinātu kvalitatīvu IS darbību, ir regulāri jāveic šādi pasākumi:

- reizi mēnesī jāveic ārējs tīkla audits;
- reizi pāris mēnešos jāveic iekšējs tīkla audits, lai nodrošinātu, ka arī no iekšēja tīkla nav iespējams izmantot kādas ievainojamības;
- Maršrutētājam *WATERFALL* un serveriem *RIEXC* un *RR* regulāri jāatjaunina programmatūra, lai programmatūras kļūdas, tiklīdz tādas tiek atklātas, tiktu novērstas; jaunu programmatūras versiju esamība jāpārbauda **vismaz** 3 reizes nedēļā;
- Tiklīdz tas ir iespējams, jālikvidē serveris *IKARUSS*.

3.3.3. Rezerves kopiju veidošanas plāns

Datu rezerves kopēšana tiek veikta tikai uz servera *RIEXC* esošajai:

- mapei */etc* (servera uzstādījumi);
- mapei */root* un mapei */home* (lietotāju un administratora dati);
- mapei */www* (mājaslapas);
- mapei */var/lib/mysql* (datubāzes)
- mapei */var/log* (žurnāli)
- failam */quota.user* (informācija par lietotāju kvotām).

Kopēšana notiek katra mēneša 1., 3., 7., 11., 15., 21., 25., 27. un 31. (ja tāds ir) datumā tiek izveidots arhīvs, kurš tiek caur tīklu noglabāts uz servera RR, kas atrodas cita ēkas stāvā. Jaunākā arhīva kopija tiek saglabāta arī uz servera *RIEXC*, bet serveris *RR* uztur visas esošā mēneša kopijas, trīs kopijas no iepriekšējā mēneša (1., 11. un 21. datuma) un vēl iepriekšējo 11 mēnešu 1. datuma kopijas.

Pēdējo rezerves kopiju var atjaunot to atarhivējot pāri esošajai sistēmai vai arī atarhivējot noteiktas mapes no tās, ja nav vajadzības atjaunot rezerves kopiju pilnībā. Tas neatgriezeniski izmainīs sistēmā esošos datus. Ja ir vēlme, atjaunot rezerves kopiju **paralēli** esošajiem datiem, tad arī to ir iespējams izdarīt. Vienkārši atarhivēšana jāveic uz citu diska vietu.

Citas rezerves kopijas (visas, izņemot pēdējo) sākumā kopējamas no servera *RR* uz serveri *RIEXC*, izmantojot datortīklu, stingri ieteicams, šifrētu savienojumu, piemēram SSH. Pēc tam atjaunošanas process ir identisks tam, kāds tas ir pēdējai rezerves kopijai.

3.3.4. Drošības pasākumi

Lai veidotu drošu IS, ir pielietotas un ieviestas sekojošas tehnoloģijas, procesi un rīki:

- pēc darba pabeigšanas ir veikts tīkla drošības audits (skat. pielikumu nr. 2: "Lietotāju apakštīkla drošības audits" un pielikums nr. 3: "Serveru apakštīkla drošības audits");
- Bezvadu tīkls veidots, izmantojot WPA2 standarta AES algoritmu;
- Bezvadu tīkls naktī tiek automātiski izslēgts;
- LILO parametru maiņa ir aizsargāta ar paroli;
- iekārtām, kurām ir BIOS, tas ir aizsargāts ar paroli;

- serveri un tīkla aparatūra atrodas telpās ar ierobežotu piekļuvi;
- lietotāju darbstacijas ir nodalītas no serveriem, jo tās atrodas atsevišķā tīklā;
- iekārta datortīklā nedarbojas, kamēr tās MAC adrese netiek piereģistrēta uz maršrutētāja;
- lai piekļūtu ārvalstu Internetam, lietotājiem ir jāautentificējas;
- tīmekļa un komandrindas administrēšanas saskarnes pieejamas, izmantojot šifrētu kanālu (SSL – HTTPS un SSH);
- uz servera *RIEXC* (un servera *RR*) tiek izmantotas ēnotās paroles;
- servera *RIEXC* svarīgākajam mainīgajam saturam tiek veidotas rezerves kopijas;
- lietotāju paroles nedrīkst būt īsākas par 8 simboliem.

4. REZULTĀTI

Pēc mana kvalifikācijas darba beigām, Rīgas Valsts 1. ģimnāzijas IS ir piedzīvojis lielus uzlabojumus. Tīklā vairs nav nevienas iekārtas, kuras teorētiskais ātrums būtu 10 Mbit vai zemāk, kā rezultātā ir stipri palielinājies tīkla ātrums starp jebkuriem diviem punktiem Rīgas Valsts 1. ģimnāzija lokālajā tīklā.

Ir palielināta IS drošība, ieviešot rezerves kopēšanas sistēmu, veicot profilaktiskus pasākumus pret surogātpasta saņemšanu un uzstādot tīkla aizsardzība ne tikai no Interneta, bet arī iekštīkla. Tagad darbstacijas vairs nav atvērtas uzbrukumiem no Interneta, un arī iespēja apdraudēt serverus no darbstacijām ir samazināta.

Datortīklam iespējams pieslēgt tikai tādu aparatūru, kas tiek reģistrēta uz maršrutētāja *WATERFALL*, visa pārējā aparatūra tīkla nedarbosies. Atļaujas tiek rūpīgi reģistrētas un problēmu gadījumā ir iespējams noteikt vainīgo.

Ir izpētīta citu bezvadu tīklu klātbūtne Rīgas Valsts 1. ģimnāzijas teritorijā un izveidots ērts bezvadu tīkls, kas, manuprāt, raisīs lietotājos vēlmi, izpētīt jaunās tehnoloģijas un palielināt to īpatsvaru savā dzīvē un mācību procesā.

Esmu atvieglojis administratoru (t.i., galvenokārt, savu) darbu, ieviešot vienotu, drošu administrēšanas paneli ar tīmekļa saskarni, caur kuru iespējams pārvaldīt lietotājus un novērot sistēmu stāvokli. Arī datubāze, ar kuras palīdzību iespējams noteikt katras iekārtas atrašanās vietu tīklā, ir noderīga.

Ir arī sniegta palīdzība krīzes gadījumos un citās neparastās situācijās, kā piemēram, atjaunojot servera *BETONS* cietā diska saturu vai atvieglojot informātikas skolotāju darbu informātikas ieskaites laikā.

Esmu kārtojis arī formalitātes, sazinoties ar IPS – gan lūdzot mainīt tīkla iekārtas, gan piešķirt papildu tiesības. Esmu atjauninājis Rīgas Valsts 1. ģimnāzijas informāciju RIPE datubāzē, kad mainījās telefonu numerācija Latvijā un kad ieviesu bezvadu tīklu.

Gala rezultātā uzskatu, ka esmu izveidojis stabilu un drošu IS, kas pienācīgā kvalitātē pilda tās funkcijas, ko lietotāji no tās gaida un tai uztic.

5. SECINĀJUMI

Izdevies paveikt daudz svarīgu lietu. Salīdzinot Rīgas Valsts 1. ģimnāzijas IS pirms darba uzsākšanas un tagad redzu, ka ir paveikts liels darbs un kopsummā ir palielinājusies Rīgas Valsts 1. ģimnāzijas IS drošība, uzticamība, caurspīdīgums un kvalitāte.

Ja iepriekš tīkls bija lēns, tad tagad tas ir ātrs. Ja tīkls bija nedrošs – nu tas ir kļuvis ievērojami drošāks. Ja IS bija nestabila un neuzticama – tagad lietotāji to lieto ar vien vairāk, dodot priekšroku informācijas glabāšanai digitālā formā. Protams, nevar atkārtoti nepieminēt bezvadu tīkla ieviešanu, kas, manuprāt, būs viens no galvenajiem faktoriem Rīgas Valsts 1. ģimnāzijas IS popularitātes un izmantošanas biežuma kāpumam.

Nav jau arī tā, ka viss iecerētais izdevās. Līdz galam nerealizēta palika ideja par sekundāra tīkla savienošanu ar esošo datortīklu. Radās neliela aizķeršanās nodrošinot Rīgas Valsts 1. ģimnāzija IS aizsardzību no sekundārā datortīkla esošās bezvadu iekārtas. Šobrīd ēkā vēl ir palikuši 6 koncentratori – 100BASE-T standarta iekārtas –, taču tās tiks mainītas, tiklīdz esošais risinājums vairs nespēs strādāt pieņemamā kvalitātē(1) un vairumam lietotāju pašreizējā risinājuma ātrums vairs nebūs pieņemams. Neizdevās arī ieviest IPv6, taču tas jau arī nebija mans sākotnējais mērķis...

Tā vietā, lai IPv6 ieviestu, esmu guvis daudz ko jaunu, stipri padziļinājis savas pirms tam seklās zināšanas par šo protokolu, kā arī sagrāvis vairākus mītus. Esmu uzlabojis savas komunikācijas spējas, cenšoties panākt to, kas apmierina lielāko daļu lietotāju, bet kam varbūt nedaudz pietrūka finansējuma vai vēlmes iziet uz kompromisu. Un vairumā gadījumu esmu to arī panācis. Esmu pierādījis pats sev un citiem, ka arī iestādē ar tik specifiskām lietotāju grupām ir iespējama IS stabila un droša darbība, kā arī nepieciešama IS modernizācija.

Nobeigumā varu secināt, ka Rīgas Valsts 1. ģimnāzijas IS turpmākajai attīstībai ir ielikts stabils pamats un tuvākos gadus turpināsies attīstības un modernizācijas process, kas novedīs pie arvien lielākas IS izmantošanas ikdienā un gala rezultātā sabiedrības un informācijas sistēmu ciešākas integrācijas.

PATEICĪBAS

Vēlos izteikt pateicību cilvēkiem (ieguldījuma laika secībā) bez kuriem šis darbs būtu tapis daudz grūtāk un ilgāk, ja vispār.

- Savai mātei Larisai Solovjovai, kas man ir veltījusi neaprakstāmi daudz laika un nervu mani auklējot, audzinot un arī daudz naudas mani skolojot. Ja ne viņas palīdzība un labā roka, tad tagad es droši vien būtu pavisam kur citur.
- Savai ģimnāzijai par to, ka izaudzināja manī raksturu, kā arī par to, ka ļāva man pietiekoši daudz brīvas vaļas eksperimentēt un mācīties gan šī darba izstrādes gaitā, gan visus tos gadus pirms tam, bet īpaši

  klases audzinātājai Viktorijai Vārpiņai par mīļumu, izpratni un sirsnīgo un personīgo attieksmi, ko tā man (un arī maniem klasesbiedriem) veltīja,

  skolotājai Ingrīdai Siliņšmitei par to, ka tagad spēju rakstīt gramatiski un stilistiski pareizi,

  klases audzinātājai un skolotājai Aijai Lūsei par pareizā profesionālā dzīves ceļa ierādīšanu un saturīgo stundu vadīšanu, kā arī to, ka viņa ik pa brīdim lūdz informācijas sistēmā ieviest kādu jaunu iespēju, kas man arvien liek meklēt risinājumus.
- Savai Universitātei, kura mani ved un, ceru, vēl turpmāko piecgadi vedīs pretī zvaigznēm, bet īpaši

  savam darba vadītājam un pasniedzējam Leo Trukšānam, par cilvēcīgo attieksmi, par to, ka palīdzēja saprast daļu no tā, kā Universitātē viss ir iekārtots un ka atbildēja uz maniem neskaitāmajiem jautājumiem sakarā ar šī darba izstrādi.
- Saviem draugiem un kolēģiem par to, ka piecieta, ka šo pēdējo mēnesi biju tik aizņemts, ka izlikos tos neredzam šajās saulainajās un siltajās dienās.

IZMANTOTĀ LITERATŪRA UN AVOTI

1. Grāmatas

1. **Ogletree, T. W.** *Модернизация и ремонт сетей Второе издание.* Москва: Вильямс, 2001. 928 стр.

2. **Mueller, S.** *Модернизация и ремонт ПК Одиннадцатое издание.* Москва: Вильямс, 2000. 1152 стр.

3. **Briere, D., Hurley, P., Ferris, E.** *Wireless Home Networking For Dummies.* New Jersey: Wiley, 2006. 374 p.

4. **Desmeules, R.** *Cisco Self-Study: Implementing IPv6 Networks (IPV6).* Indianapolis: Cisco Press, 2003. 468 p.

2. Standarti, normatīvie akti un līgumi

5. *Letter symbols to be used in electrical technology: Telecommunications and electronics.* **IEC 60027-2.**

6. *Vispārējās izglītības likums.* LR likums.

7. *Līgums par starptautiskā datoru tīkla Internet izmantošanu visu diennakti no Pasūtītāja darba vietas*. Līgums Nr. **23-91-580.** (Nav spēkā.)

8. *Telecommunications Industry Association Commercial Building Telecommunications Cabling Standard – Part 1: General Requirements.* **TIA/EIA-568-B.1-2001.**

9. *Noteikumi par radiofrekvenču spektra joslu sadalījumu radiosakaru veidiem un iedalījumu radiosakaru sistēmām, kā arī par radiofrekvenču spektra joslu izmantošanas vispārīgajiem nosacījumiem.* MK noteikumi Nr. **276.**

10. *Elektromagnētiskā saderība un radiofrekvenču spektra jautājumi - Platjoslas pārraides sistēmas - Datu pārraides iekārtas, kas darbojas 2,4 GHz ISM joslā un pielieto spektru paplašinošu modulācijas paņēmienu.* ICS 33.060 Radiokomunikācijas: LVS EN **300 328:2001.**

11. ERC RECOMMENDATION 70-03 (Tromsø 1997 and subsequent amendments) *RELATING TO THE USE OF SHORT RANGE DEVICES (SRD).* ***ERC/REC 70-03.***

12. Selection and Operation of Secondary DNS Servers. **RFC 2182.**

3. Lietošanas instrukcijas un dokumentācija

13. *SuperStack 3 Switch 330 XM, SM, TM, MM User Guide.* Santa Clara: 3Com Corporation, 2001. 64 p.

14. **Barinovs, R.** *Rīga, Raiņa bulvāris 8. Datoru tīkli*: izpilddokumentācija. Rīga: Rīgas Valsts 1. ģimnāzija, 2001. 7 lpp.

4. Zinātniski pētnieciskie darbi

15. **Maļinovskis, R.** *Linux serveris*: zinātniski pētnieciskais darbs. Rīga: Rīgas Valsts 1. ģimnāzija, 1999. 40 lpp.

5. Elektroniskie informācijas avoti

16. *The LWN.net Linux Distribution List* [tiešsaiste] – [atsauce 20.03.2007.] Pieejams: http://lwn.net/Distributions/

17. *Ethernet auto-sensing and auto-negotiating* [tiešsaiste] – [atsauce 23.03.2007.] Pieejams: http://www.cites.uiuc.edu/network/advanced/autosense.html

18. *Slackware Package Browser* [tiešsaiste] – [atsauce 21.04.2007.] Pieejams: http://packages.slackware.it/

19. *DD-WRT Supported Devices* [tiešsaiste] – [atsauce 21.05.2007.] Pieejams: http://www.dd-wrt.com/wiki/index.php/Supported_Devices

20. *Channels, Power Levels, and Antenna Gains* [tiešsaiste] – [atsauce 21.05.2007.] Pieejams: http://www.cisco.com/univercd/cc/td/doc/product/wireless/cb21ag/acau01/auappb.htm

21. *If you happen to have a Linksys WRT54G wireless router…* [tiešsaiste] – [atsauce 21.05.2007.] Pieejams: http://roachfiend.com/archives/2006/01/02/if-you-happen-to-have-a-linksys-wrt54g-wireless-router/

22. *Norton Ghost 12.0* [tiešsaiste] – [atsauce 30.04.2007.] Pieejams: http://shop.symantecstore.com/DRHM/servlet/ControllerServlet?Action=DisplayProductDetailsPage&SiteID=symnahho&Locale=en_US&ThemeID=106300&Env=BASE&productID=73048200

23. *Creating a self-signed SSL certificate* [tiešsaiste] – [atsauce 17.03.2007.] Pieejams: http://www.tc.umn.edu/~brams006/selfsign.html

24. *INSTRUCTIONS FOR UPGRADING FROM 11.0* [tiešsaiste] – [atsauce 28.04.2007.] Pieejams: http://slackware.osuosl.org/slackware-current/UPGRADE.TXT

25. *Slackware-current ChangeLog* [tiešsaiste] – [atsauce 28.04.2007.] Pieejams: ftp://ftp.slackware.com/pub/slackware/slackware-current/ChangeLog.txt

26. *A simple script for filtering incoming email through SpamAssassin* [tiešsaiste] – [atsauce 16.05.2007.] Pieejams: http://www.gbnet.net/~jrg/qmail/ifspamh/

PIELIKUMU SARAKSTS

Kvalifikācijas darbam ir sekojoši pielikumi:

- Pielikums nr. 1: "Servera *IKARUSS* drošības audits"
  - ↗ Pielikums satur ar programmatūru *nessus* veiktu servera *IKARUSS* auditu kvalifikācijas darba izstrādes sākumā.
  - ↗ Audita atskaite ir saīsināta izdzēšot katras konkrētās problēmas un informatīvā ziņojuma aprakstu, bet saglabājot to identifikatorus. Tas pielikuma apjomu samazināja apmēram 10 reizes. Apraksts ir pieejams tīmeklī, izmantojot CVE, BID un Nessus identifikators, piemēram, šajā adresē (aizvietojot **ID** ar konkrēto numuru): http://www.nessus.org/plugins/index.php?view=single&id=**ID**
- Pielikums nr. 2: "Lietotāju apakštīkla drošības audits"
  - ↗ Pielikums satur ar programmatūru *nessus* veiktu servera *IKARUSS* auditu kvalifikācijas darba izstrādes sākumā.
  - ↗ Audita atskaite ir saīsināta izdzēšot katras konkrētās problēmas un informatīvā ziņojuma aprakstu, bet saglabājot to identifikatorus.
- Pielikums nr. 3: "Serveru apakštīkla drošības audits"
  - ↗ Pielikums satur ar programmatūru *nessus* veiktu servera *IKARUSS* auditu kvalifikācijas darba izstrādes sākumā.
  - ↗ Audita atskaite ir saīsināta izdzēšot katras konkrētās problēmas un informatīvā ziņojuma aprakstu, bet saglabājot to identifikatorus.
- Pielikums nr. 4: "Lokālā tīkla ātruma mērījumi"
  - ↗ Pielikums satur TCP datu pārraides ātruma mērījumu (darba sākumā un beigās) starp divām lietotāju darbstacijām veikšanas izklāstu un rezultātus.
- Pielikums nr. 5: "*WATERFALL* skripti"
  - ↗ Pielikums satur manis veidotus nestandarta skriptus, kas nodrošina ugunsmūra *iptables* un starpniekservera *squid*, kas atrodas uz maršrutētāja WATERFALL, sekmīgu darbību.
  - ↗ Pielikums iekļauj arī skripta SWIST: SWitcher and Internet Stopper kodu.

PIELIKUMS NR. 1: "SERVERA *IKARUSS* DROŠĪBAS AUDITS"

Scan Details

Hosts which were alive and responding during test	1
Number of security holes found	18
Number of security warnings found	14

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
ikaruss	ssh (22/tcp)	Security hole found
ikaruss	smtp (25/tcp)	Security notes found
ikaruss	http (80/tcp)	Security hole found
ikaruss	netbios-ssn (139/tcp)	Security hole found
ikaruss	imap (143/tcp)	Security hole found
ikaruss	mysql (3306/tcp)	Security warning(s) found
ikaruss	netbios-ns (137/udp)	Security notes found
ikaruss	general/tcp	Security notes found
ikaruss	general/udp	Security notes found
ikaruss	general/icmp	Security notes found

Security Issues and Fixes: ikaruss

Type	Port	Issue and Fix
Vulnerability	ssh (22/tcp)	CVE : CVE-2002-0083 BID : 3560, 4241, 4560 Nessus ID : 10802
Vulnerability	ssh (22/tcp)	CVE : CVE-2002-0575 BID : 4560 Nessus ID : 10954
Vulnerability	ssh (22/tcp)	CVE : CVE-2003-0682, CVE-2003-0693, CVE-2003-0695 BID : 8628 Nessus ID : 11837
Vulnerability	ssh (22/tcp)	CVE : CVE-2002-0639, CVE-2002-0640 BID : 5093 Nessus ID : 11031
Vulnerability	ssh (22/tcp)	CVE : CVE-2001-0872 BID : 3614 Nessus ID : 10823
Vulnerability	ssh (22/tcp)	CVE : CVE-2002-0083 BID : 4241 Nessus ID : 10883
Warning	ssh (22/tcp)	CVE : CVE-2003-0386 BID : 7831 Nessus ID : 11712

Informational	ssh (22/tcp)	Nessus ID : 10330
Informational	ssh (22/tcp)	Nessus ID : 10267
Informational	ssh (22/tcp)	Nessus ID : 10881
Informational	ssh (22/tcp)	CVE : CVE-2001-0361 BID : 2344 Nessus ID : 10882
Informational	smtp (25/tcp)	Nessus ID : 10330
Informational	smtp (25/tcp)	Nessus ID : 10263
Vulnerability	http (80/tcp)	CVE : CVE-2004-0079, CVE-2004-0081, CVE-2004-0112 BID : 9899 Nessus ID : 12110
Vulnerability	http (80/tcp)	CVE : CVE-2004-1018, CVE-2004-1019, CVE-2004-1020, CVE-2004-1063, CVE-2004-1064, CVE-2004-1065 BID : 11964, 11981, 11992, 12045 Nessus ID : 15973
Vulnerability	http (80/tcp)	CVE : CVE-2004-0488 BID : 10355 Nessus ID : 12255
Vulnerability	http (80/tcp)	CVE : CVE-2003-0542 BID : 8911 Nessus ID : 11915
Vulnerability	http (80/tcp)	BID : 11334 Nessus ID : 15436
Vulnerability	http (80/tcp)	CVE : CVE-2004-0700 BID : 10736 Nessus ID : 13651
Vulnerability	http (80/tcp)	CVE : CVE-2002-0392 BID : 5033 Nessus ID : 11030
Warning	http (80/tcp)	CVE : CVE-2002-0839, CVE-2002-0840, CVE-2002-0843 BID : 5847, 5884, 5887, 5995, 5996 Nessus ID : 11137
Warning	http (80/tcp)	BID : 13143, 13163, 13164 Nessus ID : 18033
Warning	http (80/tcp)	CVE : CVE-2002-0985, CVE-2002-0986 BID : 5562 Nessus ID : 11444
Warning	http (80/tcp)	CVE : CVE-2003-0078, CVE-2003-0131, CVE-2003-0147 BID : 6884, 7148 Nessus ID : 11267
Informational	http (80/tcp)	Nessus ID : 10330
Informational	http (80/tcp)	Nessus ID : 10662
Informational	http (80/tcp)	Nessus ID : 10107
Informational	http (80/tcp)	Nessus ID : 10302
Informational	http (80/tcp)	CVE : CVE-2004-2320 BID : 9506, 9561, 11604 Nessus ID : 11213
Informational	http (80/tcp)	Nessus ID : 24260
Informational	http (80/tcp)	CVE : CVE-2005-0524, CVE-2005-0525

		BID : 12962, 12963 Nessus ID : 17687
Vulnerability	netbios-ssn (139/tcp)	CVE : CVE-2004-1154 BID : 11973 Nessus ID : 15985
Vulnerability	netbios-ssn (139/tcp)	CVE : CVE-2003-0085, CVE-2003-0086 BID : 7106, 7107 Nessus ID : 11398
Vulnerability	netbios-ssn (139/tcp)	CVE : CVE-2002-1318 BID : 6210 Nessus ID : 11168
Vulnerability	netbios-ssn (139/tcp)	CVE : CVE-2003-0196, CVE-2003-0201 BID : 7294, 7295 Nessus ID : 11523
Warning	netbios-ssn (139/tcp)	CVE : CVE-2004-0829 BID : 11055 Nessus ID : 14381
Informational	netbios-ssn (139/tcp)	Nessus ID : 11011
Informational	netbios-ssn (139/tcp)	Nessus ID : 10785
Informational	netbios-ssn (139/tcp)	CVE : CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595 BID : 494, 990, 11199 Nessus ID : 10394
Informational	netbios-ssn (139/tcp)	Nessus ID : 10400
Informational	netbios-ssn (139/tcp)	CVE : CVE-2004-0815 BID : 11216, 11281 Nessus ID : 15394
Vulnerability	imap (143/tcp)	CVE : CVE-2004-0224, CVE-2004-0777 BID : 9845, 10976 Nessus ID : 12103
Informational	imap (143/tcp)	Nessus ID : 10330
Informational	imap (143/tcp)	Nessus ID : 11414
Warning	mysql (3306/tcp)	BID : 11435, 11432 Nessus ID : 15477
Warning	mysql (3306/tcp)	CVE : CVE-2005-0709, CVE-2005-0710, CVE-2005-0711 BID : 12781 Nessus ID : 17313
Warning	mysql (3306/tcp)	CVE : CVE-2003-0780 BID : 8590 Nessus ID : 11842
Warning	mysql (3306/tcp)	CVE : CVE-2002-1373, CVE-2002-1374, CVE-2002-1375, CVE-2002-1376 BID : 6368, 6370, 6373, 6374, 6375, 8796 Nessus ID : 11192
Warning	mysql (3306/tcp)	CVE : CVE-2004-0835, CVE-2004-0837 BID : 11357 Nessus ID : 15449
Warning	mysql (3306/tcp)	CVE : CVE-2004-0457 BID : 10969 Nessus ID : 14343

Warning	mysql (3306/tcp)	CVE : CVE-2005-2558 BID : 14509 Nessus ID : 19416
Warning	mysql (3306/tcp)	CVE : CVE-2004-0836 BID : 10981 Nessus ID : 14319
Informational	mysql (3306/tcp)	Nessus ID : 11153
Informational	mysql (3306/tcp)	Nessus ID : 10719
Informational	mysql (3306/tcp)	CVE : CVE-2006-1516 BID : 17780 Nessus ID : 21632
Informational	netbios-ns (137/udp)	CVE : CVE-1999-0621 Nessus ID : 10150
Informational	general/tcp	Nessus ID : 11936
Informational	general/tcp	Nessus ID : 25220
Informational	general/tcp	Nessus ID : 12053
Informational	general/udp	Nessus ID : 10287
Informational	general/icmp	CVE : CVE-1999-0524 Nessus ID : 10114
Informational	general/icmp	Nessus ID : 12264

PIELIKUMS NR. 2: “LIETOTĀJU APAKŠTĪKLA DROŠĪBAS AUDITS”

Scan Details

Hosts which were alive and responding during test	2
Number of security holes found	0
Number of security warnings found	0

Host List

Host(s)	Possible Issue
85.254.197.1	Security note(s) found
85.254.197.3	Security note(s) found

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.197.1	domain (53/udp)	Security notes found
85.254.197.1	general/udp	Security notes found
85.254.197.1	general/icmp	Security notes found
85.254.197.1	general/tcp	Security notes found

Security Issues and Fixes: 85.254.197.1

Type	Port	Issue and Fix
Informational	domain (53/udp)	Nessus ID : 11002
Informational	domain (53/udp)	Nessus ID : 11951
Informational	general/udp	Nessus ID : 10287
Informational	general/icmp	CVE : CVE-1999-0524 Nessus ID : 10114
Informational	general/icmp	Nessus ID : 12264
Informational	general/tcp	Nessus ID : 12053

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.197.3	ssh (22/tcp)	Security notes found
85.254.197.3	domain (53/tcp)	Security notes found
85.254.197.3	cbt (7777/tcp)	Security notes found
85.254.197.3	domain (53/udp)	Security notes found
85.254.197.3	general/udp	Security notes found
85.254.197.3	general/tcp	Security notes found
85.254.197.3	general/icmp	Security notes found

Security Issues and Fixes: 85.254.197.3

Type	Port	Issue and Fix
Informational	ssh (22/tcp)	Nessus ID : 10330
Informational	ssh (22/tcp)	Nessus ID : 10267
Informational	ssh (22/tcp)	Nessus ID : 10881
Informational	domain (53/tcp)	Nessus ID : 11002
Informational	cbt (7777/tcp)	Nessus ID : 15588
Informational	cbt (7777/tcp)	Nessus ID : 11032
Informational	cbt (7777/tcp)	Nessus ID : 10107
Informational	cbt (7777/tcp)	CVE : CVE-2004-2320 BID : 9506, 9561, 11604 Nessus ID : 11213
Informational	cbt (7777/tcp)	Nessus ID : 24260
Informational	domain (53/udp)	Nessus ID : 11002
Informational	domain (53/udp)	Nessus ID : 11951
Informational	general/udp	Nessus ID : 10287
Informational	general/tcp	Nessus ID : 25220
Informational	general/tcp	Nessus ID : 12053
Informational	general/icmp	CVE : CVE-1999-0524 Nessus ID : 10114

PIELIKUMS NR. 3: “SERVERU APAKŠTĪKLA DROŠĪBAS AUDITS”

Scan Details

Hosts which were alive and responding during test	16
Number of security holes found	0
Number of security warnings found	0

Host List

Host(s)	Possible Issue
85.254.196.129	Security note(s) found
85.254.196.130	Security note(s) found
85.254.196.131	Security note(s) found
85.254.196.136	Security note(s) found
85.254.196.137	Security note(s) found
85.254.196.138	Security note(s) found
85.254.196.143	No noticeable information found
85.254.196.144	No noticeable information found
85.254.196.150	No noticeable information found
85.254.196.151	No noticeable information found
85.254.196.152	No noticeable information found
85.254.196.153	No noticeable information found
85.254.196.154	No noticeable information found
85.254.196.155	No noticeable information found
85.254.196.156	No noticeable information found
85.254.196.157	No noticeable information found

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.129	domain (53/udp)	Security notes found
85.254.196.129	general/udp	Security notes found
85.254.196.129	general/icmp	Security notes found
85.254.196.129	general/tcp	Security notes found

Security Issues and Fixes: 85.254.196.129

Type	Port	Issue and Fix
Informational	domain (53/udp)	Nessus ID : 11002
Informational	domain (53/udp)	Nessus ID : 11951
Informational	general/udp	Nessus ID : 10287
Informational	general/icmp	CVE : CVE-1999-0524 Nessus ID : 10114

Informational	general/icmp	Nessus ID : 12264
Informational	general/tcp	Nessus ID : 12053

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.130	ssh (22/tcp)	Security notes found
85.254.196.130	domain (53/tcp)	Security notes found
85.254.196.130	domain (53/udp)	Security notes found
85.254.196.130	general/udp	Security notes found
85.254.196.130	general/icmp	Security notes found
85.254.196.130	general/tcp	Security notes found

Security Issues and Fixes: 85.254.196.130

Type	Port	Issue and Fix
Informational	ssh (22/tcp)	Nessus ID : 10330
Informational	ssh (22/tcp)	Nessus ID : 10267
Informational	ssh (22/tcp)	Nessus ID : 10881
Informational	ssh (22/tcp)	CVE : CVE-2003-0190 BID : 7342, 7467, 7482, 11781 Nessus ID : 11574
Informational	domain (53/tcp)	Nessus ID : 11002
Informational	domain (53/udp)	Nessus ID : 11002
Informational	domain (53/udp)	Nessus ID : 11951
Informational	general/udp	Nessus ID : 10287
Informational	general/icmp	CVE : CVE-1999-0524 Nessus ID : 10114
Informational	general/tcp	Nessus ID : 12053

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.131	general/udp	Security notes found
85.254.196.131	general/tcp	Security notes found

Security Issues and Fixes: 85.254.196.131

Type	Port	Issue and Fix
Informational	general/udp	Nessus ID : 10287
Informational	general/tcp	Nessus ID : 12053

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.136	general/udp	Security notes found
85.254.196.136	general/icmp	Security notes found
85.254.196.136	general/tcp	Security notes found

Security Issues and Fixes: 85.254.196.136

Type	Port	Issue and Fix
Informational	general/udp	Nessus ID : 10287
Informational	general/icmp	CVE : CVE-1999-0524 Nessus ID : 10114
Informational	general/icmp	Nessus ID : 12264
Informational	general/tcp	Nessus ID : 12053

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.137	general/udp	Security notes found
85.254.196.137	general/icmp	Security notes found
85.254.196.137	general/tcp	Security notes found

Security Issues and Fixes: 85.254.196.137

Type	Port	Issue and Fix
Informational	general/udp	Nessus ID : 10287
Informational	general/icmp	CVE : CVE-1999-0524 Nessus ID : 10114
Informational	general/icmp	Nessus ID : 12264
Informational	general/tcp	Nessus ID : 12053

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.138	general/udp	Security notes found
85.254.196.138	general/icmp	Security notes found
85.254.196.138	general/tcp	Security notes found

Security Issues and Fixes: 85.254.196.138

Type	Port	Issue and Fix
Informational	general/udp	Nessus ID : 10287
Informational	general/icmp	CVE : CVE-1999-0524 Nessus ID : 10114

Informational general/icmp Nessus ID : 12264
Informational general/tcp Nessus ID : 12053

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.143	smtp (25/tcp)	No Information

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.144	smtp (25/tcp)	No Information

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.150	ftp (21/tcp)	No Information
85.254.196.150	smtp (25/tcp)	No Information
85.254.196.150	unknown (26/tcp)	No Information
85.254.196.150	http (80/tcp)	No Information
85.254.196.150	pop3 (110/tcp)	No Information
85.254.196.150	ssh (22/tcp)	No Information
85.254.196.150	https (443/tcp)	No Information

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.151	ftp (21/tcp)	No Information
85.254.196.151	ssh (22/tcp)	No Information
85.254.196.151	smtp (25/tcp)	No Information
85.254.196.151	unknown (26/tcp)	No Information
85.254.196.151	http (80/tcp)	No Information
85.254.196.151	pop3 (110/tcp)	No Information
85.254.196.151	https (443/tcp)	No Information

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.152	https (443/tcp)	No Information
85.254.196.152	http (80/tcp)	No Information

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.153	https (443/tcp)	No Information
85.254.196.153	http (80/tcp)	No Information

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.154	smtp (25/tcp)	No Information
85.254.196.154	http (80/tcp)	No Information

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.155	http (80/tcp)	No Information
85.254.196.155	ftp (21/tcp)	No Information
85.254.196.155	ssh (22/tcp)	No Information
85.254.196.155	smtp (25/tcp)	No Information
85.254.196.155	unknown (26/tcp)	No Information
85.254.196.155	pop3 (110/tcp)	No Information
85.254.196.155	https (443/tcp)	No Information

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.156	ftp (21/tcp)	No Information
85.254.196.156	ssh (22/tcp)	No Information
85.254.196.156	smtp (25/tcp)	No Information
85.254.196.156	unknown (26/tcp)	No Information
85.254.196.156	pop3 (110/tcp)	No Information
85.254.196.156	https (443/tcp)	No Information
85.254.196.156	http (80/tcp)	No Information

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
85.254.196.157	http (80/tcp)	No Information

PIELIKUMS NR. 4: "LOKĀLĀ TĪKLA ĀTRUMA MĒRĪJUMI"

Mērījumiem izmantoti divi identiski datori ar 100BASE-TX tīkla kartēm – *bat* un *bay.* Lai OS izmaiņas neietekmētu rezultātus, kā OS tika izvēlēts *Ubuntu 5.04 Linux 2.6.10 Live CD*.

Testēšanai kāda komplicētāka rīka vietā, tika izraudzītas vienkāršās un daudzpusīgās komandas *dd* un *nc*. To priekšrocība pār, piemēram, *netperf,* ir iespēja redzēt oriģinālos datus, pirms vēl tie tiek automātiski ievietoti formulās. Šādā veidā bija iespējams novērot atkārtoti izsūtīto baitu daudzumu, kam būtu jābūt tieši proporcionālam kolīziju skaitam.

Testēšana tika veikta palaižot katru no trim rindām pa vienai uz katra no datoriem vienlaicīgi. Komandas būtība ir 60 sekundes pārraidīt nulles bitus uz otru datoru. Pirmais tests pārraida datus virzienā no *bat* uz *bay*, otrais – no *bay* uz *bat,* bet trešais – abos virzienos vienlaicīgi. Pusdupleksa tīklā tam vajadzētu radīt lielu daudzumu kolīziju, kas arī tika novērots.

Izraksts no *bat* termināļa, veicot testēšanu **pirms** tīkla uzlabošanas:

```
ubuntu@bat:~$ (dd if=/dev/zero | nc bay 4001 &); sleep 60; killall nc

104922+0 records in
104921+0 records out
53719552 bytes transferred in 60.006516 seconds (895229 bytes/sec)

ubuntu@bat:~$ nc -l -p 4002 | dd of=/dev/null 74613+37645 records in

76382+24947 records in
105626+1 records out
54080536 bytes transferred in 60.063625 seconds (900387 bytes/sec)

ubuntu@bat:~$ (nc -l -p 4002 | dd of=/dev/null &); (dd if=/dev/zero | nc bay 4001 &);
sleep 60; killall nc

38355+19327 records in
54273+1 records out
27787840 bytes transferred in 60.016462 seconds (463004 bytes/sec)

53690+0 records in
53689+0 records out
27488768 bytes transferred in 60.015188 seconds (458030 bytes/sec)
```

Izraksts no *bay* termināļa, veicot testēšanu **pirms** tīkla uzlabošanas:

```
ubuntu@bay:~$ nc -l -p 4001 | dd of=/dev/null

74112+37399 records in
104909+1 records out
53713632 bytes transferred in 60.075620 seconds (894100 bytes/sec)

ubuntu@bay:~$ (dd if=/dev/zero | nc bat 4002 &); sleep 60; killall nc

105650+0 records in
105649+0 records out
```

```
54092288 bytes transferred in 60.013570 seconds (901334 bytes/sec)

ubuntu@bay:~$ (nc -l -p 4001 | dd of=/dev/null &); (dd if=/dev/zero | nc bat 4002 &);
sleep 60; killall nc

37924+19123 records in
53677+1 records out
27482888 bytes transferred in 60.015585 seconds (457929 bytes/sec)

54348+0 records in
54347+0 records out
27825664 bytes transferred in 60.015183 seconds (463644 bytes/sec)
```

Izraksts no *bat* termināļa, veicot testēšanu **pēc** tīkla uzlabošanas:

```
ubuntu@bat:~$ (dd if=/dev/zero | nc bay 4001 &); sleep 60; killall nc

1379123+0 records in
1379122+0 records out
706110464 bytes transferred in 60.014628 seconds (11765639 bytes/sec)

ubuntu@bat:~$ nc -l -p 4002 | dd of=/dev/null

978688+486595 records in
1379069+1 records out
706083536 bytes transferred in 60.062315 seconds (11755850 bytes/sec)

ubuntu@bat:~$ (nc -l -p 4002 | dd of=/dev/null &); (dd if=/dev/zero | nc bay 4001 &);
sleep 60; killall nc

957697+425818 records in
1305860+1 records out
668600576 bytes transferred in 60.036418 seconds (11136583 bytes/sec)

1316194+0 records in
1316193+0 records out
673890816 bytes transferred in 60.038247 seconds (11224359 bytes/sec)
```

Izraksts no *bay* termināļa, veicot testēšanu **pēc** tīkla uzlabošanas:

```
ubuntu@bay:~$ nc -l -p 4001 | dd of=/dev/null

978704+486585 records in
1379112+1 records out
706105456 bytes transferred in 60.077245 seconds (11753293 bytes/sec)

ubuntu@bay:~$ (dd if=/dev/zero | nc bat 4002 &); sleep 60; killall nc

1379081+0 records in
1379080+0 records out
706088960 bytes transferred in 60.015584 seconds (11765094 bytes/sec)

ubuntu@bay:~$ (nc -l -p 4001 | dd of=/dev/null &); (dd if=/dev/zero | nc bat 4002 &);
sleep 60; killall nc

970923+422718 records in
1316171+1 records out
673879640 bytes transferred in 60.038604 seconds (11224106 bytes/sec)

1305955+0 records in
1305954+0 records out
668648448 bytes transferred in 60.043848 seconds (11136003 bytes/sec)
```

Mērījums	1. pirms	2. pirms	3. pirms	1. pēc	2. pēc	3. pēc
izsūtīti no *bat*	53719552	0	27787840	706110464	0	673890816
saņemti uz *bat*	0	54080536	27488768	0	706083536	668600576
izsūtīti no *bay*	0	54092288	27825664	0	706088960	668648448
saņemti uz *bay*	53713632	0	27482888	706105456	0	673879640
kopā izsūtīti	53719552	54092288	55613504	706110464	706088960	1342539264
kopā saņemti	53713632	54080536	54971656	706105456	706083536	1342480216
atkārtoti izsūtīti	5920	11752	27787840	5008	5424	59048
kopējais ātrums	7.2 Mbps	7.2 Mbps	7.3 Mbps	94.1 Mbps	94.1 Mbps	179.0 Mbps

Augstāk esošajā tabulā apkopotie skaitļi ir mērāmi **baitos šo 60 sekunžu laikā**, izņemot pēdējā rindā, kur mērvienības ir norādītas. Atkārtoti izsūtītie baiti tiek aprēķināti atņemot izsūtīto baitu skaitu no saņemto baitu skaita. Kopējais tīkla ātrums tiek aprēķināts, izdalot kopā izsūtīto baitu skaitu (60 sekundēs) ar 60 sekundēm un pārveidojot mērvienības.

PIELIKUMS NR. 5 "*WATERFALL* SKRIPTI"

Maršrutētāja *WATERFALL* ar *crontab* palīdzību reizi nedēļā palaiž skriptus *getlvip, iptables-compile* un *squid-restart*. Tas tiek panākts crontab veicot ierakstu:

```
0 1 * * sun getlvip; iptables-compile; squid-restart
```

Šīs komandas jebkurā brīdī drīkst palaist arī maršrutētāja administrators, taču jārēķinās, ka tās var izraisīt IS pakalpojumu pārtraukumu uz laiku līdz 5 sekundēm.

Skripts */usr/sbin/getlvip*:

```
#!/bin/sh

lynx http://net.02.lv/lvnet -dump | grep -v '^#' | grep '^[0-9]' > /etc/iptables/lv.ip
[ ! -f /etc/iptables/lv.ip ] && echo NAV DATU && exit 0
```

Izmantojot tīmekļa pārlūku *lynx,* kas nāk *Linux Slackware* komplektācijā, skripts pieprasa adrešu sarakstu, izlaiž rindas, kas sākas ar komentāru un iekļauj tikai tās rindas, kas sākas ar ciparu. Tad tas rezultātu noglabā failā */etc/iptables/lv.ip*.

Skripts */usr/sbin/squid-restart*:

```
#!/bin/sh

echo "#DO NOT EDIT!!! Use .pre and .post. (C) Kirils">/usr/local/squid/etc/squid.conf
cat /usr/local/squid/etc/squid.conf.pre>>/usr/local/squid/etc/squid.conf
sed 's/^.*$/acl latvia dst &/' /etc/iptables/lv.ip  >>/usr/local/squid/etc/squid.conf
cat /usr/local/squid/etc/squid.conf.post>>/usr/local/squid/etc/squid.conf

killall -9 squid

/usr/local/squid/sbin/squid
```

Šis skripts izveido jaunu squid konfigurāciju no failiem *squid.conf.pre* un *squid.conf.post,* pa vidu ierakstot rindas "acl latvia dst 1.2.3.4/5" par katru apakštīklu no faila *lv.ip.*

Skripts */usr/sbin/iptables-compile* ir sarežģītākais un pamatīgākais skripts no visiem:

```
#!/bin/sh

cd /etc/iptables/

touch tmp_dotables
chmod 700 tmp_dotables
rm /etc/swist/lock/* 2>/dev/null

> tmp_dotables
echo "#!/bin/sh" >> tmp_dotables
echo "#Generated by iptables-compile v0.3 on `date`" >> tmp_dotables
echo "iptables -P INPUT DROP" >> tmp_dotables
echo "iptables -P FORWARD DROP" >> tmp_dotables
echo "iptables -P OUTPUT DROP" >> tmp_dotables
echo "iptables -t nat -P PREROUTING DROP" >> tmp_dotables
echo "iptables -t nat -P POSTROUTING DROP" >> tmp_dotables
echo "iptables -t nat -P OUTPUT DROP" >> tmp_dotables
echo "iptables -t mangle -P PREROUTING DROP" >> tmp_dotables
```

```
echo "iptables -t mangle -P INPUT DROP" >> tmp_dotables
echo "iptables -t mangle -P FORWARD DROP" >> tmp_dotables
echo "iptables -t mangle -P POSTROUTING DROP" >> tmp_dotables
echo "iptables -t mangle -P OUTPUT DROP" >> tmp_dotables
echo "iptables -F" >> tmp_dotables
echo "iptables -t nat -F">>tmp_dotables
echo "iptables -t mangle -F" >> tmp_dotables
echo "iptables -X" >> tmp_dotables
echo "iptables -t nat -X" >> tmp_dotables
echo "iptables -t mangle -X" >> tmp_dotables
echo "iptables -N latvia" >> tmp_dotables
echo "iptables -N lvok" >> tmp_dotables
echo "iptables -N lvbad" >> tmp_dotables
echo "iptables -N serversin" >> tmp_dotables
echo "iptables -N serversout" >> tmp_dotables
echo "iptables -N localmacs" >> tmp_dotables
echo "iptables -N macok" >> tmp_dotables
echo "iptables -N macfowok" >> tmp_dotables

#DYN begin

for x in `cat macs|grep -v \#`; do

 if [ "`echo \"$x\" | cut -d \| -f 2`" != "" ]; then
  echo "iptables -A FORWARD -p tcp -m tcp -m mac --mac-source `echo \"$x\" | cut -d \|
-f 1` -s ! `echo \"$x\" | cut -d \| -f 2` -j REJECT --reject-with icmp-host-prohibited”
>> tmp_dotables ;
  echo "iptables -A FORWARD -p udp -m udp -m mac --mac-source `echo \"$x\" | cut -d \|
-f 1` -s ! `echo \"$x\" | cut -d \| -f 2` -j REJECT --reject-with icmp-host-prohibited”
>> tmp_dotables ;
  echo "iptables -A localmacs -p tcp -m tcp -m mac --mac-source `echo \"$x\" | cut -d
\| -f 1` -s ! `echo \"$x\" | cut -d \| -f 2` -j REJECT --reject-with icmp-host-
prohited” >> tmp_dotables ;
 fi

 echo "iptables -A FORWARD -m mac --mac-source `echo \"$x\" | cut -d \| -f 1` -j
macfowok" >> tmp_dotables ;
 echo "iptables -A localmacs -m mac --mac-source `echo \"$x\" | cut -d \| -f 1` -j
macok" >> tmp_dotables ;

done

echo "iptables -A FORWARD -i eth0 -j macfowok" >> tmp_dotables
echo "iptables -A FORWARD -j REJECT --reject-with icmp-host-prohibited" >> tmp_dotables
echo "iptables -A localmacs -j REJECT --reject-with icmp-host-prohibited" >>
tmp_dotables

sed 's/^.*$/iptables -A latvia -d & -j lvok/' lv.ip  >> tmp_dotables
echo "iptables -A latvia -j lvbad" >> tmp_dotables

cat filter |cut -d \# -f 1 | delblanklines > tmp_table
sed 's/^.*$/iptables &/' tmp_table  >> tmp_dotables
cat mangle |cut -d \# -f 1 | delblanklines > tmp_table
sed 's/^.*$/iptables -t mangle &/' tmp_table  >> tmp_dotables
cat nat |cut -d \# -f 1 | delblanklines > tmp_table
sed 's/^.*$/iptables -t nat &/' tmp_table >> tmp_dotables
rm tmp_table

#DYN end

echo "iptables -P INPUT ACCEPT" >> tmp_dotables
echo "iptables -P FORWARD ACCEPT" >> tmp_dotables
echo "iptables -P OUTPUT ACCEPT" >> tmp_dotables
echo "iptables -t nat -P PREROUTING ACCEPT" >> tmp_dotables
echo "iptables -t nat -P POSTROUTING ACCEPT" >> tmp_dotables
echo "iptables -t nat -P OUTPUT ACCEPT" >> tmp_dotables
```

```
echo "iptables -t mangle -P PREROUTING ACCEPT" >> tmp_dotables
echo "iptables -t mangle -P INPUT ACCEPT" >> tmp_dotables
echo "iptables -t mangle -P FORWARD ACCEPT" >> tmp_dotables
echo "iptables -t mangle -P POSTROUTING ACCEPT" >> tmp_dotables
echo "iptables -t mangle -P OUTPUT ACCEPT" >> tmp_dotables

./tmp_dotables #sheit reaali tiek izpildiits sakompileetais skripts
chmod 600 tmp_dotables
rm tmp_dotables

/usr/sbin/iptables-save>iptables-current
```

Tā kā šis skripts, manuprāt, vairāk klasificējas kā programmēšanas, nevis administrēšanas darbs, neiedziļināšos tā rakstiskā izskaidrošanā pa soļiem, bet īsi paskaidrošu būtību. Šis skripts izveido ("kompilē") citu skriptu, kuru pēc tam pats palaiž. Tajā viņš iekļauj komandas, kas

1. uzstāda ķēžu noklusēto politiku uz DROP,
2. iztīra ķēdes (šajā brīdī dēļ 1. punkta nekādi savienojumi nav iespējami – drošības dēļ),
3. uzbūvē jaunu politiku, kas atļauj tikai reģistrētajām MAC adresēm pieslēgties tīklam,
4. iekļauj FILTER, NAT un MANGLE ķēdes, kas tiek definētas atsevišķos failos,
5. uzstāda ķēžu noklusēto politiku uz ACCEPT (jo tagad ugunsmūris ir drošs).

Šādā veidā tiek panākts, ka tīkls ne sekundi nav neaizsargāts. Protams, ka *iptables-current*, tiek ielādēts ar *iptables-restore* palīdzību, arī startējot un pārstartējot sistēmu.

Pārskatam iekļauju **nelielu fragmentu** no faila */etc/iptables/filter*:

```
-A INPUT -d 192.168.19.15 -i eth0 -p icmp -m icmp --icmp-type 8 -j ACCEPT # atljaut
pingu, lai ISP var paarbaudiit savienojumu
-A INPUT -i eth1 -j localmacs # no shiem interfeisiem driikst ienaakt tikai
regjistreetaas MAC adreses
-A INPUT -i eth2 -j localmacs # --”--
-A INPUT -j macok
-A macfowok -s 85.254.196.128/255.255.255.224 -i ! eth1 -j DROP # paarbauda, vai
pareiza ieeja - lai, piemeeram, aareeja int klients nevareetu izlikties par ieksheejo
-A macfowok -s ! 85.254.196.128/255.255.255.224 -i eth1 -j DROP
-A macfowok -s 85.254.197.0/255.255.255.0 -i ! eth2 -j DROP
-A macfowok -s ! 85.254.197.0/255.255.255.0 -i eth2 -j DROP
-A macfowok -d 159.148.60.2 -p udp -m udp --dport 53 -j ACCEPT #latnet DNS
-A macfowok -s 159.148.60.2 -p udp -m udp --sport 53 -j ACCEPT
-A macfowok -d 159.148.60.11 -p udp -m udp --dport 123 -j ACCEPT #latnet NTP
-A macfowok -s 159.148.60.11 -p udp -m udp --sport 123 -j ACCEPT
-A macfowok -p igmp -j REJECT --reject-with icmp-proto-unreachable #igmp nav jaaljauj
-A macfowok -d 85.254.197.0/255.255.255.0 -p icmp -m icmp --icmp-type 8 -j DROP
#neljauj pingot workstationus
```

Otra skriptu kopa ir Interneta atslēgšanas datorklasē skripti, kurus, pielietojot *bash* pamatzināšanas, iespējams viegli saprast:

/sbin/swist:

```
#!/bin/bash

pidfile="/var/run/swist.pid"
d=$1
total=$#

if [ -f "$pidfile" ]; then
echo "ERROR: swist is running at `cat $pidfile`"
exit 0
fi
echo $$>$pidfile
for (( x=1; x<total; x++ )); do
shift

/sbin/swist.do $d $1

done

if (( $total < 2 )); then
echo "ERROR: not enough params"
fi
rm $pidfile
```

/sbin/swist.do:

```
#!/bin/bash

#SWitcher and Internet Stopper
#(C) Kirils Solovjovs

basedir="/etc/swist/"
lockdir=$basedir"lock"
mlockdir=$basedir"maclock"
anlockdir=$basedir"antilock"
cfgdir=$basedir"conf"

function togcon () {

iptables -$1 FORWARD -j REJECT -m mac --mac-source $2
iptables -$1 INPUT -j REJECT -m tcp -p tcp --destination-port 8080 -m mac --mac-source
$2

}

if [ `id -u` != 0 ]; then
echo "non root user"
exit 2
fi


if [ "$1" != "I" ] && [ "$1" != "D" ] && [ "$1" != "A" ] && [ "$1" != "U" ]; then
echo "first param failed (I or D or A or U)"
exit 1
fi

if [ -f "$anlockdir/$2" ] && [ "$1" != "A" ] && [ "$1" != "U" ]; then
echo "STOP: Blocked"
exit 2
fi


if [ "$1" == "I" ]; then

if [ -f "$lockdir/$2" ]; then
echo "ERROR: already locked!"
exit 1
```

```
fi

fi

if [ "$1" == "D" ]; then

if [ ! -f "$lockdir/$2" ]; then
echo "ERROR: not locked"
exit 1
```

DOKUMENTĀRĀ LAPA

Kvalifikācijas darbs “Rīgas Valsts 1. ģimnāzijas datortīkla modernizācija” izstrādāts LU Fizikas un matemātikas fakultātē.

Ar savu parakstu apliecinu, ka kvalifikācijas darbs veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: Kirils Solovjovs

Rekomendēju darbu aizstāvēšanai.

Vadītājs: pasniedzējs B.dat. Leo Trukšāns

Recenzents:

Darbs iesniegts Datorikas nodaļā

Metodiķe:

Darbs aizstāvēts kvalifikācijas gala pārbaudījuma komisijas sēdē

_____ prot. Nr. __, vērtējums

Komisijas sekretārs: