LATVIJAS UNIVERSITĀTE
FIZIKAS UN MATEMĀTIKAS FAKULTĀTE
DATORIKAS NODAĻA

MAZO OFISU TĪKLA RISINĀJUMI

KVALIFIKĀCIJAS DARBS

Autors: **Jurijs Tomilovs**
Stud. apl. jt05012
Darba vadītājs: Mag. Sc. Comp. Jānis Judrups

RĪGA 2007

Anotācija

SIA "TRIALINE" ir jauna firma, kura piedāvā IT pakalpojumus. Viens no šiem pakalpojumiem ir tīkla konfigurācijas plānošana, ieviešana, uzturēšana un attīstīšana saskaņā ar klienta vajadzībām. Šajā darbā tika izstrādāta viena kopēja shēmām, kas tika uzbūvēta maziem ofisiem ar līdzīgām un populārākam vajadzībām. Galvenais mērķis bija izveidot tīkla risinājumus, kuri apmierinātu klientu vajadzības, būtu viegli administrējami un kuros tiktu izmantoti vienoti izstrādāšanas principi, kurus varētu aprakstīt zem vienas shēmas. Ar risinājumiem būtu domāts šis shēmas dažādas konfigurācijas.

Abstract

SIA “TRIALINE” is young firm, which offer IT services. One of those services is network configuration planning, implementation, support and upgrading in accordance with client's wishes. There was developed one schema in this work, which was made for small offices with common and most popular demands. The main aim was to develop network solutions, which granted clients demands, would be easy administrated and had common development principles, what can be overviewed under one schema. Solution is this different this schema configuration.

Анотация

SIA „TRIALINE”- молодая фирма, прелагающая IT услуги, одна из которых является планирование, введение, техническая поддержка и развитие компьютерной сети в соответствии с желаниями клиента. В этой работе была разработана схема сети для маленьких офисов с общими потребностями. Главная цель - разработать сетевые решения, которые удовлетворяли бы запросы клиентов, были легко администрируемые и имели общие принципы развития, которые можно рассмотреть под одной схемой. Под решениями подразумевается различные конфигурации этой схемы.

Atslēgvārdi

Datortīklu risinājumi

Drukas serveris

Failu serveris

Terminmāls

Windows XP

Windows Server 2003

Linux Ubuntu

Satura rādītājs

IEVADS

Esošās tīkla struktūras apraksts un analīze

Kvalifikācijas darba tēma ir „Mazo ofisu tīkla risinājumi”, kas ietver sevī tieši tīklu izveidošanu saskaņā ar noteikta klienta vajadzībām (darbā būs aprakstīti populārākie no tiem), tāpēc nav iespējams runāt par esošo struktūru. Varētu pieminēt, ka dažiem klientiem pastāv kaut kāda tipa struktūra (piemēram, datori, kas nav lokāla tīklā), bet, kā rāda prakse, tā ir neefektīva un neapmierina klienta vajadzības, tāpēc to ir ērtāk un ātrāk uzbūvēt no jauna nekā veikt to analīzi un pārbūvēšanu.

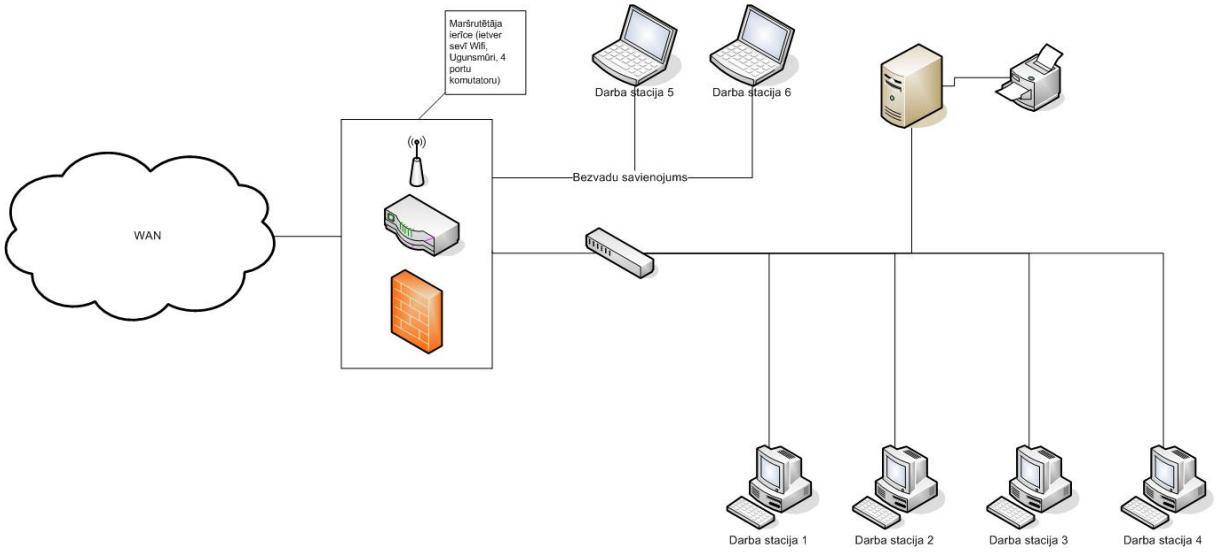
Problēmu un uzdevumu definīcijas

Pētāmās problēmas

Mūsdienās Informācijas tehnoloģijas ienāk katrā dzīvē un arī jebkurā darbības sfērā. Lielās kompānijās parasti ir daudz datoru un arī cita veida tehnoloģijas. Parasti, lai apkopotu, administrētu, kā arī izstrādātu tīkla risinājumus, šādos lielos uzņēmumos strādā cilvēki, kas atbild par to visu. Bet ko darīt mazām firmām un ofisiem, kuri nevar atļauties turēt cilvēku, kurš nodarbotos ar šāda veida problēmām? Tieši tādos gadījumos SIA „Trialine” piedāvā pakalpojumu: tīkla konfigurācijas plānošana, ieviešana, uzturēšana un attīstīšana saskaņā ar klienta vajadzībām. Šīs administrēšanas darbs ir arī aprakstīts šajā darbā.

Darba mērķi un uzdevumus

Tā kā parasti mazi ofisi ir vienāda tipa, no tīkla veidošanas viedokļa, tad tika izdalītas galvenās un populārākas klientu prasības, un izveidota shēma tīkla veidošanai.



1. att. Kopēja tīkla shēma.

Galvenais darba uzdevums ir aprakstīt šo shēmu, kura arī bija izstrādāta kā piemērs un demonstrācijas vide klientiem, un to dažas konfigurācijas iespējas, kas parasti ir atkarīgas no klientu vajadzībām (dažāda veida servisu darbības (failu serveris, drukas serveris, terminmāls un citi), darba staciju OS un arī citas vajadzības, Wireless risinājumi). Apskatot šo aprakstu, klients var novērtēt katra komponenta nepieciešamību sev, apskatīt kopējo risinājumu darbā, uzzināt tīkla iespējas un noformulēt savas prasības SIA „Trialine" darbiniekiem, kuri vārēs izplānot un ieviest tieši vajadzīgo tīkla risinājumu.

Problēmas ietekmes analīze uz tīkla struktūru kopumā

Darbā pamatā tiek apskatīta situācija, kad IS struktūra tiek būvēta no jauna, nodrošinot dažādu komponenšu savietojamību un drošu darbu. Gadījumos, kad noteikta tīkla struktūra jau eksistē, apskatītais risinājums to var mainīt visnotaļ būtiski

Risinājuma izstrāde un plānošana

Risinājums tiek izstrādāts balstoties uz izmantojam metodēm (aprakstīts zemāk). Plānošana notika balstoties uz populārākiem klientu prasībām, kuras aprakstītas, apskatot noteikto risinājumu daļu.

Izmantotās metodes

Šajā darba tika izmantotas:

1. LAN konfigurēšanas principi
2. Wireless tīkla principi
3. Windows XP, Ubuntu Linux instalēšanas un konfigurēšanas principi
4. Windows 2003 Server instalēšanas un konfigurēšanas principi
5. Maršrutētāju konfigurēšanas principi
6. Dažādu lietojumu vai servisu darbību instalēšanas un konfigurēšanas principi (File, Print, Terminal un citi)
7. LAN aizsardzības principi

Faktoloģiskā materiāla avoti

Šajā darbā pētāmas problēmas analīzei un risinājumam tika izmatots SIA „Trialine" aprīkojums, uz kura tika nokonfigurēts viens tīkla risinājums, jeb kopēja shēma, kura sevī iekļauj vairākus mazākus iespējamos risinājumus.

Risinājuma ieviešana

Tīkla risinājumi tiek ieviesti periodiski SIA „Trialine" klientiem, ar šī darba autora palīdzību (daži darbu piemēri būs pieminēti šajā darbā, neieskaitot kopējo testa tīkla shēmu). Testa tīkla konfigurācija tika ieviesta pēc tas plānošanas un tiek administrēta saskaņa ar tālāk pastāstītiem principiem.

Darba struktūra

Šis darbs apraksta nokonfigurētu lielu tīkla shēmu, kā arī to komponentes, kuras, ja tas ir iespējams, var tikt aizstātas ar citām. Šo darbu varētu sadalīt piecos lielos punktos :

1. Konfigurācijas apraksts (IS struktūra un to iespējamās konfigurācijas atkarība no klienta vajadzībām, maršrutizēšanas jautājumi, datu centralizēšana, darba stacijas un serveru instalācijas un OS izvēle, perifērijas ierīču pieslēgšanas (drukas serveris), Specialie gadījumi (Termināls un citi) un t.t.)
2. Kvalitātes nodrošināšanas pasākumu apraksts (apraksta darbības, kuras ir veiktas no administrēšanas daļas, lai nodrošinātu kvalitāti tīklu izmantošanā)

3. Nepārtrauktas darbības nodrošināšana
4. Rezerves kopiju veidošanas plāns (datu rezervēšanas plāns un realizācija)
5. Drošības pasākumu apraksts (aizsardzība no ārienes (ugunsmūris), pieejas tiesībās un t.t.)

Šie punkti ir arī šis dokumentācijas daļas, kuri veido galveno darba uzdevumu.

1. OFISA TĪKLA KONFIGURĀCIJAS APRAKSTS

Šajā nodaļa ir aprakstīta izstrādāta kopēja shēma datortīklam priekš maziem ofisiem, kā arī dažas to komponēšanas iespējas. Tā kā komponentes var būt dažādas un daži servisi nav vajadzīgi visiem klientiem, tad ar risinājumiem ir domāti šo shēmu konfigurācijas. Šīs konfigurācijas varētu būt ļoti daudz. Katrā apakšnodaļa ir aprakstīta komponenšu nepieciešamība un iespējamie citi risinājumi šīm komponentēm (OS izvēle un t.t.). Nodaļas beigās ir aprakstīti daži populārākie iespējamie klientu vajadzību un prasību scenāriji, kuriem būs piedāvāti risinājumi kopā ar to komponentēm. Šī nodaļa ir izstrādā tā, ka apraksts sakas ar populārākām klientu prasībām un to risinājumiem, un, virzoties uz priekšu, veido pilnu iepriekšminēto shēmu.

1.1 Darba stacijas

Vispopulārākā un viena no primārajām klientu prasībām ir darba staciju ātra un droša darbība. Tāpēc viens no galvenajiem uzdevumiem, veidojot jebkuru tīkla risinājumu, ir darba stacijas operētājsistēmas izvēle. Lai izvelētos operētājsistēmu jādomā par dažiem svarīgiem faktoriem:

1. Klientu vajadzības
2. Darba stacijas jaudīgums
3. Operētājsistēmas izmaksas

Pārsvara, kā rada statistika, klienti izvēlas Microsoft izstrādātos produktus darbam ar darba stacijām, tāpēc aplūkosim dažus no tiem. Tāpat tiks aprakstīts gadījums, ja darba stacijai tiks uzstādīta Linux operētājsistēma, kā arī aplūkos gadījums, kad darba stacija izmanto mašīnu, kura izmanto Termināli (par ko tiks stāstīts vienā no nākošām nodaļām).

Windows XP ir pašlaik vispopulārākā operētājsistēma. Tās minimālās prasības darba stacijai ir procesors ar takts frekvenci 300 Mhz; 128 Mb RAM, 1,5 Gb brīvas vietas uz cietā diska [1]. Šis prasības apmierina jebkuru mūsdienīgo datoru. Šī sistēma ir funkcionāla, stabila un droša. Taču ir viens mīnuss - tas ir maksas produkts, un dažiem maziem klientiem tas ir ļoti būtiski.

Windows 2000 - ir vienu paaudzi vecāka par Windows XP. Šī sistēma parasti tiek instalēta uz mazjaudīgiem datoriem, lai darba stacija strādātu ātrāk vai arī, ja dators ir licenzēts ar Windows 2000 un nav vajadzības pariet uz Windows XP, papildus maksājot. Sistēma kopumā ir droša un stabila.

Linux ir atvērta koda operētājsistēma, kuras galvenais pluss ir tas, ka tā ir bezmaksas , bet galvenais trūkums ir tās nepopularitāte ikdienas parasto lietotāju izmantošanā. Cilvēki negrib mācīties kaut ko no jauna jau ierastās Windows operētājsistēmas vietā. Linux var labi kalpot tādiem lietotājiem, kā termināla pieslēguma dators, kas ļauj stādāt ar Windows serveriem ierastā vidē.

Darbā aprakstītajās shēmās darba stacijām tika izvelētas gan Windows XP, gan Linux operētājsistēmas.

1.2 Serveri

Serveri ir funkcionālie datoru tīkla bloki (dators, stacija), kas nodrošina citām tā stacijām koplietošanas pakalpojumus (piemēram, datņu serveris, drukas serveris) [2]. Viena servera stacija var nodrošināt vairākus pakalpojumus. Pakalpojumu izvēle tiek noteikta ar prasībām un klienta vajadzībām. Es aplūkošu populārākos no tiem - failu serveri, drukas serveri, kā arī terminālu.

1.2.1 Failu serveris

Datus labāk glabāt vienā vietā, jo:

1. ir vieglāk tos administrēt un noteikt pieejas tiesības;
2. rezervēšanas darbus ir vieglāk izplānot un veikt, ja dati atrodas vienā vietā;
3. šos datus vienlaicīgi spēj izmatot daudzi lietotāji.

Lai to veiktu ir vajadzīgs failu serveris. Failu serveris piedāvā sistēmas drošību, limitējot pieeju failiem, lietotajiem vai lietotāju grupām (lielās organizācijas šis uzdevums ir attiecināts uz direktoriju servisiem, tādiem kā Novell's e Directory vai Microsoft Active Directory). Pie tam datņu serveris ļauj veikt monitoringu failu izmantošanai. Pastāv tāda iespēja, ka var uzlikt disku kvotas, lai limitētu direktoriju izmērus, piemēram, neļaut lietotājam rakstīt savā privāta direktorija vairāk par 10 Gb, kā arī brīdināt to, ja viņš tomēr sasniedza to izmēru. Dažas sistēmas var neļaut lietotājiem rakstīt noteikta tipa datus uz datņu servera, piemēram, mūziku vai filmas. Pie tam, kā jau iepriekš teikts, ka, ja visi svarīgākie firmas dati glabājas vienā vietā, tos var vieglāk rezervēt, un ar to domāts arī atgriezt kādas kļūdas dēļ. To būtu daudz grūtāk izdarīt, ja visi dati nebūtu centralizēti. Informācijas centralizēšana ļauj viegli apmainīties ar datiem un ātri meklēt vajadzīgo informāciju. Tā ir neaizstājama lieta ofisu datortīklos.

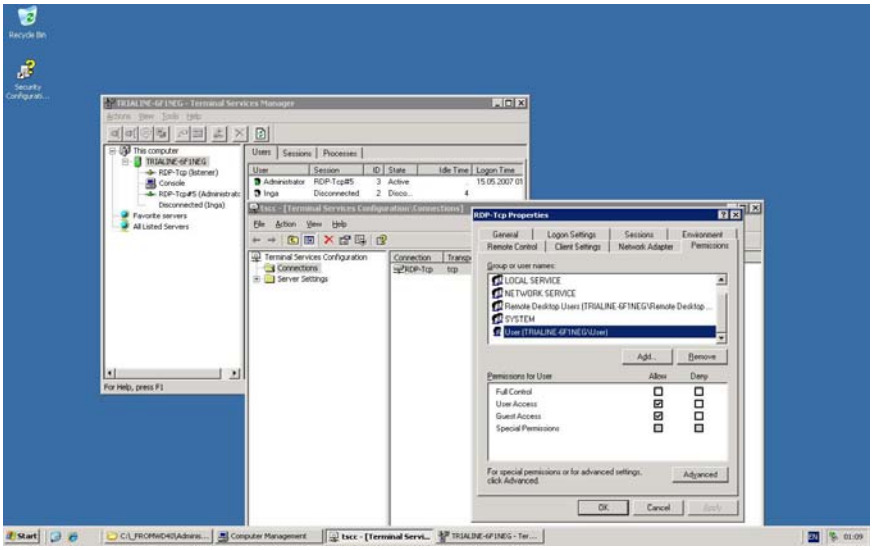
1.2.2 Drukas serveris

Ja mums ir nepieciešamība centralizēt drukas risinājums, tad mums jātaisa drukas serveri. Tas ļauj visiem tīkla lietotājiem izmantot vienu noteiktu printeri un tādā veidā nav vajadzības pirkt daudz printeru. Tas pieņem drukāšanas darbus no arējiem datoriem, kuri ir savienoti ar to, un kuriem ir tiesības uz drukāšanu, un pēc tam sūta uz pievienoto printeri. Par drukas serveri parasti izmantosim mūsu tīkla serveri, bet dažreiz par printera serveri var izmantot atsevišķu ierīci gadījumos, ja negribam izmantot servera resursus vai, ja servera izvietošana nav ērta priekš printera izvietošanas. Par drukas serveri vēl var kļūt jebkurš dators tīklā, kurām ir pievienots dators.

1.2.3 Terminmāls

Ja mēs saskaramies ar tādu situāciju, kad darba stacijas ir ar maziem resursiem, vai, piemēram, mums ir cita operētājsistēma (nevis Microsoft Windows), mēs varam izdarīt tā, lai lietotāji strādātu fiziski uz servera (lietotu nepieciešamas programmas un aplikācijas, kas ir uzinstalētas uz termināļa), bet savas darba stacijas izmantotu tikai kā pieslēgšanās un manipulēšanas ierīces. Lai to paveiktu, Windows Server 2000 un 2003 ir tāds dienests, kā terminmāls. Aktivizējam šo iespēju, taisām lietotājus un pieejas tiesības, izveidojam lietošanas tiesības un mēs varam pieslēgties un strādāt uz servera, nepatērējot daudz mūsu darba stacijas resursus. Pie tam mēs varam izmantot šo iespēju ne tikai no darba stacijām aprīkotām MS Windows operētājsistēmu, bet arī Linux.

Mūsu piemērās shēma bija uzstādīts Windows Server 2003 terminmāls.



1.2.1. att. Terminmāls

1.2.4 OS izvēle

Lai veiktu datņu serveri un drukāšanas darbus mums nevajag instalēt īpašo serveru operētājsistēmu. Mēs pilnīgi varām iztikt ar Windows 2000, XP. Protams, ir jādomā arī par to, ka Windows 2000, XP neļauj vairāk par 10 saiknēm ar to mašīnu, uz kuru tas ir uzstādīts. Gadījumos, kad mums jārūpējas par lielāko skaitu lietotāju, kuri izmanto serveri un arī gadījumos, kad ir vajadzīgs terminmāls, mums jāizmanto MS Windows Server 2000 vai 2003 operētājsistēmas, kur šī iespēja ir implementēta. Pie tam šī sistēma ir daudz funkcionālāka nekā failu serveris, drukas serveris jeb terminmāls, bet to citas funkcijas mēs neapskatīsim šajā darbā.

Serveriem labs risinājums ir Linux/Unix operētājsistēmas. Mūsu gadījumā mēs to neapskatīsim sīkāk, jo parasti mazos ofisos serveri arī papildus kalpo, kā darba stacijas, un darba staciju operētājsistēmas izvēle tika apskatīta darbu staciju sadaļā.

Lai paradītu termināla darbību par, piemēra, tīkla servera operētājsistēmu, bija izvēlēts Windows 2003, uz kura tika nokonfigurēts failu serveris, drukas serveris, un terminmāls. Visiem servisiem bija nokonfigurētas pieejas tiesības.

1.3 LAN

Apskatot iepriekšējās nodaļas, mēs apskatījām risinājumus tikai dažam prasības, pie tam atsevišķā veidā, bet tagad apskatīsim to, kā to visu panākt strādāt kopā, un tātad apmierināt prasību par lokālo tīklo izveidi kā tādu.

1. att. paradīta fiziska tīkla struktūra, jeb kopēja izstrādāta shēma. Ejot no kreisas puses uz labo, ir redzams Firewall jeb ugunsmūris. To galvenais uzdevums ir atļaut vai aizliegt datu saites (mūsu gadījumā ar Internetu), vadoties pēc firmas uzstādītas aizsardzības. Tam jābūt nokonfigurētam Internet jeb Wan ieejas punktā, kurš parasti ir maršrutētājs. Maršrutētājs ir nākošais elements shēmā un veic datu maršrutizēšanu un pieņem lēmumus par pakešu sūtīšanu to adresātam, kā arī maršrutizēšanas ceļu. Maršrutizēšana būs aprakstīta nākošajā dokumentācijas daļa.

Tālāk mūsu shēmā ir komutators (Switch), kura galvenais uzdevums ir savienot datortīkla mezglus vienā segmenta ietvaros. To parasti izmanto, lai datortīklā ieslēgtu vairākus datorus. Ja maršrutētājā ir vairāki pieslēgšanas porti, kuru skaits ir lielāks vai vienāds ar datoru skaitu mūsu tīklā, tad komutators nav nepieciešams.

Tālāk mūsu shēma ir darba stacijas jeb paši datori, uz kuriem strādā lietotāji. Pēc tam mūsu shēmā parādās serveris jeb dators, kurš strādā vienmēr un dara kādu no viņam uzliktiem servera darbiem. Šos datora resursus un darbības izmanto visās darba stacijās mūsu tīklā.

Mums parādās arī bezvadu risinājumi, kuri arī ir tīklā daļa un tas ir domātas tādās pašas darba stacijās, kas bija minētas iepriekš, tikai tie ir savienoti nevis ar vadu palīdzību, bet ar bezvadu tikla iespējām. Sīkāk par bezvadu tikliem būs pastāstīts tālāk dokumentācijā.

Tātad no shēmas ir redzams, ka lokālais tīkls ir pieslēgts pie Interneta caur maršrutētāju, kurš parasti arī kalpo kā ugunsmūris. Tālāk pie maršrutētāja ir pieslēgts komutators, no kura vadi iet uz visām darbā stacijām, tai skaitā arī serveri. Kā viena no iespējam pastāv arī bezvadu risinājums, kurā parasti tiek izmantots maršrutētājs, kurš aprīkots ar bezvadu tīkla ierīcēm, caur kuru darba stacijas, kuras ir aprīkotas ar bezvadu tīkla kartēm, pieslēdzas pie lokāla tīkla, un pēc tam caur to Internetam.

Šajā piemērā ugunsmūra, maršrutētāja, bezvadu signāla raidītāja, komutatora (ierīce ļauj pieslēgt četrus datorus, ja vajag vairāk, tad komutators būs atsevišķa ierīce) funkcijas ir apvienotas vienā ierīcē.

1.4 Wifi risinājumi

Mūsdienās populāri ir bezvadu tīkla risinājumi, kas pirmkārt attiecas uz tādām darba stacijām, kā portatīvajiem datoriem. Tieši tāpēc šī iespēja ir neatņemama daļa no mūsdienīga tīkla risinājuma. Parasti par bezvadu signāla raidītāju kalpo maršrutētājs. Visām darba stacijām jābūt aprīkotām ar bezvadu signālu uztvērēju, jeb bezvadu tīkla karti. Lai novērstu nesankcionētu pieeju tīklam caur viegli uztveramo bezvadu signālu, tiek veikti daži aizsardzības pasākumi un maršrutētāju uzstādījumi. Tie būs apskatīti "Drošības pasākumu aprakstā".

1.5 WAN

Viena no galvenajām prasībām klientiem ir Internēta pieslēgums katrai stacijai jeb izdarīt tā, lai katram darbiniekam būtu pieeja internetam. Lai to paveiktu, mums jāatrisina maršrutizēšanas jautājums.

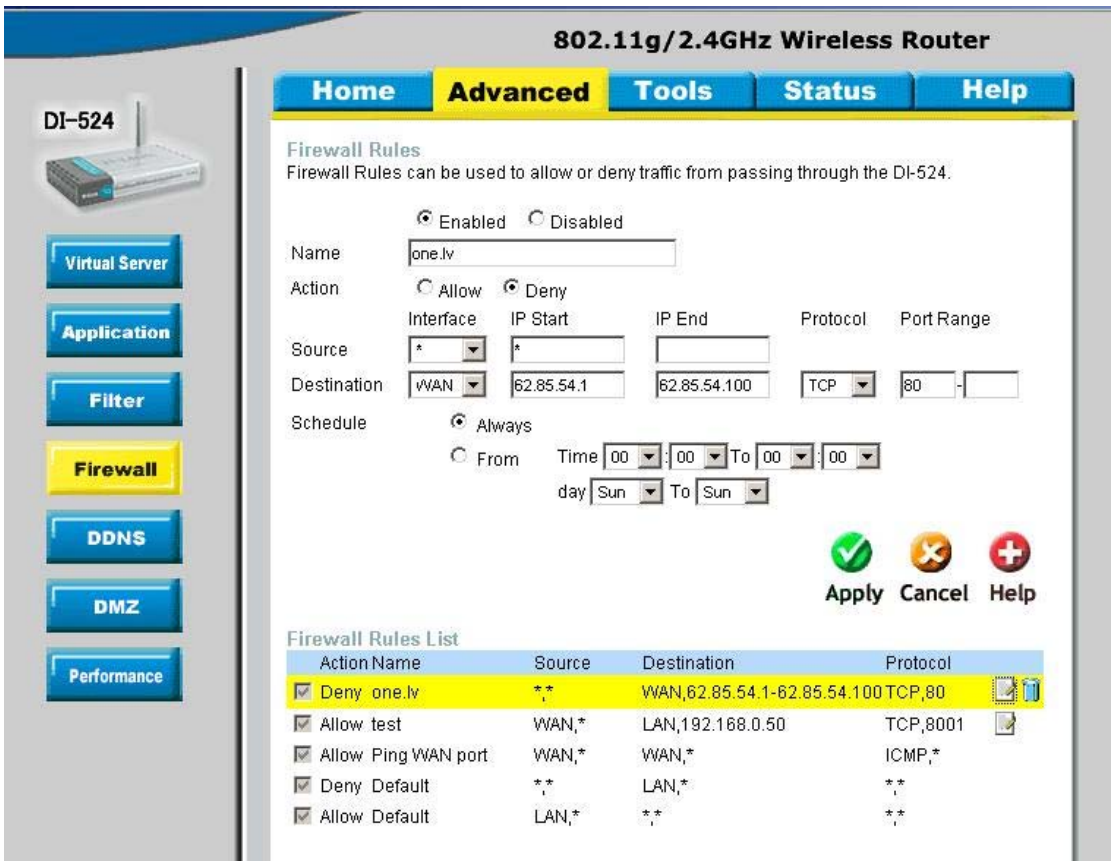
1.5.1 Maršrutizēšana

Maršrutizēšana ir informācijas ceļošanas maršruta noteikšanas process datortīklos. Tas tiek īstenots ar specialām ierīces, kurus sauc par maršrutētajiem. Tie palīdz samazināt tīkla noslogošanu, pateicoties to sadalīšanai kolīziju domēnos, ka arī pakešu filtrācijai. Pārsvarā tos izmanto apvienojot dažādu tipu tiklu apvienošanai, kas dažreiz nav savienojami pēc arhitektūras un protokoliem, piemērām ,(arī mūsu gadījumā) priekš lokālā tīkla Ethernet un globālā tīkla Wan apvienošanai. To izmanto arī priekš lokā tīkla pieejas globālajā tīklā (Internet), īstenojot adrešu translācijas un starptīklu ekrāna funkcijas [3]. Adrešu translācija jeb NAT (Network Address Translation) ir mehānisms TCP/IP tīklos, kas ļauj ekonomēt IP-adreses, translējot vairākus iekšējos IP-adresēs vienā publiskā IP-adresē (vai vairākos, bet mazāk nekā iekšējos). Tas arī izveido specifisko ugunsmūri, kas ļauj pasargāt un aprobežot arējos pieprasījumus pie iekšējām darba stacijām, bet neaprobežojot pieprasījumus no iekšas uz āru [4]. Maršrutētājs var būt gan speciala ierīce (pārsvara izmantots mūsu klientiem), kā arī dators, kurš izpilda vienkāršākās maršrutētāja funkcijas.

Mēs apskatīsim vienas ierīces konfigurēšanas iespējas, kuras parasti ir visos maršrutētajos un turpmāk visos risinājumos (ari ar cita veida maršrutētajiem) centīsimies izmantot tieši tādus uzstādījumus vai analoģiskus. Piemērās shēmas gadījumā tas ir atsevišķa ierīce D-Link DI-524.

Pārsvara mēs izmantosim parametrus pēc noklusēšanas, bet dažus vajadzēs pielabot klienta vajadzībām. Apskatīsim populārākos no tiem.

1. Firewall- ugunsmūris (aizliegumi pēc adresēm) – dažreiz uzņēmumā ir vajadzīga kontrole dažam adresēm un arī interneta pakalpojumiem. Piemēram, dažreiz vadība grib neļaut cilvēkiem uz darba darīt lietas, kuras neattiecas pie darba, piemēram, tērzēt (1.5.1 att.). Ugunsmūris ļauj mums atslēgt pieeju pie dažam saitēm, vai veidot pieslēgšanas noteikumus.



1.5.1. att. Aizliegums uz www.one.lv

2. DHCP (Dynamic Host Configuration Protocol) – tīkla protokols, kurš ļauj datoriem saņemt automātiski IP adreses un citus parametrus, kuri ir vajadzīgi darbā TCP/IP. Priekš tam dators griežas pie specialā servera, kurš saucas DHCP serveris (mūsu gadījumā tā funkcijas ir iebūvētas maršrutētājā). Tīkla administrators var uzdot adrešu diapazonu, kas ir izdotas starp datoriem. Tas ļauj apieties bez katra datora konfigurēšanas un samazina kļūdu skaitu [5].

3. Portu pāradresēšana- dažreiz mums vajag izmantot šo uzstādījumu, ja gribam pāradresēt kādu noteiktu portu uz noteikta datora portu. Mēs to iespēju izmantosim attālinātajai pieejai, kuru aprakstīsim sīkāk vienā no nākošām nodaļām.

Vēl ir daudz citu uzstādījumi, kuri būs aplūkoti nākošās nodaļas.

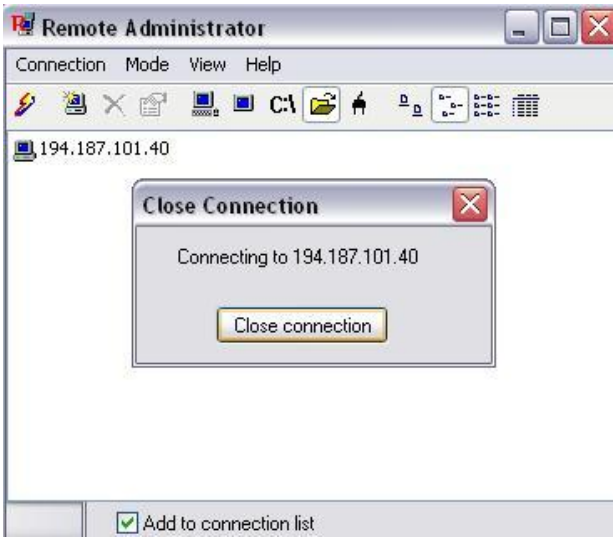
1.5.2 Attālināta pieeja

Dažreiz klientiem ir prasība, lai viņiem būtu iespēja strādāt ar savu darba datoru no mājām vai citām vietām. Lai to paveiktu, vajag izmantot attālinātu pieeju, kas savukārt ir arī labs veids tīkla administrēšanai un apkalpošanai neatrodoties ofisā. Realizējot to, ir nepieciešama portu pāradresēšana uz maršrutētāja, lai, pieslēdzoties caur noteiktu portu, mēs zinātu, pie kura datoru tīklā mēs savienojāmies, kā arī caur kuru dienestu. Pie tam, mums

vajadzētu izvēlēties dienestu, kuru izmantosim. Vai nu mēs izvēlēsimies Microsoft produktus kā Remote Desktop, jeb citu firmu produktus (Remote Administrator un citi). Dienestu izvēle ir atkarīga no noteikta uzdevuma, ko veic administrators vai lietotājs, kā arī vadoties pēc savām simpātijām noteiktiem produktiem. Bet parasti, lai nodrošinātu klientiem pieslēgumu no sava darba datora uz cita arējā datora, es izmantoju Remote Desktop, pirmkārt, jo tas klients ir iebūvēts MS Windows XP, kas savukārt ir viena no populārākajām operētājsistēmām, un klientam nav jādomā par programmatūru instalēšanu datorā no kura viņš pieslēdzas. Attālinātu pieeju ir ļoti ērti izmantot arī sniedzot konsultācijas un tehnisko apkalpošanu klientiem, jo, lai to paveiktu, tev nav jābūt uz vietas, klients var visu paskaidrot pa telefonu jeb citiem saziņas rīkiem par problēmu, un savukārt administrators var to paradīt jeb izdarīt noteiktu lietu neatrodoties pie paša datora. Lai to paveiktu parasti es izmantoju Remote Administrator programmatūru, kura ļauj pieslēgties attālinātam datoram un neizejot no sistēmas (log off), un veikt darbības, kuras būtu redzamas klientam.

Piemērā tika nokonfigurēts gan Remote Desktop (1.5.2. att.), gan Remote Administrator (1.5.3) lai paradītu klientiem tās atšķirības, priekšrocības un pašu darbību.

1.5.2. att. Remote Desktop



1.5.3. att. Remote Administrator

1.6 Dienestu ārpakalpojumi

Iepriekš netika aprunāti tādi speciāli gadījumi, kā Web mājas lapas izvietošana, e- pasta izmantošana, FTP un DNS (Domain Name Server). Šīs prasības SIA „Trialine" piedāvā kā atsevišķu pakalpojumu un prasti šī darbības netiek īstenotas uz klienta aprīkojuma, bet gan SIA „Trialine" aprīkojumā. Apskatīsim katru sīkāk.

1.6.1 Web mājas lapas izvietošana

Šis pakalpojumu sauc arī par hostingu. Ja klientam ir mājas lapa, tad parasti tā tiek izvietota uz SIA „Trialine" Linux serveriem, ar Apache Serveri un MySQL datu bāzēm. Tas ir darāms, sekojoši, ja šo mašīnu aprīkotu ar attiecīgu uzturēšanas programmatūru, ka arī paveiktu visus pasākumus, lai garantētu nepārtrauktu un drošu darbību visām mašīnām uz kuriem ir izvietota mājas lapa.

1.6.2 E- pasta izmantošana

Parasti ir apskatīti 2 veidi e-pasta izmantošanai:

1. Klienti grib izmantot Interneta e-pastu jeb web-mail
2. Klienti grib izmantot e-pastu ar savu domēnu jeb firmas nosaukumu

Pirmais veids ir tad, kad klients izmanto specialas interneta saites, kuras piedāvā tādu pakalpojumu, kā e-pasta kastītes izvietošanu (www.inbox.lv, www.gmail.com,). Tad, lai nodrošinātu to, ir tikai jānodrošinās interneta pieeju klientiem. Kā arī, ja tas ir iespējams, jānokonfigurē e – pastas klients (Outlook, Mozila Thunderbird, Lotus).

Otra veidā administratoram jānodrošina e-pastas klienta konfigurēšanu, lai savienotos ar e-pasta serveriem, kurus parasti arī nodrošina SIA „Trialine" darbinieki, izejot no tādām pašam domām kā mājas lapas izvietošanai, tātad serveri jau ir aprīkoti ar attiecīgo programmatūru un rīkiem e-pasta uzturēšanai, kā arī paveikti visi pasākumi lai garantētu nepārtrauktu un drošu darbību visām mašīnām, kur glabājas e- pasts.

1.6.3 FTP

FTP (File Transfer Protocol) jeb protokols, kas ļauj informāciju un failu apmaiņu internēta, var būt realizēts:

1. FTP ir ielikts kā viena no File servera direktorijam
2. FTP ir realizēts uz SIA „Trialine" serveriem

Pirmā veida realizēšanai tiek izmantots Microsoft IIS (tika realizēts piemērās shēmā).

Otrs veids var dažreiz garantēt stabilāku FTP darbību, kā arī piemērots tām firmām, kur failu serveris nav realizēts.

1.6.4 DNS

DNS ir domēnu vārdu sistēma internetā, kura asociē dažāda veida informāciju ar tā saucamiem domēnu vārdiem. Tā tulko cilvēka lasāmos datoru hosta vārdus uz IP adresēm, kas ir vajadzīgs informācijas nogādāšanai. Tā arī glabā informāciju, tādu kā e-pasta apmaiņas serveru sarakstu, kas pieņem e-pastus priekš dotā domēna [6]. Tātad mūsu globālajā tīklā ir piereģistrēts kāds vārds, piemēram, „trialine.lv", un tas nozīme, ka pieslēdzoties adresēm vai sūtot e-pastus nonāksim uz „trialine.lv" DNS servera, kurš savukārt nolems, kur pāradresēt saikni, no vārda, kas būs pirms „trialine.lv". Piemērām „jt.trialine.lv" tiek pāradresēts un ekvivalentu adresei 194.187.101.40. DNS ir realizēts SIA TRIALINE serveriem, tas ir darāms tā, ka šo mašīnu aprīkotu ar attiecīgu uzturēšanas programmatūru, kā arī tiktu paveikti visi pasākumi, lai garantētu nepārtrauktu un drošu darbību visām mašīnām uz kuriem ir ievietots DNS.

1.7 Konfigurāciju piemēri

Šajā apakšnodaļā būs apskatāmi divi piemēri no konfigurācijas viedokļa, ar kuriem nācās sastapties šī darba autoram. Šo piemēru firmu prasības ir kopumā vispopulārākās.

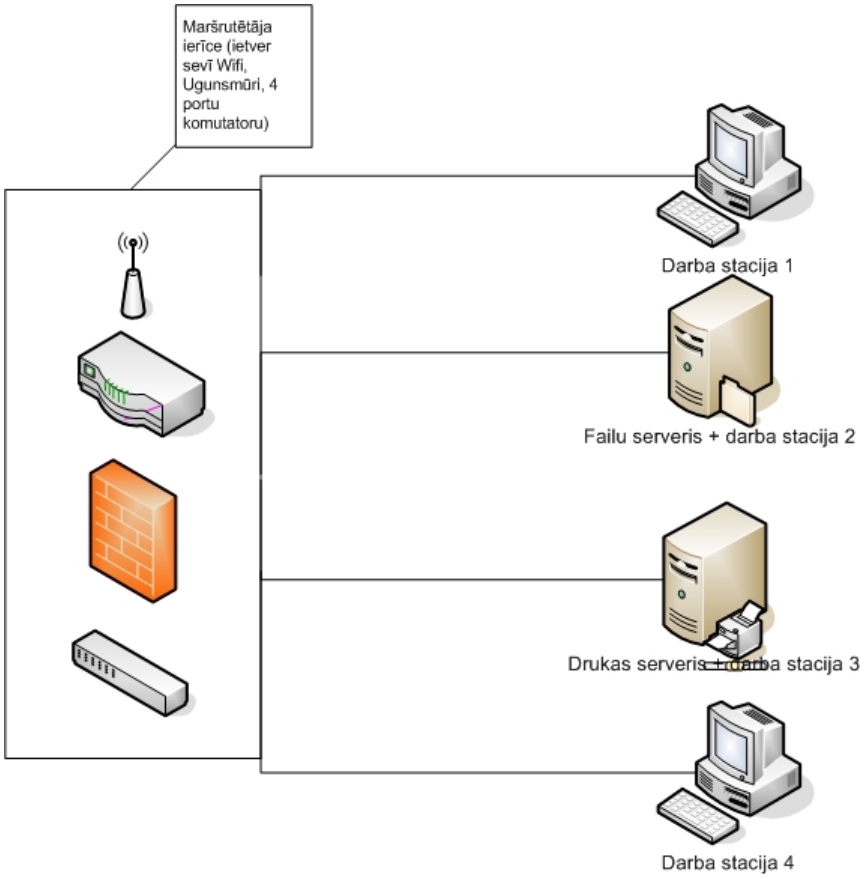
Firma A ir politiska organizācija, kura nodarbojas ar konferenču organizēšanu, kā arī citiem politiskiem jautājumiem.

Galvenās prasības:

1. iztaisīt datortīklu, kurā būtu viegli apmainīties ar informāciju, būtu vieta informācijas apskatīšanai visiem firmas darbiniekiem, kā arī vietas priekš katra darbinieka failiem, kuri būtu apskatāmi tikai viņam.
2. lai informācija nepazustu, kādu avāriju dēļ
3. būtu droša, no vīrusiem pasargātā darba vidē
4. būtu iespēja, lai partneriem, kuri atnāk uz viņu ofisu ciemos, būtu iespēja pievienoties Internētam ar bezvadu tīkla iespēja
5. Būtu iespēja drukāt uz viena printera

Esošais aprīkojums: 4 datori ar Windows XP operētājsistēmu.

Risinājums (1.7.1 att.): lai apvienotu datorus vienā tīkla, kā arī izvairītos no izveidojušas situācijas, kad internets tiek piegādāts pie katra datora ar atsevišķu maksu par katru kabeli interneta piegādātajam, un arī nepieciešamību bezvadu tīklu risinājumiem tika nolemts pirkt bezvadu maršrutētāju. Kuram tika pievienota viena interneta ieeja un arī nokonfigurētas DHCP iespējas, portu pāradresēšana (lai veiktu attālinātu pieeju tīklu uzturēšanai), un bezvadu tīkla iespējas ar WPA-PSK šifrēšanu (tas priekšrocības tiks apskatītas drošības pasākumu aprakstā). Atslēga tika iedota vienam firmas A darbiniekam. Lai apvienotu datus un veiktu rezerves kopijas tiem, tika izvelēts viens no datoriem, kurš tika izvēlēts par datņu serveri. Bija izveidota kopēja direktorija visiem lietotajiem, kā arī personīgās lietotāju direktorijas, kuras būtu pieejamas tikai konkrētam lietotājam. Dati tiek rezervēti uz cita datora pēc rezerves kopijas veidošanas plāna (aprakstīts tālāk). Vēl viens dators tika izvēlēts par drukas serveri, kuram tika pieslēgts printeris un citos tīkla datoros tika nokonfigurēta pieeja tam. Katra darba stacija tika nokonfigurēta attiecīgi ar drošības pasākumu aprakstu un aprīkota ar antivīrusu programmām. Lietotajiem tika piešķirtas tikai lietotāju tiesības. Administrēšanas darbs tika uzdots tīkla ierīkošanas firmas darbiniekiem.



1.7.1. att. Firmas A risinājums

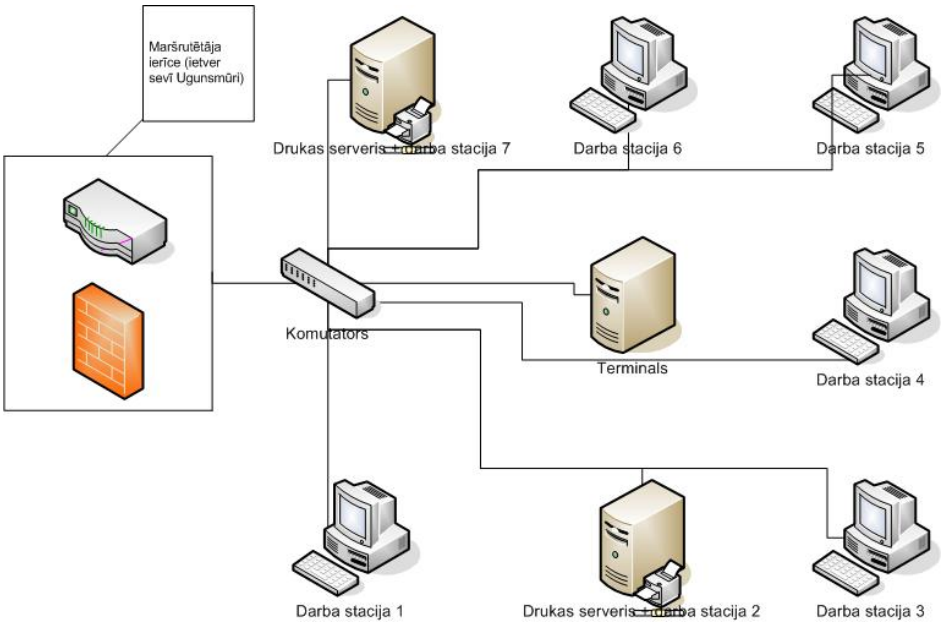
Firma B ir firma, kura nodarbojas ar žurnāla veidošanu.

Galvenās prasības:

1. uztaisīt datortīklu, kur būtu viegli apmainīties ar informāciju, būtu vieta informācijas apskatīšanai visiem firmas darbiniekiem, kā arī vieta priekš katra darbinieka failiem, kuri būtu apskatāmi tikai viņam
2. lai informācija nepazustu, kādu avāriju dēļ
3. būtu droša darba vidē
4. būtu iespēja drukāt uz viena vai vairākiem printeriem

Esošais aprīkojums: 7 mazjaudīgi datori ar Windows 95, 98 operētājsistēmām.

Risinājums (1.7.2. att.): lai apvienotu datorus vienā tīkla tika uzstādīts maršrutētājs, kuram tika pievienota viena interneta ieeja . Lai apvienotu datus un veiktu rezerves kopijas, ka arī paaugstinātu darba efektivitāti (lai firmas B darbinieki nestrādātu ar veciem datoriem un vecām operētājsistēmām), tika nolemts nopirkt un uzstādīt jaudīgu serveri ar termināla iespējam. Par izvelētu servera operētājsistēmu tika izvelēts Windows Server 2000. Serveris arī kalpo par datņu serveri. Bija izveidota kopēja direktorija visiem lietotajiem, kā arī personīgas lietotāju direktorijas, kuras būtu pieejamas tikai konkrētam lietotājam. Dati tiek rezervēti uz speciali ierīkota diskā pēc rezerves kopijas veidošanas plāna (aprakstīts tālāk). Vēl daži datori tika izvēlēti par drukas serveriem (vadoties pēc ērtāka izvietošanas principa), kuram tika pieslēgti printeri un nokonfigurēta pieeja tam. Katra darba stacija tika nokonfigurēta ar attiecīgu programmatūru lai pieslēgtos terminālim. Administrēšanas darbs tika uzdots tīkla ierīkošanas firmas darbiniekiem.



1.7.2. att. Firmas B risinājums

2. KVALITĀTES NODROŠINĀŠANAS PASĀKUMU APRAKSTS

Lai nodrošinātu kvalitāti tīkla apkalpošanai un konfigurēšanai bija uzstādīti daži pasākumi. Kuri savukārt dalās trīs stadijās:

1. Konfigurācijas testi pēc tīkla uzstādīšanas vai maiņas
2. Klientu apmācība
3. Tīkla uzturēšana un apkalpošana (Support)

Konfigurācijas testi pēc tīkla uzstādīšanas vai maiņas - ir testi, kuri ir veikti pēc tīkla uzstādīšanas vai konfigurācijas maiņās un pirms nodošanas ekspluatācijā. Ietver sevī katras darba stacijas un servera nepieciešamās programmatūras pareizas darbības testi, tīkla savienojumu testiem, pieejas tiesības testiem, perifērijas ierīču testi.

Klientu apmācība - ir tīkla kopējas struktūras lekcija, kura ir veikta katram darbiniekam, kā arī visu iespēju un tiesību paskaidrošana.

Tīkla uzturēšana un apkalpošana (Support) - ietver sevī tiešsaistes konsultācijas ar klientu un atbildes uz jautājumiem, kuri tiek veikti caur saziņas rīkiem (mobilais telefons, e-pasts) vai nu tiešo konsultāciju uz vietas, pie tam tas iekļauj sevī problēmu un trūkumu novēršanu. Problēmas un trūkumi sadalās divos veidos: tie, kurus atrod klients, vai tie, kuri ir noskaidroti ar nepieciešama monitoringa palīdzību. Tie tiek novērsti ar nepieciešamo klātbūtni jeb izmantojot attālināto pieeju. Tie klasificējas sekojoši:

1. Problēmas ar aparatūru (risināšanai nepieciešama klātbūtne)
2. Problēmas ar jaunam versijām un atjauninājumiem (parasti risināšanai nav nepieciešama klātbūtne, un viss darās attālināti , bet ir gadījumi, kad nepieciešama klātbūtne)
3. Trūkumi tīkla konfigurācijā (risināšanai bieži vien nepieciešama klātbūtne)
4. Jauno tīkla daļu un komponentu pievienošana (risināšanai bieži vien nepieciešama klātbūtne)

Monitorings ir neatņemama kvalitātes nodrošināšanas pasākums, kurš arī attiecas pie tīkla apkalpošanu. Monitoringu jāveic periodiski, izmantojot logus, kā arī specialas programmas. Logus jālasa ne retāk kā vienu reizi nedēļā.

Galvenais princips ir pēc iespējas vairāk izanalizēt un novērst kļūdas tīklā pirms nodošanas ekspluatācijā, bet, ja tomēr gadījās tā, ka tie tomēr tiek atrasti tīklam jau darbojoties, tad tos vajadzētu pēc iespējas ātrāk novērst.

Lai nodrošinātu kvalitāti jābūt arī datu rezervēšanas plānam, kurš ir parakstīts šajā darba, par to ir jābrīdina klients un jāpaskaidro to vajadzību. Ir jāveic pastāvīgo monitoringu rezervēšana procesam.

Piemēra shēma tika izveidota un strādā saskaņa ar kvalitātes nodrošināšanas plānu.

3. NEPĀRTRAUKTAS DARBĪBAS NODROŠINĀŠANA

Nepārtrauktu darbību nodrošina divas lietas:

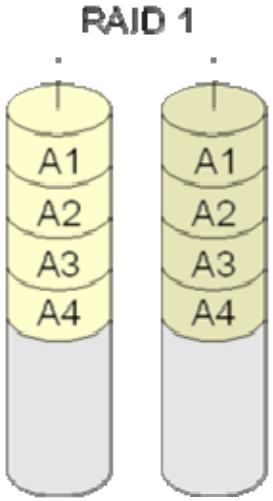
1. Datu nepārtrauktība - izmanto neatkarīgu disku redundantu kārtojumu (RAID), kas ļauj izmantot datus pat tad, kad viens no diskiem ir salūzis fiziski.

2. Barošanas nepārtrauktība – izmanto nepārtrauktas barošanas ierīces (UPS), kuras ļauj datoriem darboties kādu laiku pēc elektrības neparedzētas izslēgšanas, kā arī gadījumos, kad elektrība ir nestabila (sprieguma lēcieni un etc).

3.1 RAID

Ir specials gadījums, kad dati reālā laikā ir ļoti vajadzīgi, tad izmanto neatkarīgu disku redundantu kārtojumu (RAID). Izšķir dažus veidus, apskatīsim populārākos no tiem:

1. RAID 1 (Mirroring- „spogulis" 3.1.1 att.). Tā jēgā ir tāda, ka dati tiek rakstīti uzreiz 2-os diskos . Tas ir, ja viens salūzis, tad dati saglabāsies uz otra. Trūkums ir tajā, ka vajag maksāt 2 disku summu. To shēma ir paradīta zīmējumā.

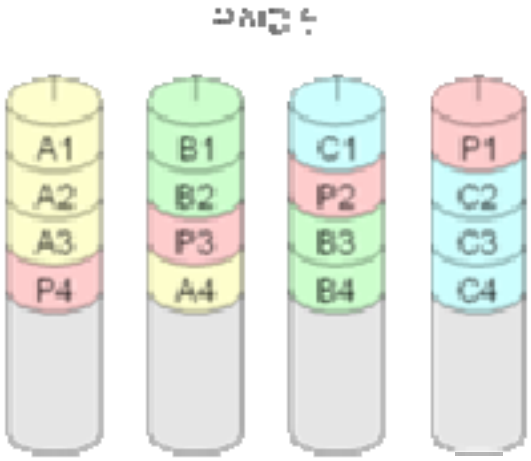


3.1.1. att RAID 1

2. RAID 5 (3.1.2 att.) – Vispopulārākais disku kārtojums, pirmkārt sava ekonomiskuma dēļ. Redundancei atdodot tikai viena diska ietilpību, mēs dabūjam aizsardzību pret jebkura diska izeju no ierindas. RAID 5 rakstīšanai tiek tērēti papildus resursi, kas tiek izmantoti papildus rēķiniem, bet lasīšana (salīdzinot ar vienu disku) ir ātrāka tāpēc, ka informācija tiek ņemta no vairākiem diskiem un tiek ņemta paralēli.

RAID 5 trūkums ir tāds, ka kad viens disks iziet no ierindas, viss kārtojums pāriet kritiskā režīmā, visas lasīšanas un rakstīšanas operācijas tiek veiktas ar papildus

manipulācijām, tāpēc strauji krīt ražotspēja, diski sāk karst. Ja savlaicīgi nepieņemtu mērus - var zaudēt visu kārtojumu [7].



3.1.2. att RAID 5

3.2 Nepārtrauktā barošana (UPS)

Nepārtrauktā barošana ir automātiska ierīce, kas ļauj aparatūrai funkcionēt kādu laiku no tās akumulatoriem, ja elektrība pazūd vai to parametri iziet no pieļaujamām normām. Pie tam, tas ļauj koriģēt barošanas parametrus (spriegumu, frekvenci).

Ir trīs nepārtrauktas barošanas shēmas:

Rezerves- kas tiek izmantots personālo datoru vai lokālo tīklu darbu staciju barošanai. Kad barošana iziet no normām vai tas vienkārši nav, automātiski pārslēdz slodzi uz akumulatoru barošanu. Parādoties normālam spriegumam atkal pārslēdz barošanu no tīkla. Šāda veida barošanas trūkumi ir nesinusoidālā izeja un samēra ilgs pārslēgšanas laiks uz barošanu no baterijas.

Interaktīvais – tas pats kā rezerves, bet vēl ieeja ir pakāpjveidīgais sprieguma stabilizators, kas ļauj dabūt sinusoidālas formas spriegumu.

Tiešsaistes- tiek izmantots failu serveru un lokālo tīklu darba staciju, kā arī cita veida aparatūrai, kurai ir paaugstināti pieprasījumi pie tīkla elektrobarošanas kvalitātes, barošanai. Darba princips: vispirms ieejas maiņas spriegums tiek pārveidots līdzstrāvā, un pēc tam atkal maiņas strāvā ar invertora palīdzību.

Dažas nepārtrauktas barošanas iekārtas ļauj padot datoram informāciju par savu stāvokļi, izmantojot noteikto programmatūru, izanalizējot situāciju, ļauj izslēgt datoru, apstādinot visu programmu darbību [8].

Parasti tiek izmantota klientiem, kuru ofisi atrodas sliktas elektrības zonās. Kā arī klientiem, kuri ir interesēti lai viņu dators pēkšņi neizslēgsies, un to rezultāta varētu zaudēt kādu daļu informācijas. Ir vērts izmantot serveriem

4. REZERVES KOPIJU VEIDOŠANAS PLĀNS

Rezerves kopijas veidošana ir neatņemams administratora darbs. Tajā tiek iekļauts gan neatkarīgu disku redundants kārtojuma RAID izveide (ja to ļauj aparatūra), gan datu rezerves kopijas izveide jeb backup, kuros mēs varam glābāt datus, kas bija dienu, nedēļu, mēnesi vai pat vairāk atpakaļ. Lai noteiktu kā mēs veidosim un īstenosim savu rezerves kopiju plānu, mums jānoteic cik svarīgi ir dati un kā tos izmantos. Mums jāparedz kādos gadījumos tiks izmantotas rezerves kopijas. Šī pieeja ir ļoti individuāla, tāpēc apskatīsim vispopulārāko plāno, kas ir parasti izmantots mūsu klientiem.

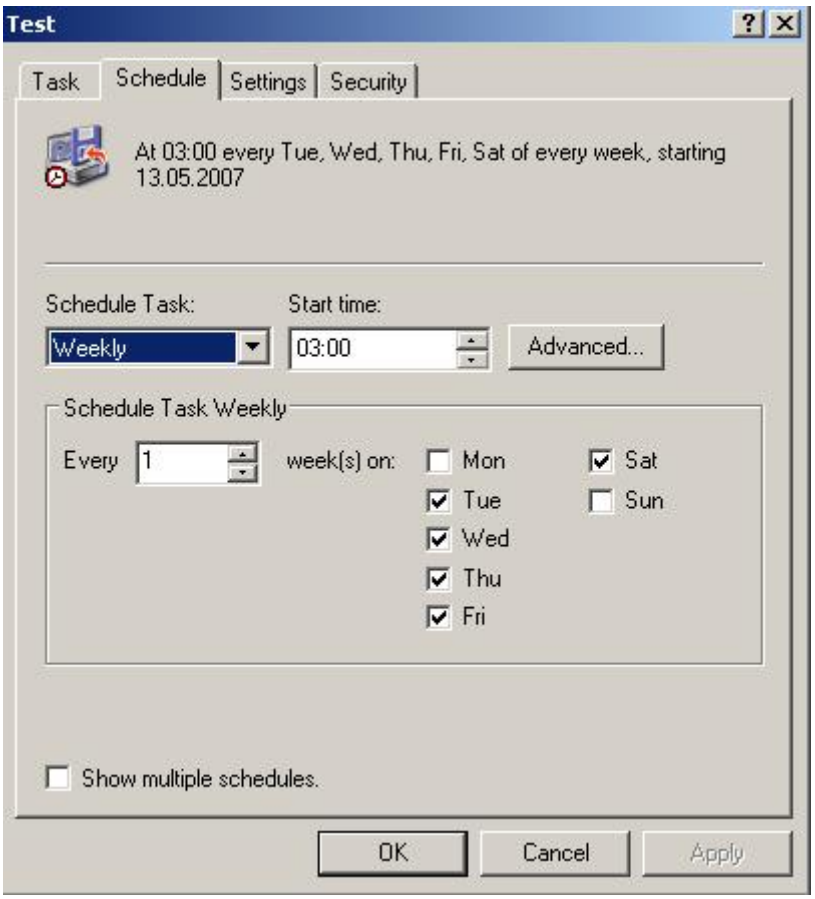
4.1 Datu rezervēšanas plāns

Rezerves kopijas tiek veidotas uz citiem datoriem tīklā. Parasti tie veidojas naktī vai brīvdienas, kad tīkls ir mazāk noslogots. Datu rezervēšanas plāns ir sekojošs:

1. Izmantoti dati uz datņu servera ir rezervēti katru darba dienu ar dziļumu - viena nedēļa. Tas nozīmes, ka tiks izveidotas 5 vai 6 rezerves kopijas, kuras atbildes katrs par savu dienu. Un tie pārrakstīsies tikai pēc nedēļas. Šāds plāns mums ļauj atgriezt jebkurus datus nedēļās garumā, t.i. ja mēs kaut ko esam sabojājuši pirmdienā, bet pamanījuši tikai piektdien mēs bez problēmām varām to atgriezt no pagājušās piektdienas rezerves kopijas. Rezerves kopijas tiek veidotās katrā darba dienas naktī 3.00 vai 4.00, kad darbinieki parasti nestrādā.
2. Katra datora un servera sistēmas datiem ir arī jāveido rezerves kopijas, lai, ja rastos kāda kļūda, sistēmu varētu atgriezt tajā stāvoklī, kad tā strādāja. Mēs piedāvājam to veikt reizi divos nedēļās, arī naktī un darīt to tajā laikā, lai tas nesakristu ar datu rezervēšanu, tātad labāk to veikt brīvdienās naktī.

4.2 Realizācija

Tā kā pārsvarā mūsu tīklu visas darba stacijas un serveris ir uz Windows platformas, tad rezerves kopijas veidošanai izmantosim iebūvēto rīku, kurš saucas backup (4.2. att.). Tas mums ļauj veidot izvēlēties kāda veida informāciju saglabāt, kur, kā arī kad. Parasti mēs izvēlāmies datus, kurus jāsaglabā, vietu uz cita datora, jeb diska, ka arī taisām uzdevumus, kad sākt rezervēšanu.



4.2. att. Backup

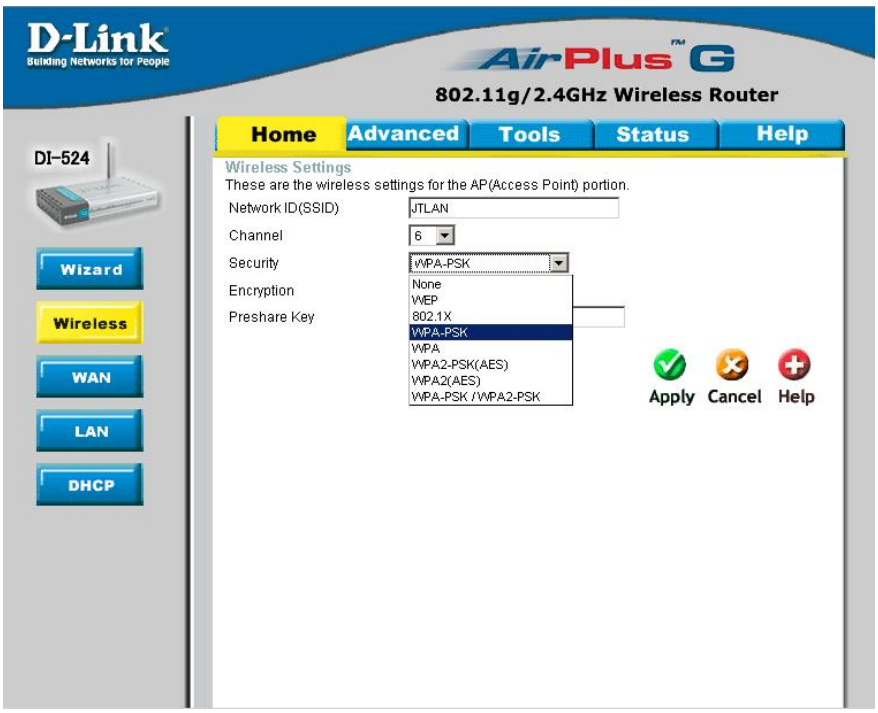
5. DROŠĪBAS PASĀKUMU APRAKSTS

5.1. Maršrutētājs

Saksim ar piejās tiesībām maršrutētajam. Saksim ar to, ka maršrutētam obligāti jāsamaina paroli (jo parasti pēc noklusēšanas paroli ir uzstādīti pēc vienas shēmas, un tos var viegli uzminēt). Pie tam būtu labi ja pieeja maršrutētajam tiktu nokonfigurēta tikai noteiktajiem IP adresēm, jeb labāk (tas ari īstenots parasti TRIALINE drošības plāna) pieeja tikai noteiktajiem datoriem (pieeja pēc MAC adresēm). Tas ir īpaši efektīvs drošības pasākums bezvadu tīkla aizsardzībai.

Runājot par pašu maršrutētāju, vēl jāatzīmē, kā bezvadu tīklam signālu, lai būtu maksimāli drošāk, vajag šifrēt (5.1.1 att.). Pirmais un visvieglākais šifrēšanas veids ir WEP protokolu izmantošana (Wired Equivalence Privacy), kurs ļauj pievienoties tādai pat aizsardzībai, kā izmantojot vadu tīklus. Izmantojot WEP šifrēšanu vajag, lai visos pieslēguma punktos būtu izmantotas identiskas atslēgas. Jo garāka ir atslēga, jo grūtāk to atšifrēt. Modernas bezvadu ierīces izmanto 64- bitu, 128- bitu un 256- bitu atslēgas.

128- bitu atslēga – tas ir 13 simboli ASCII formātā, bet 64- bitu atslēga- tas ir 5 simboli. Parasti tiek izmantoti 128-bitu vai 256- bitu atslēgas. Mūsdienīgā aprīkojumā mēs varam ierakstīt līdz 4 WEP atslēgām un izvelēties aktīvo pēc saskaņas ar klientu. Piemēram, vienu katru nedēļu. Izveidojot šīs atslēgas maršrutētājā, vajag ierakstīt tos arī darba stacijās.



5.1.1 att. Šifrēšanas veidi.

Bet ir iespēja, kura nepieprasa nekādu atslēgu ieviešanu. Iekārtas, kuras atbalsta 802.11g protokolu var izmantot vairāk progresīvo šifrēšanas metodi- WPA (Wi-Fi Protected Access). Tas standarts apvieno divas metodes- TKIP un MIC.

TKIP šifrēšanas metodes jēgā ir tā, ka 128- bitu atslēgas tiek ģenerētas katrai 10 kilobaitu datu sūtīšanai. Kopējais atslēgu skaits tiek skaitīts vairākos miljardos. Tas nozīme, ka, piemēram, priekš 5 megabaitu failu sūtīšanai, trafiks būs sašifrēts ar 512 atslēgu izmantošanu, katrs no tiem ir 13 simbolu garumā. Tāda sistēma dod augstas garantijas no datu atšifrēšanas un pārtveršanas. Pie tam, specialais algoritms MIC (Message Integrity Check) pārbauda atsūtītos un saņemtos datus, lai izslēgtu gadījumu, kad tie var mainīties ceļā. Hakeris vairs nevarēs iebūvēt kaitīgus kodus jūsu datos atsūtīšanas ceļā.

Standarts WPA protokols pieprasa RADIUS servera uzstādīšanu, kas nav pieņemams mazo ofisu tīklos. Tāpēc izmantosim vairāk parastāku režīmu WPA-PSK, kas atbalsta agrāk izveidotas atslēgas (Pre-Shared Keys). Šī atslēga, kā atslēga WEP režīmā, tiek uzdota uz visam darba stacijām un maršrutētājā, lai nodrošināt pirmējo staciju identifikāciju. Darba stacijās arī tiek izvēlēts TKIP šifrēšanas veids, un autentifikācijas metode WPA PSK. Šīs šifrēšanas veids tiek uzskatīts visdrošāko aizsardzību pret hakeriem un ir uzstādīts piemērās shēmā [9].

Uzliksim ugunsmūra vajadzīgos uzstādījumus un pieejas noteikumus, kurus jau organizēsim pēc katra klienta vajadzībām. Tagad padomāsim par filtriem ar kuriem varētu aprobežot un padarīt mūsu tīklu drošāku. Vispirms mēs varām aprobežot pieeju dažam adresēm, kuri pēc mūsu domam varētu būt nedroši. Aizliegt dažu portu izmantošanu, tāda veidā bloķējot dažus mums nevajadzīgus dienestus vai servisus.

Par vienu no aizsarglīdzekļiem no interneta uzbrukumiem var pieminēt NAT, kurš bija aprakstīts WAN sadaļā, un parasti ir katrā maršrutētājā.

5.2 Piekļuves tiesībās

Tagad apskatīsim piekļuves tiesības mūsu tīklā. Izdalīsim divas lietotāju grupas.

1. Administrators
2. Lietotājs

Administratora tiesības ir neierobežotas. Tas ir cilvēks, kurš konfigurē tīklu un visas tiesības, kā arī veic sistēmas monitoringu, tāpēc viņam ir tiesības uz konfigurēšanu, lietotāju pārvaldību, jaunu programmatūru instalēšanai un resursu neaprobežotai pieejai un citām darbībām. Tagad apskatīsim katru no aprakstītam tiesībām no drošības viedokļa, kā administratora funkcijas.

1. Konfigurēšana- tīkla konfigurēšana un arī operētājsistēmas konfigurēšanu ir labāk nodot profesionāļa rokās, un aizliegt lietotājam konfigurēt lietas, kuras drīkst konfigurēt tikai profesionālis, tādā veidā pasargājot tīklu no veiktspējas zaudēšanas neprofesionālas attieksmes dēļ.
2. Lietotāju pārvaldība- viens no svarīgākiem uzdevumiem ir reģistrēt lietotājus. Domāt par to kādas rīcības būs atļautas lietotājam, kā arī kādi resursi un dati būs pieejami lietotājam un arī attiecīgi izveidot lietotāja profili. Vēl šeit var pieminēt paroles pārvaldību un izveidošanas noteikumus.
3. Jaunu programmatūru instalēšana- tā ir svarīga daļa. Ir pareizi, kad programmatūru var instalēt tikai administrators, jo tas, pirmkārt, palīdz nošķirt, kuras programmas ir vajadzīgas un kuras ne (jo lietotāji parasti instalē un pēc tam domā, ko viņi ir uzinstalējuši un vai tas viņiem ir vajadzīgs), otrkārt, tas pasargā sistēmu no netīšas programma uzinstalēšanas, kā arī pasargā no vīrusiem. Jo dažas programmas var uzinstalēties netīšam, īpaši pārlūkojot internētu. Ka arī, ja paskatīties no tā viedokļa, ka vīrusi arī ir programmas, tad programmu instalēšanas aizliegumi palīdz cīnīties arī ar tiem.
4. Resursu neaprobežotai pieeja- ļauj kontrolēt informācijas saturu, lai tīklā nebūtu kādi pretlikumīgi materiāli, autortiesību pārkāpumi un t.t. Tas ļauj regulēt un uzlikt kvotas informācijas plūsmai, šķirot informāciju vajadzības pakāpumos, lai resursu izbeigšanas gadījumos varētu izveidot plānu informācijas samazināšanai un t.t.
5. Sistēmas monitorings- administratora tiešais pienākums ir sekot izmaiņām tīkla, analizēt, kas ir noticis, lai varētu laicīgi novērstu kaut kādu problēmu, ja tā rodas, kā arī kontrolēt visas citas lietotāju darbības un atdalīt tās, kuras ir bīstamas tīklu drošībai. Parasti monitorings ir veikts caur specialo programmatūru jeb operētājsistēmu - tā saucamajos žurnālos, kuros ir visāda veida informācija, ko raksta sistēma. Administratora uzdevums ir arī pārdomāt kāda veida informāciju vajag rakstīt žurnālos, lai nodrošinātu tīkla normālo darbību un drošību.

Lietotāji ir cilvēki, kuri lieto tīklu, bet viņiem parasti nav jārūpējas par to darbspēju un drošību tāpēc, ka tas ir administratora darbs. Dažreiz lietotāji var netīšam izdarīt darbību, kas varētu apdraudēt tīklu drošumu. Tāpēc vajag lietotājiem aprobežot tiesības. Vēl vajag izdarīt piekļuves aprobežošanu, lai viens lietotājs nevarētu piekļūt cita dokumentiem, kā arī direktorijām, kurām tam nevajadzētu būt, kā arī radītu personīgus privātus datus.

SECINĀJUMI

Darbā laika tika izveidota un aprakstīta tīkla kopēja shēma, kur tika paskaidrots katra tīkla sastāvdaļa un konfigurācijas iespējas, administrēšanas darbi, kuri ir veicami, lai atbalstītu tīklu pareizu un drošu darbu. Iepazīstoties ar šo shēmu, katrs SIA "Trialine" klients var secināt, kas viņam ir vajadzīgs un kas nē, un balstoties uz izvēlēto, tiks veikt noteiktais tīkla risinājums, un arī administrēšanas darbs. Darba autors izstrādāja kopējo shēmu SIA "Trialine" uzņēmumā lai katrs klients var iepazīt to darbu praksē, un veikt savējos secinājumus. Shēma ir ieviesta darbībā un ir pilnīgi realizēta. Administrēšanas darbs ir uzlikts uz šī darba autora. Tīkls strādā droši un veic uzliktos tam uzdevumus. Tīkla konfigurācija ļauj to attīstīt, parādoties jaunām vajadzībām.

IZMANTOTĀ LITERATŪRA UN AVOTI

1. *Операционные системы MS WINDOWS* [tiešsaiste] – Pieejams: http://www.alta.ru/windows.php
2. *Server* [tiešsaiste]– [atsauce 03.09.1993]. Pieejams: http://termini.lv
3. *Маршрутизатор* [tiešsaiste]– [atsauce 23.04.2007.]. Pieejams: http://ru.wikipedia.org/wiki/Маршрутизатор
4. *NAT* [tiešsaiste]– [atsauce 09.04.2007.]. Pieejams: http://ru.wikipedia.org/wiki/NAT
5. *DHCP* [tiešsaiste]– [atsauce 07.05.2007.]. Pieejams: http://ru.wikipedia.org/wiki/DHCP
6. *Domain name system* [tiešsaiste]– [atsauce 07.05.2007.]. Pieejams: http://en.wikipedia.org/wiki/DNS
7. *RAID* [tiešsaiste]– [atsauce 25.05.2007.]. Pieejams: *http://ru.wikipedia.org/wiki/RAID*
8. *Источник бесперебойного питания* [tiešsaiste] – [atsauce 06.04.2007.]. Pieejams: http://ru.wikipedia.org/wiki/Источник_бесперебойного_питания
9. *Настраиваем безопасность беспроводной сети Wi-Fi* [tiešsaiste] – [atsauce 06.07.2005.]. Pieejams: http://www.hardwareportal.ru/Network/Wlan.security/index.html

Kvalifikācijas darbs „Mazo ofisu tīkla risinājumi” 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: Jurijs Tomilovs

Rekomendēju darbu aizstāvēšanai

Vadītāja: Mag. Sc. Comp. Jānis Judrups

Recenzents:

Darbs iesniegts Datorikas nodaļā _____.

Metodiķe:

Darbs aizstāvēts kvalifikācijas gala pārbaudījuma komisijas sēdē

_____ prot. Nr. , vērtējums

Komisijas sekretāre: