ŠIAULIŲ UNIVERSITETAS

MATEMATIKOS IR INFORMATIKOS FAKULTETAS

INFORMATIKOS KATEDRA

Mindaugas Legeckas
Informatikos specialybės II kurso dieninio skyriaus studentas

TARNYBINĖS STOTIES APKROVOS TYRIMAS

SERVER'S LOAD TESTING

MAGISTRO DARBAS

Darbo vadovas:
Prof. L Sakalauskas

Recenzentas:
Lekt. L. Kaklauskas

Šiauliai, 2009

Tvirtinu, jog darbe pateikta medžiaga nėra plagijuota ir paruošta naudojant literatūros sąraše pateiktus informacinius šaltinius bei savo tyrimų duomenis.

Darbo autorius Mindaugas Legeckas .....

(parašas)

TURINYS

I. ĮVADAS

Temos aktualumas ir svarba

Kadangi informacijos srautai šiuolaikiniuose tinkluose pasižymi didele sparta ir kintamumu, šių srautų detali analizė yra aktuali problema. Šios analizės rezultatai gali būti panaudoti tinklo aptarnavimo kokybei QoS (Quality of Service – Paslaugos kokybė) vertinti ir valdymo sprendimams priimti. Šiame darbe nagrinėjama programinė įranga, skirta tirti srautų dinamiką ir padėti administratoriui (toliau vartotojas) aptikti lokaliame tinkle įsilaužimus, šiukšles, perkrovas, gedimus.

Praktinis temos aktualumas

Vartotojas, gavęs informaciją apie išanalizuotus srautus, gali įvertinti tinklo aptarnavimo kokybę ir priimti atitinkamus sprendimus.

Problemos aiškumas ir tikslas

Yra žinoma daug tinklapių bei programinės įrangos, skirtos tinklų analizei. Tačiau ši įranga yra labiau integruota į TVS (Turinio Valdymo Sistemas), pvz. „PHP Fussion“, „Mambo server“, arba CRM (Customer Relationship Management – santykių su klientais valdymas). Todėl yra reikalingas įrankis, kuris galėtų paprastai ir nesunkiai suteikti tinklo informaciją, dirbant paprastoje tinklapio sąsajoje. Dauguma tokių programų yra sudėtingos, nes norint išmokti ir dirbti su jomis, reikia papildomai skirti nemažai laiko.

Šiame darbe kuriama sąsaja yra paprastas ir patogus įrankis interneto srautams tirti.

Darbo tikslas

Panaudojant „PHP“ programavimo kalbą, sukurti nesudėtingą ir lengvai suprantamą vartotojo sąsają, kurią būtų galima pritaikyti tarnybinės stoties srautų analizei.

Darbo uždaviniai:

Sukuriant sąsają, iškelti tokie uždaviniai:

- Panaudoti „Wireshark“ programą srautams registruoti;
- Sukurti sąsają eksportuotų srautų įkėlimui į duomenų bazę;
- Ištirti tarnybinės stoties paslaugų tiekimo sistemos struktūrą, jos pagrindinius elementus;
- Sukurti lankstų ir nesudėtingą vartotojo požiūriu sąsają, srautų analizei sistemoje;
- Sukurti sistemą, funkcionuojančią kliento – serverio architektūroje;
- Parengti sistemos diegimo ir naudojimosi instrukcijas;
- Sudaryti metodus įvertinant interneto paslaugų tiekimo intensyvumą;
- Pateikti rekomendacijas paslaugų tiekimo kokybei gerinti, atsižvelgiant į ekonominius, techninius kriterijus.

Tyrimo objektas

Šio darbo tyrimo objektas – srautų analizavimas, algoritmų kūrimas, kurie padėtų aptikti problemas tinkle ir vartotojas galėtų priimti sprendimus, pateikti pasiūlymus.

Laukiami rezultatai

Tikimasi, kad bus sukurta paprasta ir nesudėtinga vartoti programinė įranga, kuri padės vartotojui aptikti tinklo problemas.

II. TEORINĖ DALIS

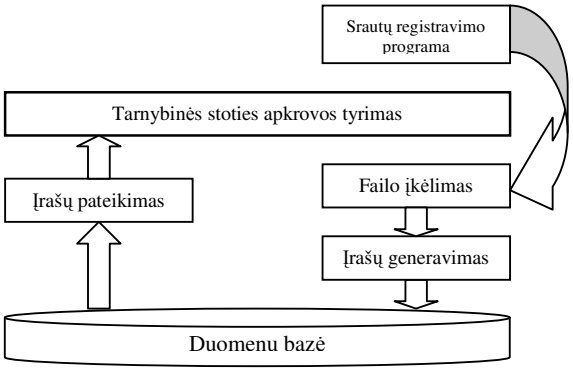
1. Temos analizė

1.1 ir 1.2 dalyse aptariamos tinklo informacijos srautų analizės priemonės bei jų struktūrą.

1.1. Srautų analizavimas

Srautų analizavimo įrankis susidaro iš keleto struktūrų (žr. 1 pav.):

- Srautų registravimo programa (Packet Sniffer) – tai įrankis skirtas skenuoti tinklą, įeinančius ir išeinančius paketus, atlikti failo eksportavimą;
- Įrašų generavimas duomenų bazėje – eksportuoto failo įrašymas į duomenų bazę;
- Apkrovos tyrimas – informacijos pateikimas, panaudojant duomenų srautus, kurie atvaizduojami panaudojant duomenų bazę.



1 pav. *Modelio struktūra*

Srautų registravimo programa, tai atskiras įrankis, kuris dirba visiškai atskirai. Moduliai, tokie kaip „Failo įkėlimas“, „Įrašų generavimas“ panaudojami vieną kartą srautinių įrašų įkėlimo procese. Įrašų pateikimas vyksta nuolat, vartotojui pateikus užklausas.

1.2. Srautų registravimo programų analizė

1.2.1. „Packet Sniffer SDK“

Svetainė: http://www.microolap.com/products/network/pssdk/

Packet Sniffer SDK plėtojimo rinkinys tinklo paketų gaudymui multi–gigabito tinklo aplinkoje. Packet Sniffer SDK bibliotekos rinkinys yra 100% visiškai savarankiškas, dinamiškai prijungiama paketų gaudymo technologija, kuri yra suderinama su Microsoft Visual C++, Microsoft Visual Basic. NET, Intel C++, Borland C++ Builder, Delphi ir daugelį kitų [1][2]. Trys pagrindiniai dalykai, kurie aprašo šią plėtotę:

- **Reguliuojami Paketų Srautai**: Tai pagrindinė priežastis dėl kurios programinė įranga nepames nė vieno paketo, paketų taikymo ir žymėjimo būdas tikslingai perkelia į PSSDK vidaus tvarkyklės branduolio režimo vietą ir atgal;
- **FastBPF (32/64bit BPF JIT kompiliatorius)**: Filtruodamas leidžia eismą 6 kartus greičiau nei tai gali būti padaryta su klasikinės BPF virtualiomis mašinomis;
- **Asinchroninės užklausos eilės paketams gauti/siųsti**: Vykdo eismą realiu laiku.

1.2.2. „Wireshark“

Svetainė: http://www.wireshark.org/

„Wireshark (anksčiau žinomas kaip ethereal) yra vienas iš svarbiausių atviro kodo produktas, kuris leidžia fiksuoti vietinio tinklo (LAN) paketus, analizuoti tinklo srautą. Įjungus „Wireshark“ paketų skenerį – nedelsiant pradedami rinkti tinklo duomenys, kurie iššifruojami ir rodomi paketų rezultatų lange[3,4].

„Wireshark“ gali aptikti ir iškoduoti daugiau nei 50000 skirtingų tinklo protokolų visuose tinklo sluoksniuose. Visa tai beveik bet kokiame fiziniame tinklo ryšyje: 100Base–T, ATM, Token Ring ir t.t.

„Wireshark“ yra tikrai vertas konkurentas visiems komerciniams paketų skanuokliams ir analizatoriams.

„Wireshark“ buvo pavadintas nauju projektu, nuo 2006 metų vidurio, ankščiau ethereal.

1.2.3. „OmniPeek Network Analyzer“

Svetainė: http://www.wildpackets.com/

„OmniPeek“ siūlo intuityvią, lengvą naudojimo grafinę sąsają, kurią inžinieriai gali panaudoti analizuojat ir sprendžiant problemas įmonės tinkluose. „OmniPeek“ suteikia tinklo inžinieriams lengva analizės sąsaja, apimdama Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n, VoIP, Video, ir WAN ryšius.

Pagrindiniai faktai:

- Integruotas palaikymas Ethernetui, Gigabit, 10 Gigabit, 802.11a/b/g/n, VoIP, Video, MPLS, VLAN, ir WAN.
- Intuityvus supratimas, kurie mazgai susisiekia, kurie protokolai ir subprotokolai yra perduodami ir kurios duomenų srauto charakteristikos paveikia tinklo atlikimą.

1.2.4. Įrankių lyginamoji analizė

Iš palygintų trijų programų didžiausią populiarumą turi „Wireshark“. Šis įrankis yra labiau orientuotas profesionaliam naudojimui, turi daugybę filtravimo, analizės pasirinkimų, yra nemokamas (Open Source). Tačiau šį įrankį pilnai įvaldyti reikia kvalifikuotų įgūdžių, žinių, daug laiko. Paprastiems srautų analizavimo vartotojams tai per daug sudėtinga.

1.3. Programinių priemonių taikymas tinklo stebėsenos sąsajai kurti

Šioje dalyje aptarsime programines sistemas, kurias galima panaudoti kuriant tinklo stebėsenos sąsają. Kuriant įrankį, didžiausias dėmesys skirtas kuriamos sąsajos paprastumui ir valdymui, su kuria dirbant vartotojui pakanka būti susipažinusiam su minimaliomis žiniomis apie tinklo srautų savybes.

Kuriama sistema veiks *www* svetainės pagrindu. Svetainėms kurti naudojamos technologijos:

- Serverio pusės „skriptų“ (scenarijų) technologija – PHP;
- Kliento pusės scenarijaus technologija – JavaScript;
- Duomenų bazės valdymo sistema – SQL ir MySQL;
- Puslapių aprašymo kalbos – HTML, CSS.

1.3.1. PHP

PHP – plačiai paplitusi dinaminė interpretuojama programavimo kalba, sukurta 1997 m. ir specialiai pritaikyta interneto svetainių kūrimui[5].

PHP sintaksė panaši į daugelį struktūrinių kalbų, ypatingai į C bei Perl.

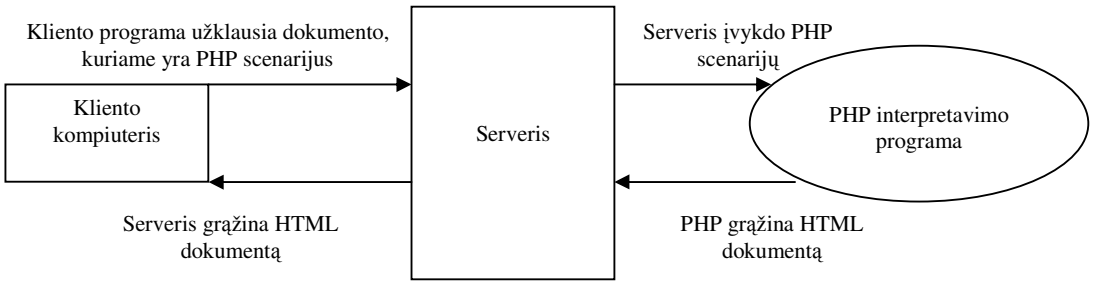
PHP kalba yra atviro kodo ir tai yra viena priežasčių, dėl ko kalba yra nors ir nesudėtinga, bet gana lanksti – veikia daugumoje operacinių sistemų, palaiko nemažai reliacinių duomenų bazių bei veikia su dauguma interneto serverių – CGI, FastCGI, ISAPI ir kitais protokolais.

Nors ir PHP yra dažniausiai naudojama interneto puslapių kūrimui, PHP yra labai galingas įrankis atlikti kitas funkcijas komandinėje eilutėje.

```
<?php
// Vienos eilutės komentaras
/* Kitoks komentaro užrašymo būdas – gali būti per kelias eilutes */

// Priskiriame kintamajam $kint reikšmę
$kint = „Sveikas, pasauli!“;

// PHP sakiniai užbaigiami kabliataškiu
print $kint;
echo $kint;

// Tiek print, tiek ir echo funkcija – išveda reikšmę rodymui
?>
```

2 pav. *php kodo pavyzdys*

PHP scenarijaus užklausos veikia skirtingai. Serverio PHP scenarijaus procedūra PHP kalba parašytą failą konvertuoja į HTML arba XML kalbos standartą atitinkantį failą ir išsiunčia jį interneto vartotojui. PHP kodas yra įterpiamas į HTML kalbos failą (3 pav.). PHP scenarijaus procedūra PHP failo grynąją HTML teksto dalį tiesiog perskaito ir dubliuoja naujai formuojame faile nieko nekeisdama, o tekstą tarp <? ... ?> ar <php ... ?> žymių apdoroja pagal PHP kalbos sintaksės ir semantikos taisykles.



3 pav. *php scenarijaus diagrama*

PHP privalumai:

- Yra visiškai nemokamas;
- Veikia įvairiose operacinėse sistemose: Win, *nix, MacOS, Solaris, HP–UX, AIX ir t.t.;
- Yra atviro kodo projektas, jį vysto didelė grupė žmonių, todėl rastos klaidos yra greitai ištaisomos ir PHP sparčiai plečiasi;
- Veikia ir daugelyje WEB serverių: Apache, IIS, PWS, OmniHTTP, BadBlue ir t.t.;

- Išmokti PHP programavimo pagrindų yra labai lengva;
- Pasižymi dideliu greičiu serverio pusėje, bei dirbant su duomenų bazėmis;
- Nedideliuose projektuose PHP paprasta įterpti į HTML kodą;
- Yra sukurta daug papildomų modulių, bei išplėtimų;
- Kadangi PHP programuotojų yra be galo daug, daugumą jau parašytų scenarijų galima rasti internete.

Trūkumai:

- PHP yra interpretuojama kalba, todėl reikia papildomos įrangos (pvz.: Apache serverio) jos naudojimui;
- Yra galimybė perskaityti PHP scenarijų išeities tekstus, nes kodas neverčiamas į mašininę kalbą, o saugomas serveryje paprasto teksto pavidalu. Kodui užšifruoti yra skirtas ZendEncoder, bet jis mokamas.

1.3.2. JavaScript

JavaScript – objektiškai orientuota scenarijų programavimo kalba, besiremianti prototipų principu. Dažniausiai kalba naudojama internetinių puslapių interaktyvumo realizacijai, bet taip pat naudojama ir kaip galimybė scenarijais manipuliuoti tam tikromis programomis. Kalba sukurta Brendano Eicho Netscape kompanijoje ir pavadinta Mocha, vėliau pervadinta į LiveScript, ir galiausiai tapo JavaScript. Vienas iš argumentų pervadinant kalbą buvo sintaksinis panašumas su Java kalba [6,7]. Paskutinė JavaScript versija – 1.5.

JavaScript kalbos sintaksė perimta iš C kalbos, su kitais komponentais bendraujama per sąsajas (dokumento objektinį modelį), palaikoma Unicode, reguliarios išraiškos (regular expresions), taip pat teksto vykdymas naudojant *eval* funkciją.

Paprastai JavaScript kalbos kodas įtraukiamas į HTML puslapius, tokiu būdu išplečiant statinius HTML puslapius dinaminiu scenarijaus funkcionalumu – galimas anketų parametrų tikrinimas, naujų langų atidarymas, suskleidžiamos hierarchinės struktūros rodymas, išsiskleidžiantis meniu ir daug kitų interaktyvumo formų. JavaScript kalba remiasi kelios pagrindinės svetainių kūrimo metodologijos – DHTML (Dinaminis HTML), AJAX (Asinchroninis JavaScript ir XML programavimas) ir kt.

1.3.3. SQL ir MySQL

SQL (Struktūrizuota užklausų kalba, Structured Query Language) – populiariausia iš šiuo metu naudojamų kalbų, skirtų aprašyti duomenis ir manipuliuoti jais reliacinių duomenų bazių valdymo sistemose. [8,9].

SQL remiasi keletu raktažodžių, kuriuos naudojant galima įvykdyti funkcijas.

Juos galima suskirstyti į keletą grupių:

- Duomenų gavimas – SELECT laukelis FROM lentele WHERE sąlyga GROUP BY laukelis ORDER BY rūšiavimo sąlyga ORDER rikiavimo tvarka;
- Duomenų valdymas – INSERT, DELETE, UPDATE;

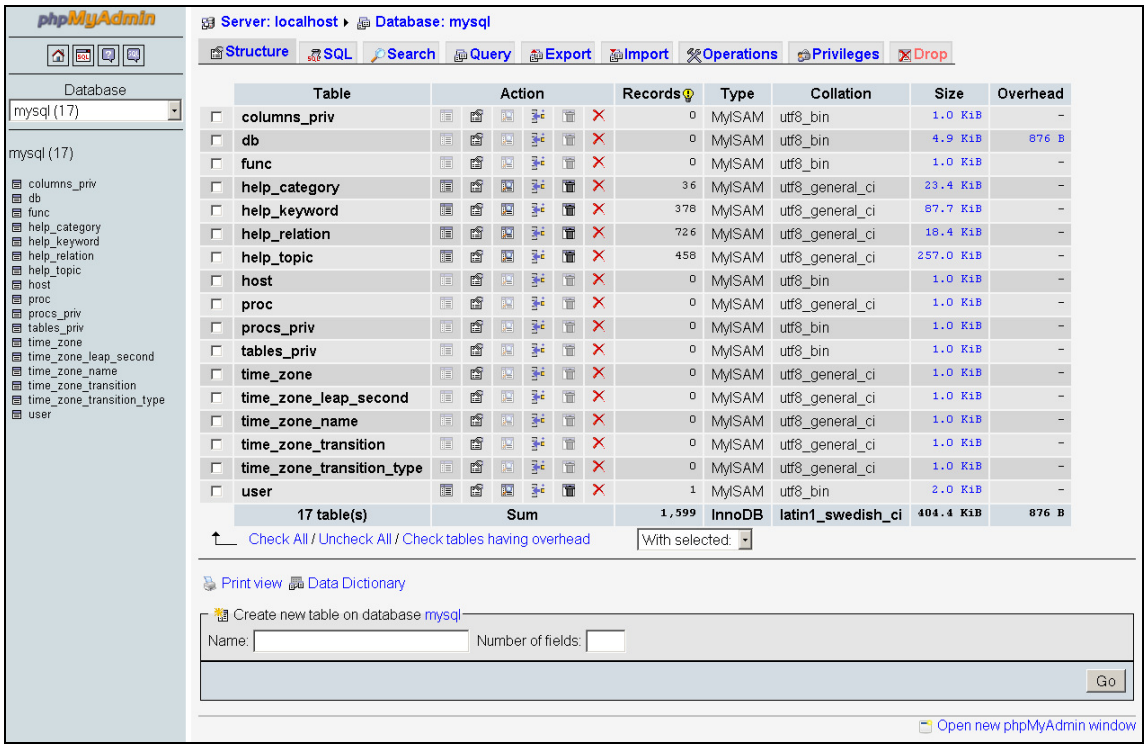
- Transakcijos – BEGIN, COMMIT, ROLLBACK. (tik sistemose, kurios palaiko transakcijas);
- Duomenų apibrėžimas – CREATE, DROP.

Trūkumai:

- Nėra standartinio būdo skaidyti sudėtingas komandas į kelias smulkesnes;
- SQL realizacijos skirtingose duomenų bazių valdymo sistemose nėra nuoseklios, nepilnai suderinamos.

Kadangi standartinių galimybių dažnai neužtenka, duomenų bazių sistemose SQL išplečiama jai pridedant daugiau programavimo kalbų funkcijų.

MySQL – viena iš reliacinių duomenų bazių valdymo sistemų, palaikanti daugelį naudotojų, dirbanti SQL kalbos pagrindu. MySQL yra atviro kodo programinė įranga, vystoma ir palaikoma švedų kompanijos „MySQL AB“ [10].



4 pav. *MySQL duomenų bazės valdymo įrankis phpMyAdmin*

MySQL įranga veikia daugelyje platformų, ji dažnai pasirenkama programuojant internetines svetaines. Šiame sektoriuje su MySQL bando konkuruoti PostgreSQL (http://www.postgresql.org).

Pastaruoju metu MySQL vis dažniau pritaikoma labai didelėse informacinėse sistemose. Pavyzdžiui kai kuriose sistemose apkrovimas kartais viršija 10 tūkstančių užklausų per sekundę arba jei reikia duomenų bazės su dideliu skaičiumi lentelių. Šiame sektoriuje pagrindinis MySQL konkurentas yra Oracle (http://www.oracle.com).

Nors priėjimui prie MySQL duomenų bazių dažniausiai pasirenkama PHP kalba, ją taip pat galima pasiekti įvairiomis kitomis programinėmis priemonėmis – C, C++, C#, Java, Perl, Python ir kitomis. Kiekvienai šių kalbų sukurtos specialios bibliotekos (API – Application Programming Interface). Taip pat MySQL duomenų bazėms yra sukurta ODBC (Open Database Connectivity)

sąsaja MyODBC (www.mysql.com/products/myodbc), leidžianti duomenis pasiekti bet kuria kalba, neturinčia specialios bibliotekos, tačiau palaikančia ODBC komunikavimo mechanizmą. PHP kalba MySQL duomenų bazei valdyti sukurtas įrankis phpMyAdmin (http://www.phpmyadmin.net).

1.3.4. HTML ir CSS

HTML (Hypertext Markup Language „Hiperteksto žymėjimo kalba“) – tai kompiuterinė žymėjimo kalba, naudojama pateikti turinį internete. Kalbą standartizuoja W3 konsorciumas [11,12].

Pagrindinis HTML kalbos vienetas yra elementas. Kaip ir XML, HTML elementas turi vardą ir gali turėti bet kokį skaičių atributų. Elemento viduje gali būti tekstas bei kiti elementai. Tiek tekstas, tiek ir dukteriniai elementai paprastai gali kartotis ir sekti bet kuria tvarka.

```
<html>
  <head>
   įžanginė informacija
    <title>antraštė<title>
  </head>
 <body>
  Puslapio medžiaga
 </body>
</html>
```

5 pav. *HTML dokumento struktūra*

Elemento atributai turi vardą ir reikšmę. Jei galimi atributai nenurodomi, paprastai galioja sutartos nutylėjimo taisyklės. Pavyzdžiui, HTML fragmentas raudona `<font color=„red“><b>r</b>raudona</font>` turi du elementus. Vienas jų (font) perjungia rodomo teksto spalvą į raudoną. Šio elemento viduje esantis antrasis elementas (b), perjungiantis šriftą į paryškintą. Pirmasis elementas turi vieną atributą (color) su reikšme red. Antrasis elementas atributų neturi.

HTML kode atributų reikšmes rekomenduojama apgaubti kabutėmis, nors HTML 4.01 standartas to nereikalauja.

CSS (Cascading Style Sheets) – kalba, skirta nusakyti kita struktūrine kalba aprašyto dokumento vaizdavimą. Dažniausiai CSS aprašomas HTML dokumentų pateikimas, tačiau ją galima taikyti ir įvairiems kitiems XML dokumentams. Kaip ir HTML kalbai, CSS kalbą standartizuoja W3 konsorciumas.

Integruoti CSS į HTML galima:

- Įrašius CSS kodą atskirame faile, o kelią iki failo nurodžius HTML dokumente tarp <*link*> žymų, patalpintų <*head*> sekcijoje. Taip sukuriamas bendras visos interneto svetainės stilius, nereikia atskirai redaguoti kiekvieno tinklapio;
- Įrašius CSS kodą į HTML dokumentą. Taip bus pakeičiama vieno puslapio išvaizda.
- Įrašius CSS kodą į HTML žymę. Tokiu atveju bus pakeista tik konkretaus HTML elemento išvaizda.

Šiuo metu rekomenduojama HTML kalba žymėti tinklalapio sandarą, o išvaizdą (teksto spalvas ir pan.) aprašyti atskirame CSS dokumente. Toks tinklalapis užima mažiau vietos ir greičiau pasirodo vartotojo naršyklėje, nes įvairių puslapių išvaizdą aprašantis CSS dokumentas iš serverio atsisiunčiamas tik vienąkart. Naudojant CSS, lengviau keisti iškart visų puslapių išvaizdą ir paprasčiau

pasiekti, jog šiuos puslapius įvairios naršyklės rodytų vienodai.

Nors ir siūlomi įvairūs akivaizdžiai CSS reikalaujantys standartai (pavyzdžiui, HTML 4.01 Strict), dauguma naršyklių palaiko ir pereinamąsias versijas, pavyzdžiui, HTML 4.01 Transitional, leidžiančias naudoti ir ankstesnius dokumento išvaizdą aprašančius HTML elementus.

1.3.5. Reguliariosios išraiškos

Reguliariosios išraiškos (Regular Expresion) – tai specialios paskirties simbolių eilutės aprašančios tam tikro teksto paieškos šabloną [13,14,15].

Reguliariąsias išraiškas galima traktuoti kaip patobulintą šablonų sistemą. Pirmiausia rašomas šablonas, o po to, naudojant PHP funkcijas, jis naudojamas tekstinėje eilutėje. Reguliariosios išraiškos naudojamos tik darbui su eilutėmis. PHP yra funkcijų grupės, naudojančios reguliariąsias išraiškas lyginimui su šablonais ir kitos dvi – kurios ieško atitikimo šablonams ir keičia vieną tekstą kitu. Abiejose grupėse viena iš funkcijų reaguoja į registrą, kita – ne.

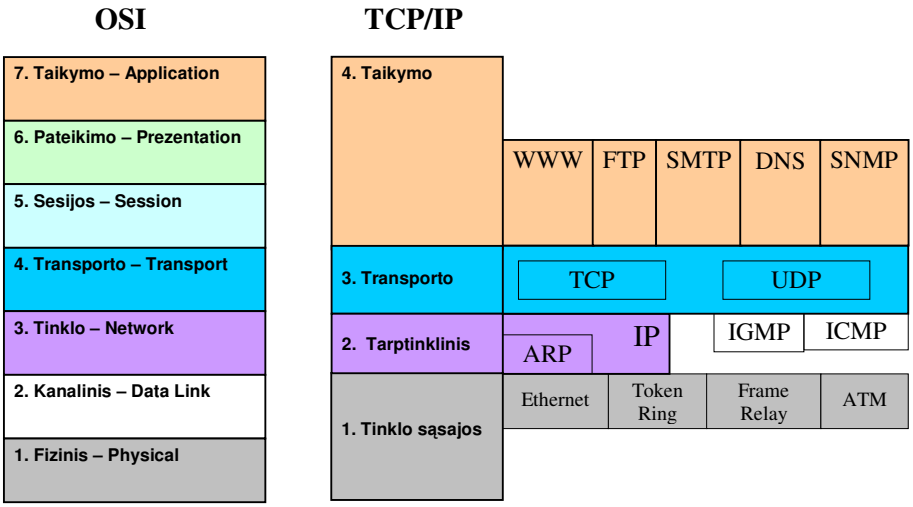
1.4. IEEE 802.3 standartas ir protokolai

Toliau aptarsime standartus bei protokolus, taikomus informacijos perdavimui bei valdymui.

Ethernet – kompiuterių tinklų technologija, dažniausiai taikoma lokaliuose tinkluose (LAN).

Visuotinai priimta laikyti, kad Ethernet protokolas sukurtas 1972 m. Šio tipo tinklas taip pat pasitarnavo IEEE-802.3 reikalavimams suformuluoti, kurie pasirodė 1980 m. Po to Digital Equipment, Intel ir Xerox kompanijos kartu sukūrė ir realizavo Ethernet (versija 2.0) reikalavimus, kurie atitiko IEEE-802.3. Šiuo metu Ethernet ir IEEE-802.3 protokolai užima vieną pagrindinių vietų LAN protokolų šeimoje. Ethernet terminas dažnai naudojamas apibrėžti visus tinklus, kurie naudoja daugkartinės prieigos su nešlio kontrole ir konfliktų aptikimu metodą (CSMA/CD- Carier Sense Multiple Access/Collision Detection). Šio tipo tinklai iš esmės atitinka Ethernet bei IEEE-802.3 reikalavimams.[31]

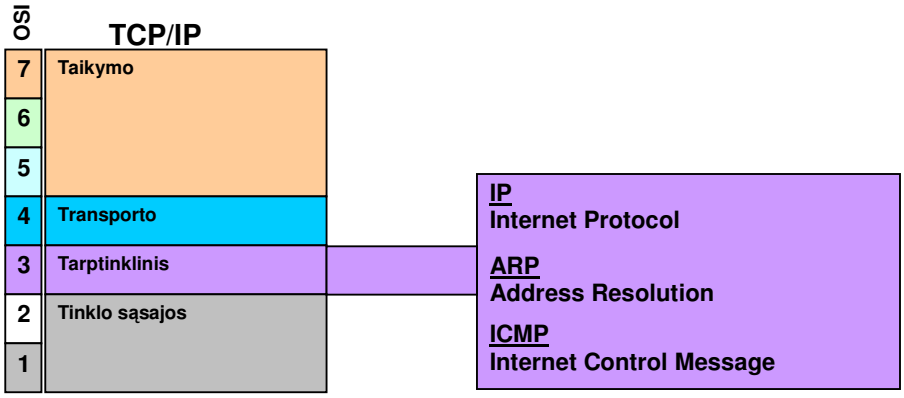
Tinklo protokolus galima suskirstyti į bendrus tinklo modelius. Tai OSI[16] arba TCP/IP[17]. Plačiau dokumente yra nagrinėjamas TCP/IP[18] (žr. 6 pav).



6 pav. *OSI ir TCP/IP lygmenys*

Trumpai paanalizuosime tarptinklinį ir transporto veikimo lygmenis.

1.4.1. Tarptinklinis lygis



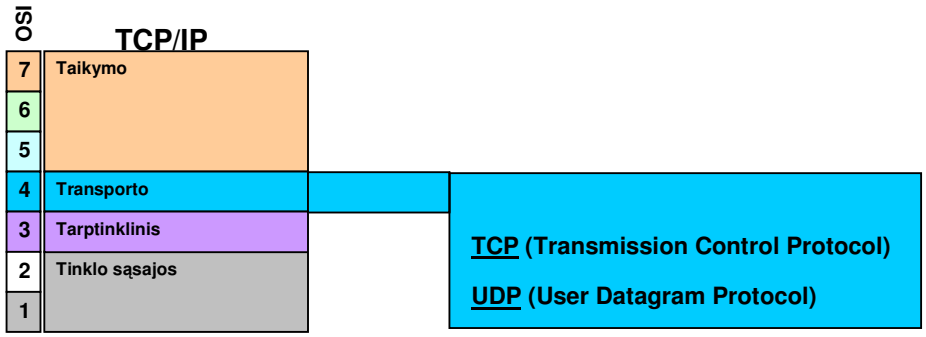
7 pav. *Tarptinklinis lygis.*

Atlieka paketų perdavimą naudojant neorientuotą jungimą (žr. 7 pav.). Yra parenkamas maršrutas, kuris duotuoju momentu yra geriausias. Pagrindinis šio lygio protokolas – IP protokolas (Internet Protocol).

ICMP protokolas yra neatskiriama IP modulio dalis. Jis užtikrina atgalinį ryšį, siųsdamas diagnostinius pranešimus siuntėjui (jei datagrama dėl vienokių ar kitokių priežasčių nepasiekė gavėjo).

ARP protokolas skirtas IP adresą paversti į MAC adresą. MAC adresai identifikuoja įrenginius, pajungtus prie fizinio kanalo[32].

1.4.2. Transportinis lygis



8 pav. *Transportinis lygis.*

Transportinio lygio protokolas užtikrina duomenų persiuntimą tarp dviejų įrenginių (žr. 8 pav.). Įrenginys gaunantis arba išsiunčiantis duomenis transportiniu lygiu, identifikuojamas jungties (angl. „port“) numeriu. Tokiu būdu siuntėjo ir gavėjo adreso vaidmenį perima jungties numeris (arba paprasčiau jungtis).

TCP (Transmission Control Protocol – perdavimo kontrolės protokolas) – patikimas protokolas su sujungimo nustatymu: jis valdo loginį ryšio seansą (nustato, palaiko ir nutraukia sujungimą) tarp įrenginių ir užtikrina patikimą (be klaidų) duomenų perdavimą nuo įrenginio iki įrenginio.

UDP (User Datagram Protocol – Vartotojo datagramų protokolas) protokolas naudojamas arba siunčiant trumpas žinutes, kai pranešimo pakartojimas yra optimalesnis variantas nei seanso sudarymas ir sėkmingas duomenų perdavimas (esant duomenų iškraipymams), arba kai pati

organizacija užtikrina sujungimą ir paketų patikrinimą. Šis protokolas neatsako už duomenų perdavimą be klaidų. Toliau nagrinėjama PRIEDUOSE 1,2,3.

Ethernet tinkle, kaip matoma, yra begalės protokolų, nekalbant apie atskirų korporacijų, kaip „Cisco“, „Novell“ ir kt. integruotus protokolus, kurie apskritai nėra nurodyti šiame apraše.

1.4.3. Paketų tipai ir paketo sudėtis

EtherType yra dviejų oktetų sritis Eterneto kadre, kaip apibrėžta Eterneto II tinklo kadravimo standarto. Jis naudojamas nurodyti, koks protokolas yra įdėtas į kapsulę kadro duomenyse. Su IEEE pasirodymu 802 rinkinys standartų, SNAP antraštės, su IEEE 802.2 LLC antraštė naudojamas, perduoti EtherType paketus į IEEE 802 tinklus išskirus Eterneto, taip pat kaip ne–IEEE tinklams, kurie naudoja IEEE 802.2 LLC antrašte, tokia kaip FDDI. Tačiau, Eternetui, Eternetui II antraštės yra vis dar naudojamos. EtherType numeracija prasideda nuo 0x0800, kuris yra didesnis nei ne JumboFrame naudingosios apkrovos dydis 1500 baitai. Tai padeda interpretavime, jei šis laukas yra panaudotas kaip „dydis“ ar „EtherType“. Išsamiau [19,27].

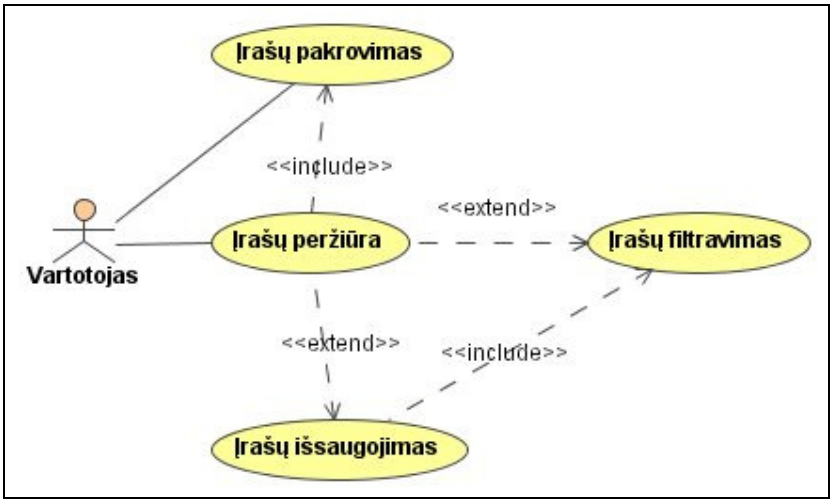
2. Darbo srities analizė

2.1.1. Sistemos architektūra

Architektūros specifikacija skirta pateikti išsamų architektūrinį sistemos vaizdą, naudojant skirtingus architektūrinius vaizdus, tokiu būdu išreiškiant skirtingus sistemos architektūros aspektus, surinkti ir pateikti svarbius architektūrinius sprendimus, kuriuos galima atlikti kuriamoje sistemoje.

2.1.2. Panaudojimo atvejų vaizdas

Panaudojimo atvejų diagrama parodo vartotojo atliekamus veiksmus sistemoje.

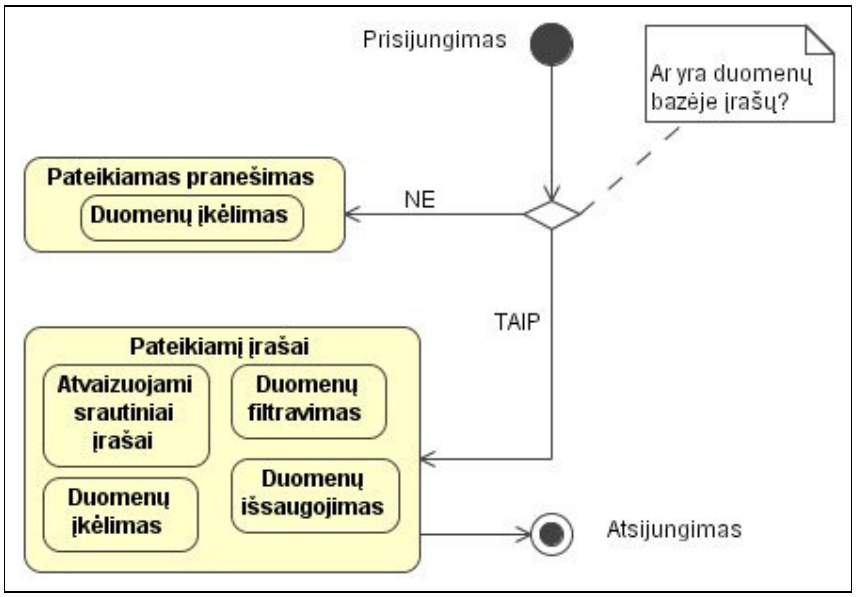


9 pav. *Panaudojimo atvejų diagrama*

Iš diagramos matyti, kad sistemoje yra vienas vartotojas, galintis viską atlikti.

2.1.3. *Sistemos dinaminis vaizdas*

Pateikiamas sistemos darbo algoritmas. Matoma veiksmų seka, kuri priklauso nuo vartotojo atliekamų veiksmų.

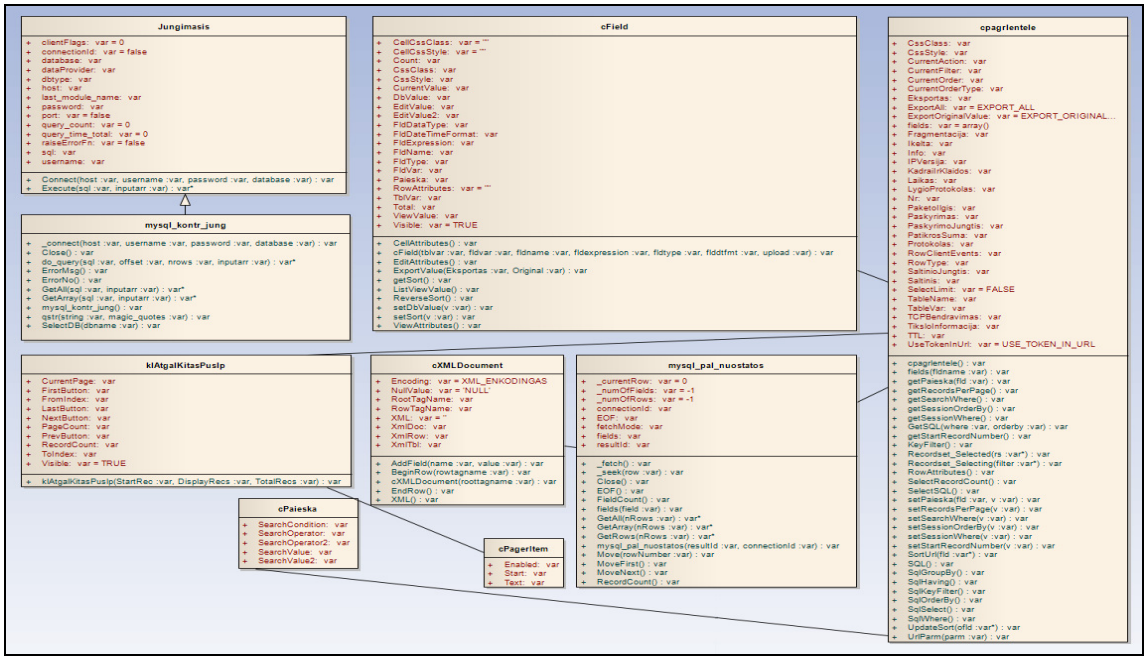


10 pav. *Bendras sistemos dinaminis vaizdas*

Diagramoje matoma, kaip sistema reaguoja, jei duomenų bazėje nėra įrašų.

2.1.4. *Klasių detalizavimas*

Visas sistemos darbas remiasi devynių klasių rinkiniu.

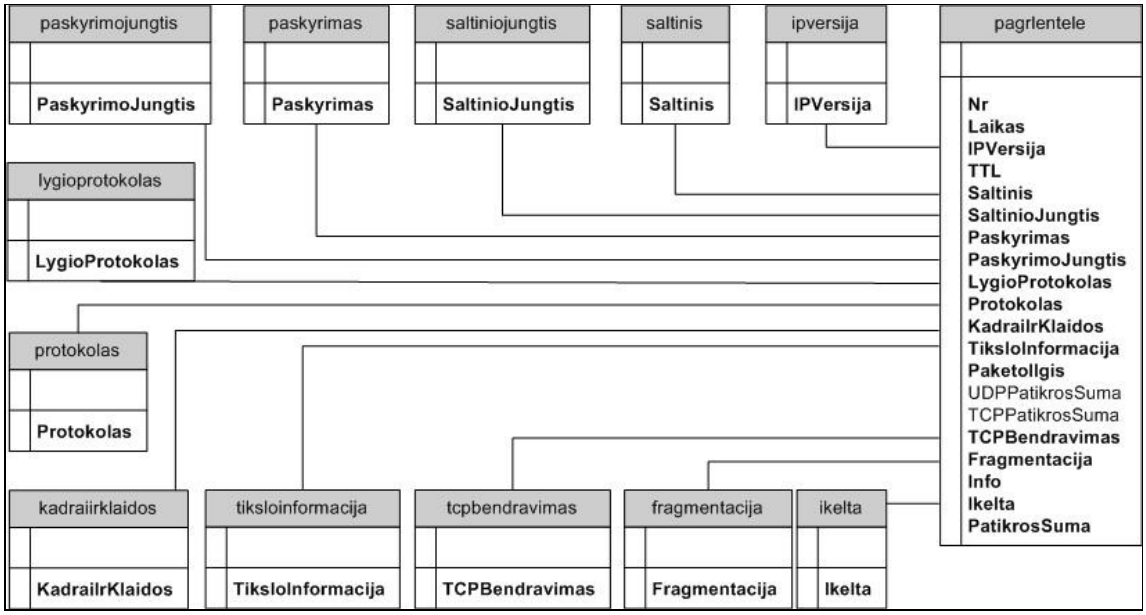


11 pav. *Klasių diagrama*

Pagrindinė klasė – „cpagrlentele“, atsakinga už įrašų atvaizdavimą. Veiksmus, atliekant filtravimą, nusako klasė „cField“. Klasė „klAtgalKitasPusl“ tvarko puslapiavimą, „cXMLDocument“ tvarko įrašų eksportavimą. Paskutinė klasė – „Jungimasis“ yra atsakinga už sklandų prisijungimą ir klaidų pateikimą.

2.1.5. Duomenų vaizdas

Duomenų vaizdo diagrama parodo, kaip sistemoje realizuota duomenų struktūra.

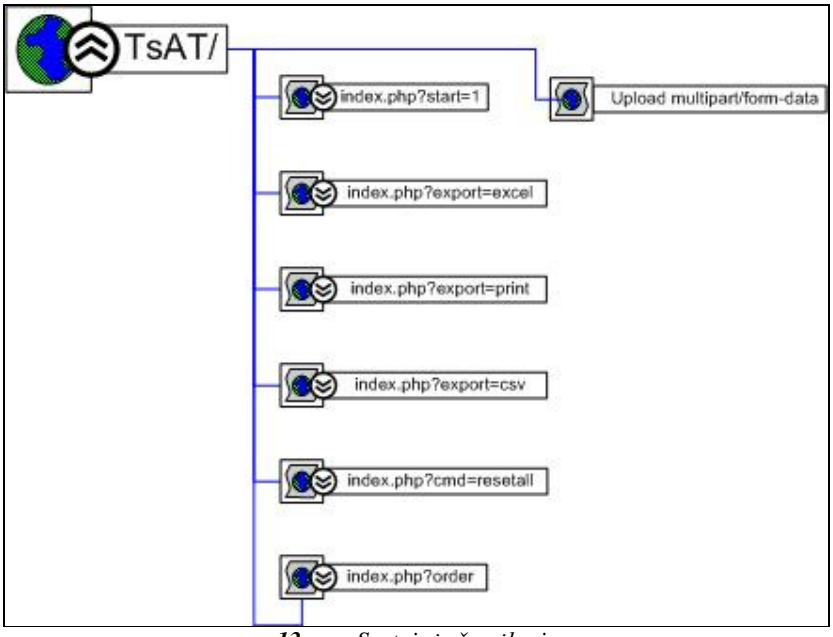


12 pav. *Duomenų vaizdas sistemoje*

Diagramoje nurodyti sąryšiai tarp duomenų bazės, lentelių ir įrašų.

2.1.6. Svetainės žemėlapis

Svetainės žemėlapio diagrama parodo pagrindinius puslapius, prie kurių vartotojas turi priėjimą.



13 pav. *Svetainės žemėlapis*

2.2. *„Wireshark“ programinės įrangos analizė*

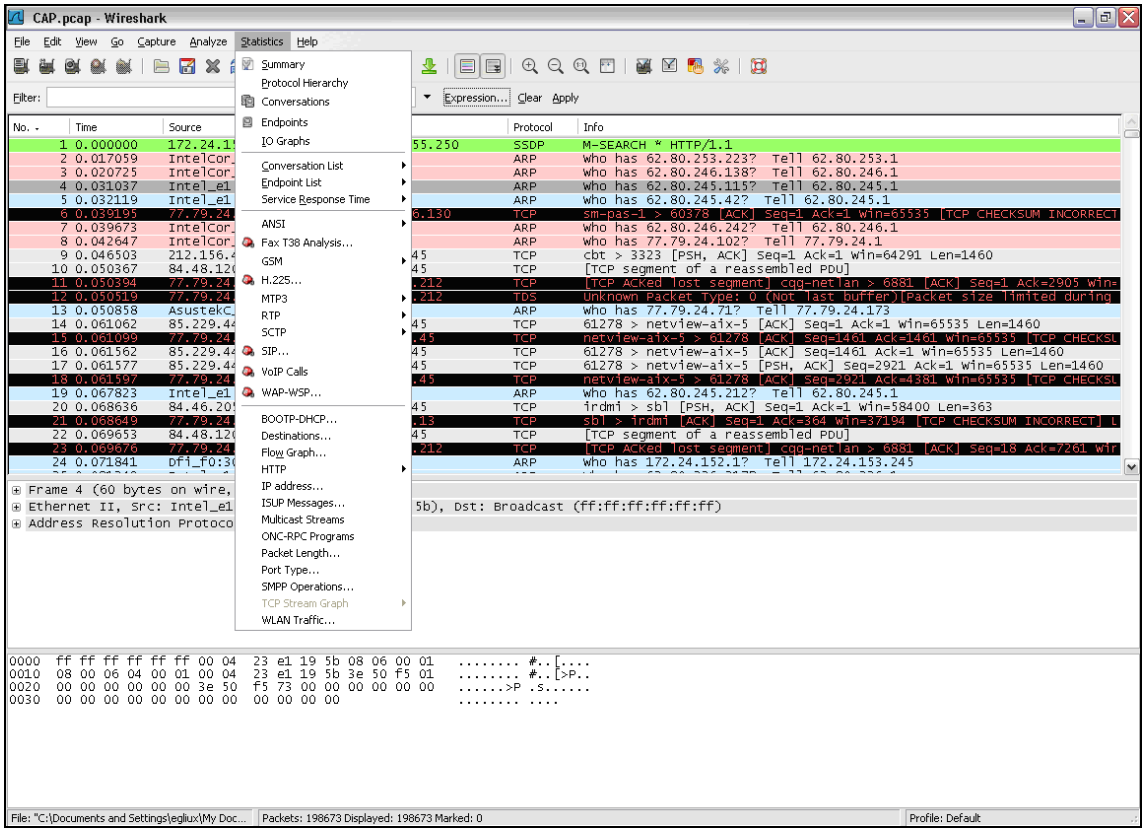
2.2.1. *Programinė įranga*

„Wireshark“ yra vienas iš svarbiausių atviro kodo produktas, kuris leidžia fiksuoti vietinio tinklo (LAN) paketus, analizuoti tinklo srautą. Įjungus „Wireshark“ paketų skenerį – nedelsiant pradedami rinkti tinklo duomenys, kurie iššifruojami ir rodomi paketų rezultatų lange[3].

„Wireshark“ gali aptikti ir iškoduoti daugiau nei 50000 skirtingų tinklo protokolų visuose tinklo sluoksniuose. Visa tai beveik bet kokiame fiziniame tinklo ryšyje: 100Base–T, ATM, Token Ring ir t.t.

2.2.2. *Vartotojo sąsaja*

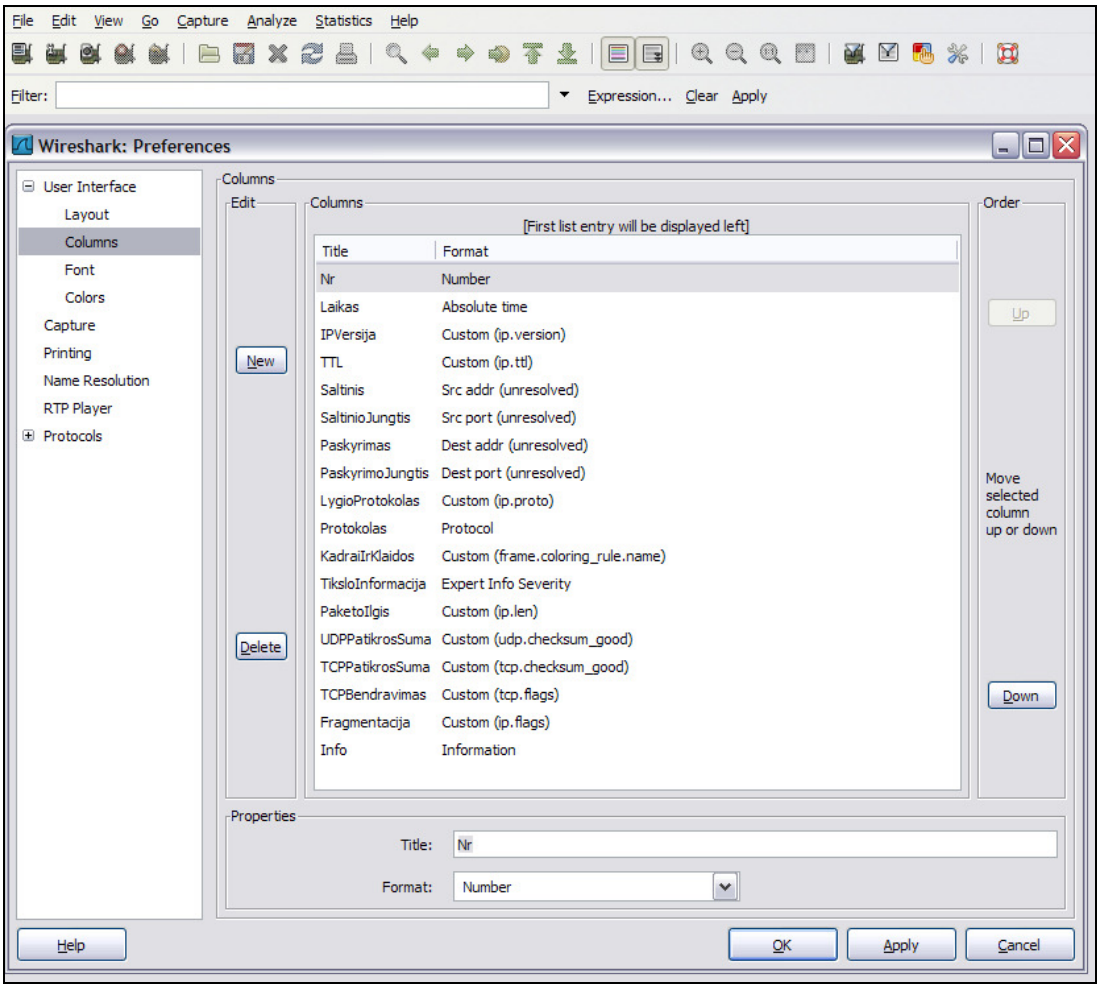
Programos vartotojo sąsaja yra labai sudėtinga: gausiai išdėstyti mygtukai, įvairūs pasirinkimai (14 pav.) .



14 pav. *Paketų sekimui–analizavimui pasirinkta programa „Wireshark“.*

Duomenų failo sukūrimą sudaro keli įvykiai (Edit–Preferences–Columns):

- Teisingas eilučių nustatymas (žr. 15 pav.);
- Srautų skanavimas;
- Duomenų išsaugojimas į .csv failo formatą.



15 pav. *„Wireshark“ nustatymai*

2.2.3. .csv failo formatas.

Norint, kad teisingai būtų atvaizduojami įrašai, reikalingas teisingas failo formatas:

„Nr“,“Laikas“,“IPVersija“,“TTL“,“Saltinis“,“SaltinioJungtis“,“Paskyrimas“,“PaskyrimoJungtis“,“LygioProtokolas“,“Protokolas“,“KadraiIrKlaidos“,“TiksloInformacija“,“PaketoIlgis“,“UDPPatikrosSuma“,“TCPPatikrosSuma“,“TCPBendravimas“,“Fragmentacija“,“Info“

„1“,“20:35:45.917051“,“„,“„,“62.80.245.1“,“„,“Broadcast“,“„,“„,“ARP“,“ARP“,“„,“„,“„,“„,“„,“„,“Who has 62.80.245.224? Tell 62.80.245.1“

„2“,“20:35:45.920843“,“4“,“4“,“b23-31.splius.lt“,“8008“,“239.255.255.250“,“1900“,“0x11“,“SSDP“,“HTTP“,“Chat“,“373“,“True“,“„,“„,“0x00“,“NOTIFY * HTTP/1.1 „

„3“,“20:35:45.923804“,“„,“„,“62.80.246.1“,“„,“Broadcast“,“„,“„,“ARP“,“ARP“,“„,“„,“„,“„,“„,“„,“Who has 62.80.246.225? Tell 62.80.246.1“

„4“,“20:35:45.925589“,“4“,“4“,“b23-31.splius.lt“,“8008“,“239.255.255.250“,“1900“,“0x11“,“SSDP“,“HTTP“,“Chat“,“318“,“True“,“„,“„,“0x00“,“NOTIFY * HTTP/1.1 „

Failo „kepurė“ nebūtinai turi būtį aprašyta „„Nr“,“Laikas“,“IPVersija“,“TTL“,...“, svarbu, kad tolimesni įrašai eitų eilės tvarka.

III. PROJEKTINĖ DALIS

1. Įrankių ir priemonių pasirinkimo analizė

1.1. Zend Studio

Srautų analizavimo programos projektavimui pasirinktas Zend Studio - 5.5.1 įrankis.

„Zend Studio" – tai tūkstančių gamintojų visame pasaulyje pripažintas PHP priedų kūrimo programa. „Zend Studio" siūlo integruotą plėtros terpę ir įgalina neatidėliotiną priedų kūrimą. Vartotojams suteikiamos patikimos gamybos priemonės, patikrinimai ir priedų išskleidimai visose paplitusiose aplinkose (įskaitant Windows, Linux ir Mac).

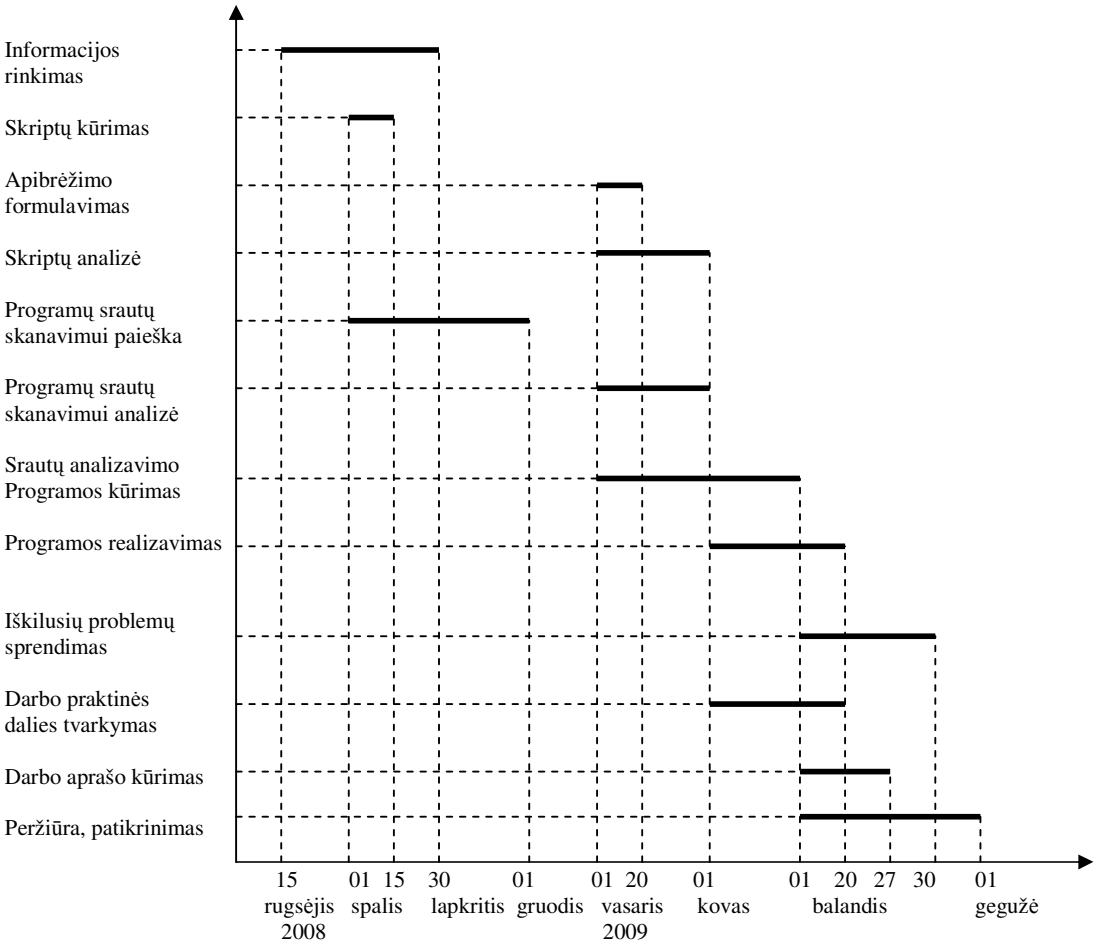
Instaliuojant „Zend Studio", automatiškai nustatomi visi būtini pilnavertės kliento – serverinės terpės gamybos komponentai, kuriai priklauso ir pilnavertis HTTP/ PHP serveris su išplėstiniu palaikymu gamintojui.

„Zend Development Environment" – tai unikalus instrumentas, kurio sudėtyje yra redaktoriaus, derintojo ir valdymo paslaugos. Šios priemonės pagalba Jūs galėsite kurti programinius kodus, juos valdyti ir atlikti patikrą. Taip pat Jūs galėsite prisijungti prie Jūsų nustatyto serverio arba „Zend Studio" serverinio komponento programinio kodo suderinimui jo natūralioje aplinkoje[33].

1.2. Notepad++

Notepad++ yra nemokamas tekstų redaktorius, skirtas pakeisti standartinį Notepad „MS Windows". Jis palaiko dauguma programavimo kalbų ir turi didelį rinkinį papildomų funkcijų. Palaikomos programavimo kalbos: ASP, Ada, ASCII art, Assembler, AutoIt, BAT, C, C#, C++, Caml, CSS, doxygen, FORTRAN, HTML, Haskell, Java, JavaScript, KiXtart, Lisp, Lua, makefile, Matlab, Objective-C, Pascal, Perl, PHP, PostScript, Python, Ruby, Scheme, Unix Shell Script, Smalltalk, SQL, Tcl, TeX, Verilog, VHDL, VB/VBScript, XML.[34]

2. Projekto (darbo) vykdymo planas



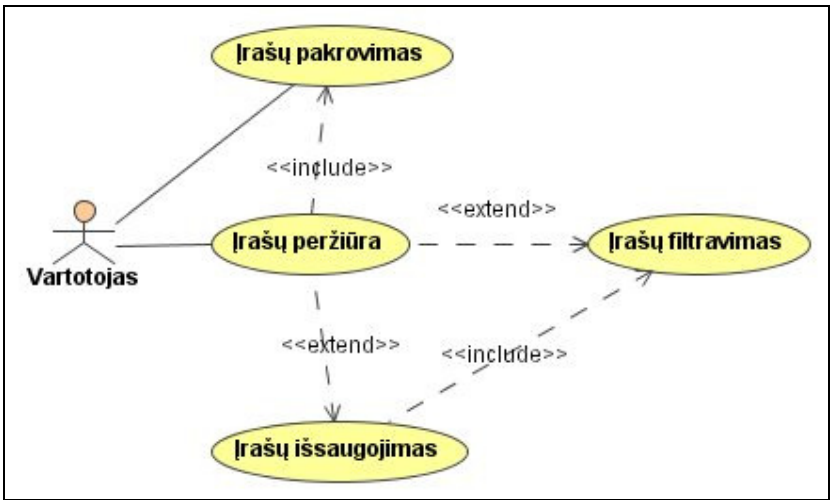
3. Pradinis projekto aprašymas

Darbe dėmesys skiriamas srautų analizavimui, tinklo šiukšlių aptikimui ir daugeliui kitų pasirinkimų, panaudojant filtravimą. Taip pat galimybė įkelti kitos tarnybinės stoties srautinį failą prieš tai apdorojant su „Wireshark“ programa. Kadangi ankščiau buvo dirbta su panašiomis programomis, nebuvo sudėtinga išsirinkti atitinkamas programas.

3.1. Programos projektavimas

Pakartotinai nagrinėjant filtravimo programas, galima pastebėti, kad kuriama programa turės nesudėtingą valdymą, neperkrautą meniu, paprastą navigaciją („atgal“, „kitas“). Iš objektyvaus supratimo, galime sudaryti bendrą programos schemą (žr. 16 pav.).

Programos projekto schema

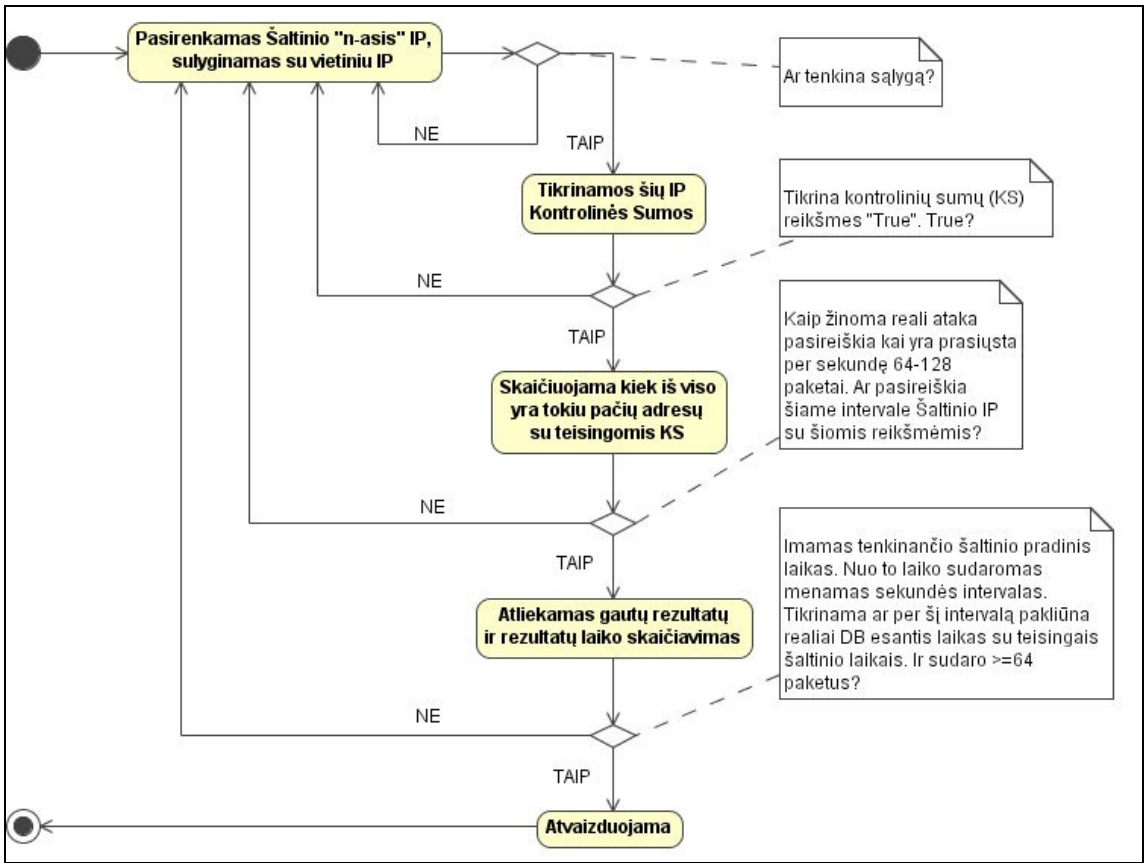


16 pav. *Panaudojimo atvejų diagrama*

Šioje schemoje matoma, jog sistemą valdys vienas vartotojas.

3.1.1. Darbas su DoS atakų aptikimu

Šio algoritmo (žr. 17 pav.) tikslas analizuoti kiekvieną Šaltinio IP, atrenkant tenkinančias sąlygas. Algoritmo veikimas pagrįstas remiantis teorinėmis žiniomis.[L.Kaklauskas]



17 pav. *DoS atakų aptikimo algoritmas*

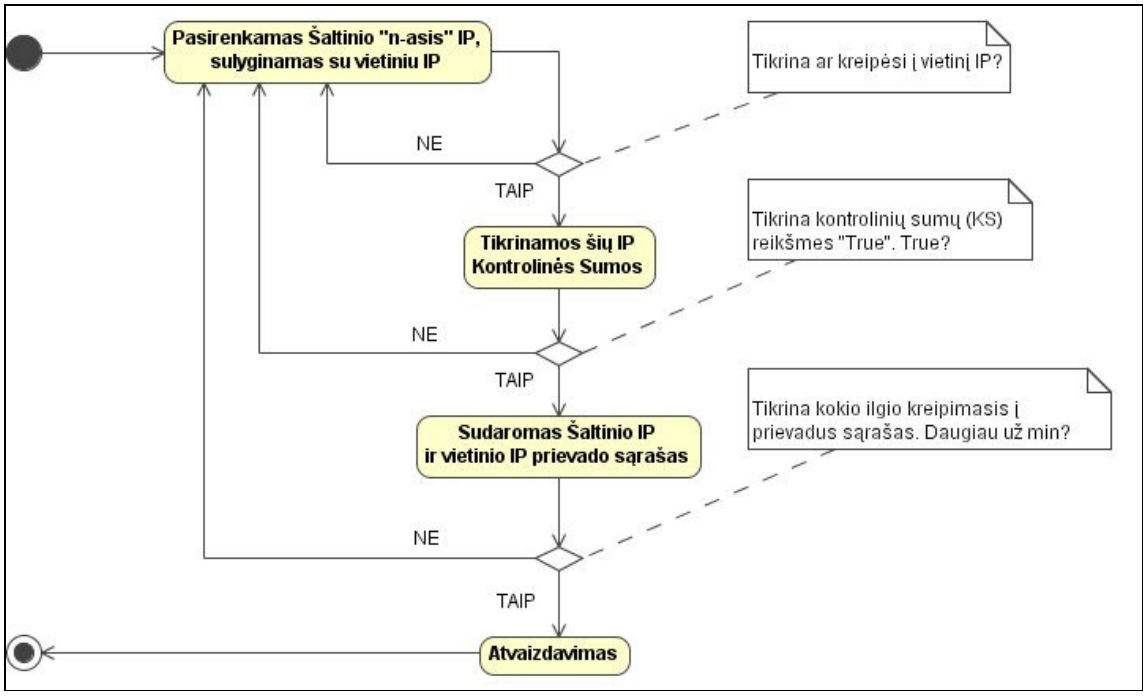
Algoritmo veikimo principas, pagrįstas atrankos būdu:

- Pasirenka n–tąjį Šaltinio IP;
- Sulygina su vietiniu IP;
- Sutikrina kontrolines sumas (UDP ir TCP paketų);
- Suskaičiuoja ar tenkinanti sąlyga yra didesnė arba lygi 64-128 paketams per sekundę;
- Atrenka tenkinančias reikšmes;
- Pasirenkamas atrinkto tenkinančio n-tajo Šaltinio IP pradžios laikas;
- Sukuriamas vienos sekundės menamas laikas;
- Lyginamas menamas laikas su DB (duomenų bazės) realiu laiku (įrašo laiku);
- Tikrinama ar jau realiame intervale pakliūna atrinktos reikšmės ir sudaro >= 64 paketus.

Sąsajoje integruotas algoritmas veikia dalinai automatiniu būdu.

3.1.2. Darbas su prievadų skanavimo aptikimu

Prievadų skanavimas siejasi su įsilaužimais, todėl nagrinėjama įsilaužimo algoritmu (žr. 18 pav.). Algoritmo veikimas pagrįstas remiantis teorinėmis žiniomis.[L.Kaklauskas]



18 pav. *Prievadų skanavimo aptikimo algoritmas*

Algoritmo veikimo principas pagrįstas taip pat atrankos būdu:

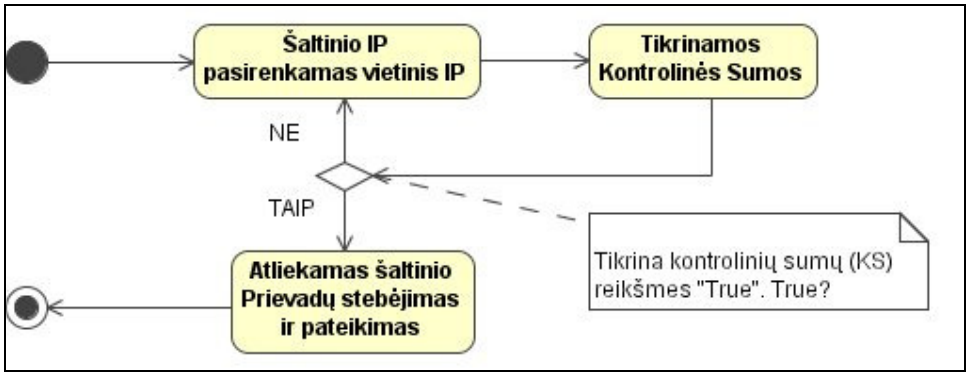
- Išrenka n–tąjį Šaltinio IP;
- Sulygina su vietiniu IP;
- Sutikrina kontrolines sumas (UDP ir TCP paketų);
- Sudaro Šaltinio IP ir tik vietinio IP prievadų sąrašą;
- Tikrina kokio ilgio sąrašas, atvaizduoja.

Sąrašo ilgio tikrinimas pagrįstas minimalia reikšme. Ši reikšmė yra nustatyta pagal vartotojo nutylėjimą, kitaip tariant, programišius neskanuos vieno paskyrimo prievado, jis skanuos visus iš eilės. Todėl pateikimo sąrašas turės būti ilgesnis nei viena eilutė.

Sąsajoje integruotas algoritmas veikia dalinai automatiniu būdu.

3.1.3. Darbas su virusų aptikimu

Virusų aptikimo algoritmas suprantamas kaip didelių srautų išsiuntimas, daug kartų pasikartojant tame pačiame prievade. Menamasis prievadų sąrašas, kuriais braunasi virusai, pateiktas internete[30].



19 pav. *Virusų išsiunčiamos informacijos aptikimo algoritmas*

Algoritmo suvokimas prasidėtų nuo vietinio Šaltinio IP pasirinkimo, kur būtų atliekamas prievadų stebėjimas ir sumuojami srautai. Prievadas, iš kurio daugiausia išsiųsta paketų, galima teigti, kad tai potencialus viruso atidarytas prievadas.

Sąsajoje integruotas algoritmas veikia dalinai automatiniu būdu.

3.1.3.1. Išvados

Algoritmus galima realizuoti sukurtoje sistemoje pilnai rankiniu būdu arba tiesiog integruojant. Integravus algoritmus, gali veikti nepilnai automatiškai nes vis tiek kai kur reikalingi vartotojo veiksmai.

Juos taip pat galima lengvai realizuoti bet kokioje programavimo kalboje. Labiausiai jie būtų naudojami programuojant MySQL užklausas, nes MySQL labai greitai įvykdo tokius reikalavimus.

Sistemoje algoritmai remiasi jau sukurtu filtru. Tai reiškia, kad nekurta sudėtingų funkcijų, o pasinaudota sistemoje jau veikiančiu filtravimu. Panaudojant algoritmo funkciją, jo atliktos užklausos automatiškai nusistato pagrindiniame filtre, kuriuo galima toliau formuoti reikalingas užklausas.

Bet kuriuo atveju algoritmams reikalingi tobulinimai veikimo optimizavimui.

3.1.4. Atvaizdavimas

Suformatuoti įrašai turi būti atvaizduojami vartotojui. Duomenų saugykloje įrašai išsaugomi sukurtos „Plain text“ kalbos formatu, sistemai išanalizavus šiuos duomenis, sugeneruojamas HTML kodas, kuris pateikiamas vartotojui, ir jis mato galutinį suformatuotą vaizdą.

3.1.5. Įrašų filtravimas

Vartotojas turi galimybę atlikti filtravimą tarp visų įrašų, pasirenkant norimą filtravimo nustatymą.

Įrašų filtravimas siejasi su ankstesniais duomenų bazėje paliktais arba vartotojo įkeltais srautiniais įrašais.

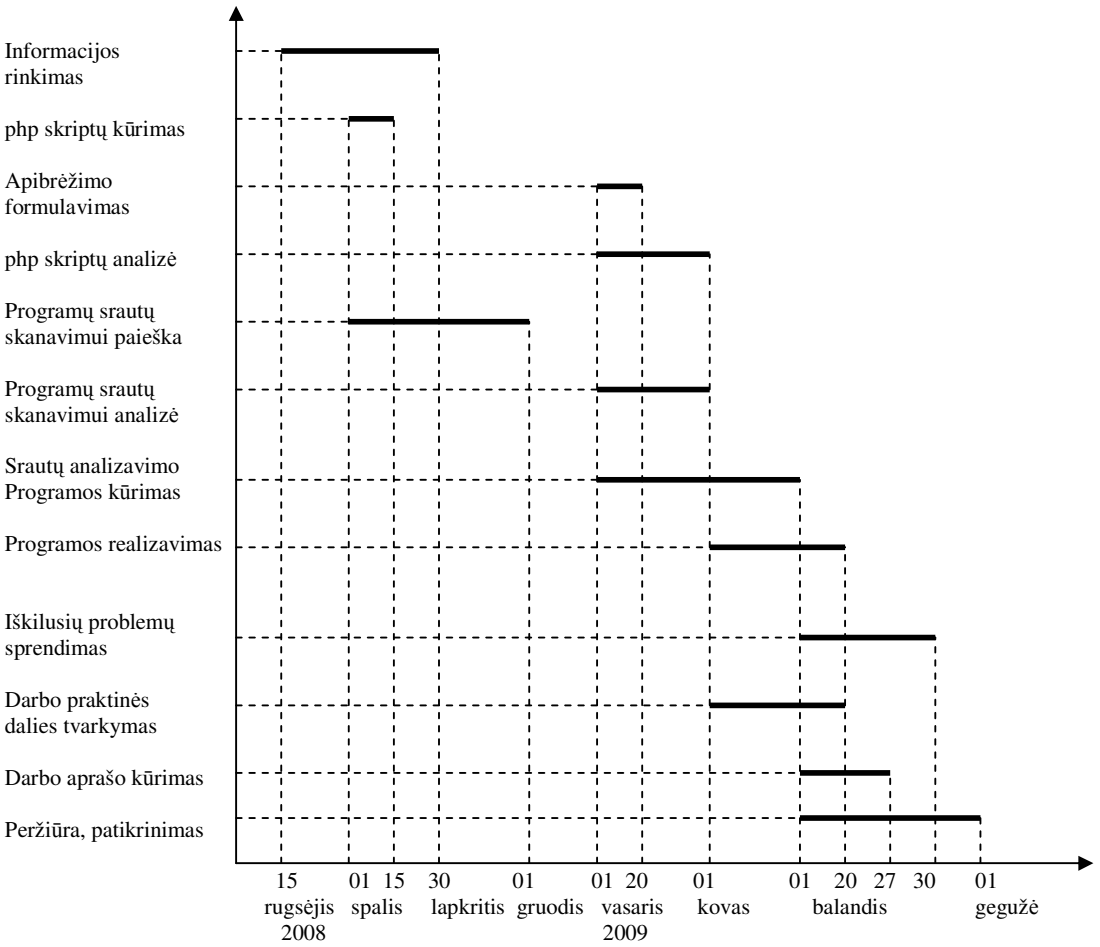
3.1.6. Failo įrašų įkėlimas

Šios sistemos kūrimo tikslas yra palengvinti failo su visais srautiniais įrašais apsikeitimą sistemoje, todėl failų įkėlimas į sistemą būtinas pilnam sistemos funkcionavimui.

Šis reikalavimas glaudžiai siejasi su įrašų formavimu. Keliant failą, automatiškai generuojami filtrams reikalingi laukai. Ankstesni įrašų laukai automatiškai iš DB trinami, be perspėjimo.

IV. DARBO EIGOS APRAŠYMAS

1. Darbų eigos grafas



Darbų eigą galima suskirstyti į keturis pagrindinius etapus:

A. Pirmojo etapo darbo rezultatų analizė. Šiame etape pasirinkta ir suformuluota darbo tema, iškelti uždaviniai ir sudarytas pradinis darbo planas. Ieškoma ir analizuojama skirtingų programų paketai, reikalingi programos sukūrimui.

B. Antrojo etapo darbo rezultatų analizė. Antrajame etape toliau nagrinėjami įrankiai, skirti srautų analizei. Daugiausia dėmesio skiriama PHP kalbai, aprašoma jos galimybės, trūkumai bei privalumai, testuojami scenarijai.

C. Trečiojo etapo darbo rezultatų analizė. Trečiajame etape realizuojamas pradinis programos produkto prototipas. Išsiaiškinami duomenų filtravimo principai. Taip pat pridedama galimybė įkelti įrašus iš failų.

D. Ketvirtojo etapo darbo rezultatų analizė. Paskutiniame etape kuriamas galutinis produkto modelis, optimizuojamas kodas, keičiamas atvaizdavimo algoritmas, rašomas baigiamojo darbo aprašas, pateikiamos išvados.

2. Problemų ir jų sprendimų aprašymai ir pagrindimai

Viena pagrindinių problemų, atvaizdavimo algoritmas. Šiame darbe sukurtas algoritmas buvo gana lėtas. Sprendimo teko ieškoti „open source“ programinės įrangos paketuose. Žinoma, ne visada sekėsi pritaikyti atvaizdavimo algoritmus, daug ką teko keisti ir optimizuoti.

Papildomų problemų sukėlė literatūra ir kiti informaciniai šaltiniai, kuriuos reikėjo versti iš anglų kalbos. Deja, techninių žinių trūkumas užkirto kelią sklandžiam vertimui. Išeitis rasta pasinaudojant automatinėmis vertimo sistemomis, vėliau tekstą redaguojant į rišlius sakinius.

Problemų sukėlė algoritmų integravimas. Dalinai atlieka savo funkcijas, tačiau pilnai išsprendžiama vartotojui pasirenkant tolimesnį filtravimą. Taip yra, kad pilnam išfiltravimui reikalingos protinės žinios.

3. Galutinio projekto stovio aprašymas

Sukurta programa yra išbaigtas produktas. Darbe panaudoti dalinai automatizuoti įsilaužimų, virusų aptikimo ir DoS atakų algoritmai.

Tolimesniam tobulinimui būtų galima sukurti:

– Prisijungimo slaptažodį, kad būtų galima dirbti nuotoliniu būdų (nors tai ne trūkumas);

– Įterpti bendrą detalią statistiką;

– Sukurti daugiau tikimybinį parenkamąjį filtravimą algoritmams (būtų tikslesnis automatinis ieškojimas);

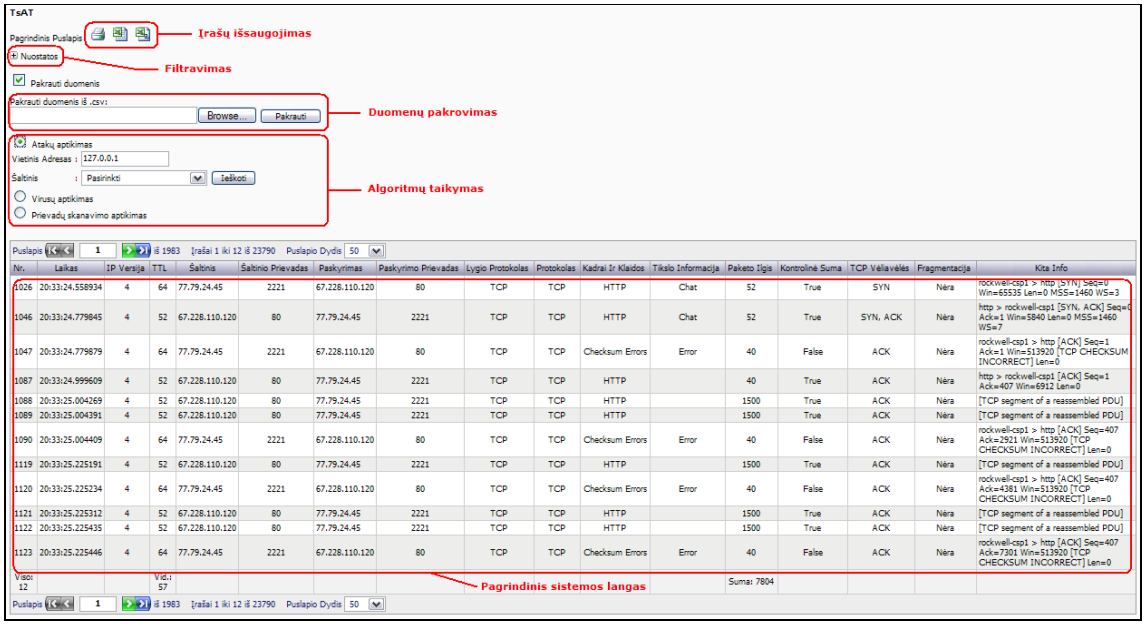
– Įterpti meniu, srautų perkėlimui į archyvą ir atgal.

3.1. Modelio aprašymas

Pagrindinis langas – atvaizduojami visi įrašai, galimybė pereiti į kitą puslapį (žr. 20 pav.).

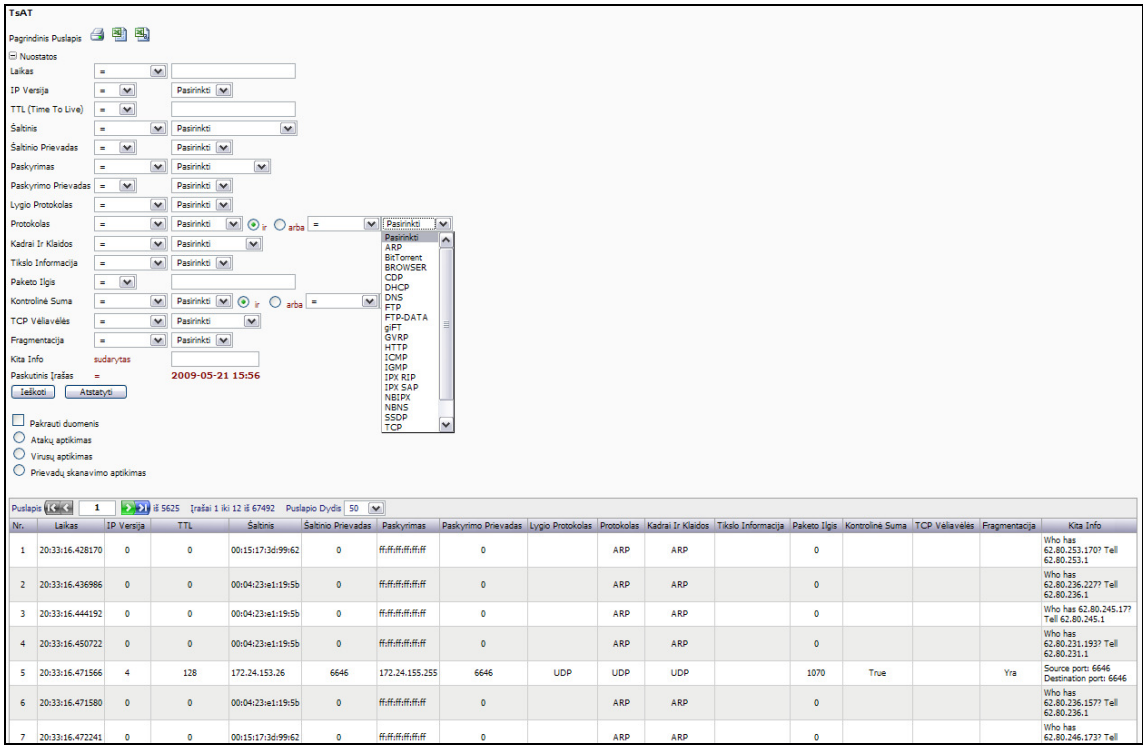
Duomenų pakrovimas – vykdomas failo įrašų įkrovimas į duomenų bazę.

Filtravimas – pasirenkami parametrai pagal tai, ką norima filtruoti (žr. 21 pav.).



20 pav. *Pagrindinis sistemos tinklapis*

Įrašų išsaugojimas – atlikus filtravimą, galima išsaugoti ar atsispausdinti išfiltruotus įrašus.



21 pav. *Įrašų ir filtravimo atvaizdavimas*

Platesnės sistemos funkcionalumas vykdomas, kai vartotojas atlieka filtravimą. Kitu atveju rodomi iš duomenų bazės atvaizduojami įrašai.

Duomenų pakrovimas reikalauja specifinio .csv failo aprašo. Be jo įrašai bus atvaizduojami nekorektiškai. Kaip susikurti .csv teisingą aprašymą žr. *2.2.3 .csv failo formatas.*

4. Darbo rezultatų analizė

Sistemos kūrimui panaudota PHP programavimo kalba. Duomenų saugojimui sudaryta MySQL duomenų bazė. Vartotojo sąsajai sukurti panaudota HTML, CSS ir JavaScript.

- PHP kodai rašomi su Zend Studio. Ši kalba pasirinkta todėl, kad ji skirta kurti dinaminius ir interaktyvius interneto puslapius, sudaro puikias galimybes bendradarbiauti su MySQL duomenų baze. Kol kas jokių tokio aukšto lygio analogų dar nesukurta;
- Notepad++ – PHP, JavaScript, CSS, HTML kodo redagavimui;
- phpMyAdmin – MySQL duomenų bazės administravimui;
- RegexBuddy – reguliariųjų išraiškų kūrimui ir testavimui;
- MagicDraw – UML diagramų braižymui;
- Kaip pagalbinė priemonė, siekiant taupyti laiką, naudojama programa Macromedia Dreamweaver CS4;
- Ikonų išpakavimui naudota Microangelo Toolset 6.

5. Patarimai, pastebėjimai, rekomendacijos

Sistemos instaliavimo instrukcija ir rekomendacijas, kaip parengti įrankį, rasite 4 priede. Arba užsukite į http://ik.su.lt/~minlgc/

Duomenų išsaugojimas neatsiejamas nuo filtravimo, t.y. pirmiausia reikia panaudoti filtravimą, tada išsaugoti įrašus.

V. IŠVADOS

Sukurta sistema lengvai ir greitai atvaizduoja įrašus internete/intranete, su galimybe įkelti naujus srautinius įrašus iš failo.

Užduoties įgyvendinimui pasirinktos HTML ir CSS puslapių aprašymo kalbos, JavaScript ir PHP programavimo kalbos, o duomenų saugojimui pasirinkta MySQL duomenų bazė. Šios technologijos pasirinktos todėl, kad yra paprastos naudoti, lengvai sąveikauja tarpusavyje.

Sudaryta reikalavimų specifikacija nusako būsimos sistemos vaizdą, iš kurios galima matyti jos atliekamas funkcijas. Sudaryta architektūros specifikacija nusako, kaip sistema turi būti realizuota. Veiklos diagrama parodo sistemos veikimo algoritmą priklausomai nuo vartotojo veiksmų, sudarytą klasių diagrama parodo sąryšį tarp skirtingų klasių, duomenų diagrama parodo kaip sistemoje realizuota duomenų struktūra, svetainės žemėlapis – pagrindinius puslapius, prie kurių vartotojas turi priėjimą.

Įintegruoti virusų, įsilaužimo, DOS („floodinimo“) dalinai automatiniai aptikimo algoritmai.

Sudaryta vartotojo dokumentacija pateikia išsamias sistemos diegimo, konfigūravimo ir naudojimosi instrukcijas.

Ištestavus sukurtą sistemą, nustatytos klaidos ir trūkumai, esantys sistemoje, į kuriuos reikėtų atsižvelgti ateityje tobulinant ją.

Tobulinant sistemą, būtų galima reorganizuoti padarant ją kuo paprastesne pradedantiesiems vartotojams, pateikiant daugiau pranešimų, kuriais būtų remiamasi priimant sprendimus apie tarnybinės stoties darbą.

Sukurta sistema tinkama naudojimui.

1. Kokybė

Sistema gali būti patalpinta daugelyje serverių, nes PHP interpretatorius veikia daugelyje platformų;

Sistema vienu metu gali naudotis neribotas vartotojų skaičius (vartotojų skaičių riboja tik serverio pajėgumas);

Sudaryta sistemos architektūra atitinka pagrindinius kokybės reikalavimus;

Sistemos funkcijos prieinamos per interneto naršyklę;

Vartotojo sąsajos formavimui naudojami tik standartiniai naršyklės palaikomi valdymo elementai, iš jų pagaminti komponentai;

Sistema užtikrina sankcionuotą duomenų priėjimą;

Sistema lengvai perkeliama į kitą kompiuterį;

Lengvai galima įkelti į sistemą kitos tarnybinės stoties srautinius įrašus, prieš tai apdorojant su „Wireshark“ programa.

VI. LITERATŪROS SĄRAŠAS

1. Top 11 Packet Sniffers. [žiūrėta 2009–03–25]. Prieiga per internetą <http://sectools.org/sniffers.html>
2. Packet Sniffer SDK: gigabit compatible sniffer/packet analyzer driver for Windows. [žiūrėta 2009–03–25]. Prieiga per internetą <http://www.microolap.com/products/network/pssdk/>
3. FrontPage – The Wireshark Wiki. [žiūrėta 2009–03–25]. Prieiga per internetą <http://wiki.wireshark.org/>
4. 1.4. Development and maintenance of Wireshark. [žiūrėta 2009–03–25]. Prieiga per internetą <http://www.wireshark.org/docs/wsdg_html_chunked/ChIntroDevelopment.html>
5. Kas yra PHP? Nikolajus Krauklis, 2002–01–28 [žiūrėta 2009–03–25]. Prieiga per internetą <http://www.php.lt/render/Articles;aid,27>
6. JavaScript, Straipsnis iš Vikipedijos, laisvosios enciklopedijos. [žiūrėta 2009–03–20]. Prieiga per internetą <http://lt.wikipedia.org/wiki/Javascript>
7. JavaScript is born – the second and third generations. [žiūrėta 2009–04–20]. Prieiga per internetą <http://www.howtocreate.co.uk/jshistory.html>
8. Kas yra MySQL, pradmenys bei naudojimasis iš PHP, Egle Karalyte. [žiūrėta 2009–04–25]. Prieiga per internetą <http://www.php.lt/render/Articles;aid,31>
9. SQL, From Wikipedia, the free encyclopedia [žiūrėta 2009–04–25]. Prieiga per internetą <http://en.wikipedia.org/wiki/SQL>
10. MySQL, From Wikipedia, the free encyclopedia. [žiūrėta 2009–05–25]. Prieiga per internetą <http://en.wikipedia.org/wiki/Mysql>
11. HTML, From Wikipedia, the free encyclopedia [žiūrėta 2009–04–25]. Prieiga per internetą <http://en.wikipedia.org/wiki/HTML>
12. Cascading Style Sheets, From Wikipedia, the free encyclopedia. [žiūrėta 2009–04–18]. Prieiga per internetą <http://en.wikipedia.org/wiki/Cascading_Style_Sheets>
13. Regular expression, From Wikipedia, the free encyclopedia. [žiūrėta 2009–04–25]. Prieiga per internetą <http://en.wikipedia.org/wiki/Regular_expression>
14. Regular Expression Library. [žiūrėta 2009–03–17]. Prieiga per internetą <http://regexlib.com/default.aspx>
15. PERL Regular Expressions. [žiūrėta 2009–03–15]. Prieiga per internetą <http://www.troubleshooters.com/codecorn/littperl/perlreg.htm>
16. X.200. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.itu.int/rec/T–REC–X.200–199407–I/en>
17. Linux Knowledge Base and Tutorial. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.linux–tutorial.info/modules.php?name=MContent&obj=page&pageid=142>
18. IP protocol suite. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.networksorcery.com/enp/topic/ipsuite.htm>
19. Ethertypes. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.networksorcery.com/enp/protocol/802/ethertypes.htm>

20. IP, Internet Protocol. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.networksorcery.com/enp/protocol/ip.htm>
21. Mobilūs Ad Hoc tinklai. [žiūrėta 2009–04–15]. Prieiga per internetą <http://kopustas.elen.ktu.lt/studentai/_media/mobilus_adhoc_tinklai.pdf?id=doktorantai&cache=cache>
22. Well known IP ports, 0 through 49151. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.networksorcery.com/enp/protocol/ip/ports00000.htm>
23. www.likit.lt. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.likit.lt>
24. Virtualūs privatūs tinklai. [žiūrėta 2009–04–15]. Prieiga per internetą <http://archyvas.vz.lt/news.php?strid=1118&id=112247>
25. PERFORMANCE – Spartinimas 2. [žiūrėta 2009–04–15]. Prieiga per internetą <http://hardas999.weebly.com/spartinimas–2.html>
26. Tractor svetaine. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.tdd.lt/~tract/new_site/kompiuteriai/1975–1976.html>
27. Ethernet Type Codes. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.cavebear.com/archive/cavebear/Ethernet/type.html>
28. Žodynas – Tinklų saugumas. [žiūrėta 2009–04–15]. Prieiga per internetą <http://www.tinklusaugumas.lt/cgi–bin/moin.py>
29. TCP and UDP port – From Wikipedia, the free encyclopedia. [žiūrėta 2009–04–15]. Prieiga per internetą <http://en.wikipedia.org/wiki/TCP_and_UDP_port>
30. Virus by Ports listing. [žiūrėta 2009–04–28]. Prieiga per internetą <http://www.jlathamsite.com/dslr/suspectports.htm>
31. Ethernet – Vikipedija. [žiūrėta 2009–04–28]. Prieiga per internetą <http://lt.wikipedia.org/wiki/Ethernet>
32. TCP/IP protokolų šeima. [žiūrėta 2009–04–28]. Prieiga per internetą <http://intra.zemko.lt/~edas/wp-content/uploads/2007/09/tcp-ip.ppt>
33. Softkey: Programos aprašymas: Zend Sturio. [žiūrėta 2009–04–28]. Prieiga per internetą <http://www.softkey.lt/catalog/program.php?ID=17802>
34. Notepad++ 5.2. [žiūrėta 2009–04–28]. Prieiga per internetą <http://forum.softas.lt/ofisas/1904-notepad-5.2.html>

ANOTACIJA

Informacijos srautai šiuolaikiniuose tinkluose pasižymi didele sparta ir kintamumu, todėl šių srautų detali analizė yra aktuali problema. Šios analizės rezultatai gali būti panaudoti tinklo aptarnavimo kokybei QoS (Quality of Service – Paslaugos kokybė) vertinti ir valdymo sprendimams priimti.

Šiame darbe nagrinėjama programinė įranga, skirta tirti srautų dinamiką ir padėti vartotojui aptikti lokaliame tinkle įsilaužimus, šiukšles, perkrovas, gedimus.

Įrankis sukurtas, naudojant PHP aprašymo kalbą, HTML, CSS, MySQL ir JavaScript technologijas. Dirbant su šia sąsaja, vartotojui pakanka būti susipažinusiam su minimalioms žiniomis apie tinklo srautų savybėmis.

SUMMARY

Information flows in modern networks describes a high speed and volatility, today's detailed analysis of these flows is an actual problem. These analytical results can be used for network quality of service (QoS) assessment and management decisions.

In this work the software is designed to investigate the dynamics of flows and to help the user detect local network attacks, garbage, congestion, failures.

The tool is designed, using the description of the PHP language, HTML, CSS, MySQL, and JavaScript technologies. Working with this interface, the user sufficient must to known minimal knowledge of the network traffic characteristics.

TERMINŲ IR SANTRUMPŲ ŽODYNAS

HTML (Hypertext Markup Language „Hiperteksto žymėjimo kalba“) – tai kompiuterinė žymėjimo kalba, naudojama pateikti turinį internete.

CSS (angl. Cascading Style Sheets) – kalba, skirta nusakyti kita struktūrine kalba aprašyto dokumento vaizdavimą. Dažniausiai CSS aprašomas HTML dokumentų pateikimas, tačiau ją galima taikyti ir įvairiems kitiems XML dokumentams.

WWW – interneto dalis, resursai, kuriuos internete galima pasiekti naudojant URL (Vieningus Resursų Identifikatorius).

HTTP – pagrindinis metodas pasiekti informaciją pasauliniame tinkle (WWW). Pradinė protokolo paskirtis – pateikti standartinį būdą HTML puslapių skelbimui ir skaitymui.

FTP (trumpinys nuo angl. File Transfer Protocol, „Failų Perdavimo Protokolas“) – standartas failų perdavimui.

XML – yra W3C rekomenduojama bendros paskirties duomenų struktūrų bei jų turinio aprašomoji kalba.

W3C – yra konsorciumas leidžiantis programinės įrangos standardus („rekomendacijas“, kaip jie jas vadina) žiniatinkliui.

JavaScript – objektiškai orientuota skriptų programavimo kalba, besiremianti prototipų principu.

IRC – Internet Relay Chat arba IRC yra ryšio protokolas ir interneto paslauga, skirti gyvam bendravimui Internete (operatyviam apsikeitimui trumpomis tekstinėmis žinutėmis).

MB – megabaitas, 1024 kilobaitai, 1024*1024 baitai (informacijos kiekio matavimo vienetas, sudarytas iš 8 bitų sekos).

Unicode – standartas, apibrėžiantis beveik visų kalbų abėcėlių bei papildomų simbolių kodavimą kompiuteriuose.

Regular expressions – tai specialios paskirties simbolių eilutės aprašančios tam tikro teksto paieškos šabloną.

DHTML – dinaminis HTML.

AJAX – arba Asinchroninis JavaScript ir XML programavimas – terminas, apibrėžiantis svetainių programavimo technologiją, naudojančią šias priemones maksimaliam interaktyvumui pasiekti.

PHP – plačiai paplitusi dinaminė interpretuojama programavimo kalba, sukurta 1997 m. ir specialiai pritaikyta svetainių kūrimui.

CGI (Common Gateway Interface) – protokolas, apibrėžiantis, kaip turi bendrauti WWW serveris ir jo vykdomos programos, skirtos iš naršyklės gautai informacijai apdoroti ir/arba dinaminiams puslapiams generuoti.

Apache, IIS, PWS, OmniHTTP, BadBlue – programinė įranga, skirta interpretuoti programavimo kalbai.

DB – Duomenų bazė yra organizuotas (susistemintas, metodiškai sutvarkytas) duomenų rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu.

SQL (Struktūrizuota užklausų kalba, Structured Query Language) – populiariausia iš šiuo metu naudojamų kalbų, skirtų aprašyti duomenis ir manipuliuoti jais reliacinių duomenų bazių valdymo sistemose.

MySQL – viena iš reliacinių duomenų bazių valdymo sistemų, palaikanti daugelį naudotojų, dirbanti SQL kalbos pagrindu.

API – Aplikacijų programavimo sąsaja (angl. Application Programming Interface) – tai sąsaja, kurią suteikia kompiuterinė sistema, biblioteka ar programa tam, kad programuotojas per kitą programą galėtų pasiekti jos funkcionalumą ar apsikeistų su ja duomenimis.

ODBC (angl. akronimas Open Database Connectivity) yra standartizuota taikomosios programinės įrangos (aplikacijų) programavimo sąsaja (API) prisijungimui prie duomenų bazių.

Failas – (angl. file, liet. byla, rinkmena, tvarkmena) – bitų seka, saugoma kompiuteryje kaip vienas vienetas.

Įrašas – sukurtoje sistemoje aprašytas teksto dalies vienetas.

PRIEDAI

1. PRIEDAS. **Tarptinklinis lygis**

Šitiems protokolams paskiriamas Ethertype[19] numeris.

Šiame lygyje sprendžiama duomenų perdavimo problema tarp tinklo mazgų, kai jau žinoma ryšio lygmens metodika. Tarptinklinis lygis nusako taisykles, kuriomis vadovaujantis duomenys perduodami vienam ar kitam tinklo komponentui. Tai vadinama maršrutizavimu. Tokie protokolai kaip ICMP yra aukštesnio lygio, tačiau atlieka tarptinklines funkcijas, todėl taip pat yra priskiriami šiam lygiui.

ARP (Address Resolution Protocol – Adresų nustatymo protokolas). Priklauso tarptinklinio lygio protokolams. Jis atsako už IP adreso vertimą į aparatūrinį adresą. ARP gavęs IP adresą iš pradžių ieško jo atitikmens savo talpyklos, jeigu atranda, tai siunčia paketą konkrečiam tinklo įrenginiui turinčiam MAC adresą. Jeigu adresas nerastas tai daromos „broadcast“ užklausos lokaliame tinkle, kad nustatyti tinklo įrenginį kuris turi tam tikrą IP adresą.

IP (Internet Protocol – Interneto protokolas). Pagrindinė šio protokolo funkcija – užtikrinti potinklių tarpusavio veiklą, tam, kad būtų galima perduoti duomenis.

IP atlieka 4 funkcijas:

- Duomenų perdavimą,
- Adresacija,
- Maršrutizaciją,
- Datagramų fragmentaciją.

IP perduoda duomenis naudodamas neorientuoto jungimo metodą. IP neužtikrina duomenų pristatymo, neužtikrina paketų be klaidų ir nesiunčia tarnybinių pranešimų dėl ryšio užmezgimo.

IPv6 (Internet Protocol version 6 – Interneto protokolas versija 6) – tai nauja interneto protokolo (IP) versija, sukurta tam, kad pakeistų dabar naudojamą IPv4 protokolą ir išspręstų su juo susijusias problemas. Pagrindiniai naujos versijos bruožai:

- Palaiko milijardus kompiuterių net jeigu adresų erdvė naudojama neefektyviai,
- Sumažina maršrutizacijos lenteles,
- Supaprastina protokolą, maršrutizatoriai gali greičiau apdoroti paketus,
- Užtikrina didesnį duomenų saugumą,
- Daugiau kreipia dėmesio į paslaugos tipą, dalinai realaus laiko duomenims,
- Transliacija, leidžianti nustatyti diapazonus,
- Galimybė keliauti su kompiuteriu, išliekant Internete ir nekeičiant IP adreso,
- Leidžia protokolui tobulėti (evolve) ateityje,
- Leidžia senam ir naujam protokolui egzistuoti daug metų.

1992 m. buvo atrinkta keletas rimčiausių pasiūlymų. Iš jų Deering ir Francis pasiūlymas

vadinamas SIPP (Simple Internet Protocol Plus). Dabar jam priskirtas ženklas IPv6. Nesuderinamas su IPv4, bet suderinamas su TCP, UDP, ICMP, IGMP, OSPF, BGP, ir DNS. Reikalingos nedidelės modifikacijos, susijusios su adresavimu. Daugiau informacijos yra RFC 1883 – 1887.

MPLS (Multi Protocol Labeling Switching) – srautų valdymas atliekamas įrašant specialias žymes į paketų antraštes. Antraščių žymės perskaitomos maršrutizatoriuose, kur priklausomai nuo įrašo priimamas sprendimas apie paketo likimą. MPLS nėra savarankiškas QoS protokolas. Jis tiktai palengvina kitų protokolų realizavimą. MPLS protokolas atlieka šias funkcijas:

- Pateikia srautų apkrovos valdymo galimybes,
- Yra nepriklausoma nuo 2 ir 3 lygmenų protokolų,
- Suteikia priemones IP adresų susiejimui su fiksuoto ilgio žymėmis,
- Suderinama su egzistuojančiais maršrutizavimo protokolais,
- Palaiko IP, ATM ir Frame Relay 2 lygmens protokolus.

ARP (Reverse Address Resolution Protocol) – protokolas skirtas pagal žinomą tame pačiame tinkle esančio mazgo MAC adresą nustatyti jo loginį IP adresą. Skirtingai nuo ARP, RARP protokolas reikalauja, kad vienas kuris nors iš mazgų (serveris) saugotų IP ir MAC atitikmenų lentelę.

2. PRIEDAS. **Transportinis lygis**

Šitiems protokolams paskiriamas IP[20] numeris.

Perdavimo lygio problematika – užtikrinti patikimą duomenų perdavimą, t.y. nustatyti, ar visi išsiųsti duomenys buvo gauti. Šiam lygiui priskirti protokolai dažniausiai skirstomi į patikimus ir nepatikimus. Patikimi protokolai užtikrina duomenų perdavimą, tuo tarpu nepatikimi protokolai nevykdo duomenų patikros ir to pasėkoje veikia sparčiau.

AH (IP Authentication Header – paketų siuntėjo autentifikacija) – tai IPSec protokolų rinkiniui priklausantis protokolas užtikrinantis paketų autentiškumą, prisegdamas užkoduota paketo kontrolinę suma (angl. checksum).

CBT (Core Based Trees) – sukuria grupėms bendrą multiperdavimo paskirstymo medį ir yra skirtas inter– arba intra–domenų multiperdavimo maršrutizavimui. CBT gali naudoti atskirą multiperdavimo maršrutizavimo lentelę, arba gali naudoti tam kad nustatytų kelią tarp siuntėjo ir gavėjo.

DSR (Dynamic Source Routing Protocol – dinaminis maršrutizavimo protokolas) – pagrįstas siuntėjo įrenginio maršrutizacijos principais[21]. Čia duomenų paketų antraštėse saugoma informacija apie eilę įrenginių, per kuriuos šie duomenų paketai turi būti persiunčiami. Taigi tik įrenginys siuntėjas turi žinoti visus reikiamo kelio tarpinius mazgus, o tarpiniai mazgai turi informaciją tik apie savo kaimynus. Kaip ir AODV protokolo atveju, įrenginiai turi laikinai saugoti žinomų kelių informaciją.

DVMRP (Distance Vector Multicast Routing Protocol) – Tiktais maršrutizuoja multiperdavimo datagramas ir tai daro su kiekviena Autonomine Sistema. DVMRP yra Atvirkštinis kelias transliuojančiųjų algoritmams.

EGP (Exterior Gateway Protocol – išorinis slenkstinis maršrutizavimo protokolas) – Šis maršrutizavimo protokolas yra naudojamas tada, kai reikia apsikeisti maršrutizavimo informacija tinkluose, valdomuose skirtingų administratorių. EGP plačiai naudojamas DDN (Defence Data Network) ir NSF (National Science Foundation Network) tinkluose.

ESP (Encapsulating Security Payload – Inkapsuliuotas saugumo turinys) – suteikia paketams konfidencialumo garantiją, juos užkoduojant pasirinktais kodavimo algoritmais. Jeigu gaunamas ESP paketas ir jį pavyko sėkmingai atkoduoti, tuomet galima tvirtinti, jog paketo jokia trečioji šalis siuntimo metu negalėjo atkoduoti su sąlyga, jog abi bendraujančios šalys dalinasi slaptuoju seanso raktu ir tik jos žino tą raktą. ESP protokolas – tai saugaus turinio uždarymo protokolas. Jis užtikrina autentifikavimą, datagramos vientisumą, vykdo datagramos duomenų šifravimą.

GGP (Gateway to Gateway Protocol) – IP protokolas yra naudojamas host–to–host datagramų sistemoje, sujungtų tinklų, kitaip vadinamas Catenet. Tinklą sujungiantys prietaisai yra vadinami tinklų sąsajomis (angl. gateway). Šie vartai bendrauja tarpusavyje kontrolės tikslais per Gateway–to–gateway protokolą (GGP). Kartais vartai ar paskirties adresas gali bendrauti su šaltinio kompiuteriu, pavyzdžiui, pranešant apdorojimo klaidą. Tokiems tikslams ICMP naudojamas.

GRE (Generic Routing Encapsulation – Bendroji maršrutizavimo inkapsuliacija) – Protokolas skirtas apsaugoti TCP/IP srautą tarp Windows 95/98/NT klientų, prisijungusių prie interneto per PPP ir Windows NT serverius, esančius vietiniame tinkle, už ugniasienės.

HMP (Host Monitoring Protocol – Pagrindinio kompiuterio Kontroliavimo Protokolas) – panaudotas, kad surinktų informaciją nuo pagrindinių kompiuterių įvairiuose tinkluose. Pagrindinis kompiuteris yra apibrėžtas kaip adresavimo interneto objektas, kuris gali nusiųsti ir gauti žinutes; tai apima pagrindinius kompiuterius tokius kaip serverio pagrindiniai kompiuteriai, asmeninės kompiuterizuotos darbo vietos, terminalų koncentratoriai, paketo jungikliai ir tinklų sietuvai.

ICMP (Internet Control Message Protocol – Interneto valdymo žinučių protokolas) – tai protokolas skirtas naudoti kaip pagalba kitiems protokolams, bei sistemos administratoriams, tam kad patikrinti sistemos jungiamumą bei aptikti konfigūracijos klaidas tinkle. ICMP klaidų pranešimai yra naudojami tada kai reikia pranešti apie problemą, kuri trukdo įvykti kažkokio tai paketo pristatymui. Paketai, nešantys ICMP pranešimą, neturi specialaus prioriteto – jie nukreipiami kaip ir bet kuris kitas paketas, su viena maža išimtimi. Jei paketas, nešantis ICMP klaidos pranešimą pats yra klaidos priežastimi, klaidos pranešimas yra nesiunčiamas[28].

ICMPv6 (Internet Control Message Protocol for IPv6) – Tas pats protokolas kaip ir ICMP su keletu patobulinimu.

IDPR (Inter–Domain Policy Routing Protocol – Tarpdomeninis maršrutizavimo protokolas) – labiau išplėtotas kriptografinis atpažinimas. Kadangi maršrutizacijos protokolai naudojasi kitais protokolais, pavyzdžiui, BGP naudoja TCP sesiją, tai pažeidžiamumas priklauso ir nuo naudojamų protokolų saugumo. Saugiems maršrutizacijos ir kitiems mechanizmams reikalingas patogus raktų paskirstymas.

IFMP (Ipsilon Flow Management Protocol) – protokolas tam, kad leistų mazgui instruktuoti gretimą mazgą prijungiant lygmenį 2 į apibrėžtą IP srautą. Tai leidžia efektyvesnę prieigą prie laikytos spartinančiojoje atmintyje maršruto parinkimo informacijos tam srautui. Taip pat įgalina mazgui perjungti tolimesnius paketus, priklausančius apibrėžtam srautui lygmenyje 2 greičiau, negu persiųsti jiems lygmenyje 3.

IGAP (IGMP for user Authentication Protocol) – variantas IGMPv2, kuris prideda vartotojų atpažinimą. IGAP įgalina IP multiperdavimo paslaugų teikėjui nustatyti autentiškumą prašymams prisijungti prie specifinės multiperdavimo grupės, pagrįstos vartotojų informacija. Visas IGAP žinutes nusiunčiamos su IP TTL lauko komplektu į 1 ir naudoja IP Router Alert parinktį jų IP antraštėje pagal IGMPv2 reikalavimus.

IGRP (Interior Gateway Routing Protocol – Vidinių vartų maršrutizavimo protokolas) – Užtikrina skirtingų greičių media paslaugas su skirtingomis vėlinimo charakteristikomis. Palaiko 3 rūšių maršrutizatorius:

- Vidaus – yra laikomi maršrutizatoriai turintys sąsają su potinkliais,
- Sistemos – skirti tinklams AS viduje,
- Išorinius – yra skirti tinklams už AS ribų.

IPPCP (IP Payload Compression Protocol) – Laiko IPv4 Protokolo lauką ar IPv6 Kitas originalios IP antraštės Antraštės laukus.

IRTP (Internet Reliable Transaction Protocol) – pilnas dupleksas, orientuotas sandoris, pagrindinis kompiuteris į pagrindinį protokolą, kuris aprūpina patikimą rūšiuotą pristatymą paketų duomenų, pavadintų sandorio paketais.

L2TP (Level 2 Tunneling Protocol – Antro lygio tuneliavimo protokolas) – Microsoft ir Cisco sujunge PPTP ir L2F protokolų geriausias savybes, taip buvo sukurtas tuneliavimo standarto protokolas pavadintas L2TP. L2TP yra tinklo protokolas palengvinantis PPP kadrų tuneliavimą per viešąjį tinklą. Jis apjungia PPP kadrus siuntimui per IP, X25, Frame Relay ar ATM tinklus. Apjungtų

PPP kadrų duomenys užšifruojami ir/arba suspaudžiami. L2Tp gali būti naudojamas tiesiai per įvairius WAN tinklus. L2TP naudoja UDP ir serija L2TP žinučių, tunelių palaikymui IP tipo tinkluose. L2TP leidžia daugialypius tunelius per tą patį abipusį ryšį.

MLD (Multicast Listener Discovery) – Šio protokolo tikslas įgalina kiekvienam IPv6 maršrutizatoriui atrasti buvimą multiperdavimo klausytojų ant jo tiesiogiai prijungtų saitų ir nustatyti specialiai, kurie multiperduoda adresus ir kelia susidomėjimą tiems mazgams.

MOSPF (Multicast Open Shortest Path First – Multiperdavimas atidarant trumpiausią kelią iš pradžių) – OSPF versijos pratesimas nr. 2.

MTP (Multicast Transport Protocol – Multiperdavimo transporto protokolas) – MTP aprūpina patikimą multiperdavimo pristatymą vieno laiku daugeliui ir daugelio–daugeliui pagrindu. Tai gali būti panaudojama kaip bet kokios tinklo architektūros Transporto lygmuo, jei datalink lygmuo apima tam tikrą palaikymą multiperdavimui.

NARP (NBMA Address Resolution Protocol – Adreso perkodavimo protokolas) – leidžia šaltinio terminalą (pagrindinis kompiuteris ar maršrutizatorius), susisiekti per Non–Broadcast, Multiprieigos lygmens (NBMA) tinklus ir sužinoti paskirties terminalo NBMA adresus, jei paskirties terminalas yra sujungtas į tą patį NBMA tinklą kaip šaltinis.

NETBLT (Network Block Transfer – Tinklo bloko perdavimas) – yra transportinis lygmens protokolas, numatytas greitam perkėlimui didelio kiekio duomenų tarp kompiuterių. Tai aprūpina perkėlimą, kuris yra patikimas ir srauto valdomas, ir yra projektuotas, kad aprūpintų maksimalų pralaidumą per plačią tinklų įvairovę. Nors NETBLT šiuo metu veikia Interneto protokolo (IP) viršūnėje, tai sugeba paveikti bet kokio duomenų paketinio protokolo funkcijas, kuris panašaus į IP.

NVP (Network Voice Protocol – Tinklo Balso Protokolas) – įgyvendintas iš pradžių 1973 m. gruodį, ir buvo naudojimas nuo tada vietiniam ir transnet skubiai atliekamam balso susisiekimui per ARPANET.

OSPF (Open Shortest Path First Routing Protocol – Pirmo atviro trumpiausio kelio) – grupes kaimyninių tinklų AS viduje sugrupuoti vienus su kitais į sritis. Kiekviena sritis turi savo atskirą duomenų bazę. Iš kitų protokolų OSPF išsiskiria dviem pagrindinėms charakteristikoms:

- Protokolas yra atviras, tai reiškia, kad jis yra priskiriamas viešam domenui,
- Protokolas veikia SPF algoritmo pagrindu, kuris kartais vadinamas Dijkstra algoritmu.

PGM (Pragmatic General Multicast – Pragmatinis bendras multiperdavimas) – patikimas multiperdavimo transporto protokolas programoms, kur reikalinga tvarkytas ar netvarkytas, neidentiškas, multiperdavimo duomenų pristatymas iš daugialypių šaltinių į daugialypius gavėjus.

PGM garantuoja, kad gavėjas grupėje ar gauna visus duomenų paketus iš perdavimo ir remonto, ar sugeba aptikti nepataisomą duomenų paketo praradimą.

PIM (Protocol Independent Multicast – Nepriklausomas nuo protokolo multiperdavimas) – šeima multiperdavimo maršruto parinkimo protokolų, kurie gali aprūpinti „vieną daugeliui“ ir dalijimui „daugelis daugeliui“ duomenų per internetą. „Nepriklausoma nuo protokolo“ dalis siejasi su faktu, kad PIM neapima savo topologijos atradimo mechanizmo, bet vietoj to naudoja maršruto parinkimo informaciją, tiektą kitų tradicinių maršruto parinkimo protokolų tokių kaip Border Gateway Protocol (BGP).

RDP (Reliable Data Protocol – Patikimas duomenų protokolas) – projektuotas, kad aprūpintų patikimą duomenų transporto paslaugą paketu pagrįstas programas tokias kaip tolimas įkėlimas ir pašalinimas. Protokolas yra numatytas, kad būtų paprasta įgyvendinti, bet vis dar būti efektyvus aplinkose, kur gali būti ilgų perdavimo užlaikymų ir praradimo ar ne–nuoseklus žinutės dalių pristatymas.

RSVP (Resource ReSerVation Protocol – Tinklo resursų rezervavimo protokolas) – darbo principas yra signalizacijos pranešimais iš tinklo mazgų pareikalaujami atitinkami tinklo resursai.

SCTP (Stream Control Transmission Protocol – Srautų valdymo perdavimo protokolas) – naujas IP transporto protokolas, egzistuojantis ekvivalentiškame lygmenyje su UDP (Vartotojų Duomenų paketo Protokolas) ir TCP (Perdavimo kontrolės protokolas), kurie aprūpina transporto lygmens funkcijas daugelio interneto programų

SEND (SEcure Neighbor Discovery Protocol – Saugus kaimyninis atradimo protokolas) – IPv6 mazgai naudoja Kaimyninį Atradimo Protokolą (NDP), kad atrastų kitus mazgus, nustatytų jų lygmens adresus, surastų maršrutizatorius ir palaikytų pasiekiamumo informaciją apie kelius aktyviems kaimynams. Jei negautas, NDP yra neapsaugotas nuo įvairių atakų.

SDRP (Source Demand Routing Protocol) – tikslas yra remti šaltinio pradėtą maršrutų pasirinkimą, papildant maršruto pasirinkimą, pateikiant esamus maršrutus protokolams, tarpdomenui ir intradomeno maršrutams.

SKIP (Simple Key management for Internet Protocol – Paprastas raktinis valdymas Interneto protokolui) – Mobili IP specifikacija nustato mechanizmus, kurie įgalina mobiliam pagrindiniam kompiuteriui palaikyti ir panaudoti tą patį IP adresą, kadangi jis keičia savo punktą priedo į tinklą. Mobilumas duoda suprasti aukštesnius saugumo pavojus negu statiška operacija, todėl, kad duomenų srautas gali kartais paimti nenuspėtus tinklo kelius su nežinomomis ar nenuspėjamomis saugumo charakteristikomis.

ST (Internet Stream Protocol – Interneto srauto protokolas) – yra protokolo bandomasis ryšį–orientuotas tarpjungimas į sistemą, kuris veikia tame pačiame lygmenyje kaip „connectionless“ IP. Tai buvo išvystyta, kad palaikytų efektyvų pristatymą duomenų srautų į vienas ar daugialypes paskirtis programose, kurioms reikalingos garantuotos paslaugos kokybės. ST2 yra dalis IP protokolo šeimos ir tarnauja kaip priedas, ne pakeitimas, IP. Pagrindiniai taikomieji protokolo taškai yra skubiai atliekamas transportas multimedijos duomenų, pavyzdžiui, skaitmeninių girdimųjų, video paketo šaltinių ir paskirstyto imitavimo/žaidimo per internetą.

TCP (Transmission Control Protocol – Perdavimo kontrolės protokolas) – į sujungimus orientuotas protokolas, kuris garantuoja patikimą baitų srauto perdavimą tarp dviejų sistemų. TCP protokolas atlieka duomenų perdavimą, klaidų aptikimą, bet jų neatstato. Prieš siunčiant duomenis, du procesai turi nustatyti tarpusavio ryšį, t.y. jie turi nusiųsti preliminarius segmentus vienas kitam, kad nustatytų parametrus ir užtikrintų duomenų perdavimą [29].

TMux (Transport Multiplexing Protocol – Transporto multipeksingo protokolas) – protokolas numatytas, kad optimizuotų perdavimą dideliais numeriais mažų duomenų paketus, kurie yra sukurti situacijose, kur daugelis interaktyvūs Telnetas ir Rlogin seansai yra sujungti į kelis pagrindinius kompiuterius tinkle. Šitose situacijose, TMux gali pagerinti tinklo ir pagrindinį atlikimą.

UDP (User Datagram Protocol – Vartotojo datagramų protokolas) – į sujungimus neorientuotas protokolas. Dėl perdavimo funkcijos ir tam tikro paprasto klaidų tikrinimo jis labai nedaug prideda papildomos informacijos prie IP – tinklo lygio protokolo. UDP neužtikrina patikimo perdavimo, todėl labiau tinka garsinei arba vaizdinei informacijai perduoti realiu laiku.

UDP–Lite (Lightweight User Datagram Protocol – Lengvojo svorio vartotojo datagramų protokolas) – yra panašus į UDP, bet gali taip pat aptarnauti programas linkusias į klaidas tinklo aplinkose, kurios gali iš dalies sugadinti tiektas naudingąsias apkrovas, o ne išmesti.

VMTP (Versatile Message Transaction Protocol – Visapusiškas žinutės sandorio protokolas) – specialiai projektuotas, kad palaikytų sandorio modelį susisiekimo, kaip iliustruotas tolimo procedūros paklausimo (RPC – Remote Procedure Call). Pilna VMTP funkcija, apimdama palaikymą saugumui, realaus–laiko, asinchroninės žinutės keitimas, srautiniam duomenų siuntimui, multiperdavimui ir „idempotency“, aprūpina naudingą pasirinkimą VMTP vartotojų lygmeniui

VRRP (Virtual Router Redundancy Protocol – Virtualus maršrutizatoriaus atleidimo protokolas) – VRRP yra projektuotas, kad pašalintų kiekvieną nesėkmės punktą, neatskiriant nuo statiškos išsiųstos aplinkos. VRRP apibrėžia rinkimų protokolą, kuris dinamiškai skiria atsakomybę už virtualų maršrutizatorių į vieną iš VRRP maršrutizatorių LAN‘e.

Šitiems protokolams paskiriamas vienas ar daugiau SCTP, TCP ar UDP jungčių[22].

Dažniausiai tinklo programinės įrangos naudojamas lygis, skirtas tinklu bendrauti su kito tinklo mazgo programine įranga. Naudojami protokolai – HTTP, FTP, SNMP, SMTP, POP3, DNS, taip pat daugelis kitų. Standartiniams protokolams yra gana griežtai išskiriami prievadų numeriai, tačiau šiuolaikinės programinės įrangos autoriai savo produktams savarankiškai priskiria prievadų numerius.

ACAP (Application Configuration Access Protocol – Taikomasis konfigūracijos prieigos protokolas) – Taikomasis Konfigūracijos Prieigos Protokolas projektas palaikyti tolimą atmintinę ir programos parinkties, konfigūracijos ir privilegijuotos informacijos prieigą.

AODV (Ad hoc On–Demand Distance Vector – Laikinas pagal pareikalavimą atstumo vektorius) – Laikinas Pagal pareikalavimą Atstumo Vektorius (AODV) protokolo maršruto parinkimas yra numatytas naudojimui mobilių mazgų laikiname tinkle.

APEX (Application Exchange Core – Taikomasis keičiamas branduolys) – aprūpina ištęsiamą, asinchroninę žinutės perdavimo paslaugą taikymo lygmenų programoms. jos branduolyje, aprūpina geriausių pastangų duomenų paketo paslaugą.

ASAP (Aggregate Server Access Protocol – Bendras tarnybinės stoties prieigos protokolas) – kartu su Endpoint Handlespace Redundancy protokolu, aprūpina aukšto tinkamumo duomenų perdavimo mechanizmą per IP tinklus.

ATMP (Ascend Tunnel Management Protocol – Didejantis tunelio valdymo protokolas) – protokolas, šiuo metu būdamas panaudotas, didėja į susisiekimo produktus, kad leistų prisijungimo telefonu kliento programinei įrangai gauti virtualų buvimą vartotojo namų tinkle.

AURP (AppleTalk Update–based Routing Protocol – AppleTalk atnaujinimu pagrįstas maršruto parinkimo protokolas) – aprūpina plačius rajono maršruto parinkimo išplėtimus AppleTalk maršruto parinkimu protokolų ir yra visiškai suderinamas su AppleTalk 2 Faze

BFTP (Background File Transfer Program – Foninė Rinkmenų persiuntimo programa) – Interneto fono rinkmenos perdavimo paslauga, kuri yra pastatyta ant trečiosios šalies FTP perkėlimo modelio. Jokie nauji protokolai nėra apimti.

BGP (Border Gateway Protocol) – tarpautonominis Sistemos maršruto parinkimo protokolas. Pirminė funkcija BGP sistema kalbėjimas, kuris turi apsikeisti tinklo pasiekiamumo informaciją su kitomis BGP sistemomis

BOOTP (Bootstrap Protocol – Pakopinio paleidimo protokolas) – leidžia pagrindiniam kompiuteriui konfigūruoti save dinamiško paleidimo laike.

CARD (Candidate Access Router Discovery) – CAR atradimas apima identifikavimą CAR IP adreso ir gebėjimo, kurį mobilus mazgas galėtų panaudoti handover sprendimui.

CFDP (Coherent File Distribution Protocol – Nuoseklus rinkmenos dalijimo protokolas) – projektuotas, kad pagreitintų rinkmenos perdavimo operacijas „vienas daugeliui“, kurie rodo duomenų srauto sąsają medijoje su transliavimo gebėjimu.

Chargen (Character Generator Protocol – Simbolių generatoriaus protokolas) – Naudingas pašalinimo ir matavimo įrankis yra simbolių generatoriaus paslauga. Simbolių generatoriaus paslauga tiesiog siunčia duomenis be dėmesio į įvedimą.

CLDAP (Connection–less Lightweight X.500 Directory Access Protocol – Ryšio lengvojo svorio katalogo prieigos protokolas X.500) – projektuotas, kad aprūpintų prieigą prie Katalogo, neužsitraukdamas išteklių reikalavimų Katalogo Prieigos Protokolo (DAP).

CMP (Certificate Management Protocols – Sertifikuotas valdymo Protokolas) – Valdymo protokolai privalo palaikyti prisijungusias sąveikas tarp Viešos Raktinės Infrastruktūros (PKI – Public Key Infrastructure) komponentų.

COPS (Common Open Policy Service – Bendra atvira saugumo paslauga) – buvo projektuota, kad paskirstytų aiškią tekstinę saugumo informaciją nuo centralizuoto Esminio sprendimo Punkto (PDP) į komplektą Saugumo Spaudimo Punktą (PEP) internete.

CRANE (Common Reliable Accounting for Network Element – Bendras patikimas sudarantis tinklo elementą) – TCP ir SCTP yra du transporto lygmens protokolai, kurie įvykdo CRANE patikimumo reikalavimą. Kiekvienas jų GALI būti panaudotas, kad perduotų CRANE žinutes.

CXTP (Context Transfer Protocol – Kontekstinis perkėlimo protokolas) – įgalina įgaliotą kontekstinį perkėlimą. Kontekstinis perkėlimas leidžia geresnį palaikymą mobiliam mazgui, kad vykdančios programos, mobiliuosiuose mazguose, galėtų veikti su minimaliais trukdžiais.

Daytime (Daytime Protocol – Dienos laiko protokolas) – tarnybinė stotis grąžina datos/laiko eilutę kūrėjui. Eilutės formatas yra nenustatytas.

DCAP (Data Link Switching Client Access Protocol – Duomenų perdavimo linija, perjungianti kliento prieigos protokolą) – panaudotas tarp darbo stočių ir maršrutizatorių, kad

transportuotų SNA/NetBIOS duomenų srautus.

DHCP (Dynamic Host Configuration Protocol – Dinamiškas pagrindinis konfigūracijos protokolas) – skirtas dinaminiam IP adresų priskyrimui (nuomai – lease). Kompiuteris gali nežinoti savo IP adreso prisijungdamas prie tinklo, tačiau specialūs DHCP serveriai gali jam tam tikram laikui suteikti šį adresą. Tokios funkcijos naudingos nešiojamuose kompiuteriuose, esant nepakankamai IP adresų erdvei, etc. Esminiai parametrai: aptarnavusio serverio adresas, priskyrimo laikas, kuriam laikui išnuomotas adresas.

DHCPv6 (Dynamic Host Configuration Protocol for IPv6 – Dinamiškas pagrindinis konfigūracijos protokolas IPv6) – įgalina DHCP tarnybinėms stotims praeiti konfigūracijos parametrus tokius kaip IPv6 tinklo adresus į IPv6 mazgus.

DIAMETRE – pagrindo protokolas yra skirtas, kad aprūpintų Identifikavimą, Leidimą ir Apskaitą (AAA – Authentication, Authorization and Accounting) struktūra programoms tokioms kaip tinklo prieiga ar IP judrumas.

DICT (Dictionary Server Protocol – Žodyninis tarnybinės stoties protokolas) – Besiremiantys serveriai/klientai leidžia keletui klientų tinklu jungtis prie vieno serverio ir vykdyti paiešką. Tačiau šis protokolas apsiriboja žodžių paieška tekstiniuose failuose ir nėra lankstus.

Discard (Discard Protocol – Atmetimo protokolas) – Naudingas pašalinimo ir matavimo įrankis – atmetimo priežiūra. Atmetimo priežiūra tiesiog atmeta bet kokius duomenis, kuriuos ji gauna.

DIXIE – projektuotas naudojimui mažesnių pagrindinių kompiuterių (pavyzdžiui, Macintosh ir asmeniniai kompiuteriai), kurie neturi apdorotos galio ar būtinos programinės įrangos, kad įgyvendintų pilną OSI protokolo dėklą

DMSP (Distributed Mail Service Protocol – Paskirstytas pašto paslaugos protokolas) – PCMAIL sistemos dalis. Pranešimai gali būti ne viename serveryje. Paštą galima atsisiųsti į savo kompiuterį ir atsijungti.

DNS (Domain Name System – Sričių vardų sistema) – taikomųjų programų lygio tarnybinis protokolas. Šis protokolas nėra simetriškas: jame apibrėžti DNS–serveriai ir DNS–klientai. DNS–serveriai saugoja dalį paskirstytos duomenų bazės apie simbolinių vardų ir IP–adresų atitikimą

DRAP (Data Link Switching Remote Access Protocol – Duomenų perdavimo linija, perjungiančios tolimosios prieigos protokolas) – panaudotas tarp darbo stočių ir maršrutizatorių, kad transportuotu SNA / NetBIOS duomenų srautas per TCP sesijas

DTCP (Dynamic Tunnel Configuration Protocol – Dinamiškas tunelio konfigūracijos protokolas) – mechanizmas, emaliuoja pilną dvikryptį ryšį tarp visų mazgų, kurie yra tiesiogiai sujungti vienakrypčio ryšio linijos.

DTLS (Datagram Transport Layer Security – Duomenų paketinis transporto lygmens saugumas) – aprūpina ryšių privatumą duomenų paketiniams protokolams. Protokolas leidžia programoms client/server susisiekti keliu, kuris yra projektuotas, kad sutrukdytų slapta klausytis, gadinimui, ar klastotei žinutes.

Echo – Labai naudingas pašalinimo ir matavimo įrankis. Jis atsako į visus paketus, išsiųsdamas paketą su tais pačiais duomenimis, ir yra numatytas testavimui, tačiau retai naudojamas praktikoje.

EMSD (Efficient Mail Submission and Delivery – Efektyvus pašto pateikimas ir pristatymas) – žinučių siuntimo protokolas, kuris yra labai optimizuotas pateikimui ir trumpų interneto pašto žinučių pristatymui.

EPP (Extensible Provisioning Protocol) – paslauga kuri leidžia registratoriams prižiūrėti domeno vardus automatiniu būdu (naujas, ištrinti, atnaujinti it t.t.) naudojant EPP protokolą, tam tikros rūšies XML protokolą.

ESRO (Efficient Short Remote Operation – Efektyvios trumpos tolimos operacijos) – protokolas aprūpina patikima „connectionless“ tolimos operacijos paslauga UDP viršūnėje (ar bet kokią kitą nepatikimą connectionless transporto paslaugą) su minimumu viršuje (overhead).

ETFTP (Enhanced Trivial File Transfer Protocol – Išplėstas nereikšmingas rinkmenų persiuntimo protokolas) – bandomasis išplėtimas NETwork BLock Transfer Protocol (NETBLT), kaip rinkmenos perkėlimo programa.

Finger – paprastas protokolas, kuris aprūpina sąsają tolimai vartotojų informacijos programai.

FTP (File Transfer Protocol – Rinkmenų persiuntimo protokolas) – kliento serverio architektūros protokolas, leidžiantis apsikeisti bet kokio tipo failais be papildomo apdorojimo. FTP dažniausiai naudoja 20 ir 21 prievadus („portus“), pirmasis naudojamas duomenų siuntimui, o antrasis – komandų perdavimui į serverį

GDOI (Group Domain of Interpretation – Interpretacijos grupės domenas) – Skirtingai nuo ISAKMP ar IKE, sausainio pora GDOI antraštėje yra visiškai nustatyta GCKS. Sausainio pora GDOI ISAKMP antraštė identifikuoja Iš naujo raktą SA, kad atskirtų saugias grupes, valdytas GCKS. GDOI

naudoja sausainio laukus kaip SPI.

Interneto Gopher sistema, ar tiesiog Gopher sistema, yra paskirstyta dokumento pristatymo tarnyba. Tai leidžia vartotojams ištirti, ieškoti ir gauti informaciją, esančią skirtingų vietų vientisame būde.

HIP (Host Identity Protocol – Pagrindinis tapatumo protokolas) – naujas protokolo lygmuo, Pagrindinis (HIP) Tapatumo Protokolas, tarpjungimo sistemoje ir transporto lygmenų

HOSTNAME - NIC interneto Pagrindinio kompiuterio vardo Tarnybinė stotis yra TCP pagrįsta pagrindinė informacijos programa ir protokolas, vykdantis SRI–NIC mašinose

HSRP (Hot Standby Router Protocol – Greito maršrutizatoriaus pakeitimo protokolas) – aprūpina mechanizmą, kuris yra projektuotas, kad palaikytų netrukdantį „failover“ IP duomenų srauto tam tikromis aplinkybėmis.

HTTP (HyperText Transfer Protocol – Hiperteksto perdavimo protokolas) – pagrindinis metodas pasiekti informaciją pasauliniame tinkle (WWW). Pradinė protokolo paskirtis – pateikti standartinį būdą HTML puslapių skelbimui ir skaitymui.

ICAP (Internet Content Adaptation Protocol – Interneto turinio adaptacijos protokolas) – nutaikytas į paprastos objektu pagrįstos patenkintos vektorizacijos HTTP paslaugoms aprūpinimą

ICP (Internet Cache Protocol – Interneto talpinimo protokolas) – lengvasvoris žinutės formatas, panaudotas tam, kad susisiektų tarp Žiniatinklio spartinančiųjų atmintinių.

iFCP (Internet Fibre Channel Protocol – Interneto skaidulos kanalo protokolas) – naudoja TCP, kad aprūpintų susigrūdimo valdymą, klaidos aptikimą ir atgavimą. iFCP pirminis tikslas leidžia tarpusavio ryšį ir jungimą į sistemą egzistuojančių pluošto kanalo prietaisų laidiniais greičiais per IP tinklą.

IKE (Internet Key Exchange – Internetinio rakto ketimas) – protokolas naudojamas pasirinkto šifravimo algoritmo AH ir ESP protokolose patvirtinimui bei raktų valdymui.

IMAP (Interactive Mail Access Protocol – Interaktyvus Pašto Prieigos Protokolas) – elektroninio pašto serverio protokolas. Šis protokolas reglamentuoja elektroninių laiškų laikymą ir tvarkymą serverio kompiuteryje, neatsiunčiant jų į gavėjo kompiuterį

IPFIX (IP Flow Information Export – Informacijos IP srauto eksportas) – srautų informacija

yra skelbiama nepertraukiamai ir nesinchroniškai. Kai konkretus srautas pasibaigia, informacija apie jį yra išsiunčiama specialiai nurodytam kolektoriui

IPP (Internet Printing Protocol – Interneto spausdinimo protokolas) – taikomasis lygmens protokolas, kuris gali būti panaudotas paskirstytam spausdinimui, naudodamas interneto priemones ir technologijas

IRC (Internet Relay Chat – Tiesioginis pokalbis internete) – ryšio protokolas ir interneto paslauga, skirti gyvai bendrauti internete (operatyviai apsikeisti trumpomis tekstinėmis žinutėmis).

ISAKMP (Internet Security Association and Key Management Protocol – interneto saugumo asociacijų ir raktų tvarkymo protokolas) – kuris leis raktams turėti papildomų atributų, tokių kaip gyvavimo trukmė, saugumo lygis ir kitų.

iSCSI (Internet SCSI) sąsaja leidžia sujungti SCSI ir „Ethernet“ technologijas ir užtikrinti įrenginių sąveiką IP protokolu.

IUA – protokolas panaudotas tarp Signalinio Tinklų sietuvo (SG – Signaling Gateway) ir Žiniasklaidos Tinklų sietuvo Valdiklio (MGC – Media Gateway Controller)

Kerberos – Tinklo autentifikavimo protokolas dažnai naudojamas šifruoti slaptažodžiams, kurie siunčiami internetu.

Kermit – Failų persiuntimo protokolas, naudojamas esant asinchroniniams informacijos mainams kompiuterių tinkluose. Labai lankstus protokolas, jį naudoja daugelis programų, skirtų informacijai perduoti telefono linijomis.

KINK (Kerberized Internet Negotiation of Keys) – apibrėžia žemą latenciją, skaičiavimui nesudėtingą, lengvai valdoma ir kriptografiškai garsų protokolą, kad sukurtų ir palaikytų saugumo asociacijas, naudodama Kerberos atpažinimo sistemą.

L2F (Layer 2 Forwarding – 2 Lygmuo Siuntimas) – leidžia ryšio linijų lygmenis tuneliuoti (t.y., HDLC, async HDLC, ar SLIP kadrai) aukštesnių lygmens protokolu.

LDAP (Lightweight Directory Access Protocol – Supaprastintos kreipties į katalogus protokolas) – skirtas prieiti prie katalogų paslaugų, pavyzdžiui, prie bendrovės adresų knygų, iš skirtingų operacinių sistemų. LDAP yra supaprastinta kreipties į katalogus protokolo (DAP) versija, skirta prieigai prie X.500 tipo katalogų.

LDP (Label Distribution Protocol – Žymės paskirstymo protokolas) – naujas protokolas, apibrėžtas tam, kad paskirstytų žymes. Tai yra komplektas procedūrų ir žinučių, prie kurios Žymės Perjungti Maršrutizatoriai (LSRs – Label Switched Routers) nustato Žymę, Perjungti Adresai (LSPs – Label Switched Paths) per tinklą, atvaizduojant tinklo lygmens maršruto parinkimo informaciją tiesiogiai į duomenų perdavimo linijos lygmenį perjungiant adresus

LDP (Loader Debugger Protocol – Įkėlimo derinimo programos protokolas) – įkėlimui, iškrovimui ir pašalinimui paskirties mašinų nuo pagrindinių kompiuterių tinklo aplinkoje

LFAP (Light–weight Flow Admission Protocol – Lengvasvoris srauto prieinamumo protokolas) – leidžia išorinei Srauto Prieinamumo Paslaugai (FAS – Flow Admission Service) valdyti srauto prieinamumą pakeitime, leisdamas lanksčias Srauto Prieinamumo Paslaugas būti išdėstytas pardavėjo ar kliento be pakeitimų, ar perdėta našta pakeitimuose.

LMTP (Local Mail Transfer Protocol – Vietinis pašto perdavimo protokolas) – Nors LMTP yra alternatyvus protokolas į ESMTP, jis naudoja (su keliais pakeitimais) sintaksę ir ESMTP semantiką.

LPR – TCP pagrįstas protokolas. Jungtis ant kurios linijos spausdintuvo demonas (***d****isk* ***a****nd* ***e****xecution* ***mon****itor*) klausymas yra 515. Šaltinio jungtis turi būti diapazone 721 iki 731, imtinai. Linijos spausdintuvo demonas atsako į komandas, siunčia į jo jungtį.

MADCAP (Multicast Address Dynamic Client Allocation Protocol – Multiperdavimo adresas dinamiškas kliento paskyrimo protokolas) – protokolas, kuris leidžia pagrindiniams kompiuteriams prašyti multiperdavimo adreso paskyrimo paslaugas nuo multiperdavimo adreso paskyrimo tarnybinių stočių.

MASC (Multicast Address–Set Claim – Multiperdavimas prie adreso nustatytas reikalavimas) – panaudotas mazgo (tipiškai maršrutizatorius), kad reikalautų ir paskirtų vieną ar daugiau adreso priešdėlių to mazgo domenui.

MATIP (Mapping of Airline Traffic over Internet Protocol – Atvaizdavimas avialinijos duomenų srautas per Interneto protokolą) – naudojama tipiškai susisiekimui tarp avialinijos įstaigos ar kelionių agentūros ir centrinės kompiuterinės sistemos vietos rezervavimui ir bilieto leidimui.

Mbus – lengvojo svorio, žinutę–orientuotas koordinacijos protokolo grupės susisiekimui tarp taikomųjų komponentų

MGCP (Multimedia Gateway Control Protocol – Pagrindinis media tinklų sietuvo valdymo protokolas) – apima kontrolinio patikrinimo komandas, kurios tiktai leidžia, kad Telefono skambučio Agentas tikrintų galutinį tašką ir/ar sujungimo išdėstymą laiku.

Mobilus IP – plečia ICMP Maršrutizatoriaus Atradimą kaip savo pirminį mechanizmą Agento Atradimui.

MPP (Message Posting Protocol – Žinutės išsiunčiantis protokolas) – protokolas buvo projektuotas tam, kad išsiųstų žinutes nuo darbo stočių į pašto tarnybos pagrindinį kompiuterį.

MSDP (Multicast Source Discovery Protocol – Multiperdavimo šaltinio atradimo protokolas) – apibūdina mechanizmą, kuris užmegztų ryšį daugialypę PIM Sparse–Mode (PIM–SM) kartu tarp domenų.

MTP (Mail Transfer Protocol – Pašto perdavimo protokolas) – projektuotas, kad būtų nepriklausomas nuo tam tikros perdavimo posistemės ir reikalingas tiktai patikimo tvarkomo duomenų srovės kanalo.

MTQP (Message Tracking Query Protocol – Žinutė, sekanti užklausos protokolą) – registras ASCII koduotės eilutės, užbaigtos CRLF kombinacijos. Reikšminiai žodžiai ir parametrai yra atskirti vienos ar daugiau vietos ir pažymi simbolius. Komandos žinutė yra apribota iki 998 simbolių prieš CRLF.

MUPDATE – projektuotas, kad leistų IMAP ar POP3 tarnybinių stočių grupei funkcionuoti su suvienyta pašto dėžute „namespace“.

NFILE – „Naujas Rinkmenos Protokolas“. NFILE buvo iš pradžių projektuotas kaip pakeitimas senesniam protokolui, pavadintam QFILE, su tikslu spręsti „tvirtumo“ problemas QFILE, kuris buvo pavadintas „Naujasis Rinkmenos Protokolas“

NFS (Network File System – Tinklo rinkmenos išdėstymo sistema) – turi skaidrų priėjimą per TCP/IP protokolą prie UNIX operacinės sistemos failų sistemų

NNTP (Network News Transfer Protocol – Naujienų persiuntimo tinklu protokolas) – naudojamas naujienų grupių laiškams siųsti, gauti, skirstyti, tvarkyti, užklausoms formuoti. Leidžia naujienų grupių laiškus laikyti duomenų bazėje, o abonentui – prisijungti prie jos ir atsisiųsdinti į savo kompiuterį tik pasirinktus laiškus[23].

NTP (Network Time Protocol – Tinklo laiko protokolas) – protokolas tam, kad sinchronizuotų tinklo laikrodžių komplektą, naudodamas paskirstytų klientų ir tarnybinių stočių kampaniją

OCSP (Online Certificate Status Protocol – Internetinis sertifikuotas statuso protokolas) – protokolas leidžiantis realiame laike tikrinti sertifikato būseną (pvz. „galioja“, „atšauktas“ ir pan.).

ODETTE–FTP (ODETTE File Transfer Protocol – ODETTE Rinkmenų persiuntimo protokolas) – buvo apibrėžtas 1986 darbo grupės keturios Organizacijos Duomenų mainams prie Tele Perdavimo Europoje (ODETTE), kad atkreiptų į elektroninį duomenų apsikeitimą (EDI) Europos automobilių pramonės reikalavimų dėmesį.

OLSR (Optimized Link State Routing – Optimizuotas ryšio linijo būklės maršruto parinkimas) – specialiai pritaikyto mobilaus belaidžio LAN reikalavimams.

PANA (Protocol for Carrying Authentication for Network Access – Atpažinimo protokolas tinklo prieigos perkėlimui) – Laukiama, kad būsimi IP prietaisai turės prieigos technologijų įvairovę, tinklo ryšio įgijimui.

Ph paslauga supa visą informacijos modelį, kliento komandos kalbą ir tarnybinės stoties atsakymus.

POP (Post Office Protocol – Pašto protokolas) – naudojamas tik laiškams gauti. Laiškai dažniausiai išsiunčiami naudojant SMTP protokolą ar kt.

Portmapper – tvarko RPC prisijungimus, kurie yra naudojami tokių protokolų kaip NFS ir NIS.

PPTP („Point–to–Point Tunneling Protocol“) – kelių skirtingų kompanijų, tarp jų – ir „Microsoft“ bendromis jėgomis sukurtas protokolas, skirtas nutolusio darbuotojo prisijungimui prie tinklo. Beveik visi naujesni „Microsoft“ produktai palaiko PPTP protokolą. Pagrindinis PPTP konkurentas kurį laiką buvo L2F („Layer 2 Forwarding“) protokolas, kuris irgi pirmiausia yra skirtas duomenų perdavimo tuneliui tarp nutolusio vartotojo ir kompiuterinio tinklo sukurti. Vėliau, gerinant L2F bei naudojant geriausius PPTP elementus, buvo sukurtas L2TP („Layer 2 Tunneling Protocol“). Tinklo[24].

PWDGEN (Password Generator Protocol – Slaptažodžio generatoriaus protokolas) – Paslauga aprūpina komplektą šešių atsitiktinai sukurtų aštuonių simbolių CRLF–atributų „žodžių“ su protingu „pronounceability“ lygmeniu, naudodama daugialygį algoritmą.

Quote (Quote of the Day Protocol – Dienos protokolo citata) – grąžina ASCII koduotės žinutę.

RADIUS (Remote Authentication Dial–In User Service – Nuotolinė vartotojų atpažinimo prisijungimo telefonu paslauga) – kompiuterių tinklo protokolas, leidžiantis centralizuoti autentikacijos (prieigos), autorizacijos ir apskaitos valdymą tinklo naudotojams arba įrenginiams, besijungiantiems prie tam tikrų tinklo paslaugų.

RAP (Internet Route Access Protocol – Interneto maršruto prieigos protokolas) – paveikia TCP su vartotojais atidarančiais simetrišką TCP ryšį tarp RAP jungčių kiekvienoje sistemoje.

RIP (Routing Information Protocol – Informacijos protokolo maršruto parinkimas) – skirtas maršrutizavimui vienos autonominės sistemos ribose. Tai yra seniausias IP maršrutizavimo protokolas. Algoritmai, kuriais remiasi RIP protokolas, buvo naudojami jau nuo 1969 metų ARPANET tinkle.

RIPng – projektuotas, kad dirbtų kaip IGP nuosaikiame dydyje AS's. Tai nėra numatoma naudojimui sudėtingesnėse aplinkose.

RLP (Resource Location Protocol – Išteklių vietos protokolas) – paprasta procedūra request/reply. Užklausimo pagrindinis kompiuteris sukuria sąrašą išteklių, kurių jis norėtų nustatyti vietą ir siunčia prašymo žinutę tinkle.

RMCP (Remote Mail Checking Protocol – Tolimas pašto patikrinimo protokolas) – komentarų užklausa apibrėžia protokolą, kad aprūpintų pašto patikrinimo paslaugą, kuri bus panaudota tarp kliento ir tarnybinės stoties.

RSIP (Realm Specific IP – Realm specifinis IP) – Alternatyva NAT‘ui architektūra, kuri leidžia pagrindiniams kompiuteriams pirmo viduje (pavyzdžiui, privatus) maršruto parinkimus tiesiogiai panaudoti adresus ir kitus maršruto parinkimo parametrus nuo antro (pavyzdžiui, publika) maršruto parinkimus.

RTCP (RTP Control Protocol – RTP valdymo protokolas) – duomenų perdavimo protokolas, užtikrinantis grįžtamąjį ryšį tarp siuntėjo ir gavėjo (grupės).

RTP (Real–Time Transport Protocol – Realaus laiko transportinis protokolas) – „skaidrus” žemesnio lygio perdavimo terpei, tačiau dažniausiai perduodamas UDP paketais.

RTSP (Real Time Streaming Protocol – Operatyvus srautinis protokolas) – taikomojo lygmens protokolas valdymui per pristatymą duomenų su skubiai atliekamomis savybėmis. RTSP aprūpina ištęsiamą struktūrą, kad įgalintų valdyti, pagal pareikalavimą pristatymus skubiai atliekamų duomenų, tokių kaip audio ir video.

RWhois (Referral Whois Protocol – Referral sistemos whois protokolas) – aprūpina paskirstytą sistemą atradimą, užklausą ir katalogo informacijos palaikymą.

SACRED (Securely Available Credentials – Saugiai pasiekiami mandatai) – protokolas, kaip vartotojas gali įsigyti šifruotus mandatus (pavyzdžiui, privatūs raktai, PKCS #15 struktūrų) nuo mandatinio tarnybinės stoties, naudodamas kompiuterizuotą darbo vietą, kuri vietoje patikėjo įdiegta programine įranga, bet be specifinės vartotojui konfigūracijos.

Send (Message Send Protocol – Siunčiamos žinutės protokolas) – panaudotas, kad nusiųstų trumpą žinutę paskirto vartotojo duoto terminalo, duotajam pagrindiniui kompiuteriui.

SFTP (Simple File Transfer Protocol – Paprastas rinkmenų persiuntimo protokolas) – Tai kuris tenkina žmonių poreikius, norinčio protokolo, kuris yra naudingesnis negu TFTP, bet lengvesnis įgyvendinti (ir mažiau galingas) negu FTP.

SGMP (Simple Gateway Monitoring Protocol – Paprastas tinklų sietuvo kontroliavimo protokolas) – protokolas yra suformuotas didelėje dalyje noro minimizuoti skaičius ir visuma valdymo funkcijų, suprastų tinklų sietuvo savarankiškai.

SIFT/UFT (Sender–Initiated/Unsolicited File Transfer – Siuntėjo–pradėtas/Neprašytas rinkmenos perdavimas) – Siuntėjo pradėti Rinkmenos perdavimo kontrastai su kitais rinkmenos perdavimo metodais tame, siuntėjas neturi turėti sąskaitos ar bet kokios registracijos paskirties pagrindinėje sistemoje ir gavimo vartotojas gali priimti mažiau žingsnių, kad paimtų nusiųstą rinkmeną (–as).

SIP (Session Initiation Protocol – Seanso iniciacijos protokolas) – protokolas sukurtas „IETF MMUSIC Working Group“. Jis pateikia interaktyvios sesijos inicializavimo, modifikavimo ir užbaigimo standartus tokiems multimedios tipams kaip video, garso, susirašinėjimo, žaidimų tinkle ir virtualios realybės. Tai vienas iš pirmaujančių protokolų IP telefonijoje.

SLP (Service Location Protocol – Tarnybinis vietos protokolas) – tikslas toks pat kaip ir SAP protokolo: supažindinti kliento procesus su serverio procesais.

SMTP (Simple Mail Transfer Protocol – Paprastasis pašto perdavos protokolas) – de facto standartas el.pašto laiškų perdavimui internete. Naudojamas elektroniniams laiškams pristatyti į gavėjo el.pašto dėžutę.

SMUX – Kai vartotojų procesas, kurį pavadinama SMUX vartotoju, nori eksportuoti MIB modulį, jis priima SMUX asociaciją vietiniam SNMP agentui, registruoja save ir (vėliau) į laukų valdymo operacijų objektus MIB modulyje.

SNMP (Simple Network Management Protocol – Paprastas tinklo stebėjimo protokolas) – vienas iš tinklo protokolų. Skirtas tinkle veikiančių įrenginių stebėjimui ir valdymui. Skirtingai nuo daugumos dabar naudojamų, veikia ne tik TCP/IP tinkluose.

SNPP (Simple Network Paging Protocol – Paprasto tinklo puslapių kaitos protokolas) – ketinimas aprūpina standartą, kokiu būdu puslapius gali pristatyti atskiriems puslapių kaitos terminalams.

SNTP (Simple Network Time Protocol – Paprastas tinklo laiko protokolas) – plačiai panaudotas, kad sinchronizuotų kompiuterių laikrodžius globaliniame internete.

SOCKS – tarpininko darbo protokolas. Pasižymi tuo, kad per SOCKS5 tarpininką gali bendrauti praktiškai visos Interneto programos: WWW, FTP, Telnet, IRC.

SRTCP (Secure RTCP – Saugus realaus laiko transportinis protokolas) – Realaus laiko Transportinio Protokolo (RTP) profilis, kuris gali aprūpinti konfidencialumą, žinutės identifikavimą ir iš naujo leisti apsaugą į RTP duomenų srautą, taip pat duomenų valdymo srautą RTP.

SSDP (Simple Service Discovery Protocol – Paprastas tarnybinis atradimo protokolas) – pajungiami automatiniai įrenginiai į tinklą palaikantys UPnP. Kol kas tai retenybė[25].

SSP (Switch–to–Switch Protocol – Nuo jungiklio prie jungiklio Protokolas) – panaudotas tarp IBM 6611 Tinklo Procesorių.

STATSRV (Statistics Server – Statistikos Serveris) – pagrįstas gimtąja pagrindine komandos kalba, pavartota statistikos kontroliavimui ir atvaizdavimui.

STUN (Simple Traversal of UDP Through NAT – Paprastas keliavimas UDP per NAT) – lengvasvoris protokolas, kuris leidžia programoms atrasti buvimą ir tipus Tinklo Adreso Vertėjų ir ugniasienių tarp viešo interneto.

SUA (Signalling Connection Control Part User Adaptation Layer – Vartotojų ryšio valdymo dalies adaptacijos lygmens signalizavimas) – projektuotas, kad būtų modulinis ir simetriškas, leisti tam dirbti skirtingoje architektūroje, tokioje kaip Signalinis Tinklų sietuvas į IP, Signalizuojantį Galutinio taško architektūrą taip pat kaip lygiarangį IP, Signalizuojantį Galutinio taško architektūrą.

Syslog – Visas paketo ilgis TURI būti 1024 baitais ar mažiau. Nėra jokio minimalaus syslog žinutės ilgio, nors syslog paketo be turinių siuntimas yra bevertis ir NETURI būti perduotas.

SYSTAT – Paprastas tekstas, protokolas tam, kad gautų sąrašą aktyvių vartotojų SYSTAT įgalintos tarnybinės stoties.

TBRPF (Topology Broadcast based on Reverse–Path Forwarding – Topologinis transliavimas, pagrįstas atvirkštinio kelio siuntimu) – proaktyvus, „link–state“ maršruto parinkimo protokolas, projektuotas mobiliems tinklams kuris aprūpina šuoliuko prie šuoliuko (hop–by–hop) maršruto parinkimą palei trumpiausius adresus į kiekvieną paskirtį.

Telnet – protokolas leidžia prisijungti prie nutolusio kompiuterio ir dirbti su juo terminaliniame režime. Taigi jums prisijungus TELNET protokolu, viskas, ką jūs rašote iš savo kompiuterio klaviatūros, yra siunčiama nutolusiam kompiuteriui.

Teredo – projektuotas, kad aprūpintų „IPv6 paskutinės priemonės prieigą“ į mazgus, kuriems reikia IPv6 jungiamumo, bet negali panaudoti nieko iš kitų IPv6 perėjimo planų.

TFTP (Trivial File Transfer Protocol – Trivialus failų perdavimo protokolas) – Savo sandara labai panašus į primityvų FTP. Perdavimui naudoja UDP protokolą. Neturi galimybės siųsti katalogų, nesupranta šifravimo, maksimalus failo dydis – 32mb.

Time (Time Protocol – Laiko protokolas) – protokolas aprūpina nepriklausomą nuo vietos, kompiuteriu apdorojamą datą ir laiką.

TRIP (Telephone Routing over IP – Telefono Maršruto parinkimas per IP) – saugumo valdomas tarpadministracinis domeno protokolas paskelbimui pasiekiamumo telefonijos paskirčių tarp vietos tarnybinių stočių ir paskelbimo požymių maršrutų į tas paskirtis.

TUNNEL – profilis aprūpina mechanizmą bendradarbiaujančius PYPSĖJIMO vartotojus, kad suformuotų taikomąjį lygmens tunelį.

UMSP (Unified Memory Space Protocol – Suvienytas atminties vietos protokolas) – tinklas–į ryšį orientuotas protokolas. Tai atitinka sesiją ir pavyzdinio OSI pristatymo lygmenis.

UUCP“ („Unix to Unix Copy Protocol“). – buvo pirmiausia failų persiuntimo priemonė, ji taip pat leido siųsti ir laiškus, netgi tuo atveju, kai siuntėjas ir gavėjas neturėdavo tiesioginio ryšio. Vėliau „UUCP“ tapo pagrindu įprastiniam elektroniniam paštui. Pats „UUCP“ buvo plačiai naudojamas maždaug iki 1990, kai jį galutinai ėmė išstumti modernesnės pašto priemonės, tačiau labai ribotai „UUCP“ yra naudojamas net ir dabar [26].

VEMMI (VErsatile MultiMedia Interface – Visapusiška multimedijos sąsaja) – Naujas URL planas, „vemmi“ yra apibrėžtas. Tai leidžia VEMMI kliento programinei įrangai ir VEMMI

terminalams užmegzti ryšį su multimedija interaktyvias paslaugas, sukalbamas į VEMMI standartą (Išplėsta Mašininė žmogumi Sąsaja Videotex ir Multimedijos/Hipermedijos Informacijos paieškos Paslaugoms), kartais sutrumpintas kaip „VErsatile MultiMedia Interface“.

WebDAV (Web Distributed Authoring and Versioning) – sukurtas HTTP protokolo pagrindu, pridėjus tam tikrus patobulinimus, skirtus grupei vartotojų atlikti veiksmus su bylomis, esančiomis nutolusioje sistemoje (serveryje), tuo pačiu sukuriant įspūdį, tartum jie būtų sistemoje, su kuria tuo metu dirba vartotojas.

WHOIS – protokolas, kuris leidžia naudotojams prieiti prie domenų vardų duomenų bazės. Naudodamiesi WHOIS, galite užklausti informacijos apie pasirinkto domeno vardą ir patikrinti jo būseną.

Pagrindinė architektūra WHOIS++ leidžia paskirstytą palaikymą katalogo turinių ir naudojimų WHOIS++ indeksuojančią paslaugą tam, kad nustatytų papildomas WHOIS++ tarnybines stotis.

XMPP (eXtensible Messaging and Presence Protocol) – supaprastintas ir specializuotas protokolas tam, kad eitų srauto XML elementai, apsikeistų sudarytą informaciją realiame laike.

4. PRIEDAS. **Vartotojo dokumentacija**

1. Sistemos funkcinis aprašymas

Sistemos atliekamos funkcijos:

- Srautų analizė pasitelkiant išsaugotus įrašus iš „Wireshark“;
- Naujų įrašų talpinimas sistemoje, pakeičiant senus;
- Įrašų filtravimas;

2. Sistemos vadovas

Sistema orientuota į vieną pagrindinį vartotoją:

- Vartotojas įkelti įrašus, išsaugoti įrašus, atlikti filtravimą.

3. Konfigūravimas ir instaliavimas

3.1. Sistemos konfigūravimas

Sistemos nustatymai saugomi faile „nustatymai.php“. Šis failas būtinai turi būti šakninėje sistemos direktorijoje.

Failo turinys:

```
define(„HOSTAS“, „localhost“, TRUE);
define(„PORTAS“, 3306, TRUE);
define(„USERIS“, „root“, TRUE);
define(„SLAPTAZODIS“, „*****“, TRUE);
define(„DB“, „minlgc“, TRUE);
...
```

Tai patys svarbiausi nustatymai reikalingi, kad sistema galėtų prisijungti prie duomenų bazės. Šie nustatymai užtikrina sėkmingą sistemos funkcionavimą.

Sistemos nustatymų reikšmės:

HOSTAS – duomenų bazės serverio adresas. Dažniausiai jis būna tame pačiame serveryje, kaip ir žiniatinklio serveris, todėl nieko keisti nereikia – pagal nutylėjimą „localhost“;

PORTAS – duomenų bazės prisijungimo prievadas. Keisti tik patyrusiems vartotojams;

USERIS – vartotojo vardas duomenų bazės serveriui;

SLAPTAZODIS – duomenų bazės serverio prisijungimo slaptažodis;

DB – duomenų bazės pavadinimas.

Tuo tarpu likusieji tik nurodo vienokią ar kitokią sistemos elgseną. Daugiau aprašyti pačiame konfigūraciniame faile.

Nustatymai turi būti aprašyti taip, kaip duota pavyzdyje. Nustatymo reikšmė rašoma tarp dvigubų arba viengubų kabučių, po kiekvienos eilutės būtina padėti kabliataškį.

3.2. Serverio konfigūravimas

Sėkmingos sistemos funkcionalumui reikalinga nustatyti serverio faile „php.ini“:

upload_max_filesize = 2000M

post_max_size = 2000M

max_execution_time = 9999

short_open_tag = On

upload_max_filesize – skirtas failų atsiuntimui į serverį;

post_max_size – skirtas užklausos dydžiui;

max_execution_time – užklausos laukimo laikas;

short_open_tag – funkcija skirta nustatyti suprastintą <?php pradžios rašymą;

3.3. Sistemos diegimas

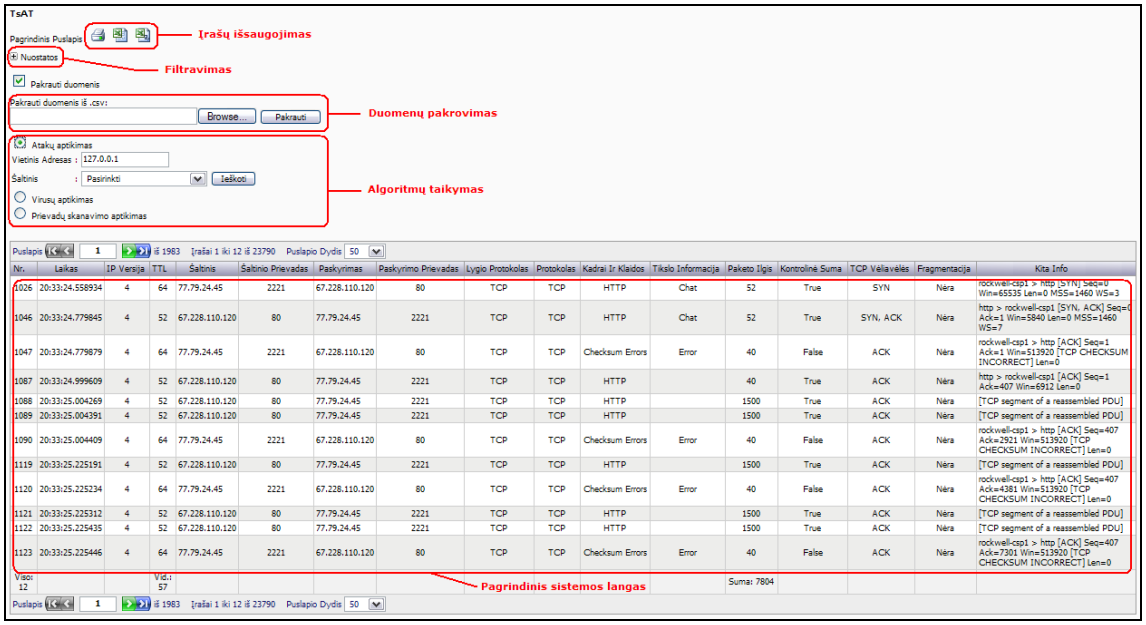
Sistemos diegimui skirtas failas „install.php“. Paleistas diegimo scenarijus paruošia duomenų bazę darbui. Dėmesio, prieš pradėdami diegimą, būtinai patikrinkite visus nustatymus faile „nustatymai.php“. To nepadarius, diegimo scenarijus neprisijungs prie duomenų bazės ir diegimas nepavyks. Prieš pradedant diegimą, sistemos failus reikia patalpinti į serverio „document root“ katalogą. Tai dažniausiai atliekama naudojantis FTP prieiga. Patalpinus failus, naršyklės adreso laukelyje renkamas sistemos adresas ir scenarijaus „install.php“ vardas, pvz.: „http://ik.su.lt/~minlgc/install.php“. Naršyklės lange matomi pranešimai apie diegimo eigą. Taip pat

labai svarbu, kad sistema turėtų galimybę rašyti į „document root“, todėl nepamirškite nustatyti failo prieigos leidimų (paprastai nustatoma skaitinė reikšmė – 0777, reiškianti, kad visiems vartotojams suteikiama pilna priėjimo teisė).

4. Sistemos naudojimas

Prieš pradedant naudoti, būtina atlikti aukščiau nurodytus veiksmus.

Norint prisijungti prie sistemos ir dirbti su ja, reikalingas interneto ryšys. Taip pat reikalinga interneto naršyklė, pvz., Internet Explorer 6, FireFox 2.0, ar vėlesnė versija.



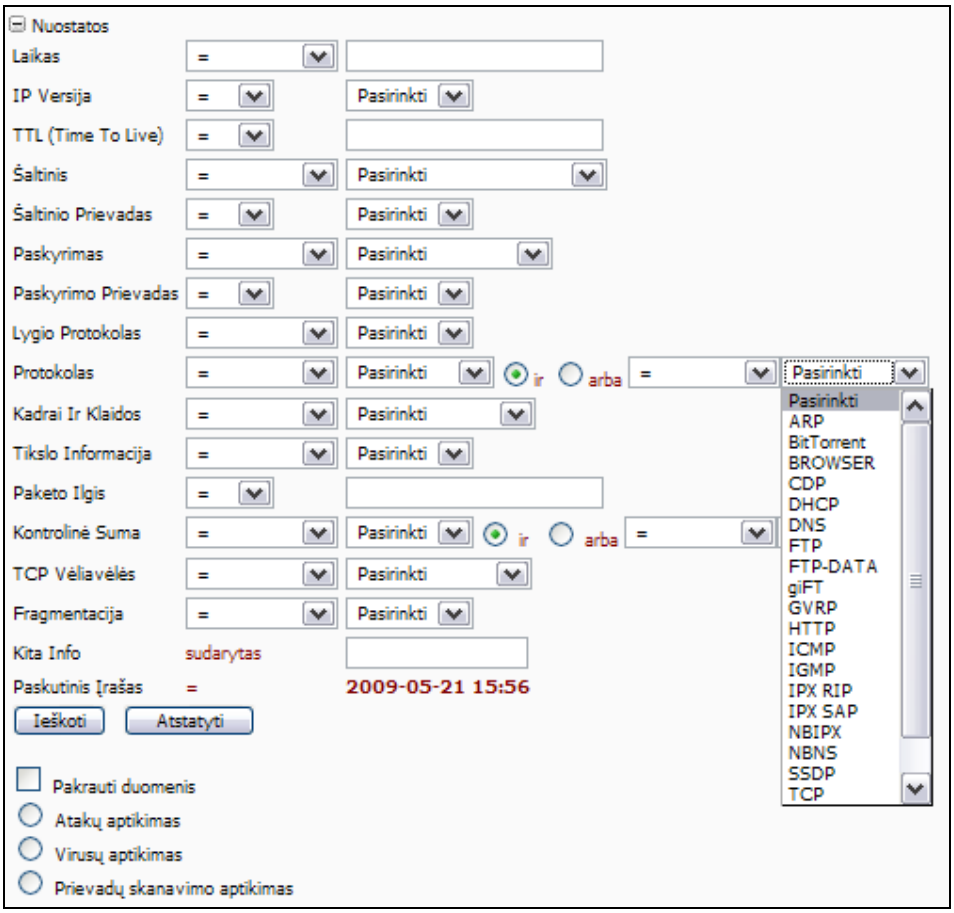
22 pav. *Pagrindinis sistemos tinklapis*

Pagrindinis langas – atvaizduojami visi įrašai, galimybė pereiti į kitą puslapį, dėl to jis vadinamas pagrindiniu.

Duomenų pakrovimas – vykdoma iš failo įrašų įkrovimas į duomenų bazę.

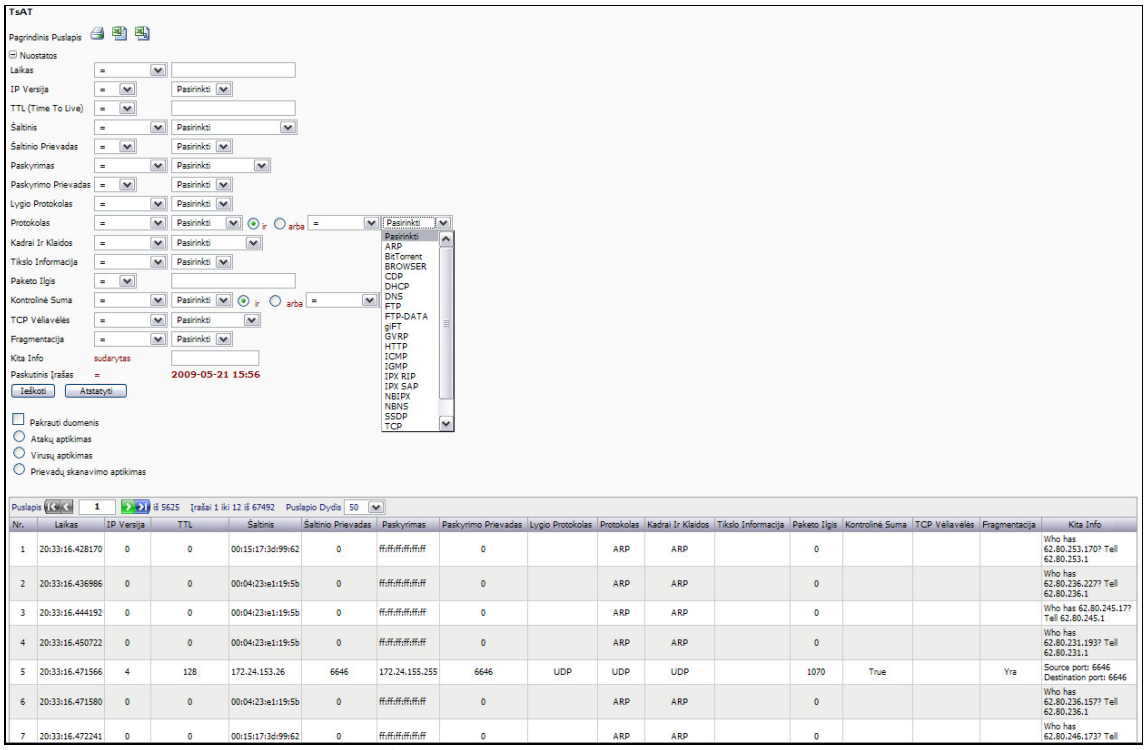
Filtravimas – pasirenkami parametrai pagal tai, ką norima filtruoti (žr. 23 pav.).

Įrašų išsaugojimas – atlikus filtravimą, galima išsaugoti arba atsispausdinti išfiltruotus įrašus.



23 pav. *Filtravimo įrankis*

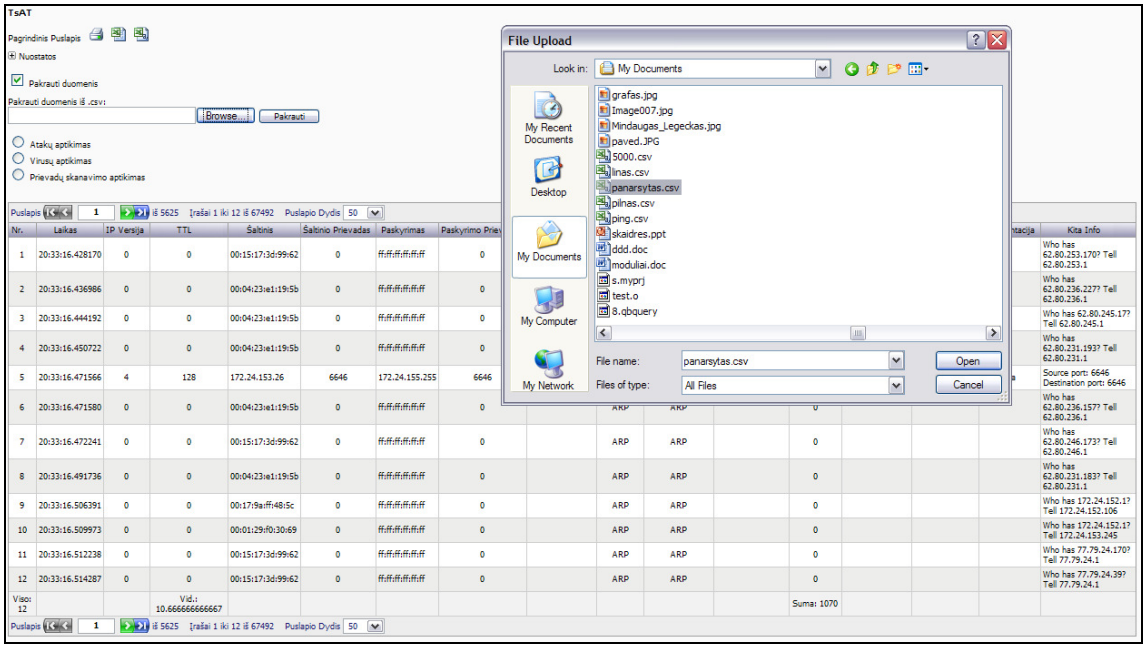
5. Vartotojo vadovas



24 pav. *Įrašų ir filtravimo atvaizdavimas*

Platesnės sistemos funkcionalumas vykdomas, kai vartotojas atlieka filtravimą. Kitu atveju rodomi iš duomenų bazės atvaizduojami įrašai.

5.1. Įrašų pakrovimas iš .csv failo.



25 pav. *Duomenų pakrovimas sistemoje*

Duomenų pakrovimas reikalauja specifinio .csv failo aprašo. Be jo įrašai bus atvaizduojami nekorektiškai. Kaip susikurti .csv teisingą aprašymą žr. *5.2 .csv failo formatas*.

5.2. .csv failo formatas.

Norint kad teisingai būtų atvaizduojami įrašai reikalingas teisingas failo formatas. Jo pavyzdys:

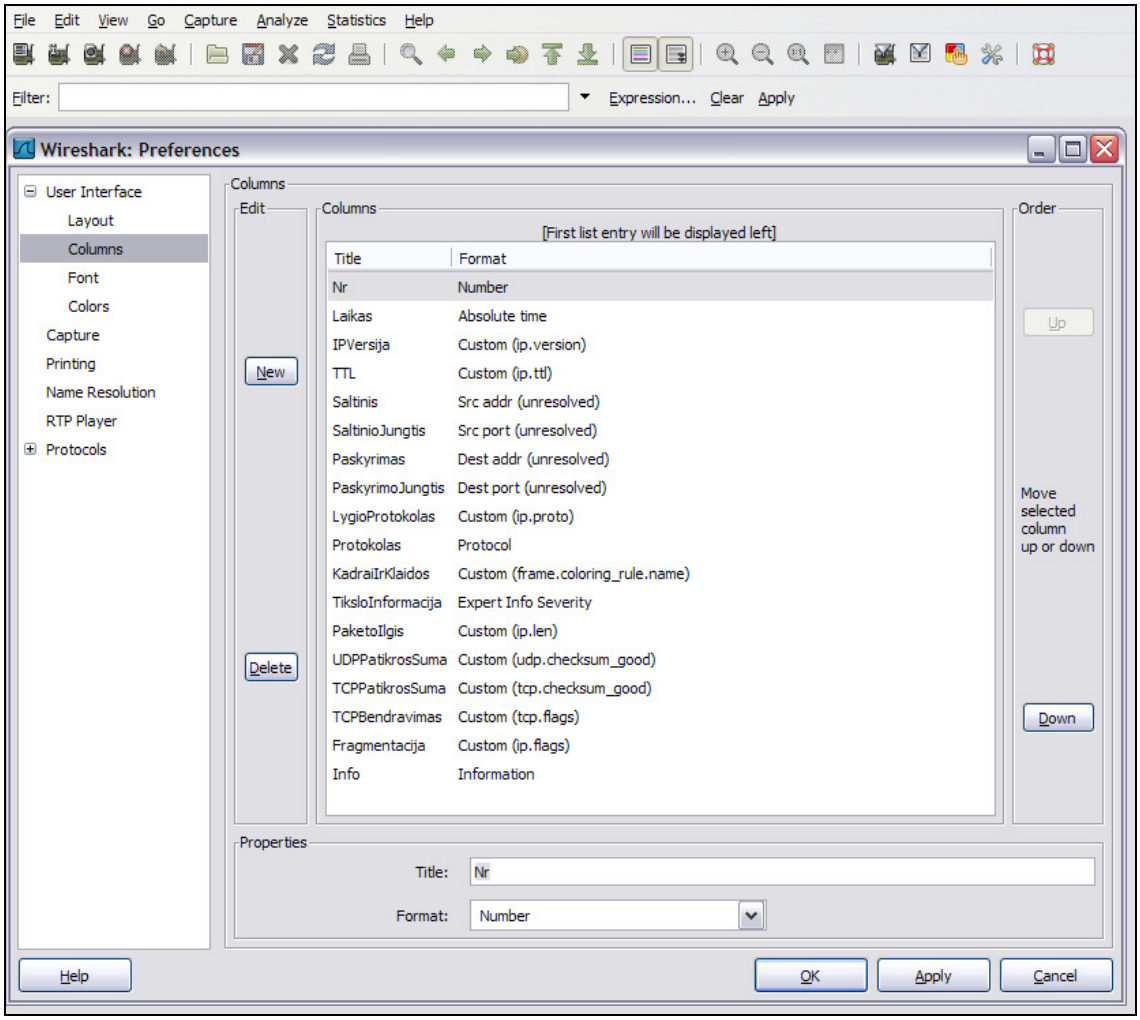
```
„Nr“,“Laikas“,“IPVersija“,“TTL“,“Saltinis“,“SaltinioJungtis“,“Paskyrimas“,“PaskyrimoJungtis“,“LygioProtokolas“,“Protokolas“,“KadraiIrKlaidos“,“TiksloInformacija“,“PaketoIlgis“,“UDPPatikrosSuma“,“TCPPatikrosSuma“,“TCPBendravimas“,“Fragmentacija“,“Info“

„1“,“20:35:45.917051“,“„,“„,“62.80.245.1“,“„,“Broadcast“,“„,“„,“ARP“,“ARP“,“„,“„,“„,“„,“„,“„,“„,“Who has 62.80.245.224?  Tell 62.80.245.1“

„2“,“20:35:45.920843“,“4“,“4“,“b23-31.splius.lt“,“8008“,“239.255.255.250“,“1900“,“0x11“,“SSDP“,“HTTP“,“Chat“,“373“,“True“,“„,“„,“0x00“,“NOTIFY * HTTP/1.1 „

„3“,“20:35:45.923804“,“„,“„,“62.80.246.1“,“„,“Broadcast“,“„,“„,“ARP“,“ARP“,“„,“„,“„,“„,“„,“„,“„,“Who has 62.80.246.225?  Tell 62.80.246.1“

„4“,“20:35:45.925589“,“4“,“4“,“b23-31.splius.lt“,“8008“,“239.255.255.250“,“1900“,“0x11“,“SSDP“,“HTTP“,“Chat“,“318“,“True“,“„,“„,“0x00“,“NOTIFY * HTTP/1.1 „
```

Failo „kepurė“ nebūtinai turi būtį aprašyta „„Nr“,“Laikas“,“IPVersija“,“TTL“,...“, svarbu, kad tolimesni įrašai eitų eilės tvarka.

5.3. „Wireshark“ nustatymas

Norint sukurti .csv failą būtina nusistatyti parametrus programoje „Wireshark“. Nustatymai rodomi žemiau esančiame paveikslėlyje (Edit–Preferences, žr. 26 pav.).

Kaip registruoti paketus ir eksportuoti į csv. failą galima pasidomėti pačioje programoje „Help meniu“.



26 pav. *„Wireshark“ nustatymai*

5. PRIEDAS. Kompaktinė laikmena

- Katalogas „TsAT“;

  Programos failai.

- Katalogas „Programinė įranga“;

  Wamp Serverio programa (nebūtina);

  „Wireshark“ programa eksportuoti .csv failai.

- Katalogas „Darbas“.

  Baigiamojo darbo aprašymas.