KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

ALMANTAS VENCKUS

VPN TINKLO DARBINGUMO MONITORINGO SISTEMA

MAGISTRO DARBAS

Darbo vadovas: doc.dr. G.Činčikas

KAUNAS, 2009 m.

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

MULTIMEDIJOS INŽINERIJOS KATEDRA

VPN TINKLO DARBINGUMO MONITORINGO SISTEMA

INFORMACINIŲ TECHNOLOGIJŲ SPECIALYBĖ

MAGISTRO DARBAS

Studentas

Almantas Venckus
IFN 6/1 gr.

2009 m. _____
.

Vadovas
Doc.Dr. G.Činičikas

2009 m. _____

Recenzentas

Doc.Dr. P.Kanapeckas

2009 m. _____

KAUNAS
2009 m.

TURINYS

SUMMARY

The study is about Virtual Private Network monitoring models. Agent – manager frame is analyzed. The SNMP protocol working rules and the possibility of using it for solving the occurred problem are analyzed. The star type of network is reviewed. Some alternative programs, which could be used for solving the problem, are compared. The requirements for the system are set. The relations between the objects are created. The program working algorithm is created and explained. Some of program interface windows, showing the different states of the program are shown. Finally, the result of the work states the conclusion, that the newly created system could be useful for other, similar network using organizations.

1. ĮVADAS

Šiuolaikinis žmogus, kuris savo darbo neįsivaizduoja be kompiuterio, retai supranta, kokia sudėtinga sistema užtikrina jo kaip vartotojo poreikius. Sistemos patikimo veikimo klausimas dažnai iškyla tik tada, kai vartotojas jau negali naudotis tinklo resursais. Neretai įmonė, įstaiga ar organizacija turi savo filialų skirtingose vietose, todėl dažnai tenka apjungti "lokalias" kompiuterinio tinklo struktūras į vieną bendra tinklą, leidžiantį bendrai naudotis resursais (el.pašto serveriu, duomenų bazėmis, bendrais tinkliniais spausdintuvais, skeneriais ar kitais tinklo elementais). Tokio tinklo priežiūra ir palaikymas dažnai būna sudėtingas ir reikalaujantis patikimų ryšių tarp lokalių tinklų. Nepaslaptis, kad ir kokį patikimą ir gerą šių paslaugų tiekėją pasirinktume, vis tiek atsiras tam tikrų trukdžių, dėl kurių sistema neveiks tam tikrą laiko tarpą, o juk už ryšio paslaugas mokami nemaži pinigai. Visada norima šias išlaidas sumažinti.

Ryšio paslaugų tiekėjai pasirašo sutartis, kuriose pasižada tiekti tam tikros kokybės ryšį. Turint sistemą, kuri analizuotų VPN tinklo ryšius ir įvertintų jų parametrus, galima šias išlaidas dalinai sumažinti.

Taip pat labai svarbus tokio tinklo saugumo klausimas, nes tinklais perduodama informacija, patekusi į pašalinių žmonių rankas, gali būti panaudota prieš įmonę. Dar ryškiau ši problema pasireiškia, jei yra perduodami asmens duomenys arba kita svarbi informacija. Kuo sistema sudėtingesnė, tuo jos priežiūra sudėtingesnė.

Kuriama sistema leis šia priežiūrą bent iš dalies palengvinti, turės "draugišką vartotojui" aplinką, leis kaupti duomenis apie tinklo darbingumą. Surinkti duomenys leis geriau vertinti tinklo parametrus, tinklo veikimą, ir tuo pačiu bus galima numatyti silpnųjų tinklo vietų tobulinimo galimybes.

Nemažai programinių produktų užsiima ir tinklo įrenginių valdymu. Mūsų atveju to atlikti negalima, nes tarpiniai įrenginiai yra paslaugų tiekėjo.

Dauguma gamintojų savo įrangai tinkle valdyti siūlo produktus, skirtus tik specializuotai jų įrangai.

Todėl vienam ar keliems sistemą prižiūrintiems asmenims tenka naudotis nemažu kiekiu programinių paketų, kuriu įsisavinimui ir konfigūravimui reikia sugaišti nemažai laiko.

Dėl šių priežasčių kurdami savo sistemą stengsimės padaryti ją kuo paprastesne, kad sukurtos sistemos įsisavinimui nereikėtų daug laiko net pradedančiam vartotojui.

Labai dažnai stengiamasi sutaupyti lėšų rengiant kompiuterines sistemas, todėl netgi dideliuose tinkluose naudojami tik pagrindiniai serverių valdymo įrankiai. Šias sistemas prižiūri sistemų administratoriai. Kartais jų darbui palengvinti yra įsigyjami tam tikri paketai, leidžiantys atlikti sudėtingų tinklų monitoringą, tačiau dažnai šiems paketams įsigyti neskiriama lėšų. Ši problema labai aktuali tampa biudžetinėse organizacijose, turinčiose ribotus finansinius išteklius. Neturint tinkamų programinių produktų, sudėtingiau kontroliuoti ir stebėti tinklo darbingumą. Dažnai tokiuose tinkluose problemos sprendžiamos tada, kai jos atsiranda, ir dalis sistemos nebefunkcionuoja. Turint tinklo darbingumo monitoringo sistemą, problemų sprendimą galima būtų galima atlikti operatyviau, kai tinklo dalis dar dirba, bet jos darbas jau nėra pakankamai stabilus. Kartais ryšio tarp skirtingų tinklo potinklių kanalas veikia nestabiliai. Tai gali būti skirtingų priežasčių sąlygotos problemos. Darbe panagrinėsime keletą elementarių nemokamų sistemų (nes įsigyti mokamą gali būti neskiriama lėšų), tinkamų elementariam VPN tinklo darbingumo monitoringui ir palyginsime jas su kuriama sistema. Dažnai turimos monitoringo sistemos neatlieka tam tikrų reikalingų funkcijų arba atlieka jas labai sudėtingu būdu.

Tinklo darbingumo statistika leidžia vertinti įvairių tinklo šakų darbingumą, todėl naudinga, kai sistema kaupia tinkamus šiai statistikai duomenis. Daug paprasčiau yra analizuoti VPN tinklo darbingumą ir imtis priemonių sutrikimams tinkle pašalinti, kol tinklo vartotojai dar jų nepajuto.

Ne visada pasirinktas ryšio tiekėjas gali užtikrinti pastovų ir nenutrūkstamą ryšio kanalų veikimą. Turint duomenis apie tai, kiek laiko minėtieji ryšio kanalai neveikė dėl ryšio tiekėjo kaltės, galima su paslaugos tiekėju derinti galimybę koreguoti paslaugos kainą ir gauti tam tikrų nuolaidų. Tai paskatintų tiekėją greičiau imtis reikiamų priemonių problemos sprendimui.

Reikia nepamiršti, laiku pastebėti sistemos trukumai užtikrina stabilų sistemos darbingumą.

2. ANALITINĖ DALIS

2.1. DARBO TIKSLAS

Sukurti specializuotą VPN tinklo darbingumo monitoringo sistemą, kuri būtų pritaikyta konkrečiam klientui, kuri panaudojant šiuolaikines technologijas užtikrintų VPN tinklo monitoringa ir analizę, leistų stebėti, kokia yra konkretaus VPN kanalo neveikimo priežastis, suteikti jam greitesnes tinklo būsenos analizės priemones. VPN tinklo analizės dėka bus galima lengviau argumentuoti tinklo poreikių kitimą ir pakeitimų būtinumą. Ši monitoringo sistema turės užtikrinti visų VPN tinklo segmentų analizę, kaupiant duomenis, kurie reikalingi tinklo darbingumui nustatyti ir statistinei analizei atlikti.

Tikslui realizuoti iškeliami šie uždaviniai:

1. Išanalizuoti VPN tinklo naudojamą architektūrą , protokolus;
2. Išanalizuoti MIB duomenų bazės, srautų valdymą;
3. Išanalizuoti monitoringo sistemos modelius;
4. Atlikti monitoringo sistemų analizę ir palyginimą.

2.2. VPN ARCHITEKTŪROS IR PROTOKOLŲ ANALIZĖ

2.2.1. VPN ANALIZAVIMAS

VPN – tai privatūs duomenų perdavimo tinklai. Jie yra neatskiriama organizacijos (didesnės) kompiuterinio tinklo dalis. Jei organizacija turi padalinius keliose skirtingose vietovėse, tai apsieiti be VPN panaudojimo yra sudėtinga. VPN leidžia sujungti skirtingų padalinių kompiuterinius tinklus į vieną bendrą visos organizacijos tinklą (virtualųjį LAN).

Iš karto matyti, kad ryšys turi atitikti organizacijos poreikius greitaveikos, patikimumo ir saugumo prasmėmis. VPN tinklo ryšiai yra tarsi bendrojo lokalaus organizacijos tinklo dalys, tik šiems sujungimams naudojami išoriniai tinklai. Išoriniu tinklu suprantama tai kas nėra vidinio organizacijos tinklo (fizinio tinklo) dalimi. Skirtinė linija nėra VPN, nes nėra galimybės komunikuoti su kitais duomenų perdavimo kanalais.

VPN galima realizuoti keletu būdų.

Pirmasis būdas naudoti pasaulinį globalųjį kompiuterių tinklą (internetą). Šis būdas nėra sudėtingas, tačiau jis yra labiausiai nesaugus. Internete dažnai bandoma VPN kanalus paveikti atakomis. Toks VPN kanalas dažniausiai naudojamas pavienių vartotojų „įjungimui“ į vidinį organizacijos tinklą, leidžiant jam naudotis tam tikrais lokalaus tinklo resursais (mūsų atveju toks kanalas nenaudojamas, todėl detaliau jo nenagrinėsime).

Antrasis būdas - tinklų sujungimui tarp skirtingų vienos organizacijos padalinių naudotis vieno ryšio paslaugų tiekėjo paslaugomis. Tai leidžia sutaupyti dalį lėšų, nes perkant didesnį kiekį paslaugos, taikomos įvairios nuolaidos. Tokiu atveju dažnai naudojamasi paslaugos tiekėjo vidiniu tinklu ir VPN kanalų duomenys perduodami juo.

Antrasis būdas yra saugesnis ir patikimesnis už pirmąjį. Jeigu vidinis organizacijos tinklas yra realizuotas žvaigždės topologija tai ji gali būti loginė, o ne fizinė. Fizinę komutacija teikiantis ryšio paslaugos tiekėjas gali naudoti žiedinę struktūrą. Tokiu atveju, net ir nesant tiesioginio veikiančio kanalo tarp konkrečių objektų, duomenys būtų perduoti žiedu ir vis tiek pasiektų adresatą. Padalinio tinklo aparatūra kreipiasi į kito padalinio tinklą, o ryšio paslaugų tiekėjo tinklas atlieka nukreipimą. Maršrutizatoriai padidina tokių sujungimų patikimumą ir saugumą. Maršrutizatorius yra paslaugų tiekėjo tinklo dalis (įrenginys). Šiuo metu dažniausiai naudojami „Cisco“ maršrutizatoriai. Maršrutizatorius, patikrinęs kur nori kreiptis konkretus duomenų paketas, ji persiunčia kitam maršrutizatoriui, kuris atitinka jo turimą kodų lentelę pagal kreipimosi adresus. Tokiu būdu paketai turintys keliauti organizacijos viduje yra atskiriami nuo paketų, išeinančių į išorę (pvz. internetą). Paketai VPN kanalu persiunčiami kitam maršrtizatoriui, kuris turi fizinę komutaciją su kito padalinio tinklu (LAN). Paketų, siunčiamų paslaugų tiekėjo tinklu, IP adresai būna „apvelkami“ šio tinklo adresais. Labai dažnai tai būna skirtingos klasės tinklai, ir jų adresacija labai skiriasi (skirtingos adresų klasės). Vidinio tinklo aparatūra, turinti fizinę komutaciją su maršrutizatoriumi, turi ne mažiau dviejų tinklo plokščių. Tai reikalinga tam, kad ji galėtu bendrauti su skirtingais tinklais (vidiniu ir paslaugos tiekėjo). Gavusi paketą iš maršrutizatoriaus organizacijos potinklio ugniasienė jį “išpakuoja“ ir persiunčia jau vidinio tinklo adresatui, kuriam ir yra skirtas šis duomenų paketas. Jei padaliniai nėra visiškai maži, dažnai juose įrengiami keletas serverių (failų saugojimui, duomenų bazėms ir t.t). Tinkluose, kurių aparatūra naudoja Microsoft programinę įrangą komunikavimui su maršrutizatorium, yra naudojami ISA serveriai. Dažniausiai sutinkami yra Microsoft ISA 2004 arba Microsoft ISA 2000 serveriai, kurie atlieka ugniasienės vaidmenį, t.y. apsaugo vidinį tinklą nuo „negerų“ paketų. Kaip jau minėjome, iš maršrutizatoriaus jie gauna „vidinio tinklo“ paketus ir paketus iš interneto.

2.2.2. TINKLŲ MONITORINGUI IR VALDYMUI NAUDOJAMŲ PROTOKOLŲ IR DUOMENŲ MODELIŲ APŽVALGA

Šiandien praktikoje naudojami du tinklų valdymo protokolai – Interneto standartai (TCP/IP), kurie veikia SNMP protokolo pagrindu, ir tarptautinių standartų protokolai ISO/ITU-T, kurie valdymui naudoja CMIP protokolą. Pastarojo standarto OSI tinklinio valdymo modelis (angl. *OSI Management Framework*) yra apibrėžtas ISO/IEC 7498-4 dokumente.

Tinklo resursų apskaitos funkcija atlieka įvairių tinklo resursų, tokių kaip įrenginiai, kanalai ir transportinės tarnybos, panaudojimo laikinę apskaitą.

Tinklų monitoringui patogu naudoti agento-menedžerio modelį. Šiuo modeliu valdomas tinklas susideda iš šių komponentų:

- valdomų įrenginių;
- agentų;
- tinklo valdymo sistemos - menedžerio;
- valdymo informacijos perdavimo protokolo;
- valdymo informacinės bazės (MIB);

Valdomas įrenginys yra tinklo mazgas, kuriame yra įdiegtas agentas kuris priklauso tinklui. Valdomi įrenginiai - tai tinklo elementai: maršrutizatoriai, prieigos serveriai, komutatoriai, tiltai, skirstytuvai, spausdintuvai ir kiti.

Agentas – tai tinklo valdymo programinis modulis, kuris priklauso valdomam įrenginiui. Agentas turi visą vietinę valdymo informaciją ir ją suderina su tinklo valdymo protokolu, t.y. išverčia į atitinkamą formatą. Agentas surenka iš įrenginio valdymo informaciją ir, naudodamas valdymo informacijos perdavimo protokolą, pateikia ją valdymo sistemai. Agentai gali skirtis pagal savo galimybes. Jie gali atlikti minimalias arba išplėstas funkcijas, kurios leidžia atlikti savarankiškus veiksmus avarinio atvejo metu (pavyzdžiui, laikinų priklausomybių sudarymas, avarinių pranešimų filtracija ir t.t.).

Tinklo valdymo sistema, kurią šiuo atveju galime vadinti menedžeriu, vykdo programas, kurios stebi ir kontroliuoja valdomus įrenginius. Menedžeris suteikia didžiąją dalį atminties resursų reikalingų tinklo valdymui. Tinklo valdymo sistema - menedžeris privalo turėti:

- sąsają, kurios dėka tinklo administratorius gali stebėti ir valdyti tinklą;

- protokolą, kuriuo tinklo valdymo sistema – menedžeris ir valdomi įrenginiai apsikeitinėja kontrolės ir valdymo informacija;
- informacijos duomenų bazę, gautą iš visų tinklo įrenginių duomenų valdymo bazių.

Vadinasi, valdymo stotis – menedžeris turi turėti visą valdymo informaciją, kuri yra kiekviename valdomame tinklo elemente.

Tam, kad valdyti resursus tinkle, jie yra pateikiami kaip objektai. Kiekvienas objektas yra būtinai duomenų kintamasis, kuris pateikia vieną tinklo valdymo sistemos aspektą. Tokių objektų rinkinys vadinamas MIB – valdymo informacine baze. Šie objektai yra standartizuoti tarp sistemų į tam tikras klases (pavyzdžiui tiltų klasė palaiko tuos pačius valdymo objektus). Papildomai dar gali būti padaryti asmeniniai išplėtimai.

Privačiuose duomenų perdavimo tinkluose valdymo informacijai tarp menedžerio ir agento keistis dažniausiai yra naudojamas SNMP protokolas. Agentas užpildo MIB tam tikromis reikšmėmis, gautomis iš tinklo mazgo arba įrenginio. Užklausus menedžeriui, agentas perduoda jam arba pakeičia įrenginio MIB bazėje esančių kintamųjų reikšmes.

Gaudama MIB objektų reikšmes, tinklo valdymo sistema - menedžeris atlieka tinklo valdymą ir stebėjimą. Agentas čia atlieka tarpininko vaidmenį tarp valdomų resursų ir tinklo valdymo sistemos. Menedžeris turi žinoti, kokias charakteristikas jis gali užklausti iš agento ir kokius parametrus jis gali keisti ar nustatyti. Jis gali pavesti agentui atlikti tam tikrą veiksmą arba, modifikuodamas, dalį specifinių kintamųjų, gali pakeisti agento konfigūracijos parametrus.

SNMP protokolas naudoja tiksliai nustatytą rinkinį komandų ir užklausų. MIB bazėje turi būti informacija apie šias komandas ir apie reikiamus objektus, t.y kontroliuojamus parametrus arba būsenos informaciją. Norint, kad agentas gautų reikiamus duomenis apie tinklo įrenginį, jis turi veikti su realiu resursu, todėl agentas yra integruojamas į įvairius tinklo įrenginius bei gali turėti sąsajas ir su išoriniais davikliais, kurie naudojami įvairiai informacijai surinkti.

2.3. VALDYMO INFORMACINĖS BAZĖS

2.3.1. MIB

SNMP protokolą naudojanti valdymo sistema valdymo informaciją “mato” kaip valdomų objektų rinkinį. Taip valdomi objektai sudaro valdymo informacinę bazę (MIB), kuri yra pasiekiama naudojant SNMP protokolą. Įrenginių MIB laikoma visa informacija, kuri reikalinga tinklo įrenginių kontrolei ir valdymui. Kiekvienas objektas MIB duomenų bazėje turi savo

identifikatorių OID (angl. *Object Identifier*), kuris unikaliai identifikuoja jį MIB hierarchijoje. Valdomas objektas (arba kitaip vadinamas MIB objektas) yra vienas iš daugelio specifinių valdomo įrenginio charakteristikų. Susijusių MIB objektų rinkinys yra apibrėžiamas kaip MIB modulis.

MIB bazės kintamų pavadinimų ir tipų apibrėžimas atliekamas atskiroje specifikacijoje, kuri yra pavadinta SMI - valdančiosios informacijos struktūra (angl. *Structure of Management Information*). Aprašant MIB kintamųjų formatą SMI specifikacija remiasi ISO priimta formalia kalba ASN.1. Ji vienareikšmiškai suderina terminus išreikštus žmonių kalba su duomenimis, kurie yra perduodami komunikaciniuose įrangos protokoluose. MIB bazės dokumentacija, parašyta naudojant ASN.1, gali lengvai būti konvertuojama į pranešimų kodus, kurie yra būdingi protokolų pranešimams. ASN.1 kalba palaiko įvairaus tipo kintamuosius, tokius kaip sveikas skaičius, eilutė ir leidžia iš šitų duomenų tipų konstruoti sudėtinius tipus, tokius taip masyvai, struktūros.

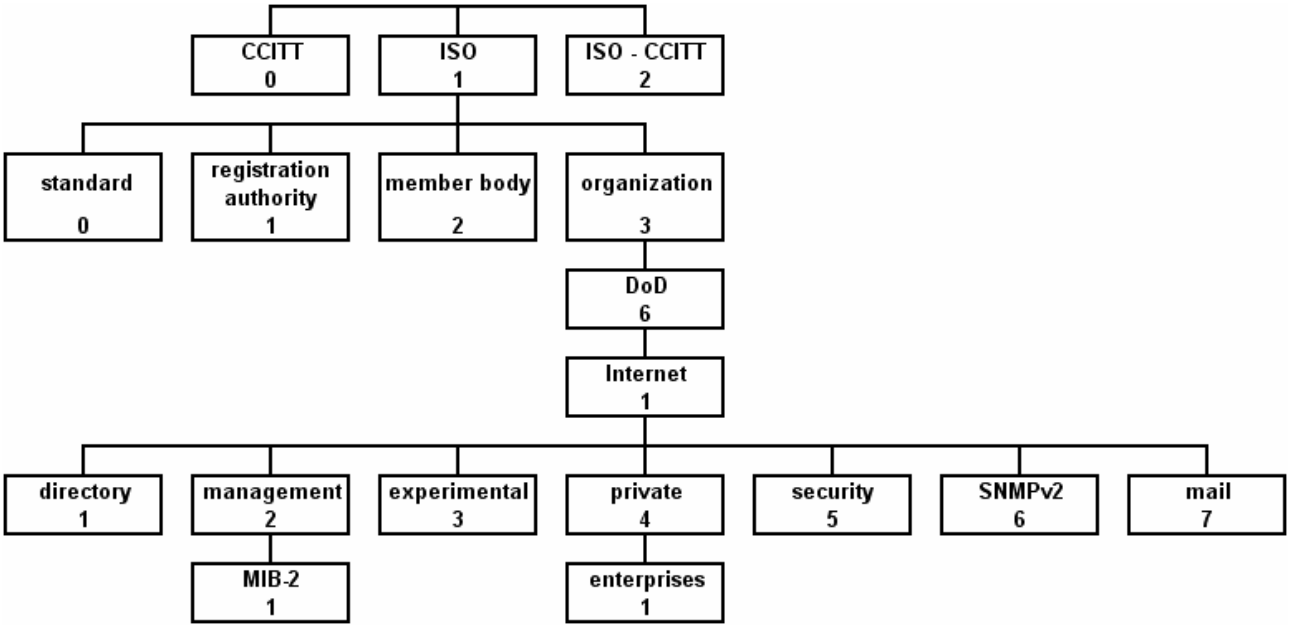
MIB kintamųjų vardai gali būti užrašyti simboliniame arba skaičių formate. Simbolinis užrašymas gali būti panaudotas atliekant užrašus tekstiniuose dokumentuose. SNMP pranešimuose naudojamas skaitmeninis pavadinimas.

Šiuo metu yra keli valdančios duomenų bazės MIB standartai, kurie pagrįsti SNMP protokolu. Pagrindiniai standartai yra MIB-I, MIB –II , o taip pat nuotolinio valdymo bazės versija RMON MIB. Be to egzistuoja specializuotų konkretaus tipo įrenginių MIB bazės, o taip pat privačių įrangos gamintojų MIB bazės.

Pradinė MIB-I specifikacija apibrėžia tik kintamųjų reikšmių nuskaitymo operaciją. MIB-I (RFC 1156) versija išskiria 114 objektų, kurie yra suskirstyti į 8 pogrupius.

MIB–II versijoje standartinių objektų skaičius padidintas iki 185, o grupių skaičius padidintas iki 10.

MIB objektų struktūra matome MIB medyje 1 pav.



1pav. MIB medis [11].

MIB-Pagrindinių grupių funkcijos:

System grupės objektai apibendrina informaciją apie sistemą.

Interfase grupės objektai tai – pagrindiniai faktai, paketų įėjimo ir išėjimo skaitikliai. Paprastai tai būna įrašų lentelės skirtos kiekvienai sąsajai.

Ip grupės objektai tai įvairūs loginiai kintamieji, skaitikliai ir maršrutizavimo lentelių kintamieji. Čia taip pat perkeliama tai, kas buvo įrašyta ARP (angl. *Address Resolution Protocol*) lentelėje.

Icmp grupė tai įvairūs skaitikliai, kurie skirti ateinantiems ir išeinantiems informacijos srautams skaičiuoti.

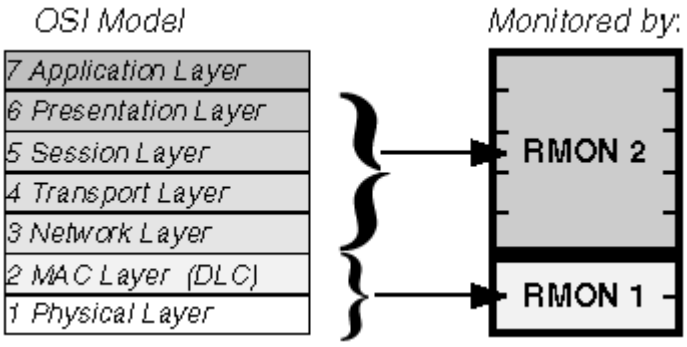
2.3.2. RMON

Naujausių SNMP protokolo funkcinių galimybių papildymu tapo RMON (angl. *Remote Network Monitoring*)– specifikacija, kuri leidžia atlikti nuotolinę sąveiką su MIB baze. RMON taip pat atlieka tinklo stebėjimą ir protokolų analizę. Su RMON1 tinklo administratorius gali surinkti informaciją iš nutolusių tinklo segmentų tam kad būtų galima aptikti gedimus ir stebėti tinklo darbą.

Iki RMON specifikacijos pasirodymo SNMP protokolas negalėjo būti panauduotas nuotoliniu būdu, jis leisdavo atlikti tik tiesioginį įrenginių valdymą. RMON MIB bazė turi visą eilę savybių, kurios leidžia atlikti nuotolinį valdymą, nes savo bazėje laiko informaciją apie valdomus įrenginius. Tai leidžia sumažinti tinkle perduodamos valdymo informacijos apimtis. RMON1 MIB suteikia:

- informaciją apie dabartinį ir ankstesnius duomenų srautus tinklo segmente.
- visapusišką signalizacijos ir įvykių mechanizmą, sudarant slenksčius ir įspėjant tinklo administratorių apie tinklo elgesio pasikeitimus.
- galingą, lankstų filtrą ir paketų gaudiklio funkciją, kuri gali būti naudojama gauti paskirstytą protokolų analizatorių.

RMON įrankis yra pristatomas kaip dviejų dalių sprendimas: klientas – serveris. Klientas yra aplikacija, kuri dirba tinklo valdymo stotyje ir teikia RMON informaciją vartotojui. Serveris tai - stebėjimo įrenginiai, paskirstyti tarp nutolusių įrenginių, kurie surenka RMON informaciją. Stebėjimo įrenginys dažnai yra vadinamas zondu (angl. *probe*) ir paleidžia programą, kuri paprastai yra vadinama RMON agentu. Tokie RMON agentai gali būti randami tokiuose tinklo įrenginiuose, kaip koncentratoriai ir komutatoriai. Agentas ir aplikacija susisiekia naudodami SNMP protokolą. RMON suprojektuota taip, kad duomenų surinkimas ir apdorojimas yra atliekamas nuotolinio zondo. Taip yra sumažinamas SNMP informacijos srautas tinkle ir valdymo stoties darbas. RMON agentų intelektualumas yra žymiai sudėtingesnis nei MIB-I arba MIB-II. Tai leidžia jiems atlikti žymią darbo dalį, kurią ankščiau atlikdavo menedžeris. Daug RMON "kliento" aplikacijų gali būti išsidėsčiusios įvairiose tinklo vietose ir gali tuo pačiu metu bendrauti ir gauti informaciją iš RMON serverio. Gauta informacija gali būti panaudota įvairių konfliktų sprendimui ir protokolų analizei, kad būtų galima atlikti tinklo stebėjimą ir plėtimo planavimą.



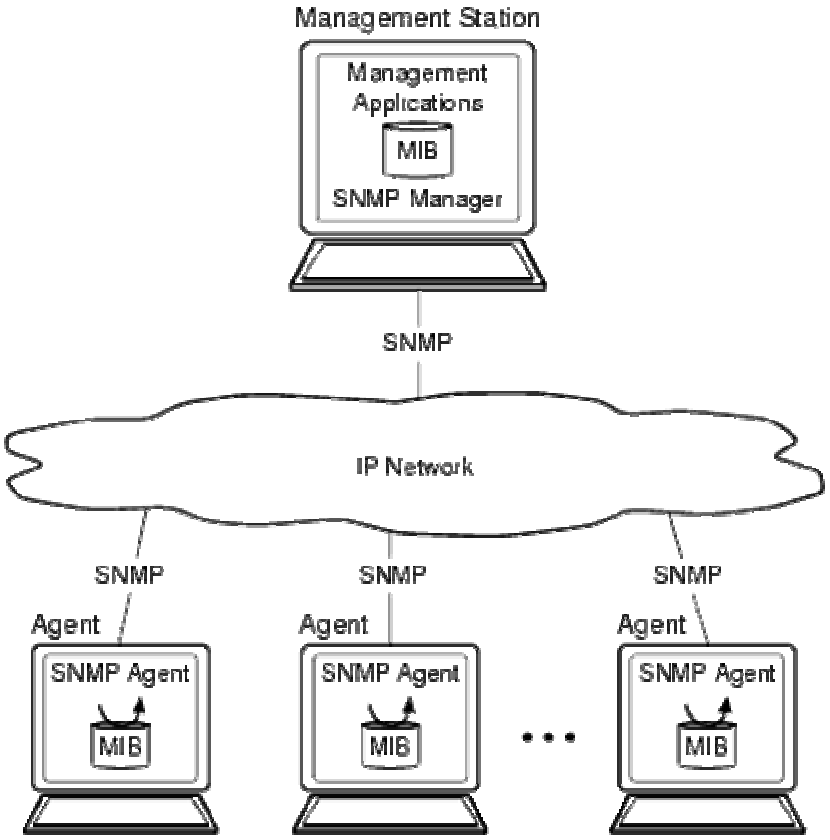
2pav.RMON1 ir RMON2 sąryšis su tinklo lygiais [12]

RMON2 specifikacija turi dar daugiau galimybių. Ji įgalina atlikti tinklo monitoringą naudojant aukštesnio lygio protokolus, tačiau RMON2 nepakeičia RMON1, nes reikalingi abudu

MIB. RMON1 teikia duomenis tinklo segmento stebėjimui ir protokolų analizei, o RMON2 - duomenis tinklo ir programų stebėjimui. RMON1 ir RMON2 sąryšis su tinklo lygiais matosi 2 pav.

2.4. AGENTO-MENEDŽERIO MODELIS

Kompiuteriniu tinklo monitoringo ir valdymo negalima apibūdinti nenaudojant agento-menedžerio modelio. Šis modelis svarbus tuo, kad jis nusako sąveiką tarp tinklo įrenginių ir programų. Agento-menedžerio modelio veikimo schema matome 3 pav.



3 pav. Agento-menedžerio modelio veikimo schema. [10]

Tokiu principu valdomas tinklas susideda iš šių komponentų:

1. Valdomų įrenginių;
2. Agentų;
3. Valdymo informacinės bazės (MIB);
4. Menedžerio ;
5. Valdymo informacijos perdavimo protokolo;

Valdomas įrenginys yra tinklo mazgas, į kurį įeina agentas ir kuris priklauso tinklui. Valdomi įrenginiai tai - tinklo elementai: maršrutizatoriai, serveriai, komutatoriai ir k.t.

Agentas – tai tinklo valdymo programinis modulis, kuris priklauso valdomam įrenginiui. Agentas turi visą vietinę valdymo informaciją ir ją suderina su tinklo valdymo protokolu, t.y. išverčia į atitinkamą formatą. Agentas surenka iš įrenginio valdymo informaciją ir, naudodamas valdymo informacijos perdavimo protokolą, pateikia ją menedžeriui. Agentai gali skirtis pagal savo galimybes. Jie gali atlikti minimalias funkcijas arba pateikti pilną informacija apie objektą.

Menedžeris vykdo programas, kurios stebi ir kontroliuoja valdomus įrenginius. Menedžeris suteikia didžiąją dalį atminties resursų reikalingų tinklo valdymui.

Menedžeris privalo turėti:

1. Sąsają, kurios dėka tinklo administratorius gali stebėti ir valdyti tinklą;
2. Protokolą, kuriuo menedžeris ir agentai apsikeitinėja kontrolės ir valdymo informacija;
3. Informacijos duomenų bazę, gautą iš visų tinklo įrenginių duomenų valdymo bazių.
4. Santrauką valdymo informacijos, kuri yra kiekviename valdomame tinklo elemente.

Tam, kad valdyti resursus tinkle, tie resursai yra pateikiami kaip objektai. Kiekvienas objektas yra būtinai duomenų kintamasis, kuris pateikia vieną tinklo valdymo sistemos aspektą. Tokių objektų rinkinys yra vadinamas MIB – valdymo informacine baze. Šie objektai yra standartizuoti tarp sistemų į tam tikras klases (pavyzdžiui tiltų klasė palaiko tuos pačius valdymo objektus). Papildomai dar gali būti padaryti asmeniniai išplėtimai.

Privačiuose duomenų perdavimo tinkluose valdymo informacijai tarp menedžerio ir agento apsikeisti pagrindinai yra naudojamas SNMP protokolas. Agentas užpildo MIB tam tikromis reikšmėmis, gautomis iš tinklo mazgo arba įrenginio. Užklausus menedžeriui agentas perduoda jam arba pakeičia įrenginio MIB bazėje esančių kintamųjų reikšmes. Todėl valdomas tinklo elementas gali dirbti su minimaliomis sąnaudomis, kurios reikalingos tik SNMP protokolo palaikymui.

Gaudamas MIB objektų reikšmes, menedžeris atlieka tinklo stebėjimą ir valdymą. Agentas čia atlieka tarpininko vaidmenį tarp valdomų resursų ir menedžerio. Menedžeris turi žinoti, kokias charakteristikas jis gali užklausti iš agento ir kokius parametrus jis gali keisti ar nustatyti. Jis gali pavesti agentui atlikti tam tikrą veiksmą arba, modifikuodamas, kai kuriuos specifinius kintamuosius, gali pakeisti agento konfigūracijos parametrus.

SNMP protokolas naudoja tiksliai nustatytą rinkinį komandų ir užklausų. MIB bazėje turi būti informacija apie šias komandas ir apie reikiamus objektus t.y kontroliuojamus parametrus arba būsenos informaciją. Norint, kad agentas gautų reikiamus duomenis apie tinklo įrenginį, jis turi

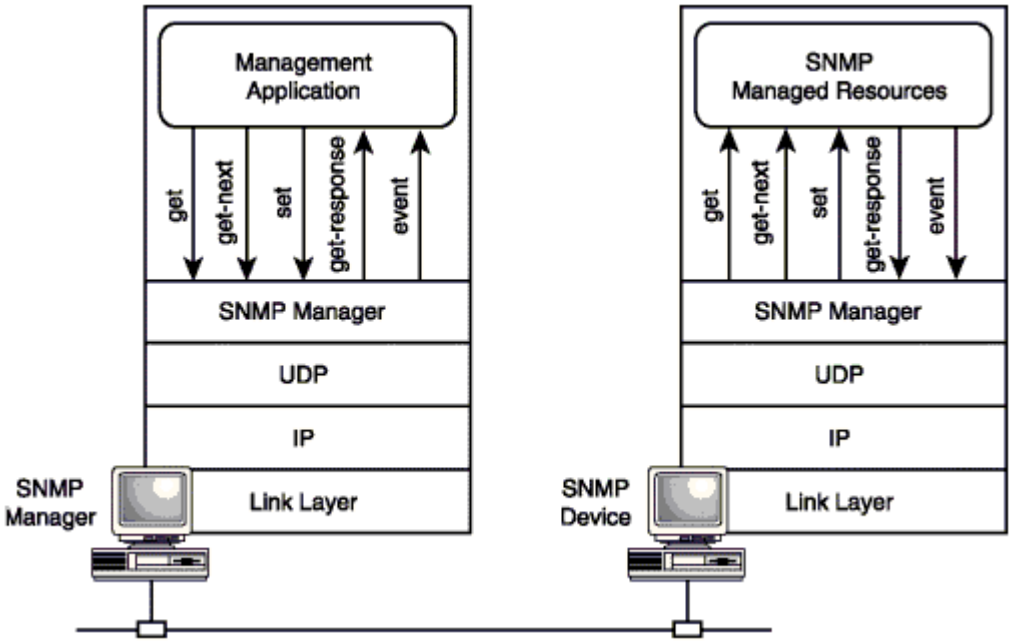
veikti su realiu resursu. Todėl agentas yra integruojamas į įvairius tinklo įrenginius. Agento prijungimo prie tinklo įrenginio taškus ir bendravimo su vidiniais mazgais būdus nustato įrenginio gamintojas.

2.5. OID (OBJEKTO IDENTIFIKATORIUS)

Kadangi SNMP protokolas gali pasiusti užklausą tik kai objektai turi griežtai reglamentuotą struktūrą, todėl kiekvienas objektas turi savo identifikatorių pagal kuri jis identifikuojamas tinkle ir pagal kurį jam yra formuojamas SNMP pranešimas. OID paprastai yra skaičių, rodančių kelią iki įranginio, seka, atskyrimui naudojant taškus. Pvz.: 1.3.6.1.2.1.2.2.1.8 . Kadangi galima situacija, kai tinklo įrenginyje yra keli vienodi objektai (pvz. tinklo plokštės), tai paskutinis skaičius šioje sekoje nusako objekto numerį. Kai objektas yra vienintelis, gale rašomas 0.

2.6. SNMP PROTOKOLO APŽVALGA

SNMP veikia pagal agento-menedžerio schemą. Protokolas vadinamas „paprastuoju“ nes reikalauja minimalaus programinio aprūpinimo. Pagrindines funkcijas atlieka menedžeris. SNMP palaiko ribotą valdymo funkcijų bei atsakymų skaičių. Menedžeris naudoja komandas *Get*, *GetNext* (jeigu duomenys lentelinės struktūros) ir *Set* (naudojama parametram keisti). Paskutinės komandos nenaudosime, nes nekeisime jokiu konfigūravimo duomenų. Agentai siunčia pranešimus apie įvykius *Traps*. Šiuos pranešimus agentas siunčia menedžeriui tik tada, kai kažkuris sistemos parametras viršijo nustatytąją ribą. Agentai, gavę iš menedžerio užklausą *Get,* formuoja atsakymą *GetResponse* (rodymo operacija). Reikia nepamiršti, kad naujausia SNMP v3 protokolo versija leidžia naudoti autorizaciją kartu su užklausomis. Tai leidžia skirtingiems vartotojams suteikti skirtingas teises gauti duomenis iš agento, kartu tai leidžia apsaugoti nuo nesankcionuoto parametru keitimo. SNMP protokolo duomenų apsikeitimo modelis pavaizduotas 4 pav. Šis paveikslėlis leidžia geriau suprasti SNMP protokolo veikimą ir tai dar parodo pereinant per protokolų lygmenis.



4 pav. SNMP protokolo duomenų apsikeitimo modelis.[13]

2.7. ALTERNATYVIŲ MONITORINGO SISTEMŲ APŽVALGA

Tinklų priežiūrai sukurta nemažai programinių paketų. Tinklus galima analizuoti standartinėmis Microsoft server priemonėmis, tačiau turint didesnį ir sudėtingesnį kompiuterinį tinklą, jos tampa nelabai patogiomis ir reikalaujančiomis nemažai laiko sąnaudų.

Yra sukurta nemažai įvairių nemokamų sistemų, leidžiančių tikrinti tam tikrus tinklo parametrus, tačiau dažnai būna, kad paketas tikrina vieną parametrą, o netikrina kito tinklo parametro. Aišku, yra sistemų, leidžiančių tikrinti daugelį tinklo parametrų, bet jos yra sudėtingo konfigūravimo ir pakankamai brangios. Šios sistemos prieinamos tik rimtoms kompanijoms, galinčioms sau leisti pakankamai investuoti į savo kompiuterinius tinklus, todėl apžvelgsime keletą paprastesnių monitoringo sistemų.

2.7.1. MONITORINGO SISTEMA „Freepinging“

Trumpas sistemos apibūdinimas: paprasta sistema tiek vartojimui, tiek tinklo įrenginių būsenų stebėjimui. Sistemos vartojo sąsajos darbo langą galima pamatyti 1 priede. Sistemą galima rasti [14]

Kaupiami parametrai:

1. Pasiekiamumas;
2. Pasiekiamumo trukmė.

Užduodami parametrai:

1. Tikrinamojo mazgo IP adresas.

Programos privalumai:

1. Paprasta vartotojo sąsaja;
2. Patogu stebėti, kai tiriamų objektų yra nedaug ir jie telpa į matomąjį langą;
3. Galima pasirašyti prierašus prie IP adresų, kokio tai objekto IP adresas.

Programos trūkumai:

1. Esant tiek objektų, kiek turėtume stebėti, nebetilptų į langą, ir nebūtų galima matyti viso vaizdo iš karto;
2. Sistema negeneruoja aliarmo signalo, o tik pažymi grafiškai šalia IP adreso, ar jis dirba tvarkingai, ar ne;
3. Vartotojas ryšius tarp objektų turi žinoti pats;
4. Programa instaliuojama į serverį ir gali būti naudojama tik prisijungus prie serverio (reikia neužmiršti, kad į Microsoft server 2003 galima prisijungti tik dviem naudotojams vienu metu ir jie turi turėt atitinkamas teises serveryje);
5. Programa nesaugo duomenų apie įvykio būsenas;
6. Atsakymo į veikimo užklausą skaitikliai, paleidus programą, skaičiuoja nuo nulinės reikšmės.

2.7.2. MONITORINGO SISTEMA „FlexibleSoft Ping v2.0“

Trumpas programos apibūdinimas: paprasta sistema tiek vartojimui, tiek tinklo įrenginių būsenų stebėjimui. Sistemos vartojo sąsajos darbo langą ir galimų išsaugoti duomenų langą galima pamatyti 2 priede (16 ir 17 pav.) Sistemą galima rasti [15]

Kaupiami parametrai:

1. Pasiekiamumas;
2. Pasiekiamumo trukmė.

Užduodami parametrai:

1. Tikrinamojo mazgo IP adresas;
2. Momentinės būsenos ataskaitos užklausimas.

Programos privalumai:

1. Parasta vartotojo sąsaja;
2. Lengvas stebėjimas, kai tiriamų objektų nedaug ir jie telpa į matomąjį langą;
3. Galima duomenis eksportuoti *.html formatu (bet tik esamu laiko momentu, kuris įrašomas kartu į failą kaip laiko žymė);

Programos trūkumai:

1. Esant tiek objektu, kiek turėtume stebėti, nebetilptų į langą, ir nebūtų galima matyti viso vaizdo iš karto;
2. Sistema negeneruoja aliarmo signalo, o tik pažymi grafiškai šalia IP adreso, ar jis dirba tvarkingai, ar ne;
3. Vartotojas ryšius tarp objektų turi žinoti pats;
4. Vartotojas turi turėti atskirą lentelę, kurioje IP adresai būtų susieti su objektu;
5. Programa instaliuojama į serverį ir gali būti naudojama tik prisijungus prie serverio (reikia neužmiršti, kad į Microsoft server 2003 galima prisijungti tik dviems naudotojams vienu metu ir jie turi turėti atitinkamas teises serveryje);
5. Programa saugo įvykių būseną tik saugojimo momentui;
6. Nėra atsakymų į veikimo užklausą skaitliukų.

2.7.3. MONITORINGO SISTEMA „Ping tester“

Programos apibūdinimas: paprasta sistema tiek naudojimuisi, tiek stebėjimui. Sistemos vartojo sąsajos darbo langą ir duomenų failo pavyzdį galima pamatyti 3 priede (18 ir 19 pav.) Sistemą galima rasti [16]

Kaupiami parametrai:

1. Tikrinimo laikas (data, valanda, minutės, sekundės);
2. Pasiekiamumas;
3. Pasiekiamumo trukmė.

Užduodami parametrai:

1. Tikrinamojo mazgo IP adresas;
2. Pasiekiamumo laukimo laikas (per kiek laiko turi gauti atsakymą);
3. Pasiekiamumo tikrinimo intervalas (laiko intervalas iki sekančio tikrinimo);
4. Duomenų išsaugojimo inicijavimas.

Programos privalumai:

1. Parasta vartotojo sąsaja;
2. Lengvas stebėjimas, kai tiriamų objektų nedaug ir jie telpa į matomąjį langą;
3. Galima išsaugoti duomenis į *.txt failo formatą, kuris yra labai patogus duomenų apdorojimui ir užima labai mažai vietos;
4. Vaizdas įprastas prie komandinės eilutės pripratusiems vartotojams.

Programos trūkumai:

1. Esant tiek objektu, kiek turėtume stebėti, nebetilptų į langą ir nebūtų galima matyti viso vaizdo iš karto;
2. Sistema negeneruoja aliarmo signalo, o tik matosi IP adreso pasiekiamumas;
3. Vartotojas ryšius tarp objektų turi žinoti pats;
4. Vartotojas turi turėti atskirą lentelę, kurioje IP adresai būtų susieti su objektu;
5. Programa gali būti naudojama tik prisijungus prie serverio (reikia neužmiršti, kad į Microsoft server 2003 galima prisijungti tik dviems naudotojams vienu metu ir jie turi turėt atitinkamas teises serveryje);

6. Programa nors ir nemokama, tačiau norint išsaugoti didesnį kiekį duomenų, prašo apmokėjimo 3 priedas 20 pav. (nemokamai leidžia saugoti iki 20 eilučių);
7. Duomenys saugomi tik inicijavus jų saugojimą.

2.8. MONITORINGO SISTEMŲ PALYGINIMAS

Monitoringo sistemų parametrai:

1. Laikas;
2. Pasiekiamumas;
3. Pasiekiamumo trukmė;
4. Tikrinamo mazgo IP adreso įvedimas;
5. Pasiekiamumo laukimo laiko įvedimas;
6. Pasiekiamumo tikrinimo dažnumo įvedimas;
7. IP adresų grupavimo pagal kanalus įvedimas;
8. Mazgo neatsakymo reikšmingumo įvedimas;
9. Vartotojo informacijos įvedimas ir teisių priskyrimas;
10. VPN tinklo būsenos atvaizdavimas interaktyviame žemėlapyje;
11. Atskiro VPN kanalo būsenos atvaizdavimas;
12. Duomenų kaupimas failuose;
13. Galimybė atlikti duomenų užklausą;
14. Galimybė atlikti stebėjimą neprisijungus prie serverio;
15. Aliarmo signalo generavimas.

1 lentelė. Monitoringo sistemų parametrų palyginimas

Monitoringo sistemos parametrai :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Monitoringo sistema „Freepinging“		+	+	+			+								
Monitoringo sistema „FlexibleSoft Png v2.0“		+	+	+								+			
Monitoringo sistema „Ping tester“	+	+	+	+	+	+						+			
Kuriamoji „VPN tinklo monitoringo sistema“	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

2.9. ANALITINĖS DALIES IŠVADOS

Išanalizavę teoriją apie VPN tinklų monitoringą ir valdymą, darbe pasirinkome agento-menedžerio schemą. Mūsų atveju agentai bus įrenginiuose, į kuriuos kreipsimės (serveriai, maršrutizatoriai).

Užklausos agentams bus formuojamos naudojant SNMP ryšio protokolą. Šis protokolas yra inkapsuliuojamas į tiriamajame kompiuterių tinkle naudojamą TCP/IP protokolą. Kadangi turėsime kreiptis į įrenginius, kurie priklauso ryšio paslaugų tiekėjui, naudosimės tik ta dalim informacijos, kuri yra prieinama ir paprastai gaunama iš visų agentų.

Manau, kad naudojamų modelių analizė, kartu su panašių programų bandymais ir bandymų analize, leis sukurti geresnę sistemą už bandytąsias sistemas.

Palyginę keletą sistemų matome, kad kuriamoji sistema turi daugiausiai monitoringo parametrų iš visų palygintų sistemų.

.

3. PROJEKTINĖ DALIS

3.1. SISTEMOS KŪRIMO PAGRINDAS IR TIKSLAI

Sistemos kūrimo pagrindas:

1. Reikalingumas turėti paprastą tinklo šakų monitoringo sistemą, į kurią galėtų jungtis keletas vartotojų;
2. Reikalingumas, kad sistema galėtų pavaizduoti VPN tinklo būseną grafiškai žemėlapyje;
3. Reikalingumas, kad sistema galėtų atkreipti vartotojo dėmesį;
4. Reikalingumas turėti VPN kanalų darbingumo duomenis analizei;
5. Reikalingumas turėti nepriklausomą nuo vidinių serverio priemonių VPN kanalų darbą atvaizduojančią sistemą.

Sistemos kūrimo tikslas:

1. Sukurti sistemą, kuri palengvintų VPN tinklo ir jo kanalų būklės stebėjimą;
2. Nenaudoti prisijungimo prie serverio resursų;
3. Pagreitinti reakcijos į sutrikimą ryšio kanale laiką;
4. Pastebėti ryšio kanalų sutrikimus, apie kuriuos neinformuoja Windows server 2003 vidinės priemonės;
5. Į sutrikimų stebėjimą įtraukti administratorius, dirbančius su kitomis sistemomis (duomenų bazių administratorius);
6. Leisti padalinio vadovui stebėti VPN tinklo darbingumą (tai leistų kartu kontroliuoti darbuotojus).

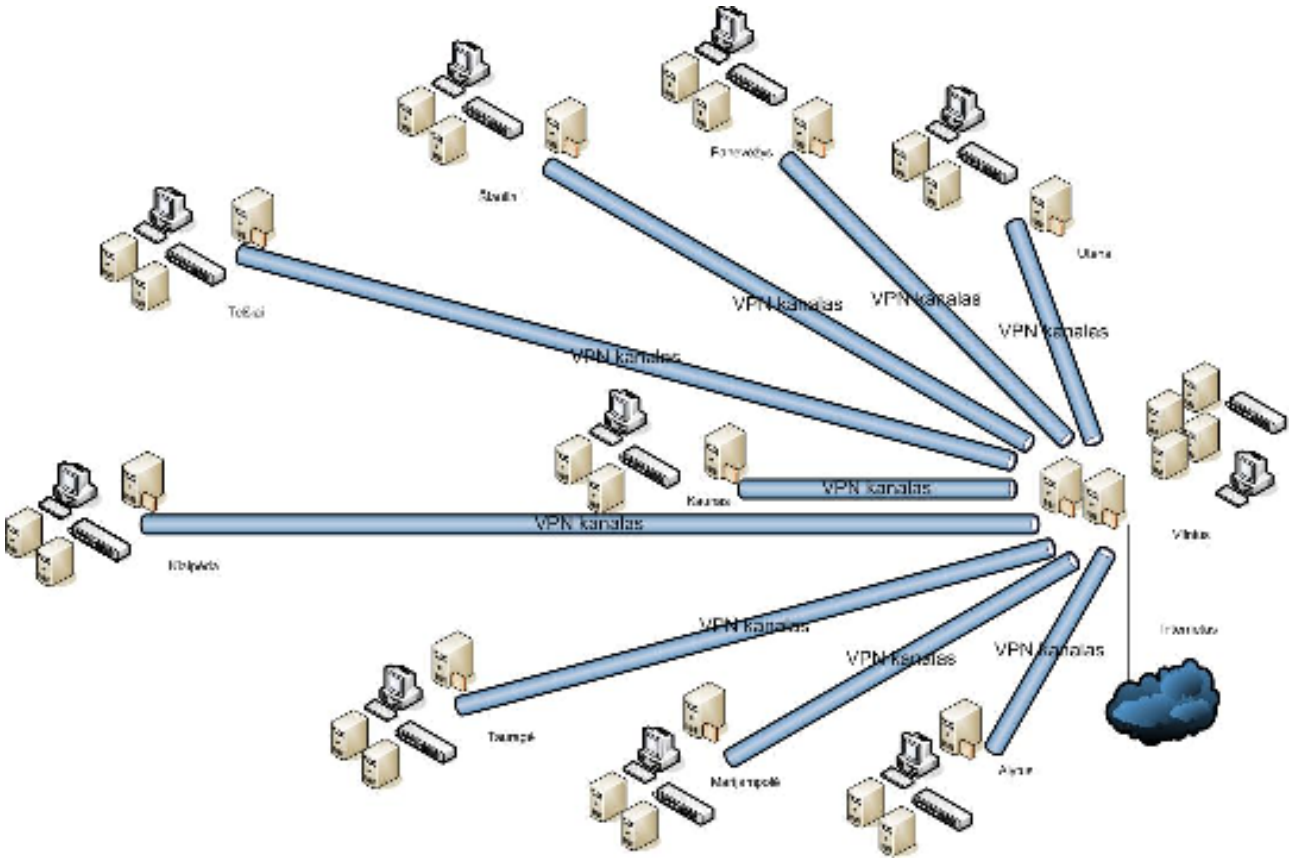
3.2. PROJEKTINEI DALIAI KELIAMI UŽDAVINIAI

Projektinei daliai keliami šie uždaviniai:

- aprašyti sistemos objektus;
- išanalizuoti ryšius tarp objektų;
- išanalizuoti reikalavimus kuriamai sistemai;
- sukurti duomenų srautų struktūras;
- suformuluoti reikalavimus kuriamai sistemai;
- sukurti sistemos veikimo algoritmą.

3.3. NAGRINĖJAMAS VPN TINKLAS

Nagrinėjamasis organizacijos VPN tinklas yra žvaigždinės architektūros.



5 pav. VPN tinklo schema.

Kaip matome, žvaigždės centras yra Vilniuje.

Pagrindinės organizacijos būstinės (Vilnius) vidinio kompiuterių tinklo architektūrą matome 4 priede.

Padalinių, esančių žvaigždės nutolusiuose mazguose tinklo struktūrą (Utena, Panevėžys, Šiauliai, Telšiai, Klaipėda, Tauragė, Marijampolė, Alytus, Kaunas) matome 5 priede.

Visuose organizacijos ISA serveriuose suinstaliuota „Microsoft ISA server 2004“ programinė įranga. Kituose serveriuose naudojama „Microsoft server 2003“ programinė įranga. Pašto serveryje - „Microsoft Exchange server 2003“. SMS serveryje yra suinstaliuota „Microsoft SMS server 2003“ programinė įranga.

Vartotojų kompiuteriuose suinstaliuota „WindowsXP Profesional“ .

3.4. MONITIRINGO SISTEMOS FUNKCIJOS

Kuriama sistema turi kreiptis į MIB ir pagal gautus duomenis formuoti aliarmus; kaupti ir pildyti duomenų bazę, kuri leistų formuoti statistiką apie tinklo darbą įvairiais pjūviais; kontroliuoti parametrų atitikimą užduotoms reikšmėms ir kaupti duomenis apie nukrypimus nuo užduotųjų parametrų; aliarmuoti, jei nukrypimas nuo užduotųjų reikšmių tęsiasi ilgesnį už nustatytą laiką. Sistema turi visą tai gerai atspindėti grafiškai. Tam galima panaudoti aktyvųjį žemėlapį, kuriame matytųsi pagrindinio tinklo struktūra. Tinklo elementai, kuriuose yra nukrypimai nuo užduotųjų reikšmių, butų žymimi signaline spalva (pvz. raudona, kai likusieji elementai - žalia.), t.y. panaudoti vadinamąjį šviesoforo principą. Pasirinkus signalizuojančio elemento apskritį iš apskričių meniu (tiems vartotojams, kuriems leista), atsivertų parametrų langas, vaizduojantis VPN tinklo šakos mazgų darbingumą.

3.5. KURIAMOS SISTEMOS OBJEKTAI IR JŲ SĄVEIKA

3.5.1. VARTOTOJAI

Tinklo administratorius

Vartotojo kategorija: pagrindinis sistemos eksploatuotojas.

Vartotojo sprendžiami uždaviniai: tinklo darbingumo užtikrinimas, ryšio atstatymas (VPN ryšio kanalo darbingumo atstatymas).

Praktinė dalis dalykinėje sferoje: profesionalas.

Patirtis informacinėse technologijose: profesionalas.

Papildoma informacija: įvykus aliarmui, sistemos langas automatiškai turi atsidaryti.

Duomenų bazių administratorius

Vartotojo kategorija: sistemos aliarmų stebėtojas.

Vartotojo sprendžiami uždaviniai: duomenų bazių darbingumo užtikrinimas, duomenų replikavimosi stebėjimas.

Praktinė dalis dalykinėje sferoje: patyręs.

Patirtis informacinėse technologijose: profesionalas.

Papildoma informacija: svarbu, kad atsiradus sutrikimams sistema generuotų garsinį signalą. Darbuotojui sistemos informacija svarbi tiek, kad informuoja jog su kažkuriuo

padaliniu nėra ryšio kanalo, todėl duomenų replikavimasis bazėje su šiuo padaliniu yra negalimas.

Vadovas

Vartotojo kategorija: tikrintojas.

Vartotojo sprendžiami uždaviniai: vadovauja IT darbuotojams, prižiūri jų darbą.

Praktinė dalis dalykinėje sferoje: bendros žinios apie sistemą.

Patirtis informacinėse technologijose: patyręs.

Papildoma informacija: prie matomo aliarmo turi būti ir laikas - kiek laiko trunka aliarmas.

3.5.2. SISTEMOS APRIBOJIMAI

Įpareigojantys apribojimai

Apribojimai sprendimui

Apribojimai informacinei sistemai:

- sistema turi būti prieinama per naršyklę (Internet Explorer ar kitas);
- spalvotas ekranas, raiška ne mažesnė nei 800X600;
- būtinas vietinis tinklas (LAN).

Diegimo aplinka

- reikalinga JVM (Java Virtual Machine) ne senesnės, nei 1.6 versijos;
- reikalinga operacinė sistema Windows server 2003;
- reikalingas Microsoft ISA server 2004 programinis paketas.

Bendradarbiaujančios sistemos

Nėra išorinių sistemų.

Komerciniai specializuoti programų paketai

Nenumatyti ryšiai su specializuotais programų paketais.

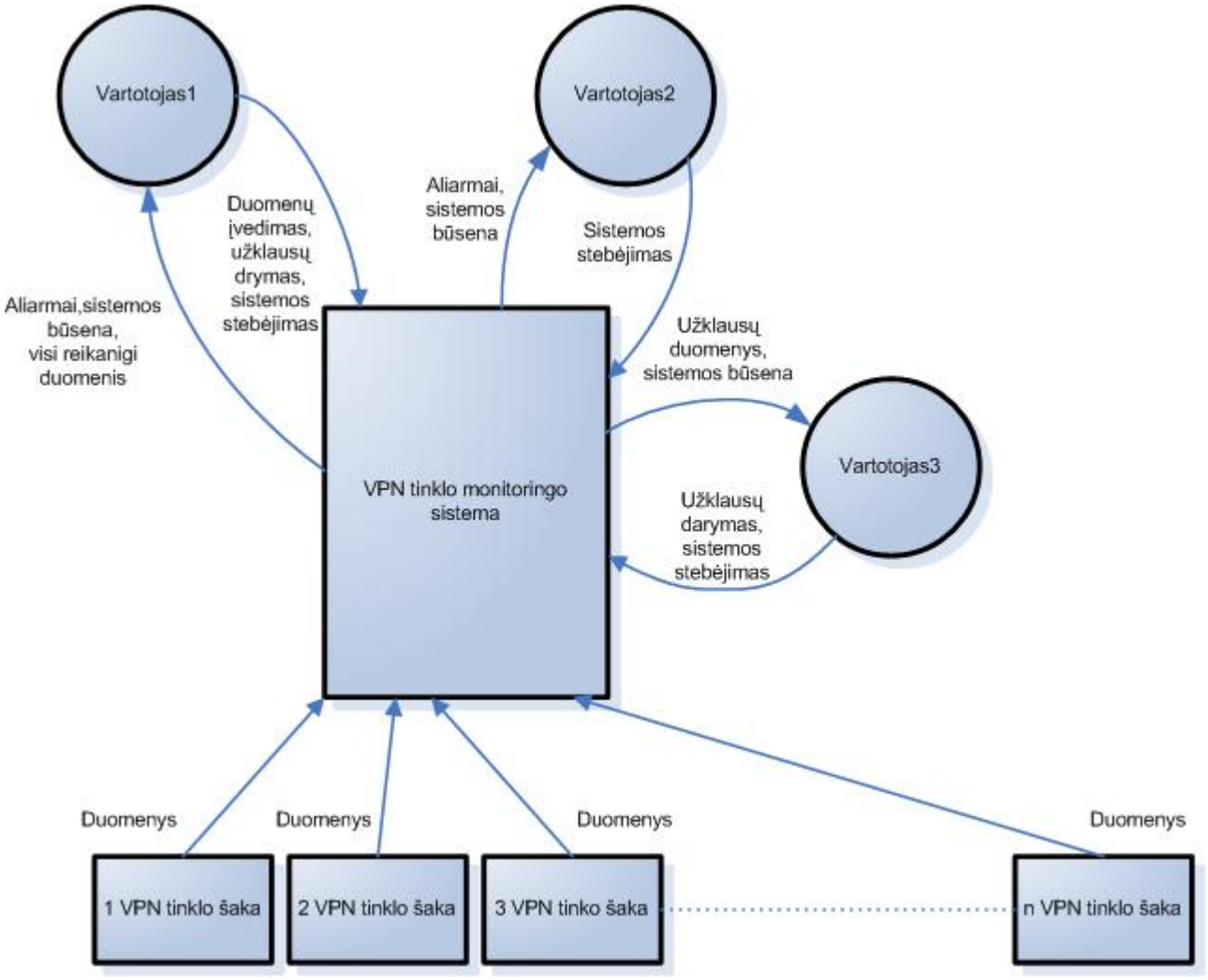
Numatoma darbo vietos aplinka

Darbo vieta turi atitikti serverinei įrangai keliamus reikalavimus, klientinei daliai – įprastinė darbo vietos aplinka.

3.5.3. FUNKCINIAI REIKALAVIMAI IR REIKALAVIMAI DUOMENIMS

3.5.3.1. VEIKLOS KONTEKSTAS

Veiklos kontekstas



6 pav. VPN tinklo monitoringo sistemos veiklos konteksto schema.

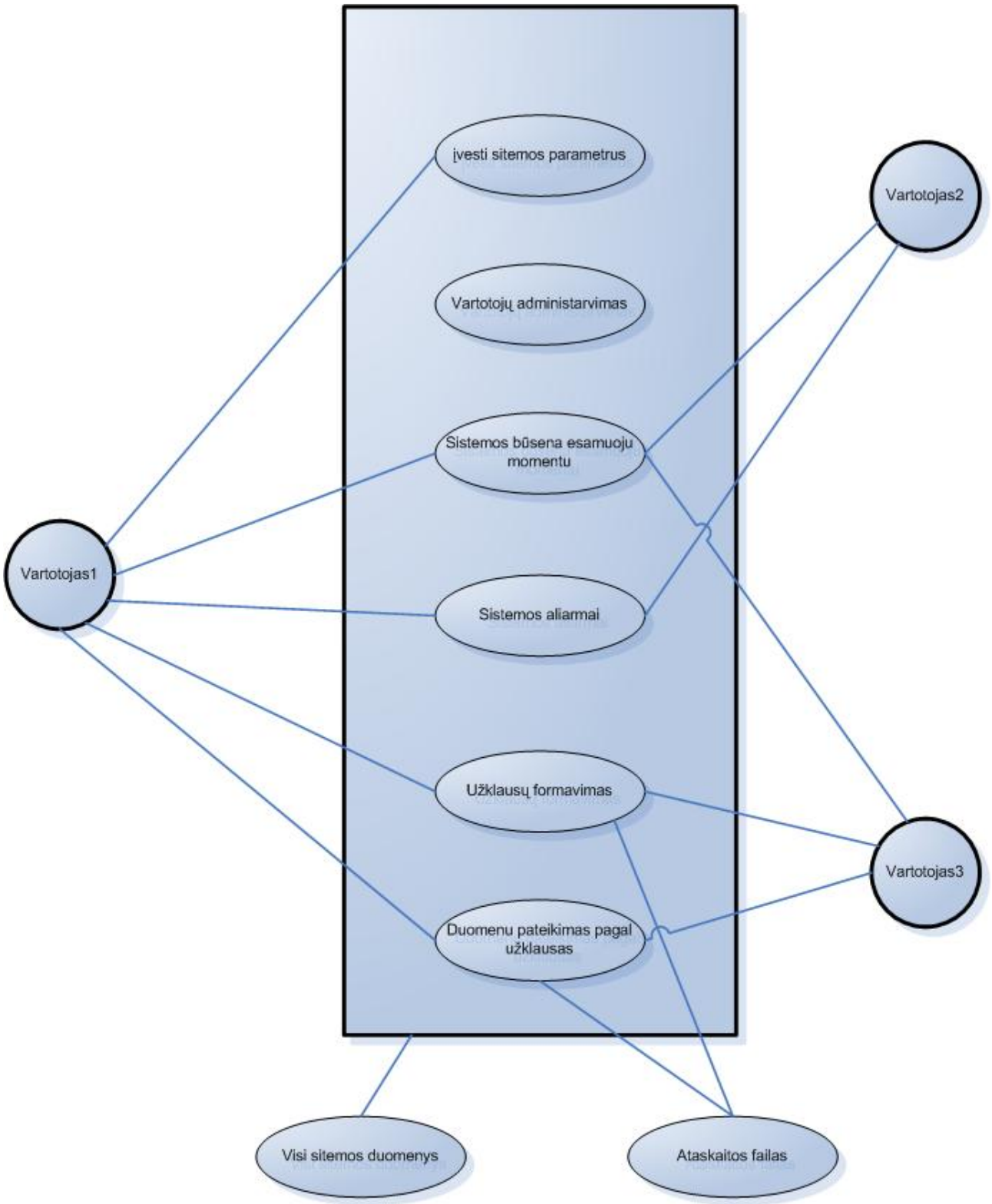
Veiklos pasiskirstymas

2 lentelė. Veiklos pasiskirstymas

Eil.	Įvykio pavadinimas	Įeinantys/išeinantys informacijos srautai
1.	n VPN tinklo šakos potinklis perduoda duomenis apie savo darbingumą	Duomenys (in)
2.	Vartotojas 1 (jis kartu yra ir sistemos administratorius) įveda informaciją, reikalingą sistemos konfigūravimui ir aliarmų būsenoms generuoti	Sistemos parametrai (in)
3.	Sistemos stebėjimo inicijavimas (visi vartotojai pagal savo teises)	Sistemos sąsajos inicijavimas (in)
4.	Užklausų generavimas (vartotojas 1 (administratorius) ir vartotojas 3 (vadovas)	Užklausos (in)
5.	Vartotojo sąsaja gauna aliarmus apie sistemos nukrypimą nuo užduotųjų parametrų	Aliarmai (out)
6.	Duomenų pagal suformuluotas užklausas pateikimas (vartotojui 1 ir vartotojui 3)	Išfiltruoti duomenys (out)

3.5.3.2. PRODUKTO VEIKLOS SFERA

Sistemos ribos



7 pav.VPN tinklo monitoringo sistemos panaudojimo atveju blokinė schema.

Panaudojimo atvejų sąrašas

3 lentelė. Panaudojimo atvejis “Įvesti reikalingus parametrus”

Nr.	1
Pavadinimas:	Įvesti reikalingus parametrus
Vartotojo/aktoriaus pavadinimas:	Vartotojas 1
Aprašas:	Atidaromas meniu langas, kuris leidžia eiti „gilyn“ ir įvesti ar redaguoti reikalingus sistemos parametrus
Prieš sąlyga:	Reikia turėti informacijos apie įvedamus ar keičiamus parametrus
Sužadinimo sąlyga:	Vartotojas per meniu pasiekia reikiama vietą ir įveda parametrus
Po sąlyga:	Duomenys įtraukiami į duomenų bazę

4 lentelė. Panaudojimo atvejis “Vartotojų administravimas”

Nr.	2
Pavadinimas:	Vartotojų administravimas
Vartotojo/aktoriaus pavadinimas:	Vartotojas 1
Aprašas:	Atidaromas meniu langas, kuriame gali redaguoti vartotojų informaciją, keisti jų teises
Prieš sąlyga:	Reikia žinoti sistemos vartotojus ir jų funkcijas, gauti leidimą apie pakeitimus iš vadovybės
Sužadinimo sąlyga:	Sistemos vartotojų pasikeitimas
Po sąlyga:	Duomenys įtraukiami į duomenų bazę

5 lentelė. Panaudojimo atvejis “Sistemos būsenos generavimas esamuoju laiko momentu”

Nr.	3
Pavadinimas:	Sistemos būsenos generavimas esamuoju laiko momentu
Vartotojo/aktoriaus pavadinimas:	Vartotojas1 Vartotojas 2
Aprašas:	Vartotojui parodoma sistemos būsena „šviesoforo“ principu aktyviame žemėlapyje

Prieš sąlyga:	Turi veikti duomenų bazė
Sužadinimo sąlyga:	Vartotojas prisijungęs prie sistemos
Po sąlyga:	Sąlygų nėra

6 lentelė. Panaudojimo atvejis “Aliarmų generavimas”

Nr.	4
Pavadinimas:	Aliarmų generavimas
Vartotojo/aktoriaus pavadinimas:	Vartotojas1 Vartotojas 2
Aprašas:	Vartotojo kompiuteryje sugeneruojamas garsinis signalas
Prieš sąlyga:	Prisijungimas prie sistemos
Sužadinimo sąlyga:	Sistemos parametrų nukrypimas nuo užduotųjų reikšmių
Po sąlyga:	Duomenys talpinami į duomenų bazę ir į ataskaitų bazę

7 lentelė. Panaudojimo atvejis “Duomenų filtravimas pagal pateiktas užklausas”

Nr.	5
Pavadinimas:	Duomenų filtravimas pagal pateiktas užklausas
Vartotojo/aktoriaus pavadinimas:	Vartotojas 1 Vartotojas 3
Aprašas:	Iš duomenų bazės išrenkami norimi duomenys
Prieš sąlyga:	Bazėje turi būti norimi duomenys
Sužadinimo sąlyga:	Sistemos naudotojas suformuoja užklausą
Po sąlyga:	Sąlygų nėra

3.5.3.3. FUNKCINIAI REIKALAVIMAI

8 lentelė. Reikalavimas 1

Reikalavimas #:	1	Reikalavimo tipas:	9.1	Įvykis/panaudojimo atvejis#:	2
Aprašymas:	Naujų vartotojų sistemoje registravimas, teisių sutekimas				
Pagrindimas:	Sistema neturinti vartotojų yra bevertė				
Šaltinis:	Vartotojas1, sistemos kūrėjas				
Tinkamumo kriterijus:	Atskiriami vartotojai pagal savo kompetenciją, apsaugo sistemą nuo išgadinimo				
Priklausomybės:	Nėra		Konfliktai:	Nėra	
Papildoma medžiaga:	Nėra				
Istorija:	Užregistruotas 2008 m. vasario mėn. 15 d				

9 lentelė. Reikalavimas 2

Reikalavimas #:	2	Reikalavimo tipas:	9.1	Įvykis/panaudojimo atvejis#:	1
Aprašymas:	Įvedami ir koreguojami parametrai, kurie yra reikalingi sistemos darbui, aliarmų generacijai, statistikai, stebimų kanalų registravimas				
Pagrindimas:	Užduodami pagrindiniai sistemos funkcionavimo parametrai				
Šaltinis:	Vartotojas1, sistemos kūrėjas				
Tinkamumo kriterijus:	Be to sistema nefunkcionuotų				
Priklausomybės:	1		Konfliktai:	Nėra	
Papildoma medžiaga:	Nėra				
Istorija:	Užregistruotas 2008 m. vasario mėn. 15 d.				

10 lentelė. Reikalavimas 3

Reikalavimas #:	3	Reikalavimo tipas:	9.1	Įvykis/panaudojimo atvejis#:	3
Aprašymas:	Galimybė vartotojui matyti sistemos būsena esamuoju laiko momentu (“šviesoforo” principu)				
Pagrindimas:	Vartotojas aiškiai mato sistemos darbingumą				
Šaltinis:	Vartotojas 1 Vartotojas 2				
Tinkamumo kriterijus:	Galimybė imtis greitų priemonių, atsiradusioms problemoms šalinti				
Priklausomybės:	1, 2		Konfliktai:	Nėra	

Papildoma medžiaga:	Nėra
Istorija:	Užregistruotas 2008 m. vasario mėn. 15 d.

11 lentelė. Reikalavimas 4

Reikalavimas #:	4	Reikalavimo tipas:	9.1	Įvykis/panaudojimo atvejis#:	4
Aprašymas:	Aliarmų generavimas				
Pagrindimas:	Galimybė greičiau informuoti vartotoją apie netvarkingą sistemos darbą				
Šaltinis:	Vartotojas 1 Vartotojas 2 Vartotojas 3				
Tinkamumo kriterijus:	Galimybė laiku perspėti vartotoją				
Priklausomybės:	1, 2		Konfliktai:	Nėra	
Papildoma medžiaga:	Nėra				
Istorija:	Užregistruotas 2008 m. vasario mėn. 15 d.				

12 lentelė. Reikalavimas 5

Reikalavimas #:	5	Reikalavimo tipas:	9.1	Įvykis/panaudojimo atvejis#:	5
Aprašymas:	Vartotojo 3 užklausa, kiek laiko jau nedirba vienas ar kitas sistemos mazgas				
Pagrindimas:	Galimybė kontroliuoti darbuotojus				
Šaltinis:	Vartotojas 3				
Tinkamumo kriterijus:	Kontrolės gerinimas				
Priklausomybės:	1, 2		Konfliktai:	Nėra	
Papildoma medžiaga:	Nėra				
Istorija:	Užregistruotas 2008 m. vasario mėn. 15 d.				

13 lentelė. Reikalavimas 6

Reikalavimas #:	6	Reikalavimo tipas:	9.1	Įvykis/panaudojimo atvejis#:	5
Aprašymas:	Vartotojui 1 reikalingų duomenų išfiltravimas iš duomenų bazės				
Pagrindimas:	Greitesnis reikiamų duomenų gavimas				
Šaltinis:	Vartotojas1				
Tinkamumo kriterijus:	Galimybė geriau įvertinti padėtį sistemoje				
Priklausomybės:	1, 2		Konfliktai:	Nėra	
Papildoma medžiaga:	Nėra				
Istorija:	Užregistruotas 2008 m. vasario mėn. 15 d.				

14 lentelė. Reikalavimas 7

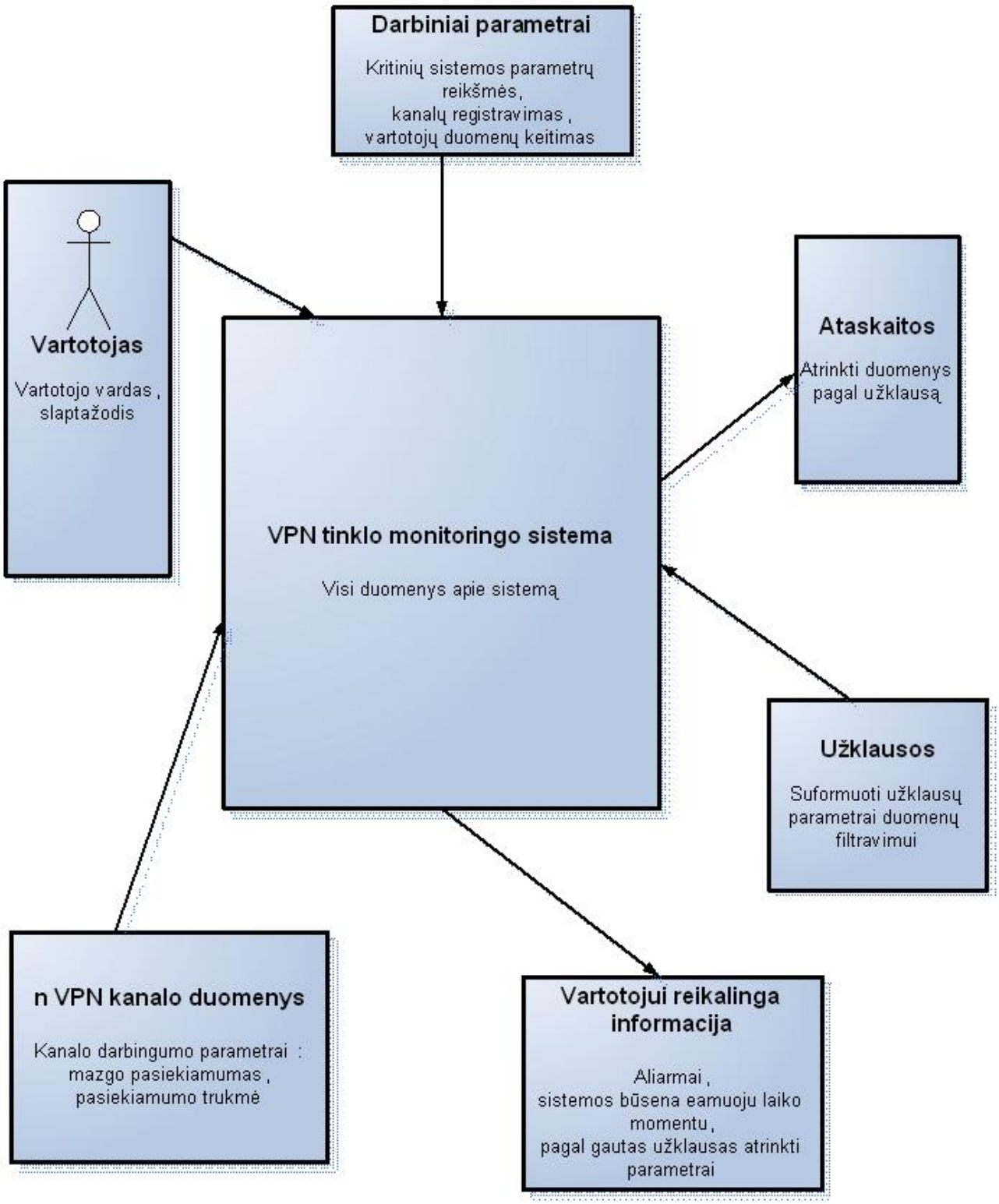
Reikalavimas #:	7	Reikalavimo tipas:	9.1	Įvykis/panaudojimo atvejis#:	6
Aprašymas:	Statistikos ir ataskaitų generavimas				
Pagrindimas:	Ilgalaikė sistemos darbo analizė				
Šaltinis:	Vartotojas 1				
Tinkamumo kriterijus:	Leidžia analizuoti sistemą, rasti silpnąsias vietas				
Priklausomybės:	1, 2		Konfliktai:	Nėra	
Papildoma medžiaga:	Sistemos parametrai				
Istorija:	Užregistruotas 2008 m. vasario mėn. 15 d.				

15 lentelė. Reikalavimas 8

Reikalavimas #:	8	Reikalavimo tipas:	9.1	Įvykis/panaudojimo atvejis#:	6
Aprašymas:	Statistikos ir ataskaitų generavimas				
Pagrindimas:	Padeda kontroliuoti darbuotojus, rengti atsiskaitymus vadovybei				
Šaltinis:	Vadovas				
Tinkamumo kriterijus:	Parodo bendrą sistemos darbingumo vaizdą				
Priklausomybės:	1, 2		Konfliktai:	Nėra	
Papildoma medžiaga:	Duomenys įrašomi į ataskaitų bazę				
Istorija:	Užregistruotas 2008 m. vasario mėn. 15 d.				

3.5.3.4. REIKALAVIMAI DUOMENIMS

Reikalavimai duomenims



8 pav. VPN tinklo monitoringo sistemos duomenų schema.

3.5.4. NEFUNKCINIAI REIKALAVIMAI

Reikalavimai sistemos dizainui

- lengvai suprantama sąsaja;
- informacija pateikiama aktyviame žemėlapyje;
- selektyvi sąsaja generuojama automatiškai, pasirinkus padalinį iš meniu;
- automatinė įvykių atvaizdavimo žemėlapyje sistema, veikianti „šviesoforo“ principu.

Reikalavimai panaudojimui

- sistema lengvai perprantama vartotojų, be papildomų apmokymų;
- nacionalinės kalbos naudojimas;
- kritinės situacijos pastebėjimo laiko sumažinimas.

Reikalavimai vykdymo charakteristikoms

- sistemos būsenos tikrinimo laikas - kas 1 min;
- sistemos aliarmo sąlygos kiekvienam atskiram kanalui įvedamos rankiniu būdu;
- duomenys kaupiami *.txt failuose;
- reikalavimai aparatūros, kurioje veiks sistema darbingumui.

Sistemos darbui specifinių reikalavimų nėra. Svarbu, kad būtų užtikrintas pastovus elektros tiekimas sistemos įrenginiams. Tam naudojami nepertraukiamo maitinimo šaltiniai.

Reikalavimai sistemos priežiūrai

Sistemoje turi būti numatytas perėjimas prie kitos kalbos panaudojimo. Taip pat, sistema turi būti nesunkai plečiama atsiradus naujiems filialams.

Reikalavimai sistemos saugai

Sistemos duomenys yra saugomi failuose, kuriuos pasiekti gali tik tam numatyti asmenys. Sistema gali naudotis duomenimis iš keleto duomenų failų vienu metu. Failai gali būti kopijuojami, o jų kopijos saugomos kitoje vietoje, nei naudojami failai.

Teisiniai reikalavimai

Sistemos darbas neturi prieštarauti Lietuvos Respublikos įstatymams.

3.5.5. SISTEMOS IŠEIGA

Galimos problemos

Tikimasi, kad sistemai dirbant problemų neturėtų iškilti.

Egzistuojantys sprendimai

Pagamintos sistemos: Jau pagamintos sistemos yra orientuotos tik į specializuotus vartotojus, turinčius nemažą patyrimą ir specifines tinklo valdymo žinias. Jų darbui stebėti tenka prisijungti prie serverio. Keletą nemokamų paketų jau apžvelgėme anksčiau. Deja, jie nepritaikyti naudotis padalinių vadovams, turintiem ribotas kompiuterines žinias.

Galimas pakartotinis panaudojimas: sistemą galima naudoti pakartotinai organizacijose, turinčiose centralizuotą struktūrą ir savo padalinius tik Lietuvos teritorijoje.

Naujos problemos

Problemos diegimo aplinkai: diegiant sistemą gali iškilti problemų naudojant JVM aplinką. Gali būti, kad senesnė sistema nepalaikys metodų, kurie užrašyti programiniame kode, todėl į programos reikalavimus įtraukta, kad versija neturėtų būti senesnė nei 6.

Sąveika su jau įdiegtomis sistemoms: sistemai naudojant JVM aplinką padidėja sistemos apkrovimas. Tai neturėtų sukelti rimtesnių problemų kitoms sistemos, nes naudojama naujausia JVM aplinka. Sistema taip pat neturėtų kelti problemų instaliuotoms sistemoms, dirbančioms tinkle, nes naudos tik mažą dalį tinklo resursų.

Vartotojų nusiteikimas

Neigiamo vartotojų nusiteikimo sistemos atžvilgiu nesitikima.

Kliudantys diegimo aplinkos apribojimai

Nustatyti reikalavimai neturėtų kelti problemų sistemos diegimo aplinkai, problema atsirastų tuomet, jei nebūtų laikomasi nustatytų reikalavimų.

Galimos naujos, sistemos įdiegimo sukeltos problemos

Sistema naudojasi duomenų perdavimo kanalu tarp tinklo padalinių, todėl galimas neženklus kitų duomenų perdavimo laiko pailgėjimas.

3.5.6. PRITAIKYMAS

Reikalavimai esamų duomenų perkėlimui

Papildomų reikalavimų duomenų perkėlimui nėra. Jie perkalimi kaip įprastiniai failai, automatiškai kopijuojant sistemą. Dar jie gali būti perkeliami iš rezervinių kopijų, patalpinant numatytoje vietoje.

Reikalingas duomenų transformavimas į naują sistemą

Perkeliant duomenis į naują sistemą, duomenų transformacijos nereikalingos, nes duomenys saugomi failuose su griežta struktūra, be to dauguma duomenų apdorojimo programų priima *.txt tipo failus, jeigu yra žinoma duomenų struktūra.

3.5.7. RIZIKOS

Galimos sistemos sukūrimo rizikos

16 lentelė. Sistemos sukūrimo rizikos

Eil. Nr.	**Rizikos faktorius**	**Tikimybė**	**Įtaka**
1.	Programuotojo patirtis	Vidutiniška	Rimta
2.	Programuotojo pasitraukimas, liga	Žema	Rimta
3.	Reikalavimų pasikeitimas	Aukšta	Leistina
4.	Poreikis pakeisti sistemą	Vidutiniška	Rimta
5.	Techninės įrangos gedimas	Žema	Leistina
6.	Vartotojams sistema sudėtinga	Žema	Leistina

3.5.8. PERSPEKTYVINIAI REIKALAVIMAI

- duomenų bazės apie įvykius sistemoje kaupimas;
- autonomiškas duomenų perkėlimas, keičiant serverį/kompiuterį;
- informacijos apie maršrutizatoriaus darbo režimus importavimas iš paslaugos tiekėjo web aplikacijos;

- sistemos papildymas apkrovimo monitorinio ir prognozavimo priemonėmis;
- kitų duomenų bazių naudojimas: MySQL, Microsoft SQL server, Microsoft Access.

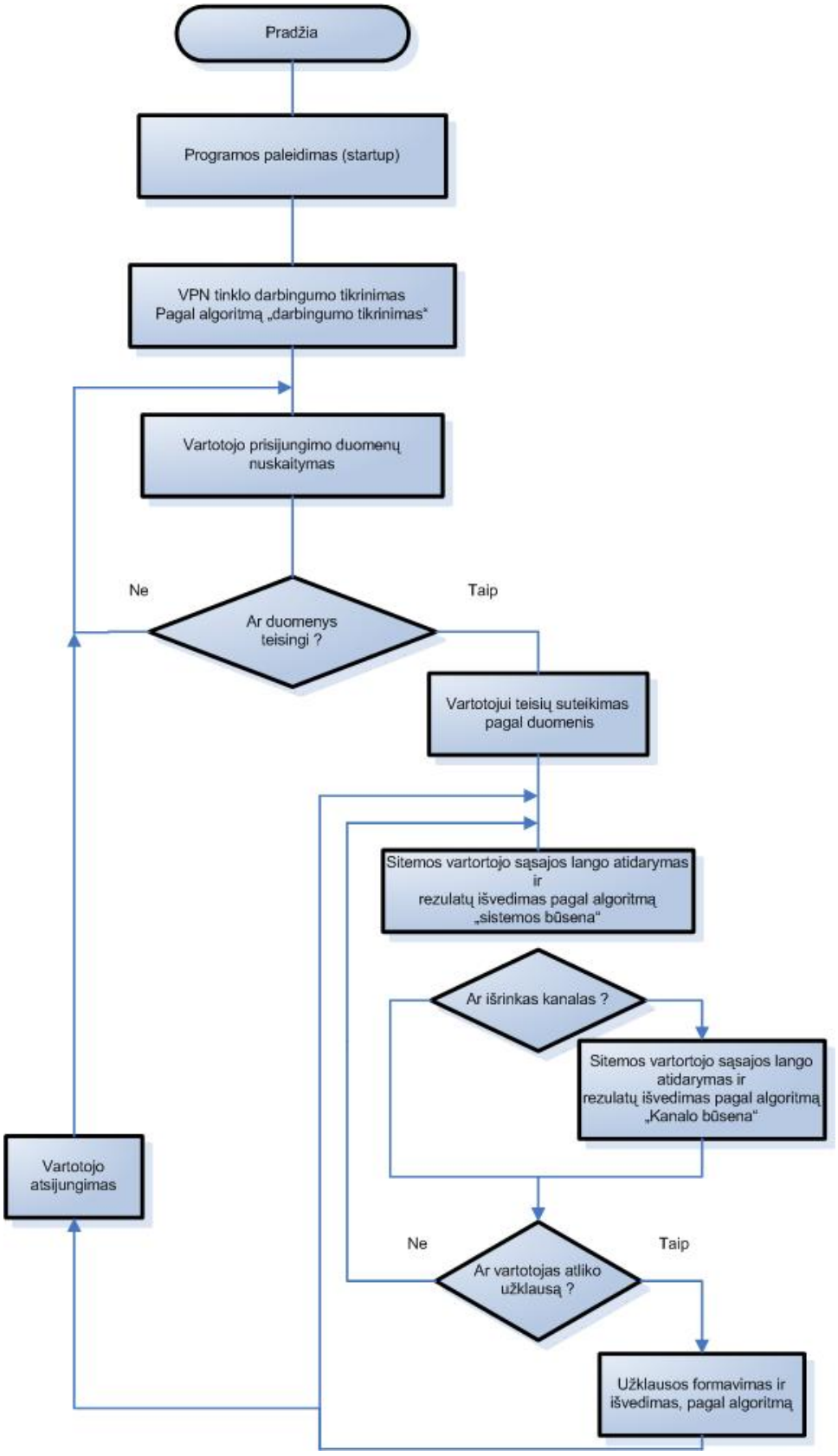
3.5.9. IDĖJOS IR SPRENDIMAI

Įtraukti į sistemą lokalių tinklų (LAN) darbingumo monitoringą.

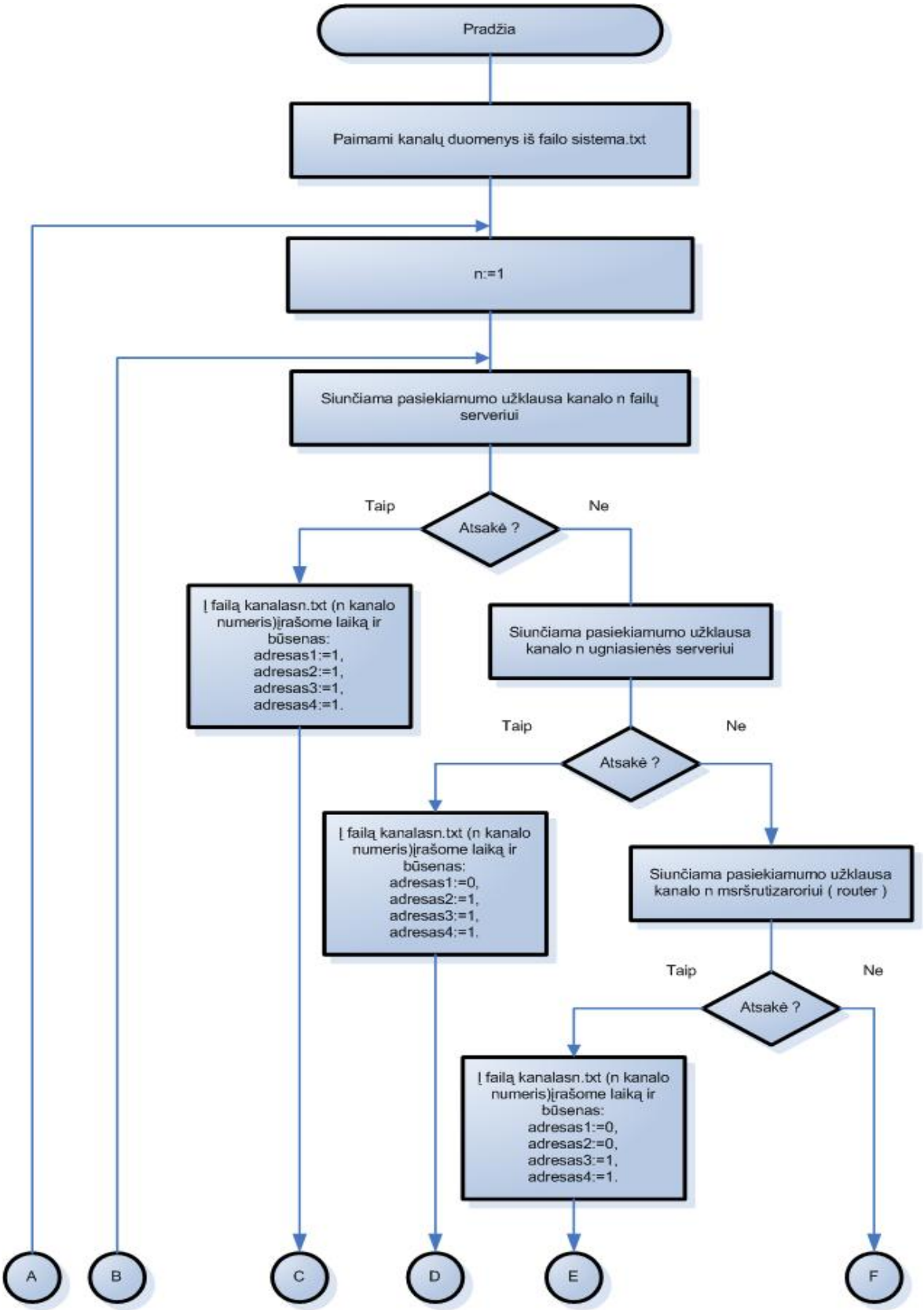
Galimi sistemos naudotojai：

1. Įstaigos, organizacijos ir verslo įmonės, turinčios centralizuotą struktūrą ;
2. Tinklo administratoriai, prižiūrintys ryšius su padalinių tinklais (LAN).

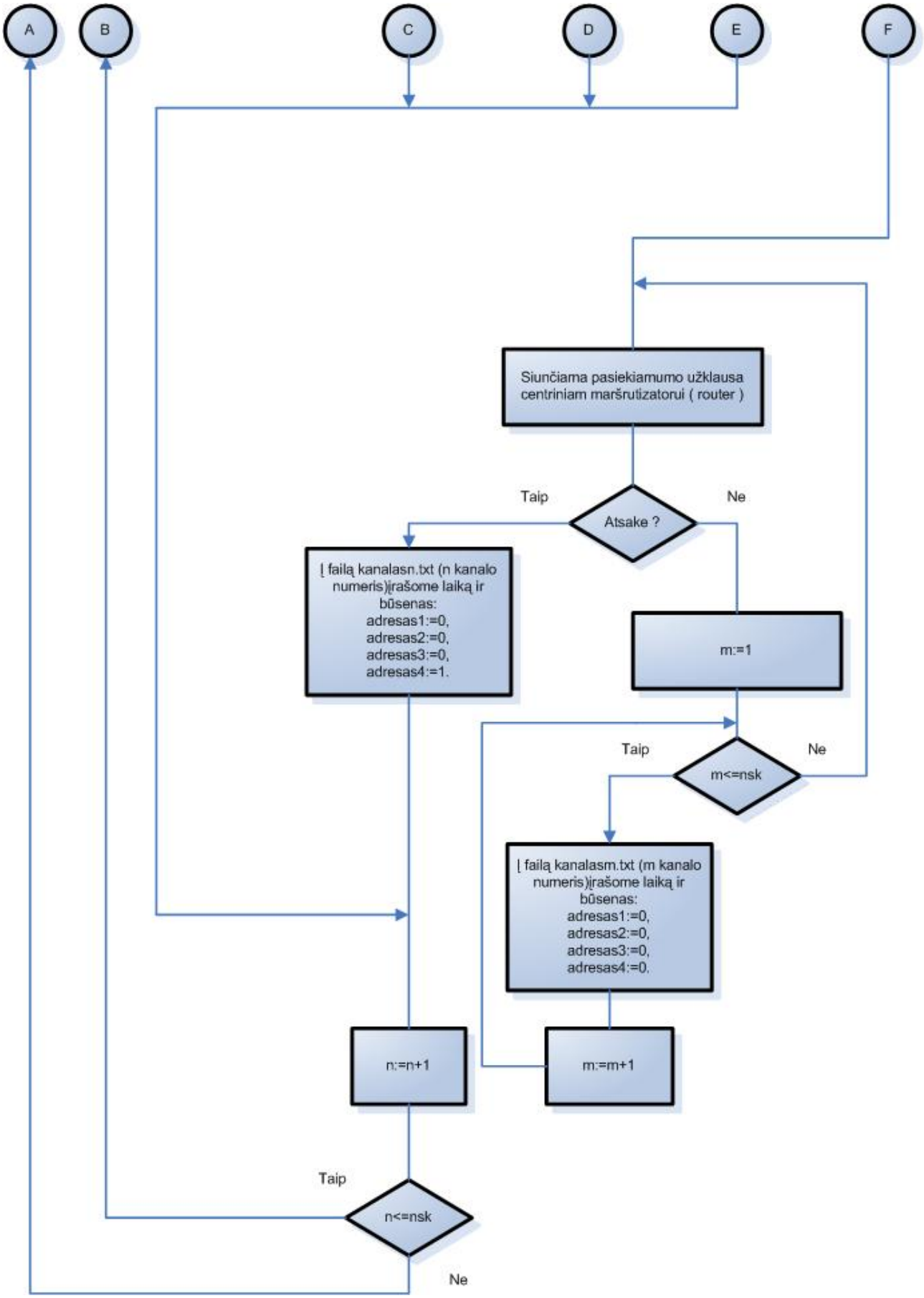
3.6. SISTEMOS VIEKIMO ALGORITMAS



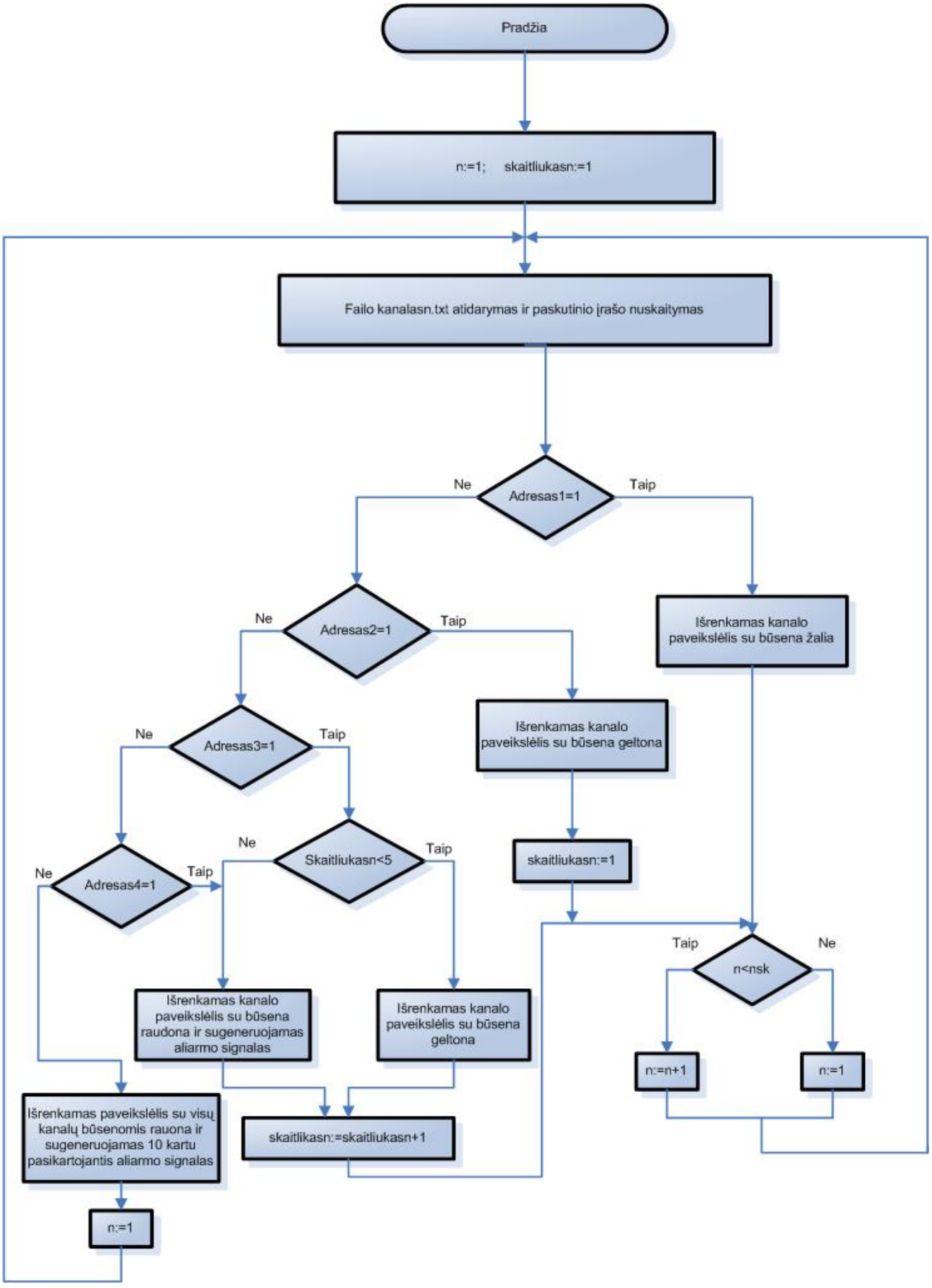
9 pav. VPN tinklo monitoringo sistemos veikimo algoritmas.



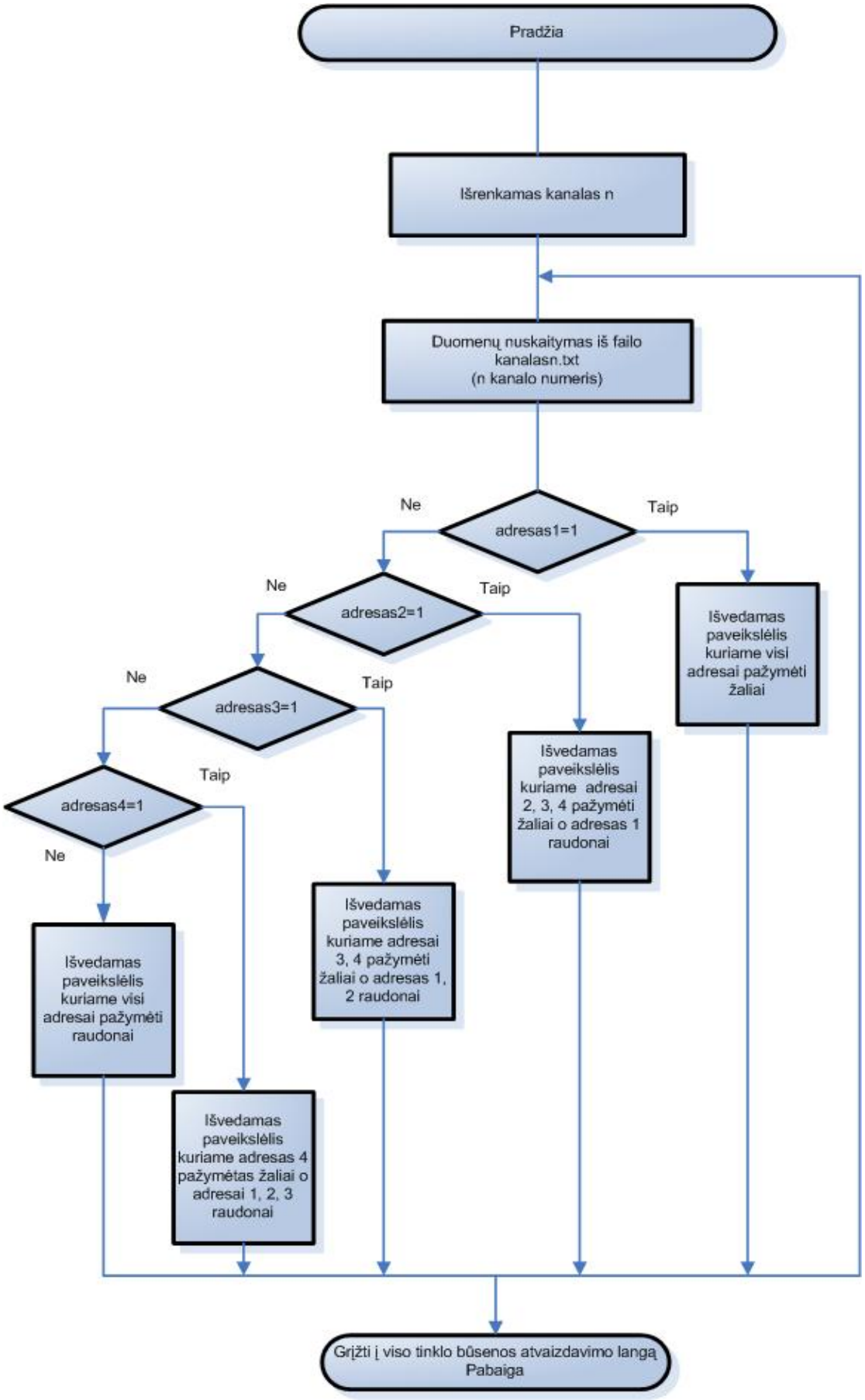
10 pav. Algoritmas „Darbingumo tikrinimas“.



11 pav. Algoritmo „darbingumo tikrinimas“ tęsinys.



12 pav. Algoritmas „sistemos būsena “.



13 pav. Algoritmas „kanalo būsena“.

4. SUKURTOS VPN TINKLO MONITORINGO SISTEMOS APŽVAGA

4.1. SUKURTOS SISTEMOS ANALIZĖ

Kaupiami parametrai:

1. Laikas;
2. Pasiekiamumo trukmė;
3. Pasiekiamumas;

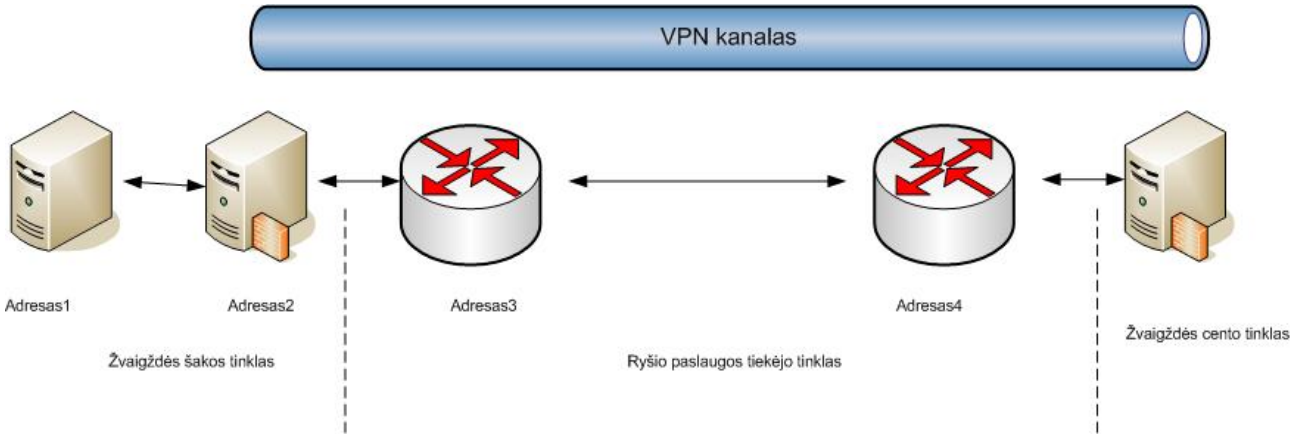
Užduodami parametrai:

1. Pasiekiamumo tikrinimo intervalas;
2. Tikrinamojo mazgo IP adresas;
3. Adresų grupavimas pagal kanalus;
4. Pasiekiamumo laukimo laikas (per kiek laiko turi gauti atsakymą);
5. Vartotojo informacija ir teisės;
6. Mazgo neatsakymo reikšmingumas;
7. Duomenų užklausa.

Išvedami parametrai:

1. VPN tinklo būsenos atvaizdavimas interaktyviame žemėlapyje;
2. Atskiro VPN kanalo darbingumo atvaizdavimas;
3. Aliarmo signalas (perspėjimui apie būsenos sutrikimą).

4.2. SUKURTOS VPN TINKLO MONITORINGO SISTEMOS VEIKIMO APRAŠYMAS



14 pav. Vieno VPN kanalo struktūra

Sukurta sistema tikrina, ar yra ryšys su serveriu už VPN kanalo. Sistemos, darbingumo tikrinimo algoritmą matome 10 ir 11 pav.

Sukurta sistema siunčia signalą VPN šakos failų serveriui, esančiam už ugniasienės 14 pav. (adresas1) , t.y. jį mes galime pasiekti tik tada, kai VPN tunelis veikia. Jeigu šis serveris atsako, sistema tai prima kaip tvarkingą VPN kanalo darbą. Tada ta sritis žemėlapyje dega žaliai (pavyzdys 6 priede (23 pav.)). Jei šis serveris neatsako, tai tikrinamas kelias iki VPN šakos potinklio ugniasienės (adresas2). Jei gaunamas atsakymas, tada sistema priima, kad kanalas gali būti, tik neveikti serveris, esantis už VPN. Tada to potinklio sritis žemėlapyje užsidega geltonai (6 priedas (24 pav.)). Jei neatsako potinklio ugniasienė, siunčiama užklausa VPN tinklo šakos maršrutizatoriui (adresas3). Jei šis atsako, tai potinklio sritis žemėlapyje užsidega geltonai, bet įsijungia skaitliukas, kuris skaičiuoja laiką. Jei tokia situacija tęsiasi daugiau kaip 5 minutes, potinklio sritis žemėlapyje užsidega raudonai (6 priedas (25 pav.)), ir sistema sugeneruoja garsinį signalą. Šis signalas indikuoja, kad sistemoje yra sutrikimas, kurį būtina pašalinti. Kai sulaukiamas atsakymas iš VPN šakos potinklio ugniasienės (adresas2), skaitiklio reikšmė grąžinama į pirminę padėtį.

Jei komutatorius 2 neatsako iš karto, potinklio sritis žemėlapyje užsidega raudonai (6 priedas (25 pav.)), ir sugeneruojamas garsinis signalas. Jei centrinis maršrutizatorius (adresas4) neatsako į užklausą, visas žemėlapis nusidažo raudonai, o sugeneruojamas garsinis signalas kartojamas 10 kartų. Kai sistema negauna atsakymo iš maršrutizatoriaus (adresas4), ji pereina į

būseną, kai nesiunčia užklausų kanalams, o tik nustatytais laiko tarpais siunčia užklausas centriniam maršrutizatoriui (adresas4). Tik gavusi atsakymą vėl atnaujina VPN tinklo kanalų apklausą pagal jau aprašytąjį mechanizmą.

Pasirinkus meniu Apskritys, jis išsiplečia, ir galime matyti pavadinimus. Pavadinimai parašyti lietuvių kalba, bet naudojantis lotyniškomis raidėmis (taip padaryta todėl, kad išvengti galimų pavadinimų iškraipymų). Apskritys meniu surašyti pagal abėcėlę (pirma Alytaus – paskutinė Utenos). Reikia paminėti, kad šį menių gali pamatyti tik Vartotojai 1 ir 2. Vartotojas 3, t.y. vadovas, šio meniu nemato. Pasirinkus apskritį žemėlapio vietoje atsiranda paveikslėlis, kuriame pavaizduoti kanalo mazgai. Mazgų išdėstymas rikiuojasi iš kairės į dešinę, t.y. VPN tinklo šakos filialo failų serveris, VPN tinklo šakos filialo ugniasienė, VPN tinklo šakos maršrutizatorius, centrinis maršrutizatorius. Šiame paveikslėlyje po kiekvienu mazgu, kuris neatsakė į užklausą, dega raudonas apskritimas (po kitais žali). Naudojamas aprašytasis VPN tinklo kanalo apklausos algoritmas. Laikoma, kad jeigu yra gautas atsakymas iš kairiau esančio mazgo, dešiniau esantys mazgai yra pasiekiami, ir jie „dega žaliai“.

Sukurta VPN tinklo monitoringo sistema turi būti paleidžiama automatiškai užsikrovus OS. (turi būti įtraukta į startup). Kitokiu atveju, jeigu sistemos paleidimą inicijuotų vartotojas, atsidarydamas stebėjimo langą, sistema negalėtų sukaupti duomenų apie VPN tinklo darbingumą, kai vartotojai nebuvo prisijungę.

Kuriamos sistemos duomenys saugomi atskiruose tekstinio formato failuose.

Vartotojų informacija saugoma faile vartotojai.txt (vartotojo vardas, slaptažodis, vartotojo numeris).

Kanalų darbingumo informacija saugoma failuose kanalasn.txt (laikas, žymė ar kanalas veikė (0 arba 1)), kur n kanalo numeris.

Užklausoms formuoti naudojami duomenys iš failo sistema.txt (kanalo numeris, VPN tinklo šakos failų serverio IP, VPN tinklo šakos ugniasienės IP, VPN tinklo šakos maršrutizatoriaus IP, centrinio maršrutizatoriaus IP).

Ataskaitos laikinai talpinamos į failą ataskaitos.txt (paprastai laikomas tuščias ir duomenys būna tik tada kai pateikiama užklausa)

Visuose failuose duomenim atskirti naudojami trys tarpo simboliai.

4.3. SUKURTOS VPN TINKLO MONITORINGO SISTEMOS PRIVALUMAI IR TŪKUMAI

Trumpas sistemos apibūdinimas: paprasta sistema tiek vartojimui tiek stebėsenai.

Sistemos privalumai:

1. Parasta vartotojo sąsaja;
2. Lengva stebėsena, nes visų objektų būsenos aiškiai matosi teritoriniame žemėlapyje (apskritis, kurioje yra sutrikimas pakeičia spalvą);
3. Keleto lygių vartotojų prisijungimo galimybė;
4. Sistemos vartotojui nereikia turėti IP adresų (reikalingi tik vartotojui 1 įvedimo momentu);
5. Sistemos administratorius mato detalesnį meniu, kuriame galima pasirinkti problemišką apskritį, matyti būsenas iki kanalo objektų ir taip susidaryti pilnesnį vaizdą apie surikusio ryšio priežastį (vaizdavimas tai pat yra spalvinis);
6. Ja galima naudotis neprisijungus prie serverio, užtenka turėti nuorodą ir internetinę naršyklę;
7. Sistemos darbas lengvai suprantamas;
8. Sistema duomenis eksportuoja į *.txt failus, ir tai leidžia juos nesunkia eksportuoti į kitas programas;
9. Duomenys apie būsenas į failą rašomi automatiškai;
10. Sistema generuoja aliarmo signalą (garsinį signalą).

Sistemos trūkumai:

1. Silpnas sistemos dizainas;
2. Nedaug atliekamų funkcijų.

5. IŠVADOS

1. Šiame darbe apžvelgėme tinklų monitoringui naudojamus protokolus ir duomenų nuskaitymo modelius. Pasirinkome agento-menedžerio modelį.
2. Sukurta sistema leidžia stebėti VPN tinklo darbingumą esamuoju laiku ir kaupia duomenis analizei.
3. Sistema sukurta Java programavimo kalba. Tai leis šią sistemą panaudoti bet kurioje OS.
4. Sistema turi autorizuotą prisijungimą ir pagal jį suteikiamas vartotojų teises sistemoje, todėl vartotojas nemato jam neaktualios informacijos.
5. Duomenų saugojimo failų formatas (*.txt) leidžia patogų duomenų eksportavimą į kitas analizavimui skirtas sistemas.
6. Sukurtos sistemos veikimo algoritmas išskaidytas į keletą paprastesnių algoritmų, lengvesniam sistemos veikimo supratimui.
7. Sukurtos sistemos trūkumai nėra esminiai sistemos darbui.
8. Sistemą galima pritaikyti VPN tinkluose, turinčiuose žvaigždinę struktūrą.

6. LITERATŪRA

1. DEVEIKIS, A. Objektinis programavimas Java kalba. Kaunas, 2008.

2. MORKŪNIENĖ, A. Grafinių dokumentų rengimas su MS VISIO. Vilnius, 2004.

3. PLĖŠTYS, R.; KAVALIŪNAS, R.; VILUTIS, G.; LAGZDINYTĖ, I.; LIUTKAUSKAS, V. Kompiuterių tinklai. Kaunas technologija, 2008.

4. RIŠKUS, A. Programavimas Java. Pirmoji pažintis. Kaunas, 2006.

5. БИГЕЛОУ, С.Дж. Сети: поиск неисправнотей, поддержка и восстановление. Санкт-Петербург, 2005.

6 . ДЭВИС, Дж.; ЛИ, Т. Microsoft Windows Server 2003. Протоколы и службы TCP/IP. Москва, 2005.

7 . ДЭВИС, Дж.; ЛЬЮИС, Э. Создание виртуальных частных сетей в Microsoft Windows Server 2003. Москва, 2006.

8 . ШИНДЕР, Т.В.; ШИНДЕР, Д.Л. ISA Server 2004. В подлиннике. Санкт-Петербург, 2006.

9. http://rk.vgtu.lt/II_semestras/Paskaitu_medziaga/Tema_11_Komp_tinklai.pps

10. http://otndnld.oracle.co.jp/document/products/tuxedo/tux91/snmpmref/1tmib.htm

11. http://commons.wikimedia.org/wiki/File:SNMP.MIB-Tree.PNG

12 . http://www.javvin.com/protocolRMON.html

13. http://technet.microsoft.com/en-us/library/cc723469.aspx

14 http://www.tools4ever.com/products/free/freeping

15. http://www.softlist.net/products/freeware_ping.html

16. http://www.pingtester.net/

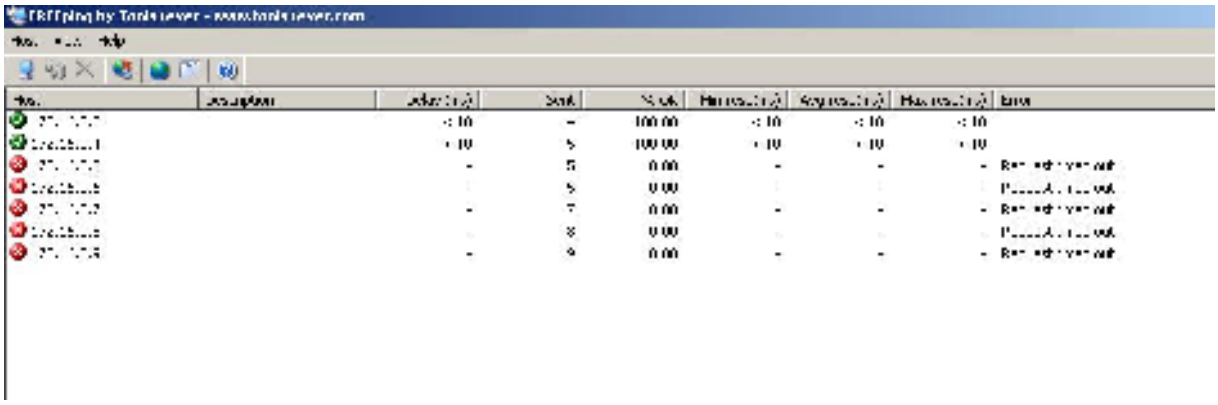
7. TERMINŲ ŽODYNAS

- **VPN –** Virtualus lokalaus ryšio kanalas (Virtual Personal Network);
- **LAN –** vietinis kompiuterinis tinklas (Local Area Network);
- **WAN –** Pasaulinis kompiuterių tinklas (Wide Area Network);
- **JVM –** Javos virtuali mašina (Java Virtual Machine);
- **Web-** gaunamų duomenų sąsaja naudojant internetą;
- **OID-**objekto indentifikatorius;
- **SNMP-**Paprastasis tinklo valdymo protokolas
- **IS-**sutrumpintas kuriamos sistemos pavadinimas;
- **OS-** Operacinė sistema (sutrumpinimas);
- **Windows server 2003-**pagridinė naudojamų serverių OS kuriuos aplinkoje diegiamos visos kitos
- **Microsoft SQL server**- duomenų bazių serveris;
- **Windows ISA server 2004-**ugniasienės serveris kuriame ir sukuriami VPN kanalai ir atsakingas už VPN kanalu saugų darbą.

8. PRIEDAI

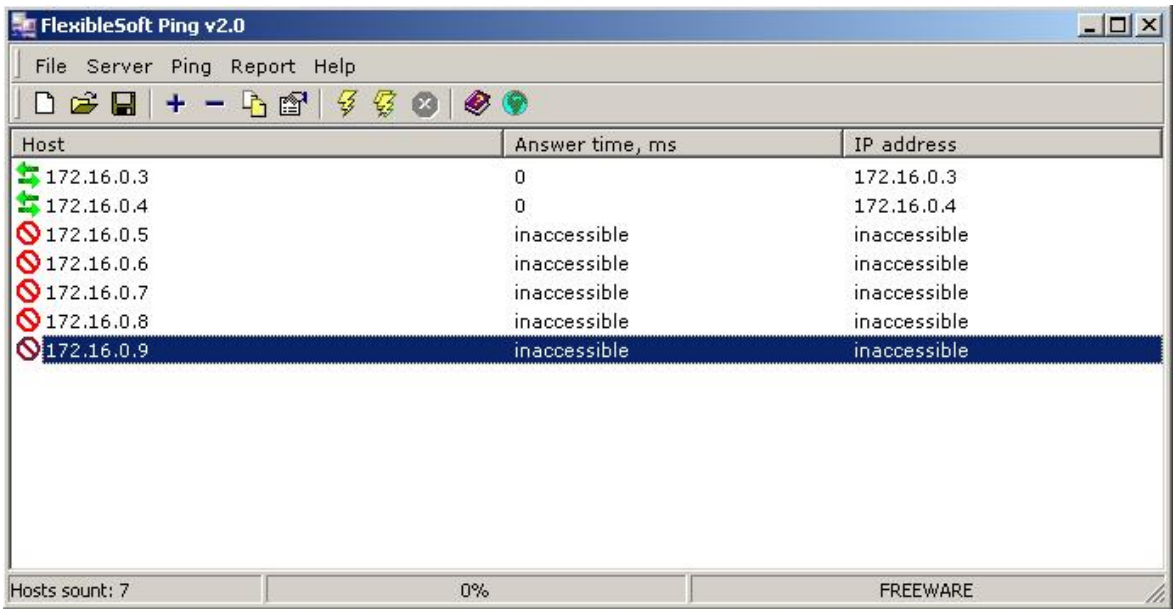
1 priedas

8.1. SISTEMOS „FREEping“ VARTOTOJO SĄSAJOS LANGAS

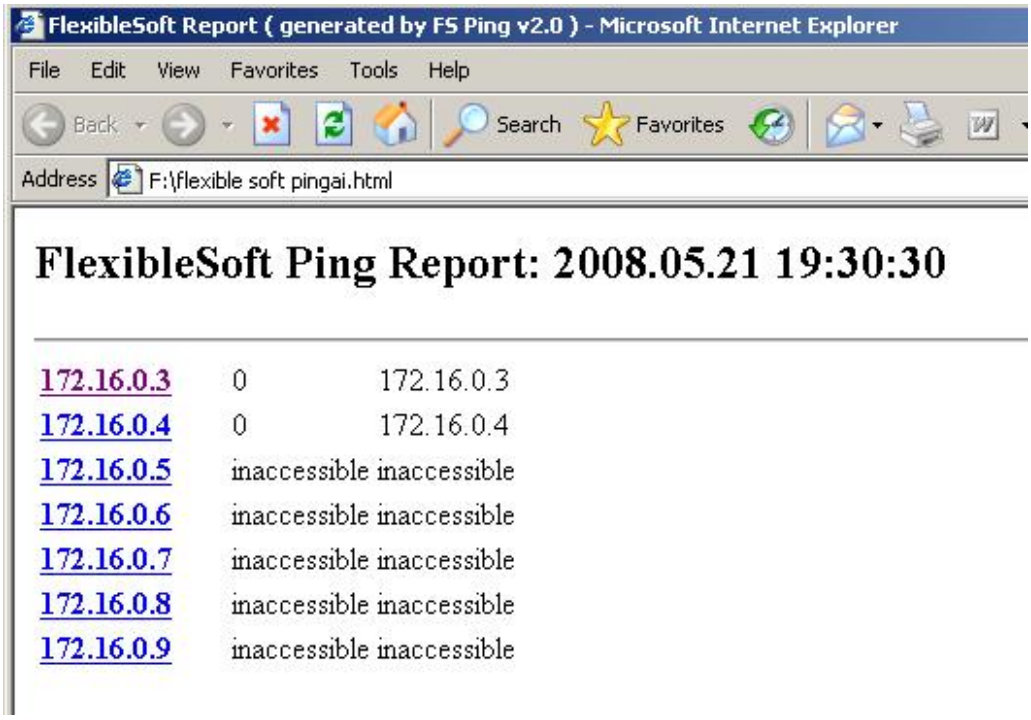


15 pav.Sistemos „FREEping“ vartojo sąsajos langas.

8.2. SISTEMOS „FlexibleSoft Ping v2.0“ VARTOTOJO SĄSAJOS DARBO LANGAI

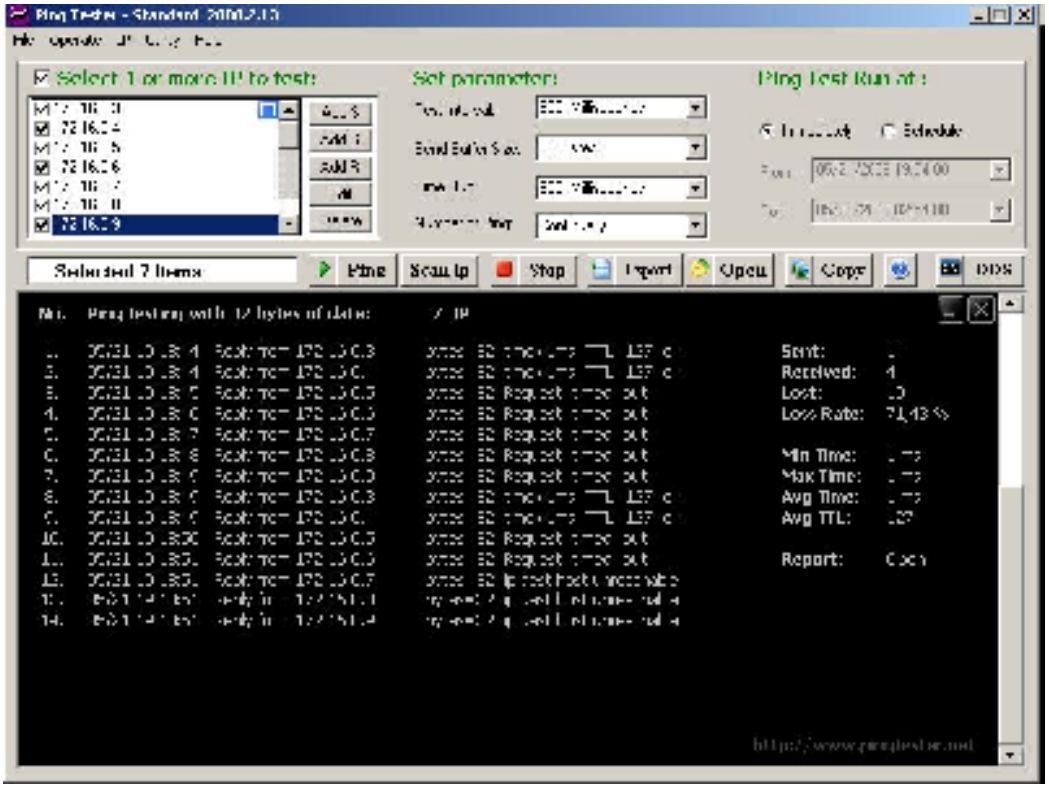


16 pav. Sistemos „FlexibleSoft Ping v2.0“ vartotojo sąsajos darbo langas.

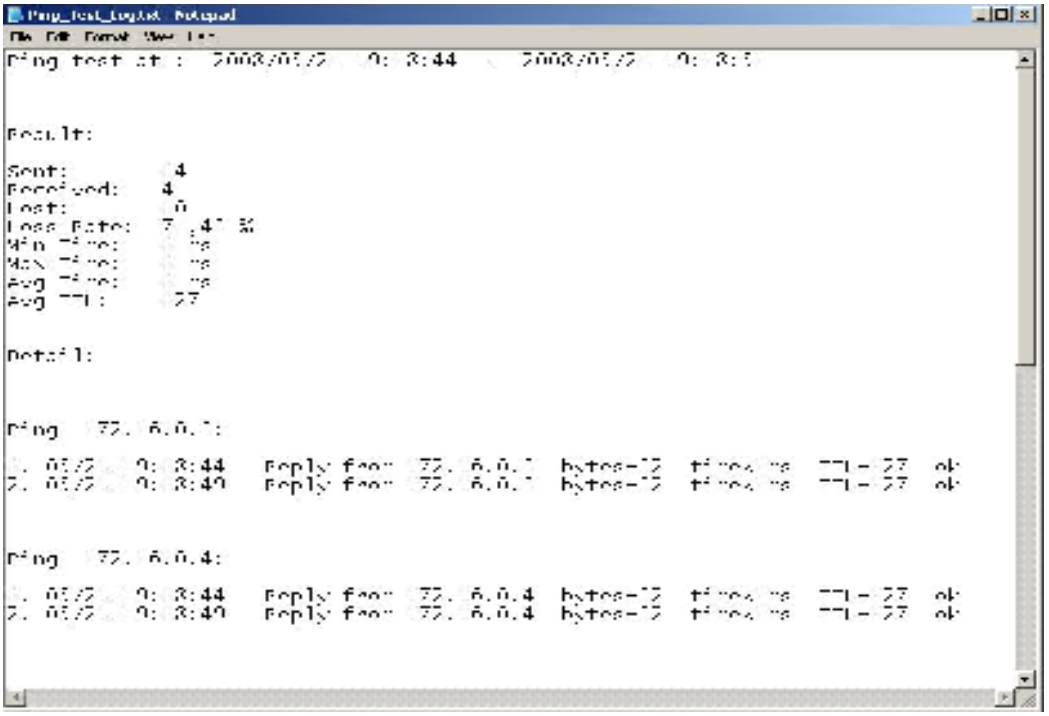


17 pav. Sistemos FlexibleSoft Ping v2.0“ galimų užsaugotų duomenų langas.

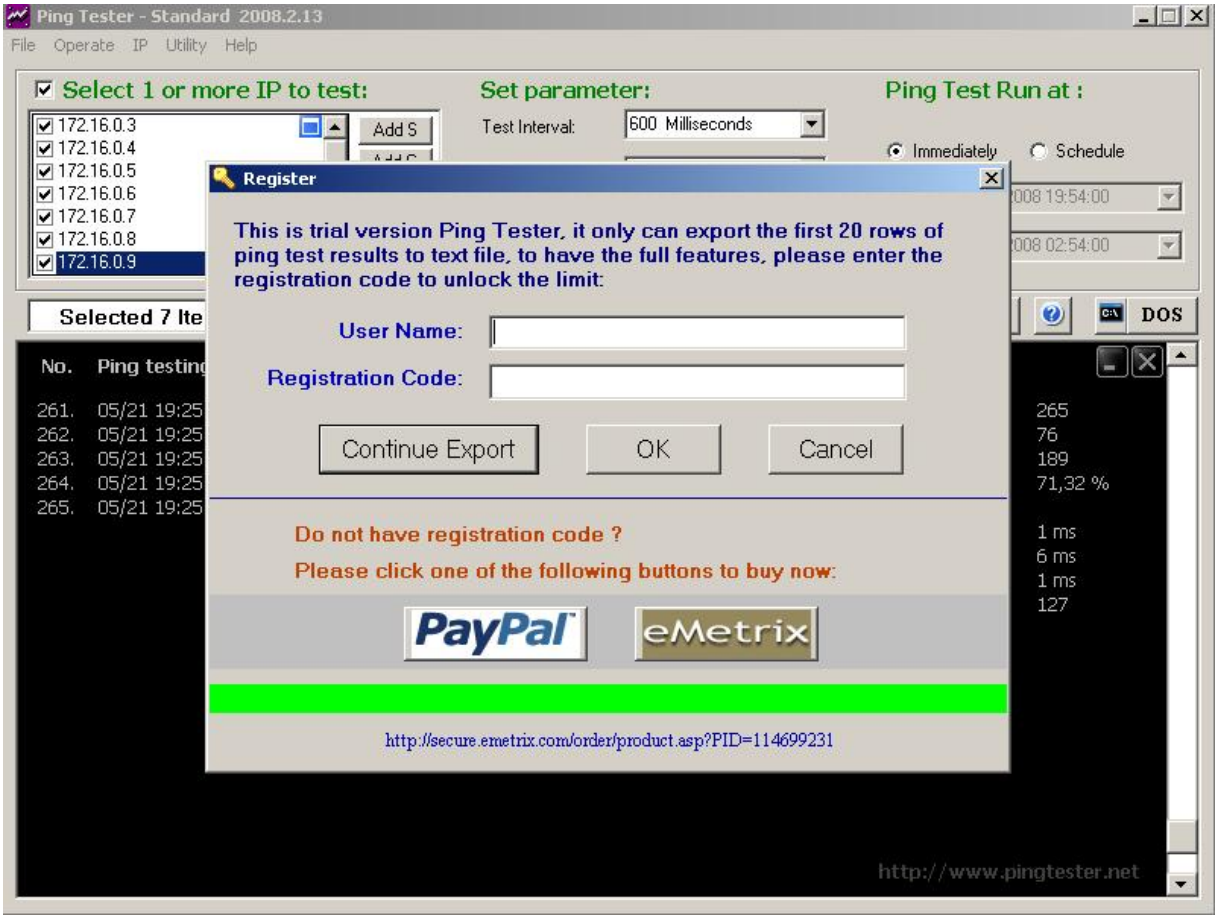
8.3. SISTEMOS „Ping Tester“ VARTOTOJO SĄSAJOS DARBO LANGAI



18 pav. Sistemos „Ping Tester“ vartotojo sąsajos darbo langas.

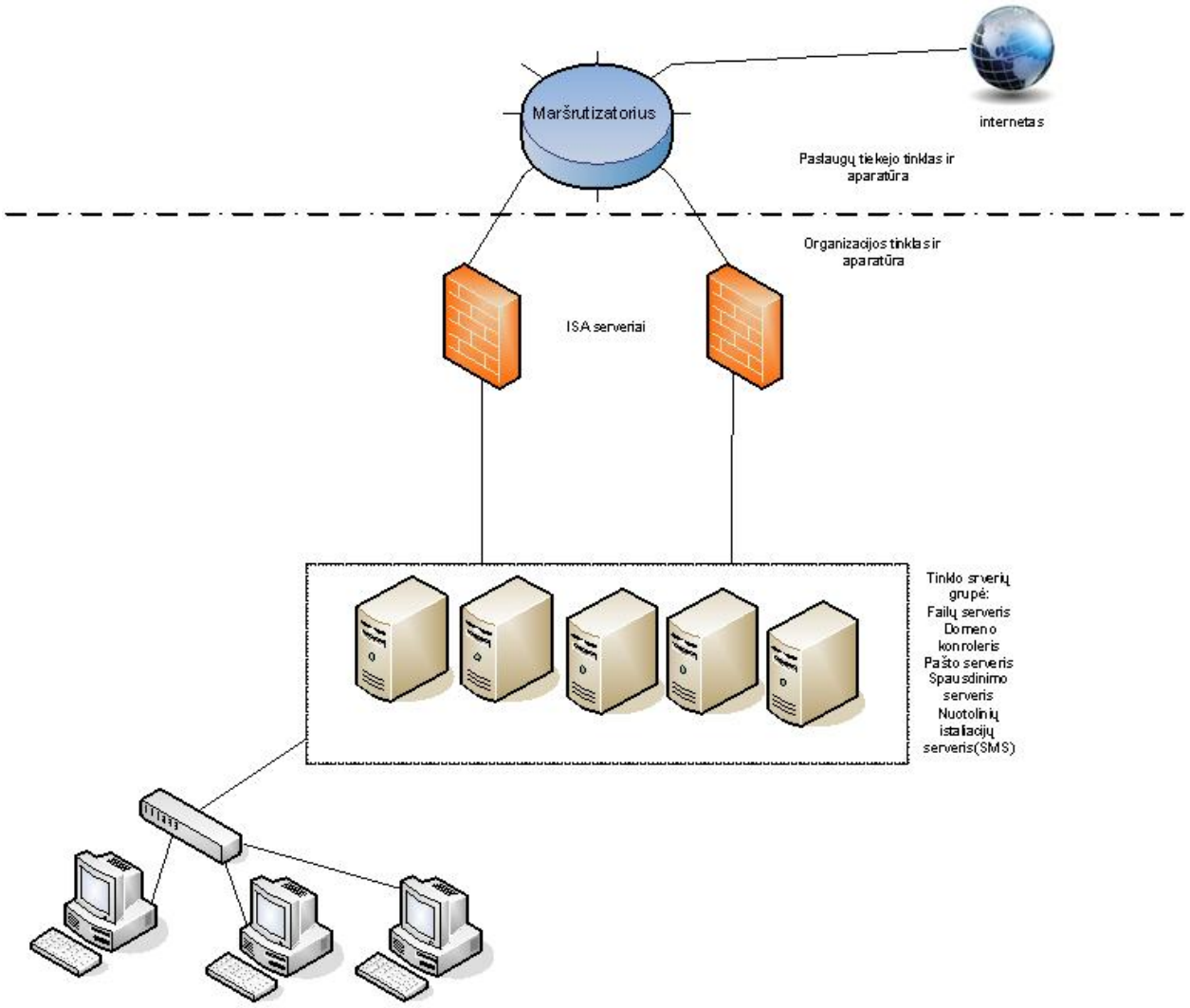


19 pav. Sistemos „Ping Tester“ duomenų failo, kuriame užsaugomi programos duomenys, pavyzdys.



20 pav. Sistema „Ping Tester“ didesniam įrašų kiekiui užsaugoti jau tampa mokama.

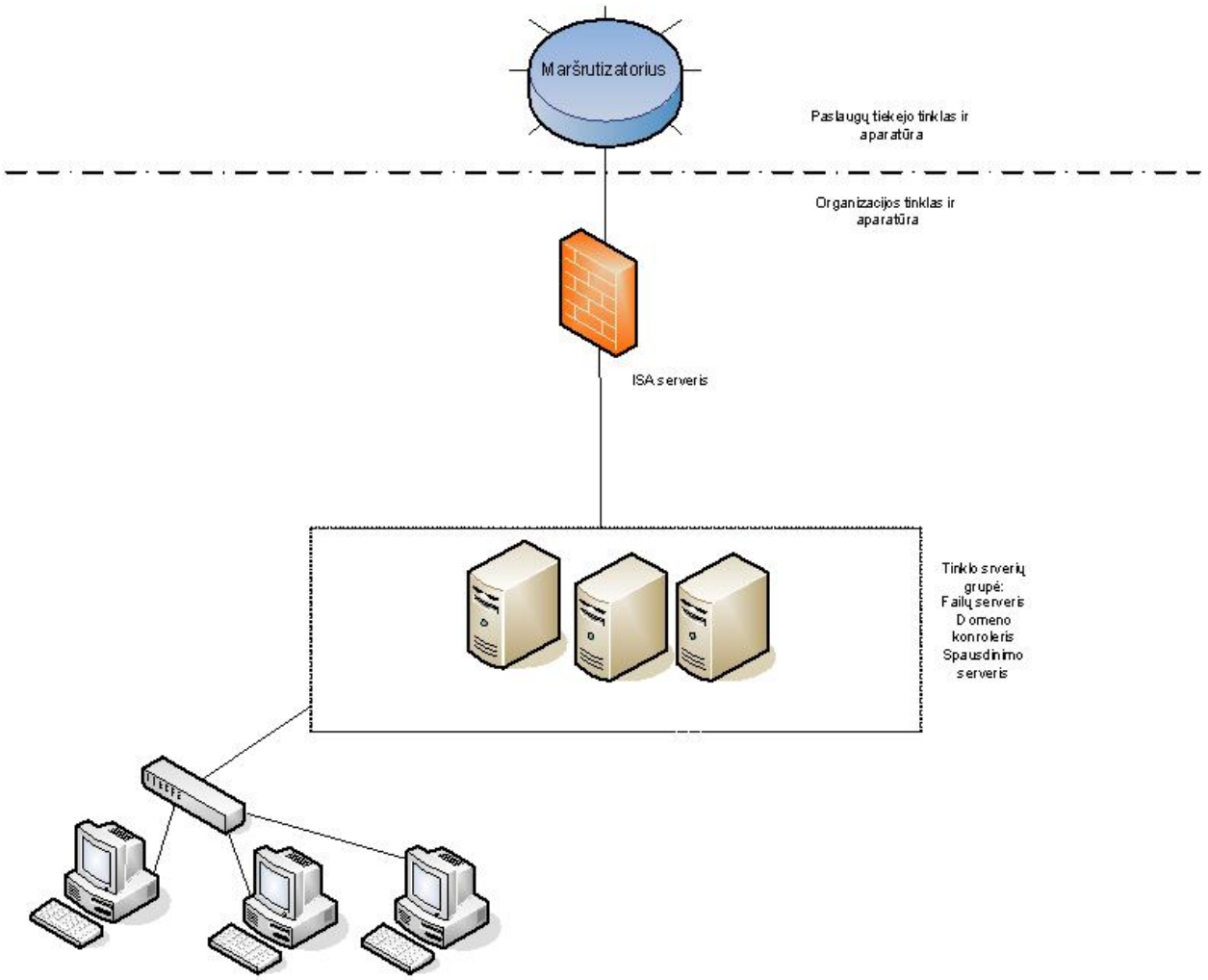
8.4. ŽVAIGŽDĖS CENTRO KOMPIUTERINIO TINKLO ARCHITEKTŪRA



21 pav. Žvaigždės centro kompiuterinio tinklo architektūra.

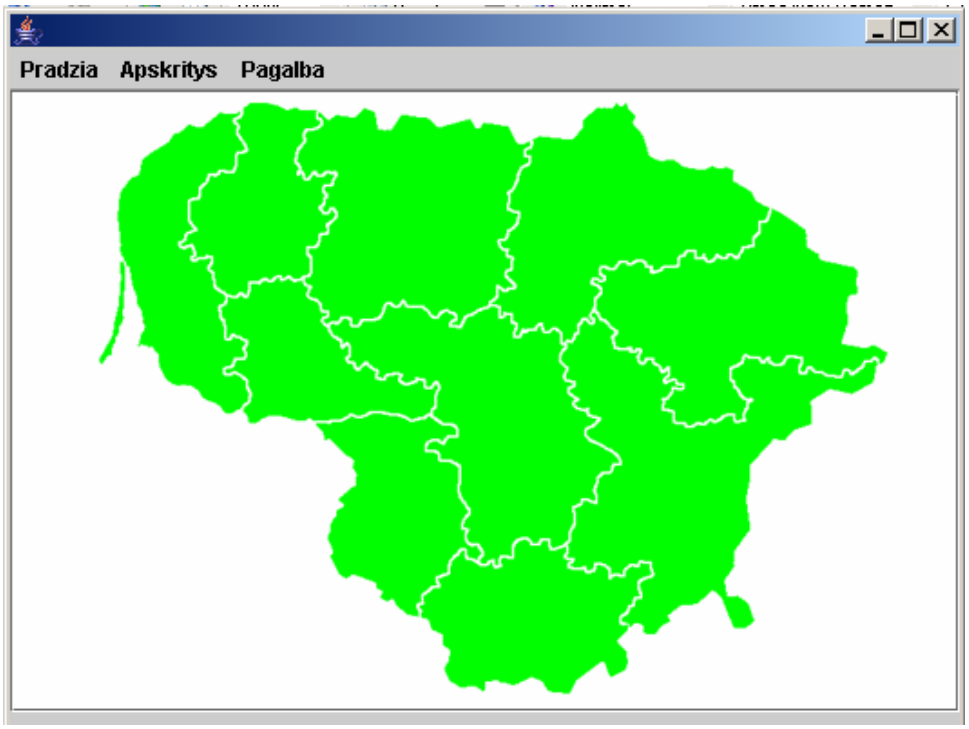
5 priedas

8.5. PADALINIŲ, ESANČIŲ ŽVAIGŽDĖS NUTOLUSIUOSE MAZGUOSE, KOMPIUTERINIO TINKLO STRUKTŪRA

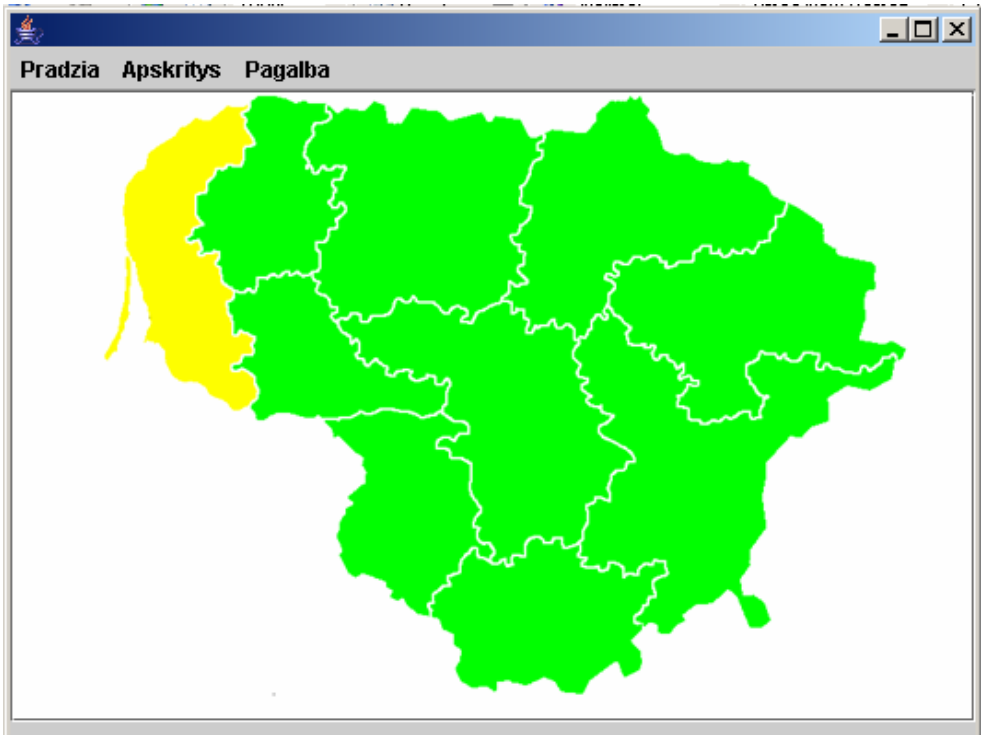


22 pav. Padalinių, esančių žvaigždės nutolusiuose mazguose, kompiuterinio tinklo struktūra.

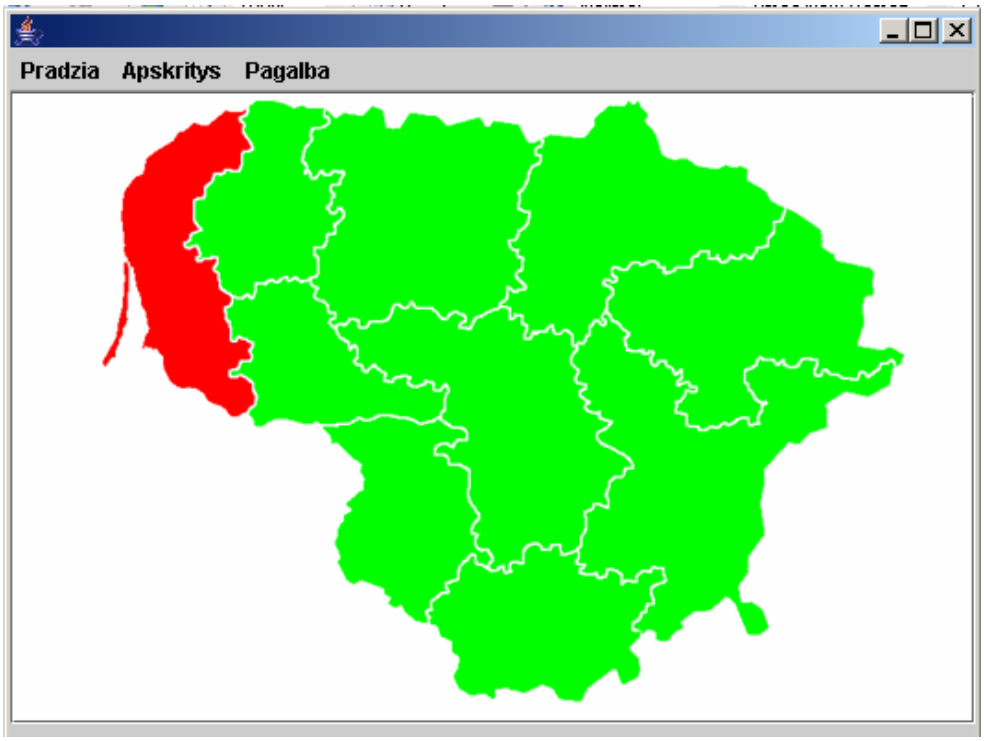
8.6. VPN TINKLO MONITORINGO SISTEMOS VARTOTOJO SĄSAJOS DARBO LANGAI



23 pav. VPN tinklo monitoringo sistemos vartotojo sąsajos darbo langas, kai VPN tinklas veikia normaliai.



24 pav. VPN tinklo monitoringo sistemos vartotojo sąsajos darbo langas, kai yra trumpalaikis sutrikimas VPN kanale.



25 pav. VPN tinklo monitoringo sistemos vartotojo sąsajos darbo langas, kai yra sutrikimas VPN kanale.