

## 27. Atvirųjų sistemų sujungimo modelis

Sujungus kompiuterius vieni protokolai sudaro sąlygas veikti kitiems protokolams.<sup>65</sup> Tokiai sudėtingai sistemai aprašyti sukurtas *OSI* modelis (angl. *Open Systems Interconnection Reference Model*)<sup>66</sup>. Tai abstraktus ryšio protokolų, naudojamų tinkluose, aprašas.

*OSI* modelis aprašo septynis lygmenis (angl. *layer*) – funkcijų, naudojamų protokoluose, grupes (27.1 pav.). Kiekvienas lygmuo naudojami žemesnio lygmens paslaugomis ir teikia paslaugas aukščiau esančiam lygmeniui. Tradiciškai pirmasis lygmuo yra vaizduojamas apačioje. Todėl ir lygmenų sąrašas dažnai pradedamas nuo septintojo – aukščiausiojo.

Application	Application layer protocol	Application	<b>Upper Layers</b>
Presentation		Presentation	
Session		Session	
Transport	Communication layer protocol	Transport	<b>Middle Layers</b>
Network		Network	
Data Link	Physical topology	Data Link	<b>Lower Layers</b>
Physical		Physical	

27.1 pav. *OSI* lygmenų klasifikacija

Kadangi sąveika vyksta tik tarp gretimų *OSI* lygmenų, tai gerokai supaprastina sudėtingų komunikacijos sistemų kūrimą ir

<sup>65</sup> [http://en.wikibooks.org/wiki/Telecommunications\\_and\\_Network\\_Security](http://en.wikibooks.org/wiki/Telecommunications_and_Network_Security)

<sup>66</sup> [http://en.wikipedia.org/wiki/OSI\\_model](http://en.wikipedia.org/wiki/OSI_model)

aprašymą. Kompiuterių tinklų specialistas privalo labai gerai išmanyti savo lygmenį ir neblogai žinoti, kas vyksta gretimuose lygmenyse. Tolimesniais lygmenimis galima nesidomėti, daugiau laiko skirti savo lygmens problemų ir galimybių analizei.

VII lygmuo – taikomųjų programų lygmuo (angl. *Application layer*) – aukščiausiasis lygmuo, nustato tinklo teikiamas paslaugas vartotojo programoms. Pavyzdžiui: *SSH, telnet, FTP, IRC, echo, VNRP, HTTP, NFS, RTSP, SIP, SMTP, POP3, SNMP, whois, XMPP*.

VI lygmuo – duomenų pateikimo lygmuo (angl. *Presentation layer*) – nustato duomenų kodavimo per sesiją taisykles. Pavyzdžiui: *MIME, XDR, ASN.1, SMB, AFP, NCP*.

V lygmuo – seansų lygmuo (angl. *Session layer*) – aprašo duomenų apsikeitimo tarp galinių sistemų taisykles. Pavyzdžiui: *ASAP, TLS, SSL, ISO 8327 / CCITT X.225, RPC, NetBIOS*.

IV lygmuo – transporto lygmuo (angl. *Transport layer*) – užtikrina skaidrų duomenų perdavimą tarp tinklo vartotojų ir suteikia norimas patikimumo garantijas. Pavyzdžiui: *TCP, UDP, RTP, SCTP, SPX, ATP, IL*.

III lygmuo – tinklo lygmuo (angl. *Network layer*) – aprašo, kaip duomenų sekos turi būti adresuojamos ir perduodamos visame tinkle. Pavyzdžiui: *IP, ICMP, IGMP, IPX, OSPF, RIP, IGRP, EIGRP, ARP, RARP, X.25*.

II lygmuo – ryšio lygmuo (angl. *Data link layer*) – aprašo ryšį tarp gretimų (tiesiogiai sąveikaujančių) tinklo komponentų, Pavyzdžiui, kadrų struktūrą. Pagrindinė funkcija – atskirti bitų sekas, jų pradžią, pabaigą. Pavyzdžiui: *Ethernet, Token ring, HDLC, Frame relay, ISDN, ATM, 802.11 (WiFi), FDDI, PPP, PPPeE*.

I lygmuo – fizinis lygmuo (angl. *Physical layer*) – aprašo fizinius perduodamo signalo ir terpės, kuria jis perduodamas, parametrus (dažnius, moduliacijas, reikalavimus kabeliams, jungtims, duomenų ir fizinio signalo virsmus). Pagrindinė jo funkcija – atskirti 0 ir 1. Pavyzdžiui: *10BASE-T, 100BASE-T, 1000BASE-T, SONET/SDH, G.709, 802.11*, kabeliai ir kita fizinė tinklo įranga.

### 27.1. Kompiuterių sujungimas vietiniame tinkle

**I ir II lygmuo pagal OSI.** Internetas nėra vienas taškas, prie kurio būtų jungiami kompiuteriai. Internetas yra tarpusavyje sujungtų kompiuterių tinklų visuma. Kompiuteris visų pirma jungiamas prie vietinio tinklo (*LAN, local area network*). Būtent tokį prisijungimą užtikrina žemiausi *OSI* hierarchijos lygmenys. Fizinį tinko sujungimą aprašantys standartai leidžia kiekvienam pagaminti įrenginį, kuris galėtų būti prijungtas prie tinklo.

Prisijungimo standartų naudą iliustruoja mobiliųjų telefonų istorija. Kiekvienas *GSM* telefonų gamintojas kūrė kroviklių ir išorinių ausinių jungtis. Vartotojas, įsigijęs naują telefono aparatą, nebegali panaudoti įrangos, kuri buvo pritaikyta kitam telefonui. Vartotojai įvertino standarto naudą, kai pradėtos gaminti ausinės ir telefonai, palaikantys *Bluetooth* standartą.

### 27.2. Kompiuterių sąveika tinkle

*TCP/IP* – populiariausia sudėtinių tinklų organizavimo priemonė. Pagrindinis tinklo lygmens protokolas yra *IP* protokolas (*Internet Protocol*). Jis buvo kurtas paketiniams duomenims perduoti sudėtiniais tinklais, kuriuos sudaro daug vietinių tinklų, susijusių vietiniais ir globaliais ryšiais. Todėl *IP* protokolas gerai veikia sudėtingos topologijos tinkluose, racionaliai išnaudoja jų posistemes ir ekonomiškai išnaudoja lėtų ryšio linijų pralaidumo gebą.

*TCP/IP* naudojami trijų tipų adresai: *MAC* (vietinis, aparatinis), *IP* adresas ir simbolinis vardas.

### 27.3. Kompiuterių fiziniai adresai

**II lygmuo pagal OSI.** Jei tinklas yra nedidelis ir paprastas, tada paprasčiausia yra naudotis kompiuterių *MAC* adresais. Tokį unikalų adresą kiekvienam įrenginiui suteikia gamintojas. Šis adresas nenurodo, kur kompiuteris yra prijungtas. Nedideliame tinkle visi kompiuteriai ar kiti įrenginiai „girdi“ vienas kitą bei pagal nurodytą *MAC* adresą kiekvienas iš jų atsirenka sau skirtus

duomenų paketus. Tai analogiška atvejui, kai kambaryje vienas žmogus vardu kreipiasi į kitą girdint ir aplinkiniams, esantiems kambaryje. Ryšys užtikrinamas tik tada, jei kalbama po vieną. Plečiant tokį tinklą kompiuteriai ima vienas kitam trukdyti. Tai yra viena iš priežasčių, kodėl tinklas turėtų būti skaidomas į potinklius, o paketai perduodami tik tam tinklui, kuriam skirti. Kita priežastis – ryšio kanalų apkrovos valdymas.

#### 27.4. Kiekvienas kompiuteris tinkle turi *IP* adresą

**III lygmuo pagal OSI.** Minėtas problemas sprendžia *IP* (internetu protokolus). Jis kiekvienam įrenginiui suteikia *IP* adresą (numerį), susidedantį iš tinklo adreso ir kompiuterio adreso tame tinkle. *IP* adresą sudaro 4 baitai, paprastai užrašomos jų dešimtainės reikšmės be tarpų, atskirtos taškais. Pavyzdžiui, „192.0.2.119“. Ši adresų sistema vadinama *IPv4*. Toks *IP* adresas yra 32 bitų seka. Konfigūruojant kompiuterius ir kitus įrenginius nustatomi jų *IP* adresai.

Prenkant *IP* adresus turėtų būti atsižvelgiama į kai kuriuos apribojimus. Mazgo adrese neturėtų būti skaičių, kurie dvejetainėje sistemoje atvaizduojami tik nuliais (00000000) arba tik vienetais (11111111). Tai – rezervuotos reikšmės: nulis (00000000) išreiškia esamo tinklo numerį, o 255 (11111111) naudojamas transliavimo pranešimui siųsti, todėl adresuoti praktiškai galima ne 256 mazgus, o  $256 - 2 = 254$ . Tinklo maršrutizatoriui, per kurį tinklo įrenginiai jungiasi prie kitų tinklų, dažnai suteikiamas pirmasis tinklo adresas.

Atskirai nurodoma, kokia *IP* adreso dalis yra tinklo numeris, likusi dalis yra mazgo numeris. Yra trys būdai tai nurodyti. Gali būti nurodoma tinklo klasė, tinklo numeriui skiriamų bitų skaičius arba *IP* adreso kaukė (*netmask*).

*RFC1466* aprašo tinklo skirstymą į A, B ir C klases pagal pirmuosius bitus<sup>67</sup> (27.1 lentelė), o jį pakeitęs *RFC2050* daugiau

<sup>67</sup> <http://tools.ietf.org/html/rfc1466>

dėmesio skiria taupiam *IPv4* adresų paskirstymui, reikalingam dėl jau juntamo adresų trūkumo<sup>68</sup>.

27.1 lentelė. *IP* tinklų tipai

Tinklo klasė	A	B	C
Pirmieji bitai	0...	10...	110...
Pirmasis baitas	0 – 127	128 – 191	192 – 223
Tinklo adreso ilgis	8 bitai	16 bitų	24 bitai
Kaukė	255.0.0.0	255.255.0.0	255.255.255.0
Vieno tinklo dydis	16 777 214	65 534	254

Gali būti ir kitaip paskirstomi *IP* adreso bitai. Pavyzdžiui, tinklas mažesnis už C klasės tinklą, turintis iki 32 unikalių *IP* adresų: tinklo numeris kartu su nurodytu tinklo dydžiu – 192.0.2.0/27, to tinklo kaukė – 255.255.255.224, vienas iš tokio tinklo *IP* adresų – 192.0.2.11, šio tinklo paskutinis adresas 192.0.2.31.

### 27.5. Specialios *IP* adresų grupės

Ne visada kiekvienam kompiuteriui tinkle suteikiamas unikalus visame internete *IP* numeris. *RFC1918* aprašo vietiniams tinklams rezervuotas adresų grupes ir jų naudojimo principus<sup>69</sup> (27.2 lentelė). Įrenginys, turintis tinklo vidinį adresą, gali jungtis prie kitų interneto resursų ir būti prieinamas iš interneto per maršrutizatorių, užsiimančią adresų nurodymu tinkle. Ši funkcija vadinama *NAT (Network adress translation)*.

<sup>68</sup> <http://tools.ietf.org/html/rfc2050>

<sup>69</sup> <http://tools.ietf.org/html/rfc1918>

27.2 lentelė. Vidinių adresų grupės

Adresų diapazonas	Tinklų klasė ir skaičius	Tinklo pavyzdys
10.0.0.0–10.255.255.255	Vienas A klasės tinklas	10.0.0.0/8
172.16.0.0–172.31.255.255	16 B klasės tinklų	172.22.0.0/16
192.168.0.0– 192.168.255.255	256 C klasės tinklai	192.168.222.0/24

Vidinių adresų naudojimas leidžia sumažinti reikalingų unikalų *IP* numerių skaičių ir palengvina bei atpigina tinklų kūrimą, nes vidiniai adresai naudojami nemokamai, nereikia atlikti jokių formalų veiksmų. Kai kam kyla klausimas, ar naudodami *NAT* negalėtume praplėsti *IPv4* adresų erdvės? Taip, *IPv4* leidžia taupyti *IP* adresus, tačiau tai nėra ilgalaikis adresų trūkumo sprendimas. *NAT* racionalu naudoti, kai nedidelio tinklo vartotojai jungiasi prie žiniatinklio, siunčia ir gauna laiškus bei failus. Šios paslaugos prieinamos taip, tarsi visi kompiuteriai būtų tiesiogiai prijungti prie interneto, bet jų prisijungimas nevisavertis. *NAT* apsunkina daugelį sudėtingesnių užduočių, pavyzdžiui, susijusių su srautinių duomenų perdavimu. Be to, tinklui veikiant per kelias *NAT* pakopas tampa vis sunkiau diagnozuoti kylančias ryšio problemas.

Apie 1990 m. imta rimtai ruoštis galimam adresų erdvės trūkumui ir 1992 m. aprašytas *IPv6*, kurio adresų erdvė turi didelį rezervą<sup>70</sup>. Tačiau internetas *IPv4* adresų trūkumo problemą kol kas sprendžia panaudodamas vidinius adresus, todėl perėjimas prie *IPv6* vyksta vangiai.

Numatyta ir daugiau rezervuotų *IP* adresų grupių. Paprastai tokie adresai, kaip ir čia minėti vidiniai adresai, gali būti naudojami specialioms tikslams, bet nėra matomi globaliame tinkle (27.3 lentelė). *RFC3330* ne tik išvardina rezervuotus adresus, bet ir

<sup>70</sup> <http://en.wikipedia.org/wiki/IPv6>

pateikia nuorodas į kitus *RFC* dokumentus, detalizuojančius kiekvienos rezervuotos adresų grupės naudojimą<sup>71</sup>.

27.3 lentelė. Kiti dažnai naudojami rezervuoti adresai

Adresų grupė	Paskirtis	Aprašas
0.0.0.0/8	nuoroda į save: „šis tinklas“	<i>RFC 1700</i>
127.0.0.0/8	nuoroda į save: „šis kompiuteris“	<i>RFC 1700</i>
169.254.0.0/16	supaprastintas vietinis tinklas	<i>RFC 3927</i>
192.0.2.0/24	tekste pateikiamiems pavyzdžiams	<i>RFC 3330</i>
192.88.99.0/24	sąveika tarp <i>IPv4</i> ir <i>IPv6</i>	<i>RFC 3068</i>
255.255.255.255	pranešimai visiems vietinio tinklo kompiuteriams	<i>RFC 1700</i>

## 27.6. Simboliniai domenų vardai

*IP* adresai užtikrina sistemos veikimą, tačiau nėra patogūs žmogui. Skaičių sekas nėra lengva atsiminti ir yra daugiau šansų suklysti nei rašant žodžius. Kartais serveris perkeliamas į kitą tinklą, todėl keičiasi ir jo *IP* adresas – būtų sudėtinga apie tai pranešti visiems serverio lankytojams. Todėl yra sugalvoti simboliniai domenų vardai, leidžiantys kreiptis į tinklo resursus lengviau įsi-menamu simboliu vardu. Pavyzdžiui, *lt.wikipedia.org*, o ne 91.198.174.2. Simbolinio vardo sudedamosios dalys atskiriamos tašku ir detalizuojamos iš dešinės į kairę.

Domeno vardo dalis po paskutinio taško vadinama aukščiausiojo lygio domenu. Pavyzdžiui, *.com* reiškia komercinę organizaciją, *.org* turėtų būti pelno nesiekianti organizacija. Ši vardu sistema sukurta, kai internetas kūrėsi JAV. Todėl kai kurie aukščiausiojo lygio vardai skirti JAV institucijoms: *.gov* – JAV vyriausybės organizacijos, *.mil* – JAV kariuomenė. Aukščiausiojo lygio domenų vardai suteikiami ir valstybėms. Pavyzdžiui, *.lt* (Lie-

<sup>71</sup> <http://tools.ietf.org/html/rfc3330>

tuva), *.lv* (Latvija), *.ee* (Estija). Politiniai pokyčiai ne visada lemia vardų pasikeitimus. Pavyzdžiui, yra panaikintas aukščiausiojo lygio domenas *.cs*, kuris buvo skirtas Čekoslovakijai, vietoj to naudojami *.cz* (Čekija) ir *.sk* (Slovakija), tačiau vis dar naudojamas domenas *.su* (*Soviet Union*), nors nebėra SSRS, o išsilaisvinusios valstybės naudoja savo domenų vardus.

Į kairę nuo aukščiausiojo lygio domeno iki antro taško yra antrojo lygio domeno vardas. Tokius vardus suteikia institucijos, atsakingos už aukščiausiojo lygio domenų vardus. Pavyzdžiui, VGTU įregistravo antrojo lygio domeną *vgtu.lt*. Aprašų pavyzdžiams yra rezervuoti šie antrojo lygio domenai: *example.com*, *example.net* ir *example.org*<sup>72</sup>.

Toliau į kairę atskirti taškais gali būti trečiojo, ketvirtojo ir žemesnių lygių domenai. Juos kuria ir prižiūri organizacija, įregistravusi pirmojo lygio domeną. Trečiojo lygio domenų vardai kartais suteikiami organizacijos padaliniams. Vardo pradžioje esantis žemiausio lygio domeno vardas paprastai nurodo paslaugą arba prisijungimo protokolą. Pavyzdžiui, *www.example.net* – žiniatinklio svetainė, o *irc.example.net* – IRC pokalbių serveris. Adresas *pop.ef.vgtu.lt* galėtų reikšti, kad tai POP3 pašto serveris Elektronikos fakultete VGTU tinkle, įregistruotame Lietuvoje.

Paketai internete adresuojami *IP* numeriais, tačiau tarp domenų vardų ir *IP* adresų nėra algoritminio ryšio, todėl būtina naudoti papildomas tarnybas, kurios tinklo mazgą vienareikšmiškai nustato pagal domeno vardą. Tokios tarnybos vadinamos *DNS* serveriais (*Domain Name Server*).

Duomenų transporto sistema *TCP* – IV lygmuo pagal *OSI*.

Kadangi *IP* protokolas paketus perduoda be sujungimo patvirtinimo, jis siekia pristatyti paketus, tačiau negarantuoja paketų pristatymo į paskirties mazgą.

Duomenų perdavimo *TCP* protokolu patikimumas paremtas loginiu sąveikaujančių procesų sujungimu. Kol *TCP* protokolo programos veikia teisingai, o sudėtinis tinklas neišsibarstęs į nesu-

<sup>72</sup> <http://tools.ietf.org/html/rfc2606>



jungiamas dalis, duomenų perdavimo klaidos *IP* protokolo lygmeniu neturės įtakos teisingiems duomenims gauti.

Protokolas *TCP* naudoja *IP* protokolą kaip transporto priemonę. Prieš išsiųsdamas duomenų blokus, *TCP* protokolas juos sudeda į *IP* paketo apvalkalą. Esant reikalui, *IP* protokolas gali šį paketą fragmentuoti ir paskui vėl sujungti, kai perdavimas vyksta per keletą tinklų bei tarpinių šliuzų.

*TCP* naudojasi *IP* protokolu ir teikia paslaugas aukštesniojo lygmens protokolo užduotims.

Šio protokolo tikslas – perduoti duomenis tarp taikomųjų procesų, vykdomų bet kuriuose tinklo mazguose. Kai *IP* protokolas pristato paketą nurodytu adresu, duomenis reikia perduoti konkrečiam procesui. Kiekvienas kompiuteris gali vykdyti keletą procesų, be to, taikomasis procesas gali turėti ir daugiau nei vieną įėjimo tašką, kuris laikomas duomenų paketo paskirties adresu.

Paketai, patenkantys į transporto lygmenį, operacinėje sistemoje organizuojami kaip daugybė eilių prie įvairių taikomųjų procesų įėjimo taškų. Tokios eilės vadinamos prievadais (angl. *ports*). Paskirties adresas, kuris naudojamas *TCP* protokole, yra taikomosios tarnybos prievado numeris. Pavyzdžiui, *FTP* tarnybai dažniausiai priskiriamas 21 prievadas, o *Telnet* tarnybai – 23. Programos kūrėjas pats gali priskirti prievado numerį, jei tas numeris nėra rezervuotas. Prievado numeris kartu su *IP* adresu vienareikšmiškai rodo taikomąjį procesą tinkle. Šis parametru rinkinys vadinamas lizdu (angl. *socket*).

*TCP* protokolo duomenų vienetas vadinamas segmentu. Informacija, patenkanti į *TCP* protokolą iš aukštesniojo lygmens protokolu, traktuojama kaip nestruktūruotas baitų srautas. Duomenys kaupiami buferyje, iš jo paskui paimama tam tikra nuosekli duomenų dalis, kuri ir vadinama segmentu.

Segmento dydis parenkamas taip, kad pakuojamas segmentas tilptų visas, t. y. maksimalus segmento dydis neturi viršyti *IP* paketo maksimalaus duomenų lauko dydžio. Kitaip reikėtų segmentą fragmentuoti, t. y. segmentą padalinti, kad jis tilptų į *IP* paketą.

Sujungimas *TCP* protokole identifikuojamas abiejų sąveikaujančių procesų lizdų pora. Formaliai sujungimą galima apibrėžti kaip parametrų rinkinį, charakterizuojantį duomenų apsikeitimą tarp dviejų procesų. Be išsamių procesų adresų, šiame rinkinyje yra ir parametrai, kurių reikšmės nustatomos per *TCP* modulį „pasi-kalbėjimą“. Tokiais parametrais gali būti segmentų dydžiai, duomenų kiekis, kurį galima perduoti negavus patvirtinimo, pradinis ir esamas perduodamų baitų numeriai. *TCP* užtikrina dviejų krypčių ryšį.

*TCP* protokole naudojamas slystančiojo lango patvirtinimų algoritmas. Tai reiškia, kad segmentų skaičius, lygus lango dydžiui, gali būti persiųstas nelaukiant patvirtinimo. Tada procesas sustoja, kol sulaukiama bent vieno patvirtinimo iš priimančiosios pusės. Jei, tarkim, sulaukta 3 segmentų gavimo patvirtinimo, langas pasislenka per 3 pozicijas – vadinasi, dar 3 segmentus galima pasiųsti, nelaukiant patvirtinimo ir t. t. Jeigu kuris segmentas persiunčiamas neteisingai, jo gavimo patvirtinimas nesiunčiamas. Taip patvirtinimo negavimas reiškia, kad arba segmentas, arba pats patvirtinimas nepasiekė adresato. Patvirtinimas siunčiamas irgi kaip segmentas, kuriame yra skaičius, vienetu didesnis už maksimalaus baito numerį gautajame segmente. Šis skaičius vadinamas eilės numeriu.

Perdavimo patikimumas užtikrinamas naudojant patvirtinimus ir eilės numerius. Kiekvienam duomenų baitui priskiriamas eilės numeris. Pirmojo duomenų baito eilės numeris segmente perduodamas kartu su šiuo segmentu ir vadinamas segmento eilės numeriu. Segmentai taip pat turi eilės numerį, kuris yra kito laukiamo duomenų baito, perduodamo priešinga kryptimi, numeris. Kai yra perduodamas segmentas su duomenimis, jo kopija pateikiama į pakartotinio siuntimo eilę ir paleidžiamas laikmatis. Gavus pristatymo patvirtinimą, segmentas pašalinamas iš eilės. Jei per nustatytą laiką patvirtinimas negaunamas, segmentas išsiunčiamas pakartotinai.

### 27.7. Perdavimo saugumas

**V lygmuo pagal OSI.** Aprašyta sistema leidžia perduoti duomenis tarp bet kurių dviejų internete veikiančių įrenginių. Duomenys perduodami per tarpinius kompiuterius, kurie dažniausiai priklauso skirtingiems savininkams. Panaudojęs specialią programinę įrangą piktavališkas asmuo galėtų perskaityti perduodamą turinį. Dar blogiau, jei neapsaugoti perduodami prisijungimo slaptažodžiai. Tuomet būtų galima įsilaužti į informacinės sistemas.

Siekiant užtikrinti saugumą kuriami šifravimo ir kitokie apsaugos protokolai. Pavyzdžiui, *SSL (Secure Sockets Layer)* – kriptografinis protokolas, skirtas šifruojant apsaugoti informacijai, sklindančiai internete. *SSL* šifruoti naudoja tiek simetrinę, tiek asimetrinę kriptografiją. Simetrinė kriptografija yra daug greitesnė už asimetrinę, todėl ji naudojama persiunčiant duomenis, taip taupomas persiuntimo laikas. Asimetrinė kriptografija naudojama tik apsikeičiant raktais. Serveris atsiunčia klientui savo viešąjį raktą, kuriuo klientas užšifruoja sugeneruotą simetrinį šifro raktą, taip jis apsaugomas nuo tarpininkų.

### 27.8. Vartotojo programos

**VII lygmuo pagal OSI.** Kiekvienas žemesnis lygmuo užtikrina aukštesniojo lygmens veikimą. Visų jų viršūnėje – VII lygmuo – vartotojo programos. Kai kuriuos paplitusius vartotojų programų sąveiką užtikrinančius protokolus aptarsime kituose skyriuose.

### 27.9. Klausimai ir uždaviniai

1. Kaip atvirieji standartai veikia tinklų plėtrą?
2. Ar gali atvirieji standartai užtikrinti saugų kompiuterių sujungimą?
3. Aprašykite kuo mažesnę namų vidinį tinklą, jei namie yra du kompiuteriai ir maršrutizatorius.

4. VGTU EF vidinis tinklas 193.219.149.0/25.
  - Kokia yra jo kaukė?
  - Kiek bitų skiriama šio tinklo numeriui, kiek bitų skiriama įrenginio numeriui? Kiek skirtingų įrenginių gali turėti unikalūs *IP* šiame tinkle?
  - Koks turėtų būti šio tinklo pranešimų transliavimo (*broadcast*) adresas?
  - Pateikite kelis šio tinklo *IP* pavyzdžius.
5. Raskite penkis naujausius *RFC* dokumentus. Apie ką juose kalbama?