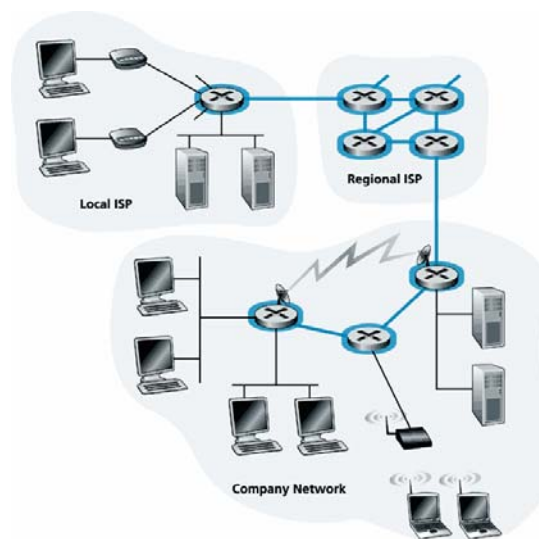


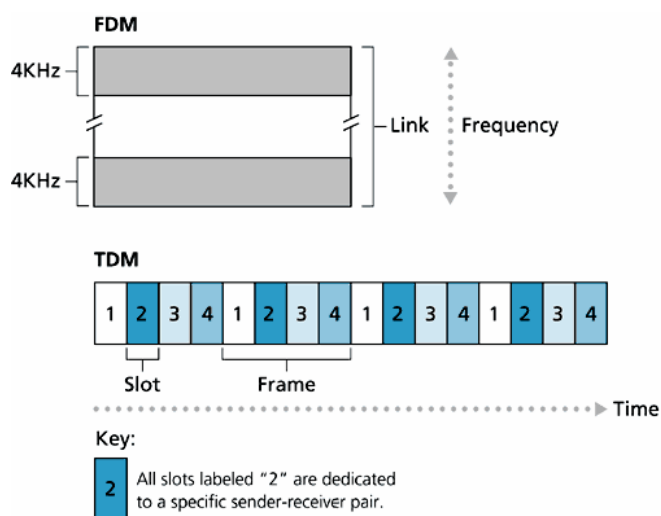
Kanalų komutavimas, paketų komutavimas

Tinklo branduolys – tai maršrutizatorių tinklas, sujungiantis Interneto galinius įrenginius. (1 pav. branduolys išskirtas mėlyna linija).

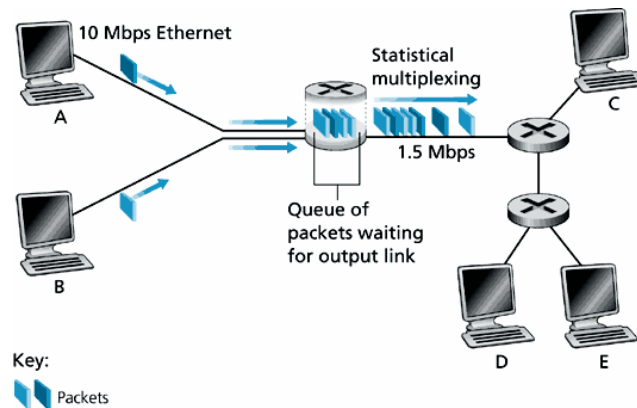


Pagal informacijos perdavimo būdą tinklas gali būti suskirstytas į tinklą su kanalų komutavimu (circuit switching) ir tinklą su paketų komutavimu (packet switching). Kanalų komutavimo tinkluose sesijos trukmei yra rezervuojami ryšiui sudaryti reikalingi resursai (kanalų pralaidumas, buferiai). Klasikinis šių tinklų tipo pavyzdys – telefoninis tinklas. Prieš pradedant siuntėjui siųsti informaciją, tinklas turi sudaryti sujungimą tarp siuntėjo ir gavėjo. Kelyje tarp siuntėjo ir gavėjo esantys komutatoriai turi palaikyti sujungimo būseną šiam sujungimui. Kai tinklas sujungia kanalą, jis rezervuoja pastovų perdavimo greitį tinklo sąsajomis visai sesijos trukmei.

Sąsajoje kanalas gali būti išskirtas panaudojant dažninį arba laikinį dalinimą. Naudojant dažninį dalinimą, iš sąsajos dažnių spektro yra išskiriamos dažnių juostos ir priskiriamos kanalams. Laikinio dalinimo atveju, laikas yra dalinamas į fiksuoto ilgio freimusus, ir kiekvienas freimusus yra skaidomas į fiksuotą skaičių intervalų. Kai tinklas užmezga ryšį, jam yra priskiriamas intervalas visuose freimusuose, kol nutrūks ryšys.



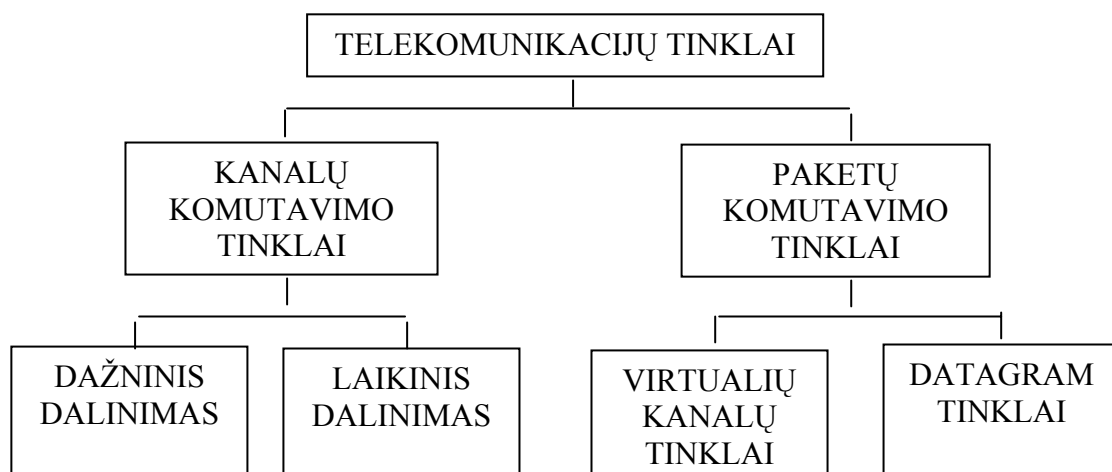
Paketų komutavimo tinkluose rezervavimas nėra atliekamas. Taikomosios programos bendrauja pranešimais. Siuntėjas ilgus pranešimus skaido į mažesnius, vadinamus paketais. Paketai keliauja sąsajomis ir paketų komutatoriais (maršrutizatoriais). Paketas yra siunčiamas sąsaja pilnu sąsajos pralaidumo greičiu. Daugumu maršrutizatorių veikia sukaupiti-ir-persiųsti principu. Tai reiškia, kad maršrutizatorius iš pradžių turi priimti visus paketo bitus, prieš pradedant juos siųsti į kitą kanalą. Kiekvienai sąsajai prijungtai prie maršrutizatoriaus, maršrutizatorius turi išėjimo buferį, kur saugomi siuntimui į tą sąsają paruošti paketai. Jei sąsaja yra užimta, tuomet paketas yra saugomas šiame buferyje. Tai įneša papildomą paketų vėlinimą. Jei persipildo išėjimo buferis, atsiranda paketų praradimas.



Egzistuoja dviejų tipų paketų komutavimo tinklai: virtualių kanalų ir datagram tinklai. Virtualių kanalų tinkluose paketų persiuntimas gavėjo kryptimi vyksta pagal virtualių kanalų numerius, o datagram tinkluose – pagal gavėjo adresą.

Virtualių kanalų tinkluose: kiekvienas paketas turi žymę (virtualaus kanalo numerį), kuri apsprendžia sekantį žingsnį; virtualaus kanalo sudarymo metu nustatytas kelias, kuriuo siunčiami paketai, išlieka tas pats visos sesijos metu.

Datagram tinkluose: sekantį žingsnį nusako gavėjo adresas; kelias, kuriuo siunčiami paketai, sesijos metu gali keistis.

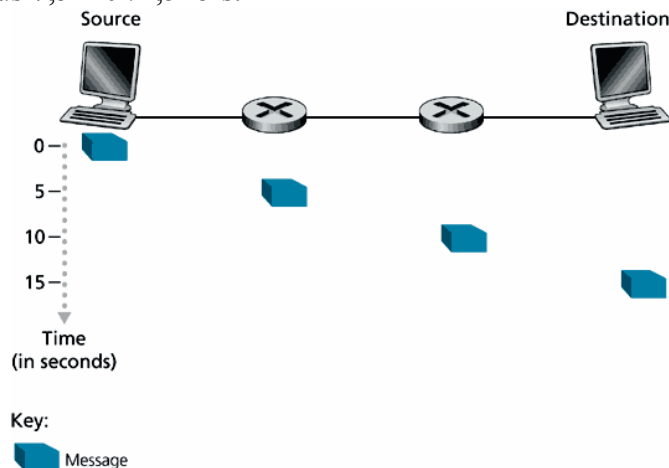


Pranešimų segmentavimas

Moderniuose paketų komutavimo tinkluose šaltinis taikomojo lygmens programos pranešimą segmentuoja (suskaido) į paketus ir juos išsiunčia gavėjui, kuris vėliau juos surenka į pirminį pranešimą. Jei šaltinis nesegmentuoja pranešimo į paketus, laikysime kad paketų komutavimo tinklas atlieka pranešimų komutavimą.

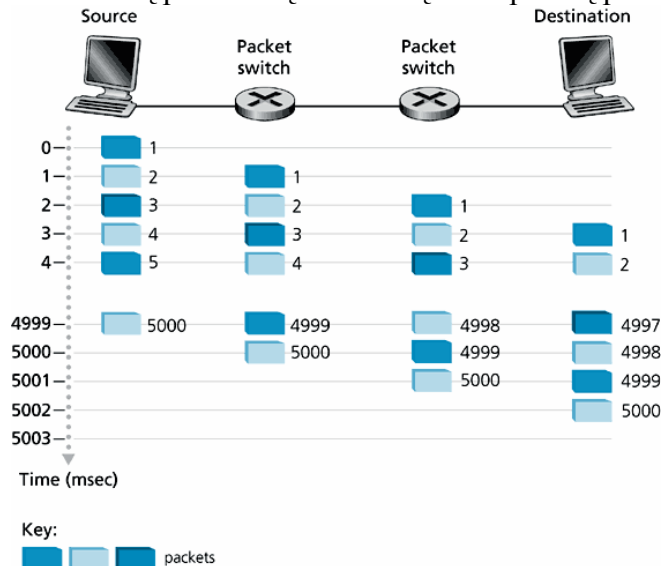
Kyla klausimas: kokia segmentavimo nauda?

Panagrinėkime pavyzdį. Turime pranešimą $7,5 \cdot 10^6$ bitų ilgio. Tarp siuntėjo ir gavėjo yra du paketų komutatoriai ir trys sąšajos, kurių kiekvienos pralaidumas 1,5 Mbps. Tinklas neužkrautas, ir naudojamas pranešimų komutavimas. Laikas per kurį bus nusiųstas pranešimas iš šaltinio į pirmą maršrutizatorių bus lygus $7,5 \cdot 10^6 / 1,5 = 5$ s.



Kadangi naudojamas sukaupti-ir-persiųsti principas, pirmasis maršrutizatorius negalės siųsti pranešimo toliau, pakol visas pranešimas nebus priimtas. Sekant šia logika, laikas per kurį bus perduotas pranešimas iš siuntėjo gavėjui bus lygus 15 s.

Sakykime, kad šaltinis visą pranešimą suskaidė į 5000 paketų po 1500 bitų.



Pirmą paketą perduoti iš siuntėjo iki pirmojo maršrutizatoriaus užtruks 1 msec. Antrasis paketas pasiekia pirmąjį maršrutizatorių po 2 msec. Sekant šia logika paskutinis paketas pasiekia pirmąjį maršrutizatorių po 5000ms 5 s. kadangi šis paskutinis paketas dar turi būti persiųstas per dvi sąšajas tai galutinis laikas 5, 002 s.

Paralelinis perdavimas.

Klaidos.

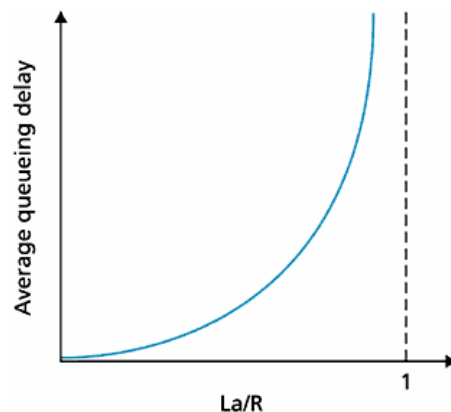
Antraštės.

Vėlinimas ir paketų praradimas paketų komutavimo tinkluose

Laikas, per kurį paketas pasiekia gavėją, priklauso nuo keturių vėlinimo laikų: mazginio apdorojimo, laukimo maršrutizatorių buferiuose, siuntimo ir sklidimo vėlinimo. Visi šie vėlinimai kartu sudaro bendrą paketo vėlinimą.

Mazginio apdorojimo vėlinimas tai laikas reikalingas išanalizuoti paketo antraštę ir nustatyti į kokią sąsają nukreipti paketą. Taip pat į šį vėlinimą gali įeiti paketo bitų klaidų aptikimo bei ištaisymo laikai. Šiuolaikiniuose M apdorojimo vėlinimas yra mikrosekundžių eilės. Po apdorojimo M paketą persiunčia į buferį. Čia paketas susiduria su laukimo M buferiuose vėlinimu. Jei buferis tuščias ir tuo metu nėra siunčiamas kitas paketas, tai tuomet šis vėlinimas lygus nuliui. Jei srautas didelis ir daug paketų laukia savo eilės buferyje, tuomet laukimo M buferiuose vėlinimas bus ilgas. Šis vėlinimas yra skirtingas kiekvienam paketui. Siuntimo vėlinimas yra lygus L/R . L – paketo ilgis bitais, R – sąsajos pralaidumas bit/s. Tai laikas, per kurį visi paketo bitai yra išsiunčiami į sąsają. Išsiųstas į sąsają bitas sklinda iki jos pabaigos. Laikas, reikalingas bitui nusklisti nuo sąsajos pradžios iki galo, vadinamas sklidimo vėlinimu. Sklidimo greitis priklauso nuo sąsajos tipo ir kinta ribose nuo $2 \cdot 10^8$ iki $3 \cdot 10^8$ m/s. Sklidimo vėlinimas yra lygus d/s , kur d – sąsajos ilgis metrais, s – sklidimo greitis.

Raide a pažymėkime vidutinį paketų pasirodymo dažnį (paketų/s). Jeigu visų paketų ilgiai lygūs L bitų, tuomet vidutinis bitų pasirodymo dažnis La (bit/s). Santykį La/R pavadinkime srauto intensyvumu. Vidutinio laukimo vėlinimo priklausomybė nuo srauto intensyvumo.



Paketai M įėjime pasirodo atsitiktiniu laiko momentu. Jei srauto intensyvumas yra artimas nuliui, tuomet vidutinis laukimo vėlinimas taip pat bus artimas nuliui. Jei srauto intensyvumas artėja prie vieneto, tam tikrais laiko momentais bitų pasirodymo dažnis gali būti didesnis už kanalo pralaidumą, tuomet susidarys paketų eilė M buferyje. Srauto intensyvumui viršijus vienetą, vidutinis laukimo vėlinimas vis didėja. M buferiai nėra begaliniai, todėl jei atėjęs paketas randa užpildytą buferį, jis yra prarandamas. Prarastų paketų santykis didėja didėjant srauto intensyvumui. Prarastas paketas gali būti persiųstas taikomosios programos ar transportinio lygmens protokolo.

Jei tarp siuntėjo ir gavėjo turime $N-1$ M , o laukimo M buferiuose vėlinimas nykstamai mažas, tuomet bendras paketo vėlinimas bus lygus:

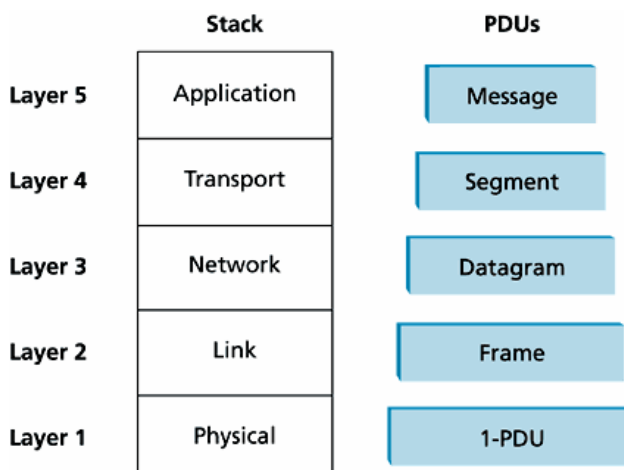
$$d = N(d_{apd} + d_{siunt} + d_{sklid})$$

Protokolų lygmenys (OSI modelis)

Siekiant sumažinti tinklų nagrinėjimo kompleksiskumą, protokolai yra sisteminami į lygmenis. Lygmeninėje protokolų architektūroje kiekvienas protokolas priklauso vienam iš lygmenų. Kiekvienas tinklo įrenginys turi n -tojo lygmens protokolus. Lygmenys bendrauja tarpusavyje n -tojo lygmens pranešimais, vadinamais n -tojo lygmens duomenų vienetais (PDU). Duomenų vieneto turinį ir formatą, taip pat ir apsikeitimo būdą aprašo n -tojo lygmens protokolas. $n-1$ lygmuo teikia paslaugas n – tajam lygmeniui. PVZ. Protokolų, surinktų iš įvairių lygmenų, visuma vadinama protokolų steku.

Kompiuterių tinkluose, kiekvienas lygmuo gali vykdyti vieną arba daugiau šių funkcijų: klaidų kontrolę, srauto kontrolę, segmentavimą ir desegmentavimą, multipleksavimą, sujungimo sudarymą.

Interneto stekas susideda iš penkių lygmenų: fizinio, kanalinio, tinklinio, transportinio bei taikomojo. Kiekvienas lygmuo, išskyrus fizinį, turi savo duomenų vieneto pavadinimą: pranešimas, segmentas, datagrama, freimas.



Taikomasis lygmuo yra atsakingas už taikomųjų programų palaikymą. HTTP protokolas palaiko Web'ą, SMTP – elektroninį pašta, FTP – failų perdavimą. Taikomasis lygmuo paprastai yra realizuojamas programiškai.

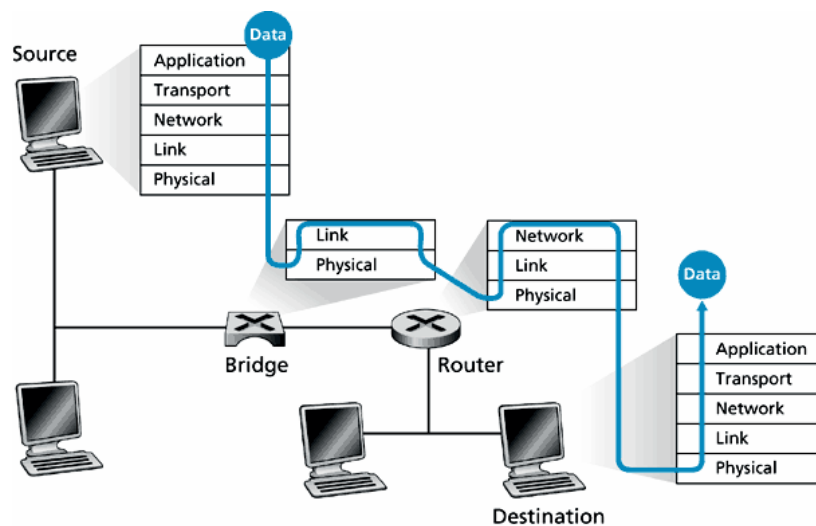
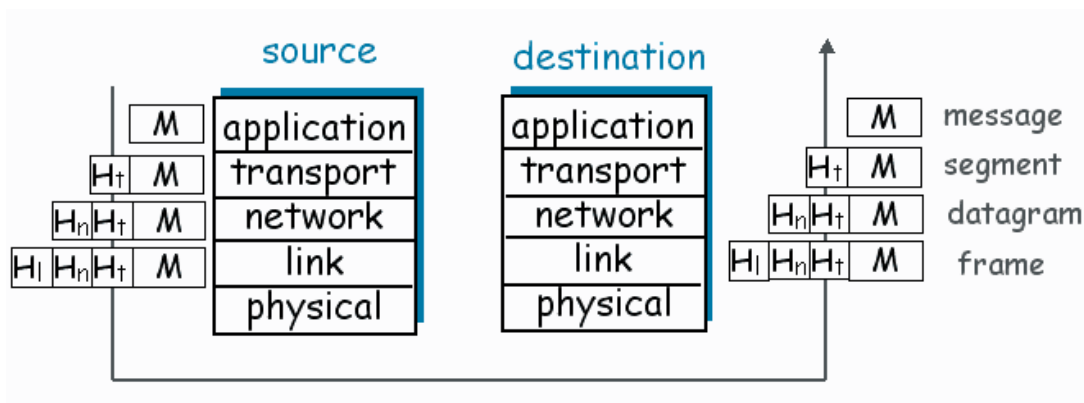
Transportinis lygmuo suteikia taikomojo lygmens pranešimų transportavimo paslaugą tarp kliento ir serverio taikomųjų programų. Šiam lygmeniui priklauso TCP ir UDP protokolai. Šis lygmuo taip pat yra realizuojamas programiškai.

Tinklinis lygmuo atsakingas už datagramų maršrutizavimą tarp siuntėjo ir gavėjo. Tinklinis lygmuo susideda iš IP protokolo bei maršrutizavimo algoritmų. Tinklinis lygmuo yra realizuojamas kombinuotai ir programiškai ir su technine įranga.

Kanalinis lygmuo yra skirtas freimų perdavimui tarp dviejų tiesiogiai sujungtų įrenginių. Šis lygmuo yra realizuojamas techninėje įrangoje (tinklo plokštėje). Pvz. Ethernet.

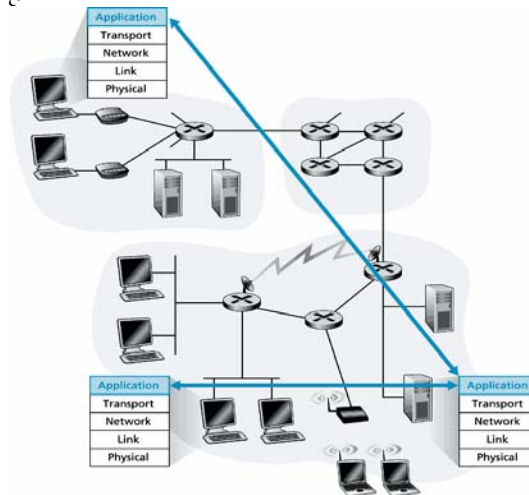
Fizinis.

Kiekvienas lygmuo gauna iš duomenis iš esančio aukščiau ir prideda antraštę taip sudarydamas naują duomenų vienetą. Naujai sudarytą duomenų vienetą persiunčia žemiau esančiam lygmeniui.



Taikomasis lygmuo

Procesu vadinsime programinę įrangą, veikiančią galiniame įrenginyje. Du procesai, veikiantys skirtinguose galiniuose įrenginiuose, tarpusavyje bendrauja apsikeisdami pranešimais, naudodami taikomąjį lygmenį.

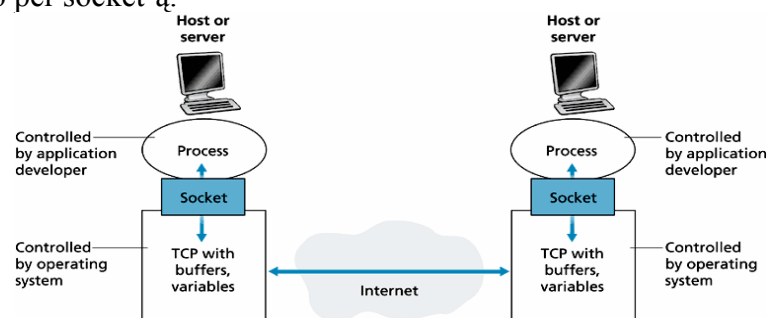


Taikomojo lygmens protokolas yra tik viena sudedamoji tinklo taikomosios programos dalis. Pvz. Web taikomoji programa susideda iš dokumentų formato standarto (HTML), Web naršyklių (Microsoft Internet Explorer, Netscape Navigator), Web serverių ir taikomojo lygmens protokolo (HTTP).

Taikomojo lygmens protokolas aprašo: apsikeičiamų pranešimų tipus (reikalavimo ir atsakymo pranešimai); įvairių pranešimo tipų sintaksę; pranešimo laukelių semantiką (ką reiškia laukelio informacija); taisykles, kurios nusako kada ir kaip procesas siunčia pranešimą ir atsako į pranešimus.

Taikomoji programa tipiškai turi dvi dalis: klientą ir serverį. Klientas, esantis viename galiniame įrenginyje, bendrauja su serveriu, esančiu kitame galiniame įrenginyje. Pavyzdžiui Web naršyklė yra klientas, o Web serveris – serveris. Daugumoje taikomųjų programų galinis įrenginys tuo pačiu metu yra ir klientas ir serveris. Pvz Telnet FTP. Paprastai, įrenginys kuris inicijuoja sesiją, vadinamas klientu.

Socket'as tai sąsaja tarp taikomojo ir transportinio lygmenų. Procesai siunčia ir priima pranešimus iš tinklo per socket'ą.



Siųsdamas pranešimą, siunčiantysis procesas turi identifikuoti priimančią procesą. Identifikacijai yra naudojami: IP adresas ir porto numeris. Populiariems taikomojo lygmens protokolams yra priskirtas specifinis porto numeris. Pvz: HTTP – 80, SMTP- 25 ir pan. RFC 1700.

Application	Data Loss	Bandwidth	Time-Sensitive
File transfer	No loss	Elastic	No
E-mail	No loss	Elastic	No
Web documents	No loss	Elastic (few kbps)	No
Real-time audio/video	Loss-tolerant	Audio: few kbps–1 Mbps Video: 10 kbps–5 Mbps	Yes: 100s of msec
Stored audio/video	Loss-tolerant	Same as above	Yes: few seconds
Interactive games	Loss-tolerant	Few kbps–10 kbps	Yes: 100s of msec
Instant messaging	No loss	Elastic	Yes and no

Applications	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP [RFC 2821]	TCP
Remote terminal access	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2616]	TCP
File transfer	FTP [RFC 959]	TCP
Remote file server	NFS [McKusik 1996]]	UDP or TCP
Streaming multimedia	Often proprietary (for example, Real Networks)	UDP or TCP
Internet telephony	Often proprietary (for example, Dialpad)	Typically UDP

HTTP protokolas

HTTP – HyperText Transfer Protocol yra WEB’o taikomojo lygmens protokolas. Šis protokolas aprašytas RFC 1945 RFC 2616 standartuose. HTTP protokolas yra realizuotas dviejuose programose – kliento ir serverio.

Web puslapis susideda iš objektų (HTML failo, JPEG paveikslo, GIF paveikslo, audio įrašo ir pan.). Paprastai Web puslapį sudaro pagrindinis HTML failas ir keli su juo susiję objektai. (1 HTML failas + 4 susiję objektai = 5 objektai). Kiekvienas objektas yra adresuojamas URL (Unique Address Locator), susidedančiu iš dviejų dalių: serverio, kuriame saugomas objektas, vardo ir objekto kelio. Pvz.

www.su.lt/tf/nuotrauka.gif

HTTP naudoja TCP, kaip transportinį protokolą.

Kadangi HTTP serveriai nesaugo informacijos apie klientą, HTTP protokolas yra vadinamas be būsenos.

Egzistuoja dvi HTTP protokolo versijos HTTP/1.0 ir HTTP/1.1. HTTP/1.0 versija naudoja nepastovius sujungimus. Sakykime Web puslapis susideda iš pagrindinio HTML failo ir dešimties JPEG paveikslų (viso 11 objektų). URL pagrindiniam HTML failui: www.su.lt/tf/index.html. Žingsniai:

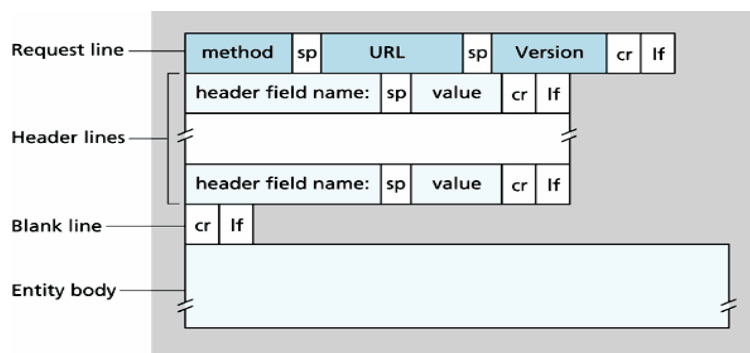
- 1) HTTP klientas inicijuoja TCP sujungimą su serveriu www.su.lt, porto numeris 80.
- 2) HTTP klientas siunčia užklauso pranešimą per pirmąjį žingsnį sudarytą socket’ą, su keliu /tf/index.html.
- 3) HTTP serveris per socket’ą priima pranešimą, iš kaupiklio ištraukia reikalaujamą objektą, jį įdeda į atsakymo pranešimą, ir išsiunčia per socket’ą klientui.

- 4) HTTP serveris nurodo TCP nutraukti TCP sujungimą.
- 5) Klientas priima atsakymo pranešimą. TCP sujungimas nutraukiamas. Klientas išanalizuoja HTML failą, ir suranda nuorodas į 10 JPEG objektų.
- 6) Pirmieji keturi žingsniai pakartojami kiekvienam JPEG objektui.

Taigi esant nepastoviam sujungimui, kiekvienam objektui yra sudaromas naujas TCP sujungimas. TCP sujungimui gali būti sudaromi nuosekliai (vienas po kito) arba lygiagrečiai (keli vienu metu 5-10). Kiekvienam sujungimui turi būti rezervuotas TCP buferis ir saugomi TCP sujungimo kintamieji. Tai apkrauna Web serverius.

Naudojant pastovius sujungimus TCP, išsiuntęs atsakymo pranešimą, nenutraukia sujungimo. Aukščiau aprašytas Web puslapis būtų persiųstas vienu pastoviu sujungimu. Paprastai Web serveris nutraukia TCP sujungimą, kai jis yra nenaudojamas tam tikrą laiką. Pastovūs sujungimai yra dviejų rūšių: 1) nauja užklausa yra siunčiama tik tuomet kai gautas atsakymas į prieš tai buvusią, 2) užklausa yra siunčiama iškart aptikus nuorodas. Pagal nutylėjimą HTTP/1.1 versija naudoja pastovius 2-os rūšies sujungimus.

Užklauso pranešimo formatas



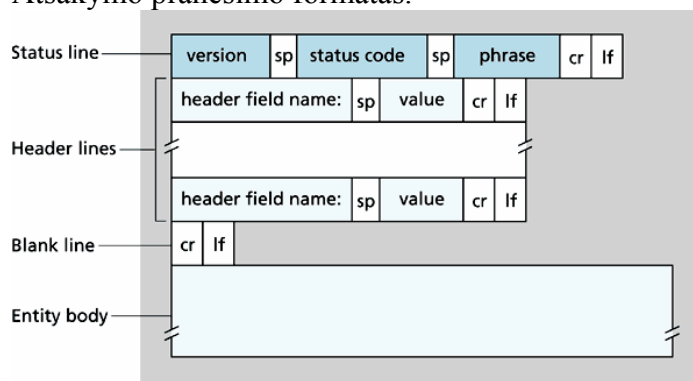
Laukelis metodas HTTP/1.0 versijoje gali įgyti sekančias reikšmes: GET HEAD POST. Plačiausiai naudojamas metodas GET.

GET /direktorija/index.html HTTP/1.1

HEAD metodas panašus į GET, tik serveris į atsakymo pranešimą neįdeda reikalauoto objekto. POST metodas naudojamas tuomet, kai vartotojas pildo kažkokią įvedimo formą, pvz. paieškos sistemoje. Vartotojo įvesta informacija yra siunčiama duomenų lauke.

HTTP/1.1 versija papildomai turi PUT ir DELETE metodus. Metodo PUT pagalba į Web serverį galime patalpinti objektą, o DELETE – ištrinti.

Antraštės eilutės yra nebūtinės. Pvz.: User-agent: Internet Explorer 6.0 Accept-language:lt. Atsakymo pranešimo formatas.



Būsenos kodai ir su jais susijusios frazės:

200 OK	301 Moved Permanently Location:
304 Not Modified	400 Bad Request
404 Not Found	505 HTTP Version Not Supported

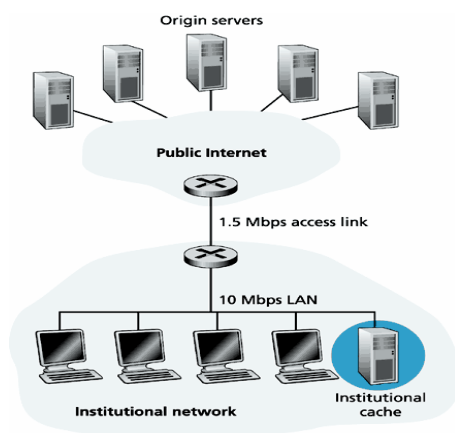
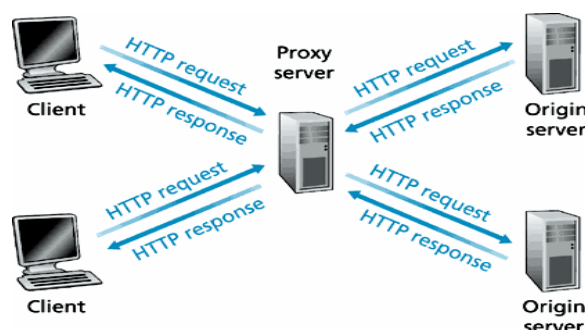
Antraštės eilutės: Date: Server: Last-Modified: Content-Length: Content-Type.

```
telnet www.su.lt 80
GET
```

```
Sąlyginis GET.
GET /su/logo.gif HTTP/1.1
If-modified-since:<date>
```

```
HTTP/1.1 304 Not Modified arba HTTP/1.1 200 OK
data data
```

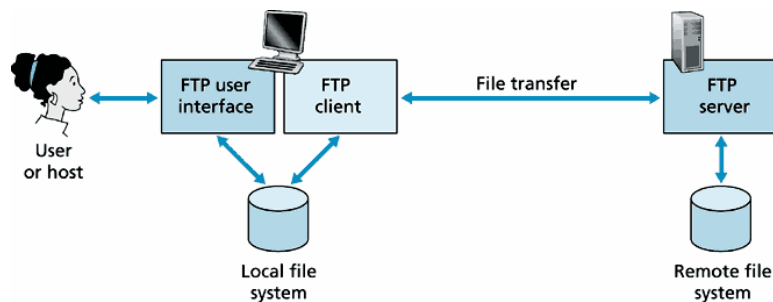
Vartotojai naršyklės nustatymuose nurodo, jog kreipimasis būtų vykdomas per proxy serverį. Tuomet naršyklė visas užklausas siųs proxy serveriui. Jei reikaujamas objektas yra proxy serveryje, jis atsakymą išsiųs atgal naršyklei. Jei objekto nėra, tuomet proxy serveris siunčia užklausa originaliam serveriui. Šis grąžina objektą, proxy serveris jį išsisaugo ir persiunčia naršyklei.



Sąlyginio GET metodo naudojimas sumažina objekto vėlinimo laiką, bei interneto Web srautus.

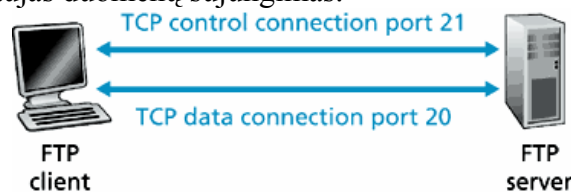
FTP protokolas

FTP protokolas skirtas failų persiuntimui iš/į nutolusio įrenginio. RFC 959.



FTP naudoja du lygiagrečius TCP sujungimus: valdymo sujungimą ir duomenų sujungimą. Valdymo sujungimas skirtas valdymo informacijai (identifikacija, slaptažodis, valdymo komandos) siųsti.

Klientas iš pradžių sudaro TCP valdymo sujungimą su serveriu, 21-uoju portu. Klientas šiuo sujungimu siunčia vartotojo vardą, slaptažodį bei komandas nutolusių direktorių pakeitimui. Kai serveris gauna failo perdavimo (iš/i serverio) komandą, jis inicijuoja TCP duomenų sujungimą. Po failo persiuntimo šis sujungimas yra nutraukiamas. Jei, tęsiantis tai pačiai sesijai, klientas nori siųsti kitą failą, yra sudaromas naujas duomenų sujungimas.



Sesijos metu FTP serveris turi saugoti informaciją apie klientą. Serveris turi susieti valdymo sujungimą su klientu, bei žinoti esamą kliento direktoriją. Dėl šių priežasčių yra ribojamas prisijungimų prie FTP serverių skaičius.

FTP komandos yra siunčiamos TCP valdymo sujungimu septynių bitų ASCII (American Standard Code for Information Interchange) formatu. Visos FTP komandos yra keturių simbolių:

USER vartotojo vardas –

PASS slaptažodis –

CWD change working directory

LIST – pateikia aktyvios nutolusios direktorijos turinį. Turinys yra siunčiamas per naujai sudarytą TCP duomenų sujungimą.

RETR failo_vardas – naudojama parsisiųsti failą iš aktyvios nutolusios direktorijos.

STOR failo_vardas – naudojama patalpinti failą į aktyvią direktoriją.

Po kiekvienos komandos seka trijų skaičių atsakymas su priedais:

331 Username OK, password required;

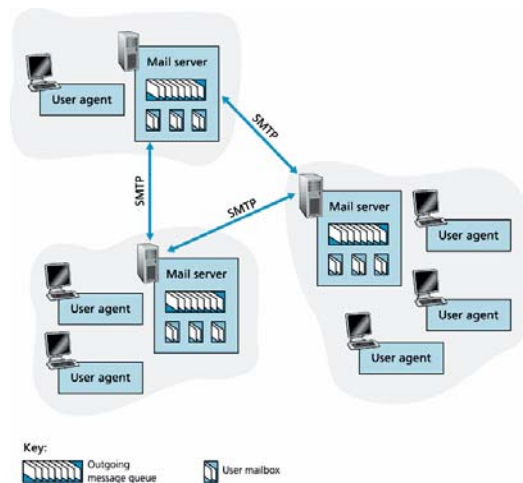
125 Data connection already open; transfer starting;

425 Can't open data connection;

452 Error writing file;

E-paštas

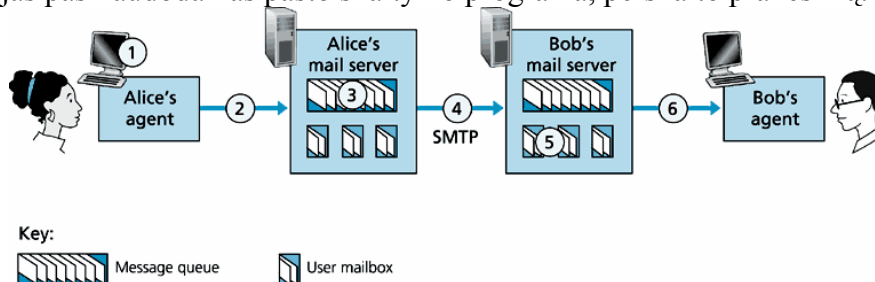
E-pašto taikomoji programa susideda iš trijų pagrindinių dalių: pašto skaitymo programų, pašto serverių, bei SMTP (Simple Mail Transfer Protocol) protokolo. Pašto skaitymo programos leidžia vartotojui skaityti, persiųsti, atsakyti bei sukurti pranešimus. Pvz.: Eudora, MS Outlook, Netscape Messenger. Pašto serveriuose, kiekvienam vartotojui yra sukurta pašto dėžutė. Joje tvarkomi ir laikomi vartotojo gauti laiškai. Pašto serveriai turi pranešimų buferį, kuriame saugomi siuntimui paruošti pranešimai.



SMTP protokolas naudojamas e-pašto pranešimams persiųsti tarp pašto serverių. SMTP aprašytas RFC 2821 standarte.

Scenarijus:

- 1) Siuntėjas pasinaudodamas e-pašto skaitymo programa sukuria pranešimą, nurodo gavėjo adresą ir nurodo išsiųsti pranešimą.
- 2) Siuntėjo pašto skaitymo programa nusiunčia pranešimą siuntėjo pašto serveriui, kur patalpinamas pranešimų buferyje.
- 3) SMTP klientas (siuntėjo pašto serveris) sudaro TCP sujungimą su SMTP serveriu (su gavėjo pašto serveriu), 25-uoju porto numeriu.
- 4) Po pradinio SMTP pasisveikinimo, SMTP klientas išsiunčia pranešimą.
- 5) SMTP serveris priima pranešimą, ir patalpina jį gavėjo pašto dėžutėje.
- 6) Gavėjas pasinaudodamas pašto skaitymo programa, perskaito pranešimą.



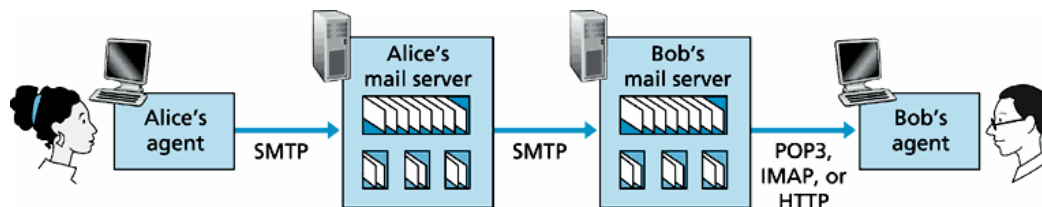
SMTP pranešimus siunčia tiesiogiai tarp siuntėjo ir gavėjo pašto serverių, nenaudojant tarpinių pašto serverių. Jei gavėjo pašto serveris neatsako, pranešimas yra laikomas pranešimų buferyje. Jei po tam tikro laiko pranešimo išsiųsti nepavyksta, serveris sunaikina pranešimą ir praneša siuntėjui.

telnet serverio_vardas 25

HELO; MAIL FROM; RCPT TO; DATA; "." QUIT;

Kam reikalingi pašto serveriai?

Naudojant SMTP protokolą, TCP sujungimas yra sudaromas to įrenginio, kuris nori siųsti pranešimą (HTTP atvirkščiai). Dėl šios priežasties SMTP protokolas tinka pranešimo siuntimui į siuntėjo pašto serverį. Tačiau netinka pranešimo parsisiuntimui iš pašto serverio. Tam tikslui yra naudojami POP3 ir IMAP protokolai.



POP3 (Post Office Protocol Version 3), aprašytas standarte RFC 1939. POP3 sesija prasideda tuomet kai vartotojas (pašto skaitymo programa) sudaro TCP sujungimą su pašto serveriu 110 – uoju portu. Po sujungimo sudarymo POP3 sesija susideda iš trijų fazių: autorizacijos, operacijos ir atnaujinimo. Autorizacijos fazės kliento komandos:

user: vart_vardas; pass: slaptažodis

Serverio atsakymai: +OK; -ERR.

Operacijos fazės metu kliento komandos:

list – pateikia pranešimų numerius;

retr <numeriai> - pranešimo, su nurodytu numeriu, parsisiuntimas;

dele <numeriai> - pranešimai, su nurodytais numeriais, pažymimi ištrynimui;

quit

Po komandos quit seka atnaujinimo fazė. Tuo metu pašto serveris ištrina pažymėtus pranešimus ir uždaro POP3 sesiją.

POP3 protokolas neturi galimybių sukurti nutolusių direktorių serveryje. Tai nepatogu vartotojui, kuris naudojasi e-pašto dėžute iš daugelio darbo vietų, ir nori turėti direktorių struktūrą nutolusiame serveryje.

Ši problema buvo išspręsta sukuriant IMAP (Internet Message Access Protocol). RFC 2060. IMAP serveryje, kiekviena žinutė yra susieta su direktorija. Šis protokolas turi komandas, leidžiančias sukurti direktorijas serveryje, perkelti pranešimus tarp direktorių, taip pat vykdyti paiešką nutolusiose direktorijose.

Beveik kiekvienas pašto serveris turi galimybę vartotojams teikti e-pašto paslaugas Web'o pagrindu. Tuomet e-pašto pranešimai siunčiami ir gaunami iš pašto serverių naudojantis WEB naršykle, HTTP protokolu (ne SMTP, IMAP ar POP3). Tarp pašto serverių pranešimų siuntimas išlieka SMTP protokolu. Daug WEB pagrindu dirbančių pašto serverių naudoja IMAP serverį, tam kad palaikytų nutolusias direktorijas.

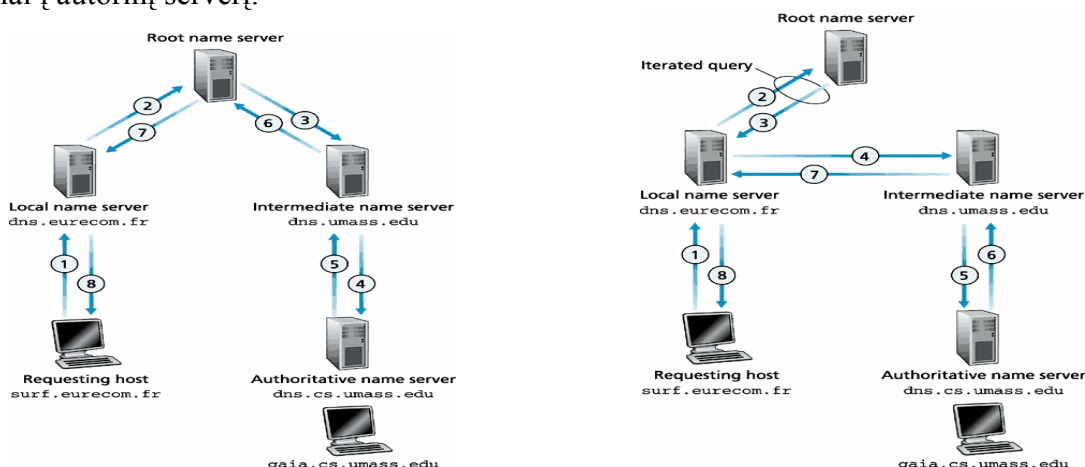
DNS servisas

Interneto įrenginiai yra identifikuojami dviem būdais: įrenginio vardu (hostname) ir IP adresu. Įrenginio vardai yra lengvai įsimenami ir vartojami žmonių (pvz. www.su.lt, www.delfi.lt). Įrenginių vardus su IP adresais susieja DNS (Domain Name System) servisas. RFC 1034, RFC 1035. DNS – tai 1) išskirstyta duomenų bazė įdiegta vardų serverių hierarchijoje; 2) taikomojo lygmens protokolas. DNS protokolas naudoja UDP ir porto numerį 53. DNS servisas plačiai naudojamas kitų taikomųjų programų (HTTP, SMTP, FTP) vartotojo įvestam įrenginio vardui paversti į IP adresą.

Paprasčiausia būtų turėti vieną vardų serverį, į kurį kreiptųsi visi klientai. Tačiau būtų susiduriama su sekančiomis problemomis: jei vardų serveris sugestų, internetas nebefunkcionuotų; vardų serveris turėtų aptarnauti visas DNS užklausas iš begalės interneto įrenginių; vienintelis vardų serveris nebūtų pastatytas vienodu atstumu nuo visų vartotojų; vardų serveris turėtų laikyti įrašus visiems interneto įrenginiams.

DNS servisas naudoja daug vardų serverių, kurie yra suskirstyti pagal hierarchiją. Yra trijų tipų vardų serveriai: vietiniai, šakniniai ir autoriniai. Kiekvienas ISP turi vietinį vardų serverį. Vartotojo DNS užklausa iš pradžių keliauja šiam vardų serveriui. Paprastai vietinis vardų serveris yra nutolęs per kelis maršrurizatorius. Jei vietinis vardų serveris neturi reikiamo įrašo, jis kreipiasi į

vieną iš dvylikos šakninių vardų serverių. Jei šakninis vardų serveris turi reikiamą įrašą, jis gražina įrašą vietiniam vardų serveriui, šis įrašą išsaugo ir gražina reikalavusiam klientui. Kiekvienas įrenginys yra užregistruojamas autoriniuose vardų serveriuose. (reikalaujama kaip min dvejuose). Jei šakninis vardų serveris neturi reikalaujamo įrašo, tuomet jis kreipiasi į tarpinį autorinį ar tiesiogiai į autorinį serverį.



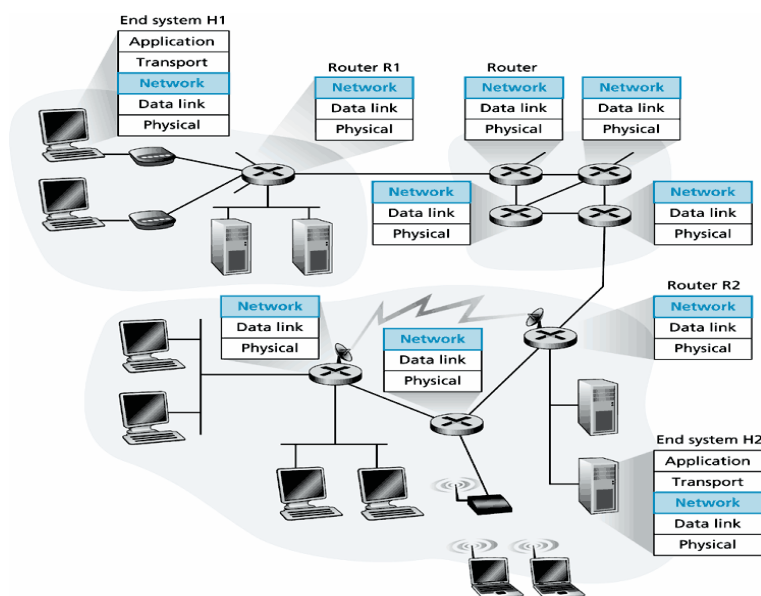
Rekursyvinės ir iteratyvinės užklausos.

DNS įrašo formatas: (Vardas Reikšmė Tipas TTL)

Jei Tipas A, tuomet Vardas – Įrenginio vardas, Reikšmė – IP adresas. Pvz.: (www.su.lt 193.219.168.10 A);

Jei Tipas NS, tuomet Vardas – Domenas (su.lt) reikšmė -

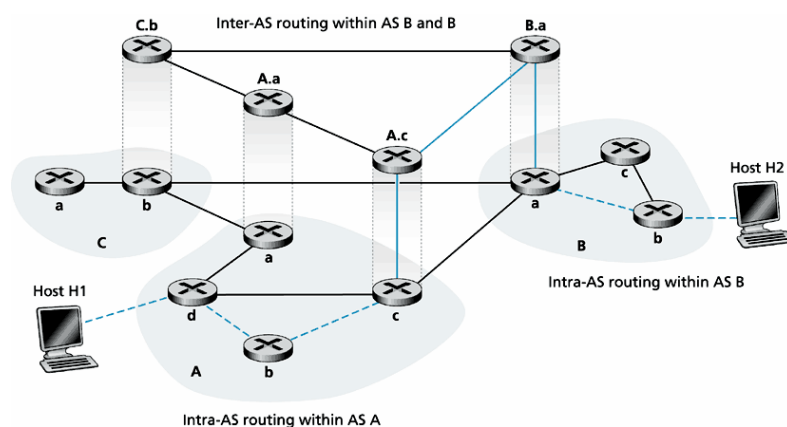
Tinklinis lygmuo



Tinklinio lygmens paskirtis perduoti siuntėjo paketus gavėjui. Trys pagrindinės tinklinio lygmens funkcijos: kelio nustatymas. Tinklinis lygmuo, naudodamasis maršrutizavimo algoritmais nustato kelią, kuriuo bus perduodami paketai; persiuntimas. Paketas atėjęs į maršrutizatorių turi būti persiustas į reikiamą išėjimą; sujungimo sudarymas. Kai kurios tinklų architektūros reikalauja iš pradžių sudaryti sujungimą tarp kelyje esančių maršrutizatorių prieš pradedant siųsti duomenis. Pvz. ATM. Interneto tinklinis lygmuo tokio sujungimo nereikalauja.

Maršrutizavimo algoritmų paskirtis iš duoto maršrutizatorių rinkinio ir juos jungiančių sąsajų surasti “minimalios kainos” (vėlinimas, kaina, apkrovimo lygis) kelią. Maršrutizavimo algoritmus galime suskirstyti į globalius ir decentralizuotus. Globaliuose min-kainos kelias yra skaičiuojamas žinant visą tinklo topologiją ir sąsajų kainas. Link state algoritmas. Decentralizuotose maršrutizatoriai turi informaciją tik apie fiziškai prijungtus maršrutizatorius ir kainas iki jų. Distance vector algoritmas. Kitas m a skirstymas: statiniai arba dinaminiai. Statiniuose maršrutizavimo algoritmuose keliai keičiasi lėtai laiko bėgyje (pvz. administratorius pakeičia maršrutizatoriaus persiuntimo lentelę). Dinaminiuose algoritmuose keliai yra atnaujinami arba periodiškai arba pasikeitus tinklo apkrovimui ar topologijai.

Internete egzistuoja hierarchinis maršrutizavimas. Internetas susideda iš autonominių sistemų (AS), kurios viduje veikiantis maršrutizavimo protokolas, vadinamas intra-AS protokolu. Skirtingose AS gali veikti skirtingi maršrutizavimo protokoliai. Kiekvienoje AS yra specialūs M, vadinami gateway M. Šis M yra atsakingas už paketų perdavimą už AS ribų. Šiuose M veikia intra-AS maršrutizavimo protokolas su visais kitais m iš AS, ir inter-AS su kitų AS gateway maršrutizatoriais.



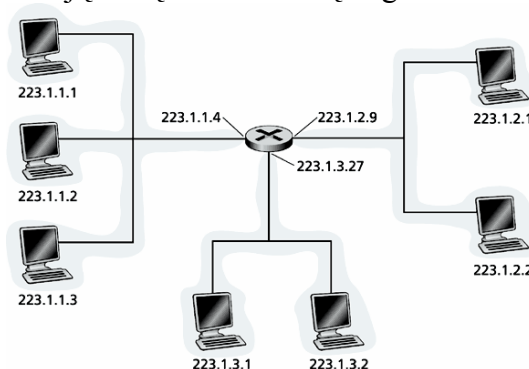
Intra-AS maršrutizavimo protokoliai: RIP (Routing Information Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol). Inter-AS – BGP4 (Border Gateway Protocol v 4).

Ipv4 adresavimas

IP adresas yra 32 bitų ilgio (4 baitai), taigi galimi 2^{32} IP adresai. IP adresai užrašomi dešimtaine su tašku forma, kur kiekvienas baitas yra išreikštas dešimtainiu skaičiumi ir atskirtas tašku. Pvz. IP adresas 193.32.216.9 išreikštas dvejetainine forma atrodytų sekančiai:

11000001 00100000 11011000 00001001

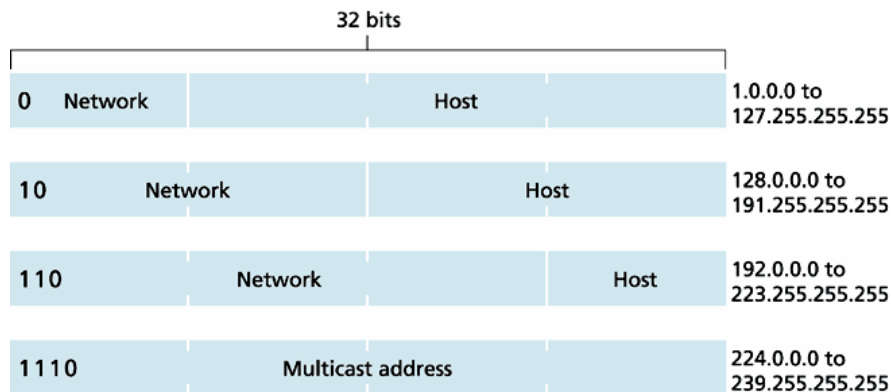
IP adresas susideda iš dviejų dalių: tinklo ID ir įrenginio ID.



Šio paveikslo kairėje pusėje esantys įrenginiai ir maršrutizatoriaus sąsaja 223.1.1.4 turi IP adreso formą 223.1.1.xxx. Tai yra, jie turi bendrus 24 vyriausius IP adreso bitus. Šie bendri bitai yra

vadinami IP adreso tinklo dalimi. Šis tinklas turės savo adresą 223.1.1.0/24, kur užrašas “/24” vadinamas tinklo kauke arba tinklo prefiksu, ir reiškia kad 24 vyriausi bitai yra skirti tinklo identifikacijai. Taigi paveiksle bus trys tinklai 223.1.1.0/24, 223.1.2.0/24, 223.1.3.0/24. Likę 8 bitai bus skirti įrenginio identifikavimui. Skaičiuojant įrenginių skaičių, iš bendro jų skaičiaus reikia atimti dvejetą, nes įrenginio numeris su visais nulinais bitais atitinka viso tinklo adresą, o su vienetiniiais – transliacijos (broadcast) visam tinklui adresą.

Pradiniai Interneto adresai buvo suskirstyti į penkias klases.



D klasės adresai yra skirti grupiniam siuntimui. Penktoji IP adresų klasė prasidedanti bitais 11110 buvo rezervuota.

Reikalavimas, kad tinklo daliai būtų skirti 1,2 ar 3 baitai, pasirodė neoptimalus. Tarkime, kad turime įmonę kur reikia adresuoti 2000 įrenginių. C klase galime adresuoti $2^8 - 2 = 254$ įrenginius, taigi per mažai šiai įmonei. Reikės naudoti B klasės adresus, kuriais galime adresuoti $2^{16} - 2 = 65534$ įrenginius. Vadinasi daugiau nei 63000 adresų liks neišnaudotų, kurie galėtų būti priskirti kitoms organizacijoms.

1993 metais IETF inžinierių darbo grupė pateikė CIDR (Classless Interdomain Routing) tinklo adresus. Pagal CIDR IP adreso tinklo daliai gali būti skirta bet koks bitų skaičius. Aukščiau pateiktame pavyzdyje organizacijai būtų galima skirti $2^{11} = 2048$ adresų bloką, kurie turėtų formą a.b.c.d/21.

ICANN (Internet Corporation for Assigned Names and Numbers) organizacija skirsto IP adresų erdvę Interneto serviso tiekėjams. Taip pat ši organizacija yra atsakinga už srities (domain) vardų suteikimą.

ISP savo ruožtu skirsto jai priskirtą adresų bloką aptarnaujamom organizacijoms. Pvz.

ISP adresų blokas	200.23.16.0/20	<u>11001000 00010111 00010000 00000000</u>
0 Organizacija	200.23.16.0/23	<u>11001000 00010111 00010000 00000000</u>
1 Organizacija	200.23.18.0/23	<u>11001000 00010111 00010010 00000000</u>
2 Organizacija	200.23.20.0/23	<u>11001000 00010111 00010100 00000000</u>
3 Organizacija	200.23.22.0/23	<u>11001000 00010111 00010110 00000000</u>
.....		
7 Organizacija	200.23.30.0/23	<u>11001000 00010111 00011110 00000000</u>

Organizacija gavusi adresų bloką, jį gali suskaidyti į potinklius. Rašant adresą su prefiksu nurodoma kiek bitų skiriama tinklui ir potinklui.

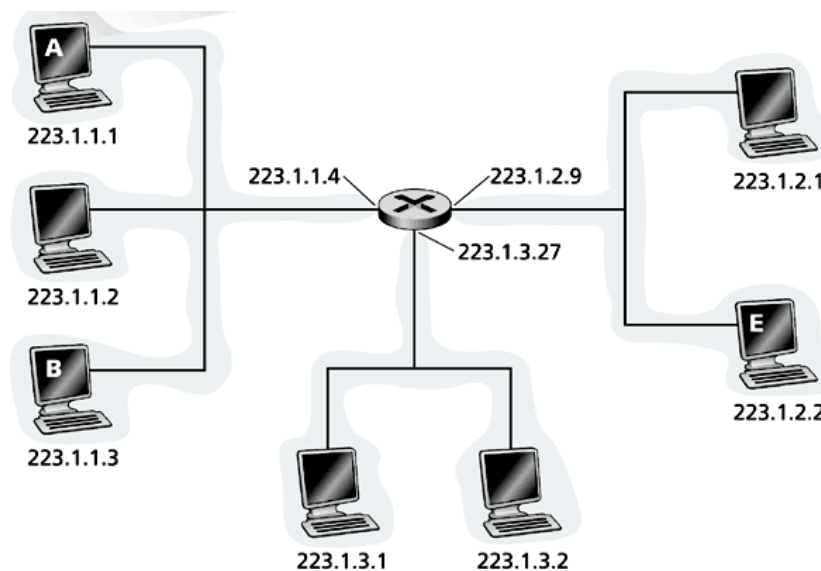
Maršrutizatorių sąsajoms IP adresai yra suteikiami rankiniu būdu. Galiniams įrenginiams IP adresai gali būti suteikiami rankiniu būdu arba automatiškai panaudojant DHCP(Dynamic Host Configuration Protocol) protokolą.

IP paketo siuntimas

Supaprastintas IP paketas pavaizduotas paveiksle. Kiekvienas IP paketas turi šaltinio IP adresą, ir gavėjo IP adresą. Šių dviejų laukų reikšmės nekinta, paketui keliaujant tinklu.

Misc fields	Source IP address	Destination IP address	Data
-------------	-------------------	------------------------	------

Kaip tinklinis lygmuo perduoda siuntėjo siųstą paketą gavėjui? Atsakymas į šį klausimą priklauso nuo to ar siuntėjas ir gavėjas priklauso tam pačiam tinklui. Tarkime, kad turime tinklus pavaizduotus paveiksle.



Sakykime, kad įrenginys A nori siųsti IP paketą įrenginiui B, kuris priklauso tam pačiam tinklui 223.1.1.0/24 kaip ir A. Visų pirma, A analizuoja savo persiuntimo lentelę (forwarding table):

Forwarding table in A		
Dest. network	Next router	Nhops
223.1.1.0/24		1
223.1.2.0/24	223.1.1.4	2
223.1.3.0/24	223.1.1.4	2

Šioje lentelėje, A randa įrenginio B tinklą 223.1.1.0/24 atitinkantį įrašą. Persiuntimo lentelė rodo, kad žingsnių skaičius (Nhops), per kurį bus nusiųstas paketas, lygus vienetui. Iš čia A sužino, kad A ir B priklauso tam pačiam tinklui ir paketo nereikės siųsti per maršrutizatorių. Įrenginio A tinklinis lygmuo perduoda IP paketą kanaliniam lygmeniui, kuris yra atsakingas už paketo perdavimą įrenginiui B. Kaip vyksta kanalinio lygmens persiuntimas, apžvelgsime vėlesniuose skyriuose.

Išnagrinėkime kitą atvejį, kai A siunčia IP paketą E: siuntėjas ir gavėjas priklauso skirtingiems tinklams. A persiuntimo lentelėje randa įrašą, atitinkantį gavėjo E tinklą 223.1.2.0/24. Žingsnių skaičius lygus dviem, vadinasi gavėjas priklauso kitam tinklui ir siuntimas turės būti

vykdomas per maršrutizatorių. Persiuntimo lentelė nurodo, kad norint pasiekti tinklo 223.1.2.0/24 įrenginius, IP paketą reikia siųsti į maršrutizatoriaus sąsają 223.1.1.4. Taigi paketas perduodamas kanaliniam lygmeniui, kuriam nurodoma paketą siųsti sąsajai 223.1.1.4. IP paketo gavėjo adreso laukas išlieka nepakitęs, tai yra jis bus lygus 223.1.2.2, o ne 223.1.1.4.

IP paketas dabar yra maršrutizatoriuje, ir jo darbas persiųsti paketą gavėjo link. Maršrutizatorius taip pat turi persiuntimo lentelę:

Forwarding table in router			
Dest. network	Next router	Nhops	Interface
223.1.1.0/24	—	1	223.1.1.4
223.1.2.0/24	—	1	223.1.2.9
223.1.3.0/24	—	1	223.1.3.27

Ją analizuodamas, maršrutizatorius randa įrašą atitinkantį gavėjo E tinklą 223.1.2.0/24. Lentelė rodo, kad norint pasiekti šį tinklą, paketą reikia persiųsti į maršrutizatoriaus sąsają 223.1.2.9. Kadangi žingsnių skaičius lygus vienam, vadinasi maršrutizatoriaus sąsaja 223.1.2.9 ir E yra to paties tinklo įrenginiai. Paketas perduodamas kanaliniam lygmeniui, kuris nusiunčia paketą galutiniam gavėjui E.

Maršrutizatoriaus persiuntimo lentelėje stulpelis sekantis maršrutizatorius (Next Router) tuščias, kadangi visi tinklai (223.1.1.0/24, 223.1.2.0/24, 223.1.3.0/24) yra tiesiogiai sujungti su maršrutizatoriumi. Jeigu tarp įrenginių A ir E būtų du maršrutizatoriai, tuomet pirmojo, kelyje tarp A ir E įrenginių, maršrutizatoriaus lentelėje atitinkamo įrašo žingsnių skaičius būtų lygus dviem bei kaip sekantis maršrutizatorius būtų nurodytas antrasis.

IPv4 paketo formatas

IP paketo antraštė pavaizduota **pav.**

32 bits				
Version	Header length	Type of service	Datagram length (bytes)	
16-bit Identifier			Flags	13-bit Fragmentation offset
Time-to-live	Upper-layer protocol		Header checksum	
32-bit Source IP address				
32-bit Destination IP address				
Options (if any)				
Data				

Versija (Version) – šie 4 bitai yra skirti IP versijos numeriui. Skirtingų IP versijų yra nevienodos antraštės. Žinodamas IP versiją, tinklo įrenginys gali sėkmingai interpretuoti kitus

antraštės laukelius. Populiariausia šiuo metu yra ketvirtoji IP versija IPv4 (0100). Ateityje bus naudojama naujosios kartos IPv6 (0110). Jei tinklo įrenginys nesugeba dirbti su priimto paketo versija, tuomet paketas yra atmetamas.

Antraštės ilgis (Header length) – kadangi IP paketas gali turėti skirtingą papildomų laukelių (Options) skaičių, šis 4 bitų laukelis skirtas nurodyti, kur baigiasi IP antraštė ir prasideda duomenys. Antraštės ilgis skaičiuojamas 32 bitų žodžiais. Minimalus antraštės ilgis 5 žodžiai (20 baitų), kai nėra papildomų laukelių; maksimalus – 6 žodžiai (24 baitai).

Serviso tipas (Type of service) – šio 8 bitų lauko, pirmieji trys bitai nurodo IP paketo prioritetą: 0 – normalus, 7 – didžiausias prioritetas. Esant apkrautam tinklui yra naudinga išskirti IP paketus pagal svarbą. Pavyzdžiui, tinklo valdymo paketus (ICMP) nuo paprastų duomenų paketų (pvz. HTTP), ar realaus laiko protokolų paketus (IP telefonija) nuo nerealaus laiko paketų (pvz. FTP). Kuo didesnis prioritetas tuo duomenys yra svarbesni, ir tuo teoriškai šis paketas turėtų greičiau būti nusiųstas adresatui. Praktiškai šio laukelio reikšmę maršrutizatoriai ignoruoja, tuomet visi paketai turi vienodą prioritetą.

IP paketo ilgis (Datagram length) – IP paketo įskaitant antraštę ilgis baitais. Kadangi šis laukelis yra 16 bitų ilgio, teoriškai IP paketas gali būti 65535 baitų ilgio. Praktiškai IP paketai retai viršija 1500 baitų, ir dažnai yra ribojami iki 576 baitų.

Identifikatorius (Identifier) – IP paketo siuntėjas sukuria unikalų 16 bitų identifikatorių kiekvienam IP paketui. Jei IP paketas bus fragmentuojamas, visi IP paketo fragmentai turės tą patį identifikatorių.

Vėliavos (Flags) – tai trijų bitų laukelis, iš kurių vyriausiasis nenaudojamas. Kiti du bitai vadinami DF (Don't Fragment) bei MF (More Fragments). Jei DF vėliavėlė lygi vienetui, tuomet IP paketo fragmentacija yra negalima. Jei IP paketas siunčiant į kanalą būtinai turi būti suskaidytas ir DF=1, tuomet paketas atmetamas ir siuntėjui išsiunčiamas klaidos pranešimas. Jei MF=1, tai po šio paketo seka fragmentas –ai, priklausantys tam pačiam pradiniam IP paketui. Paskutinis fragmentas iš originalaus IP paketo turės vėliavėlę MF=0.

Fragmento ofsetas (Offset) - kadangi IP paketai gali ateiti neeiliskumo tvarka, tai kartu su vėliavėlė MF=1 yra naudojamas 13 bitų ofsetas, nurodantis fragmento vietą originaliaame IP pakete. Ofsetas visuomet nurodomas IP paketo pradžios atžvilgiu.

TTL (Time to live) – šis aštuonių bitų laukelis skirtas tam, kad IP paketas necirkuliuotų amžinai tinkle (pvz. dėl maršrutizatorių kilpų). Šio laukelio reikšmė yra mažinama vienetu, kiekviename maršrutizatoriuje. Jei TTL reikšmė pasidaro lygi nuliui, IP paketas sunaikinamas, o siuntėjui išsiunčiamas ICMP pranešimas.

Protokolas (Protocol) – aštuonių bitų laukelis, nurodantis aukštesnio lygio protokolą, kuriam turi būti nusiųsti IP paketo duomenys. Pvz.: reikšmė 1 – duomenys skirti ICMP, 6 – TCP, 17 – UDP. Visas galimas šio laukelio reikšmės galima rasti standarte RFC 1700.

Kontrolinė suma (Checksum)- 16 bitų laukelis, skirtas antraštės klaidų aptikimui. IP paketo antraštė suskaidoma 16 bitų žodžiais, ir jų vieneto komplementinė suma įrašoma į šį laukelį. Kadangi TTL reikšmė keičiasi kiekviename maršrutizatoriuje, tai ir kontrolinė suma turi būti perskaičiuota iš naujo. Aptikę klaidą maršrutizatoriai paprastai sunaikina paketą.

Siuntėjo ir gavėjo IP adresai (Source and Destination IP addresses) – šie laukai turi 32 bitų siuntėjo ir gavėjo IP adresus. Jie yra sukuriami siuntėjo, ir išlieka nepakitę viso maršruto metu.

Papildomi laukeliai (Options) – kintamo ilgio, kurie yra neprivalomi.

Duomenys (Data) – šiame laukelyje patalpintas transportinio lygmens (TCP ar UDP) segmentas. Taip pat jame gali būti ICMP pranešimas.

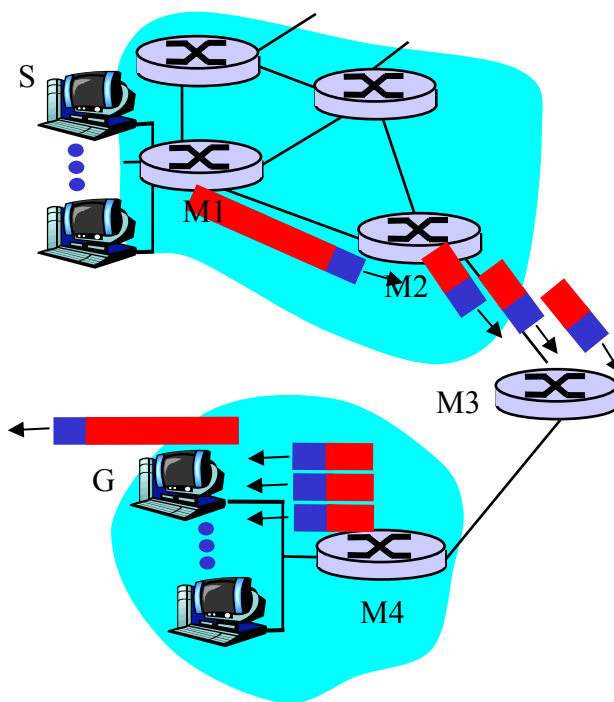
IP paketo fragmentacija

Ne visi kanalinio lygmens protokolai gali perduoti to paties dydžio paketus. Pvz. Etherneto paketai gali perduoti ne daugiau kaip 1500 baitų duomenų, o daugelis WAN kanalinio lygmens – ne daugiau kaip 576 baitus. Maksimalus duomenų kiekis, kurį gali perduoti kanalinis lygmuo vadinamas MTU (Maximum Transfer Unit). IP paketo dydis yra ribojamas kanalinio lygmens MTU, kadangi IP paketas yra įdedamas į kanalinio lygmens paketą (freimą). Problema atsiranda tuomet, kai siuntėjo-gavėjo kelyje yra skirtingi kanalinio lygmens protokolai, ir šie protokolai gali turėti skirtingus MTU.

Jeigu IP paketas yra didesnis nei kanalinio lygmens protokolo MTU, jis yra skaidomas į du ar daugiau paketų, vadinamų fragmentais. Transportinio lygmens protokolas (TCP ar UDP) tikisi priimti pradinį IP paketą, todėl defragmentacija (pradinio IP paketo sudarymas iš fragmentų) yra vykdoma tinkliniame lygmenyje. Kad neapkrauti maršrutizatoriaus papildomomis funkcijomis, defragmentaciją vykdo tik gavėjo įrenginys.

Kai gavėjo įrenginys priima IP paketų eilę, jis turi nustatyti ar kurie nors iš šių paketų yra originalaus IP paketo fragmentai ir jei yra, tai kuris iš fragmentų yra paskutinis ir kaip iš fragmentų atstatyti pradinį IP paketą. Šiam tikslui IPv4 kūrėjai į IP paketo antraštę įtraukė laukelius: identifikatorių, vėliavas, ofsetą. Sukurtas IP paketas turi unikalų identifikatorių. Jei maršrutizatoriui reikės skaidyti paketą, visi fragmentai turės vienodą pradinio IP paketo identifikatorių, bei šaltinio ir gavėjo adresus. Pagal šiuos identifikatorius gavėjas gali spręsti kurie fragmentai priklauso tam pačiam pradiniam IP paketui. Kadangi IP servisas yra nepatikimas, vienas ar daugiau fragmentų gali niekada nepasiekti gavėjo. Dėl šios priežasties gavėjas išitikinimui, kad priėmė paskutinį fragmentą, šio paskutinio fragmento vėliavėlė MF bus lygi 0, kai visų kitų fragmentų – vienetui. Taip pat tam kad gavėjas nustatytų ar trūksta kokio nors fragmento (ar galbūt atstatytų fragmentų eiliškumą), naudojama ofseto reikšmė, nurodanti fragmento vietą pradiniam IP pakete.

Paveiksle iliustruotas pavyzdys. Siuntėjas S siunčia 4000 baitų IP paketą gavėjui G. Maršrutizatorių M2 - M3 sąsajos kanalinio lygmens protokolo MTU 1500 baitų. Vadinasi pradinis IP paketas bus suskaidytas į tris fragmentus, kurie taip pat vadinami IP paketais.



Tarkime, kad pradinio IP paketo identifikatorius lygus 777. Tuomet supaprastintai šis paketas atrodys sekančiai:

...	ilgis 4000	ID 777	MF 0	offsetas 0	...
-----	---------------	-----------	---------	---------------	-----

Sudaryti trys nauji fragmentai atrodys sekančiai

...	ilgis 1500	ID 777	MF 1	offsetas 0	...
-----	---------------	-----------	---------	---------------	-----

...	ilgis 1500	ID 777	MF 1	offsetas 1480	...
-----	---------------	-----------	---------	------------------	-----

...	ilgis 1040	ID 777	MF 0	offsetas 2960	...
-----	---------------	-----------	---------	------------------	-----

IP paketo duomenys yra siunčiami transportiniam lygmeniui tik tuomet, kai yra pilnai surinktas pradinis paketas. Jei nors vieno iš fragmentų trūksta, IP paketas prarandamas.

ICMP

Galiniai įrenginiai, maršrurizatoriai naudoja ICMP (Internet Control Message Protocol) protokolą tinklinio lygmens informacijai perduoti. Šis protokolas aprašytas standarte RFC 792. Tipiškas ICMP panaudojimas – informacijos apie klaidas perdavimas.

ICMP dažnai laikomas IP dalimi, tačiau ICMP architektūriškai yra aukščiau už IP, nes ICMP pranešimai yra siunčiami IP paketu. Tai yra ICMP pranešimas yra nešamas kaip IP duomenys, taip pat, kaip TCP ar UDP segmentas. Kai tinklo įrenginys priima IP paketą, kuriame nurodyta jog aukštesnio lygmens protokolas yra ICMP, jis nusiunčia paketą ICMP.

ICMP pranešimai susideda iš tipo ir kodo laukų, bei pirmųjų 8 IP paketo, kuris iššaukė ICMP pranešimo sugeneravimą, baitų (tam, kad siuntėjas galėtų atskirti, kuris paketas iššaukė ICMP pranešimo sugeneravimą). Keletas pasirinktų ICMP pranešimų pateikti žemiau.

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

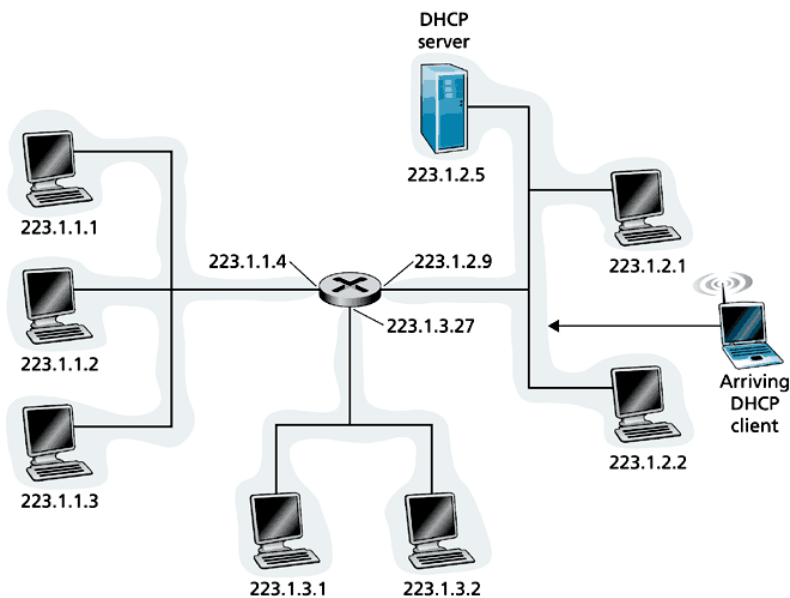
ICMP pranešimai naudojami ne tik informacijos apie klaidas perdavimui. Gerai žinoma Ping programa naudoja ICMP. Pingas siunčia ICMP pranešimą (tipas 8, kodas 0) nurodytam įrenginiui. Pastarasis gražina ICMP pranešimą, kurio tipas 0, kodas 0. Traceroute programa taip pat naudoja ICMP. Tam kad sužinoti maršrutizatorių vardus ir adresus, esančius kelyje iki nurodyto įrenginio, Traceroute siunčia visą eilę įprastų IP paketų nurodytam tinklo įrenginiui. Pirmojo šių IP paketų TTL reikšmė lygi vienetui, antrojo – dvejetui ir taip toliau. Šaltinis kiekvienam paketui paleidžia taimerį. Kai n-tasis IP paketas pasiekia n-tąjį maršrutizatorių, TTL reikšmė tampa lygi nuliui. Pagal IP taisykles, maršrutizatorius šį paketą sunaikina, o siuntėjui išsiunčia ICMP pranešimą (tipas 11, kodas 0). Šiame pranešime yra ir maršrutizatoriaus vardas, ir jo IP adresas. Kai šaltinis priima ICMP pranešimą iš n-tojo maršrutizatoriaus, jis sužino RTT laiką, maršrutizatoriaus vardą bei adresą.

DHCP

DHCP (Dynamic Host Configuration Protocol) [RFC 2131] protokolas priskiria tinklo įrenginiui IP adresą automatiškai, kai tik įrenginys prisijungia prie tinklo. Dėl to šis protokolas dažnai vadinamas plug-and-play protokolu. Be IP adreso įrenginys papildomai sužino tinklo kaukę, gateway maršrutizatoriaus adresą, DNS serverio adresą.

Tinklo administratorius gali sukonfigūruoti DHCP serverį taip, kad kiekvieną kartą jungiantis prie tinklo įrenginiui būtų priskirtas pastovus IP adresas (pagal MAC adresą). Tačiau organizacija gali neturėti užtektinai IP adresų, kad kiekvienam įrenginiui būtų priskirtas pastovus adresas. Tokiu atveju DHCP serveris įrenginiams priskiria laikinus IP adresus. Trakime, kad turime ISP, kuris aptarnauja 2000 įrenginių, tačiau ne daugiau 400 iš jų būna aktyvūs vienu metu. Kad aptarnauti visus 2000 įrenginių, ISP nereikia turėti 2000 IP adresų bloko. Naudojant DHCP serverį, ISP užteks tiks 512 adresų bloko (pvz.: 200.23.30.0/23). Kai įrenginys jungiasi ar palieka tinklą, DHCP serveriui reikia atnaujinti galimų IP adresų sąrašą. Kai įrenginys jungiasi prie tinklo, DHCP serveris jam siūlo IP adresą iš galimo sąrašo, o įrenginiui paliekant tinklą, jo naudotas adresas įtraukiamas į šį sąrašą.

DHCP yra kliento-serverio protokolas. Klientas tipiškai yra naujai prisijungęs įrenginys, kuriam reikia informacijos, kaip sukonfigūruoti tinklą (IP adresas, tinklo kaukė, gateway, DNS serveris). Paprasčiausiu atveju, kiekvienas tinklas turi DHCP serverį. Jei tinkle nėra DHCP serverio, tuomet yra reikalingas DHCP agentas (paprastai juo būna maršrutizatorius), kuris žino šio tinklo DHCP serverio adresą. Paveiksle DHCP serveris prijungtas prie tinklo 223.1.2.0/24 ir maršrutizatorius, kuris tarnauja kaip DHCP agentas klientams iš 223.1.1.0/24, 223.1.3.0/24 tinklų.

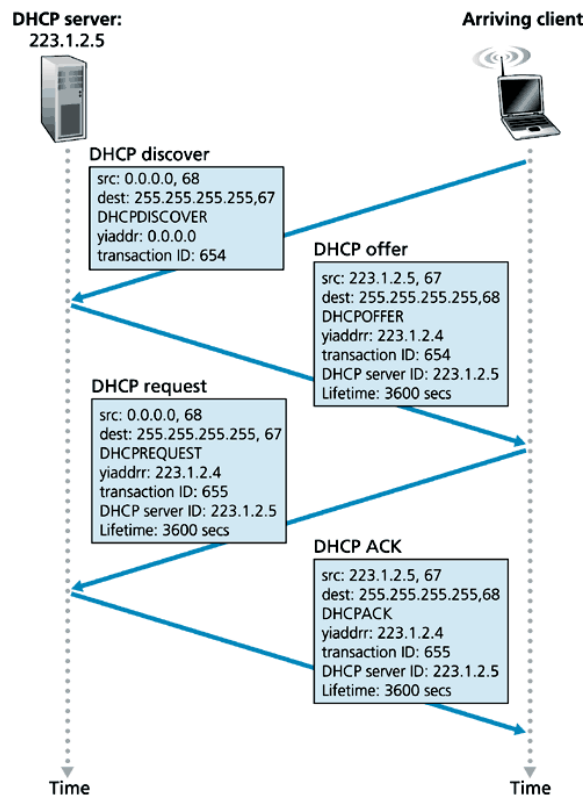


Naujai prisijungusiam klientui, DHCP protokolas yra keturių žingsnių procesas:

- DHCP serverio paieška. Pirmoji naujai prisijungusio kliento užduotis yra surasti DHCP serverį, su kuriuo toliau bendraus. Tai yra atliekama DHCP discover pranešimu, kurį klientas siunčia UDP paketu į 67 portą. Bet kam šis pranešimas turi būti adresuotas? Juk klientas nežino net tinklo prie kurio jungiasi, o tuo labiau DHCP serverio tame tinkle IP adreso. Taigi, DHCP klientas transliuoja IP paketą, su DHCP discover pranešimu, naudodamas transliacijos (broadcast) adresą 255.255.255.255, o savo adresą nurodo kaip 0.0.0.0. Šį pranešimą priims visi įrenginiai, priklausantys tam pačiam tinklui, o tuo pačiu ir DHCP serveris (ir/arba DHCP agentas). Discover pranešimas turi operacijos identifikatorių tam tikslui, kad DHCP serveris identifikuotų įrenginį, nes kol kas jis dar neturi IP adreso.
- DHCP serverio pasiūlymas. DHCP serveris priėmęs DHCP discover pranešimą, atsako klientui DHCP pasiūlymo pranešimu. Kadangi tinkle gali būti keletas DHCP serverių, tai klientas gali sulaukti keleto pasiūlymų. Kiekvienas serverio pasiūlymo pranešimas susideda iš operacijos ID, siūlomo IP adreso, tinklo kaukės ir adreso galiojimo laiko.
- DHCP užklausa. Klientas pasirinkęs iš vieno ar daugiau pasiūlymų, atsako pasirinktam serveriui DHCP užklauso pranešimu, gražindamas siūlytus konfigūracijos parametrus.
- DHCP ACK. Serveris atsako į DHCP užklauso pranešimą DHCP ACK (patvirtinimo) pranešimu, patvirtindamas reikalautus parametrus.

Kai tik klientas priima DHCP ACK pranešimą, kliento-serverio sąveika yra užbaigta ir klientas gali naudotis priskirtais parametrais IP adreso galiojimo laiką. DHCP turi mechanizmą, kuris leidžia pratęsti IP adreso galiojimo laiką.

DHCP kliento-serverio sąveika pavaizduota paveiksle.



Mobilumo atžvilgiu, DHCP protokolas turi trūkumą. Kai mobilus klientas jungiasi prie įvairių tinklų, kiekviename tinkle jam bus suteiktas vis naujas IP adresas. Taigi toks įrenginys niekuomet neturės pastovaus IP adreso. Ši problema buvo išspręsta papildant IP infrastruktūrą nauju moduliu – mobile IP, kuris leidžia mobiliam įrenginiui turėti vieną pastovų IP adresą, keičiant tinklus.

Ipv6

Didžiausias interneto plėtroje IPv4 trūkumas – mažas adresų kiekis. Nors teoriškai IPv4 adresų yra $2^{32}=4,294,967,296$, tačiau gali būti, kad IPv4 adresų pritrūksime jau už kelių metų.

IP 6 versija (IPv6) – tai nauja interneto protokolo versija, sukurta kaip tęsinys savo pirmtako IPv4 (aprašyto standarte RFC 791).

Skirtumus tarp šių dviejų protokolų galima suskirstyti į sekančias kategorijas:

- **Išplėstos adresavimo galimybės.** Vietoje 32 bitų kiekvienas IPv6 adresas turi 128 bitus. Tai įgalina palaikyti daugiau hierarchijos lygių, turėti žymiai daugiau adresuojamų mazgų ir supaprastina adresų auto-konfigūraciją. Įvestas naujas adreso tipas – „anycast address“.
- **Supaprastinta paketo antraštė.** Kai kurie senojo protokolo IPv4 antraštės laukai buvo visiškai pašalinti arba padaryti neprivalomi. Visa tai sumažina apdorojimo laiką maršrutizatoriuose ir paspartina duomenų perdavimą, kadangi sumažėja antraštės ilgis.
- **Papildomos antraštės.** Priešingai nei IPv4, kuris naudoja vienintelį antraštės formatą visiems paketams, IPv6 šifruoja informaciją į atskiras antraštes. Antraštė susideda iš

pagrindinės IPv6 antraštės, po kurios yra kelios (arba nėra iš viso) papildomos antraštės, po kurių seka duomenys.

- **Srauto žymėjimo galimybė.** Tai naujas antraštės tipas, kuris leidžia žymėti paketus, reikalaujančius specialaus apdorojimo, pvz. realaus laiko serviso.
- **Išplečiamas protokolas.** IPv6 nenustato visų galimų protokolo savybių. Vietoje to, projektuotojai pasiūlė schemą, kuri leidžia siuntėjui pridėti papildomos informacijos į paketą. Išplėtimo schema daro IPv6 lankstesniu, nei IPv4 ir reiškia, kad naujos savybės gali būti pridėtos į projektą, jei to reikia.
- **Autorizavimo bei slaptumo galimybės.** IPv6 protokole yra numatytos autorizavimo, duomenų vientisumo ir konfidencialumo (neprivaloma) galimybės.

1 paveiksle pateiktas IPv6 antraštės formatas.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
Version				Traffic Class								Flow Label																				1
Payload Length																Next Header								Hop Limit								2
Source Address																																3
																																4
																																5
																																6
																																7
Destination Address																																8
																																9
																																10

1 pav. IPv6 antraštės formatas

- **Version** – 4 bitų laukelis, skirtas IP versijos numeriui (0110).
- **Traffic Class** – (8 bitai) naudojamas IPv6 paketams priskirti skirtingus prioritetus.
- **Flow label** – (20 bitų) laukelis naudojamas duomenų srauto tipui pažymėti, kurie reikalauja specialaus apdorojimo. Pavyzdžiui video ar garso perdavimas priklauso srautui. Kai tuo tarpu failų perdavimas (file transfer) ar paštas nelaikomas srautu.
- **Payload Length** - (16 bitų) sveiko tipo skaičius, nurodantis informacijos kiekį baitais, sekančios po fiksuotos 40 baitų antraštės. Plėtinio antraščių (jei jos yra) dydis yra įskaičiuojamas į šį laukelį.
- **Next Header** – (8 bitai) sekančios antraštės tipas. Jei paketas turi plėtinio antraštę, laukas NEXT HEADER nurodo jos tipą. Jei plėtinio antraštės nėra, laukas NEXT HEADER nurodo paketo nešamų duomenų tipą (TCP, UDP).
- **Hop Limit** – (8 bitai) paketo gyvavimo trukmė (mazgų skaičius). Šio laukelio reikšmė yra dekrementuojama vienetu kiekviename mazge, kurį praeina paketas. Jei ši reikšmė pasiekia nulį, paketas yra sunaikinamas.
- **Source Address** – (128 bitai) IPv6 siuntėjo adresas.
- **Destination Address** – (128 bitai) IPv6 gavėjo adresas.

Lyginant IPv6 antraštę su IPv4 matome, kad išnyko tokie laukeliai:

- **Fragmentacija/Defragmentacija.** Naujasis protokolas nepalaiko fragmentacijos. Jei atėjęs į maršrutizatorių paketas yra per didelis, kad jį būtų galima išsiųsti į išeinantį mazgą, maršrutizatorius paprasčiausiai šį paketą atmeta. O siuntėjui išsiunčia ICMP protokolo klaidos pranešimą „Paketas per didelis“ (Packet Too Big“). Siuntėjas tuomet gali persiųsti paketą, sumažinus jo dydį. Fragmentacija/Defragmentacija – tai laiką užimanti operacija, ir ją perkėlus iš maršrutizatorių į galinius įrenginius žymiai pagreitėja IP paketų persiuntimas.

- **Checksum (kontrolinė suma).** Kadangi transportinio lygio (TCP, UDP), o taip pat fizinio lygio (Ethernet) protokolai skaičiuoja kontrolinę sumą, naujos IP versijos kūrėjai jos nematė kaip būtinos. Dar viena iš priežasčių, kodėl išnyko kontrolinė suma, tai padidinti IP paketų perdavimo greitį.
- **Options (Nustatymai).** Nustatymų laukelio nebėra standartinėje IPv6 antraštėje. Tačiau šis laukelis visiškai neišnyko. Nustatymų laukelis yra vienas iš galimų papildomų antraščių. Šio laukelio pašalinimas davė fiksuotą 40 baitų IPv6 antraštę.

IPv6 adresas yra 128 bitų ilgio ir gali būti skirtas tiek vienai sąsajai, tiek kelioms. Priklausomai nuo to išskiriami trys adresų tipai:

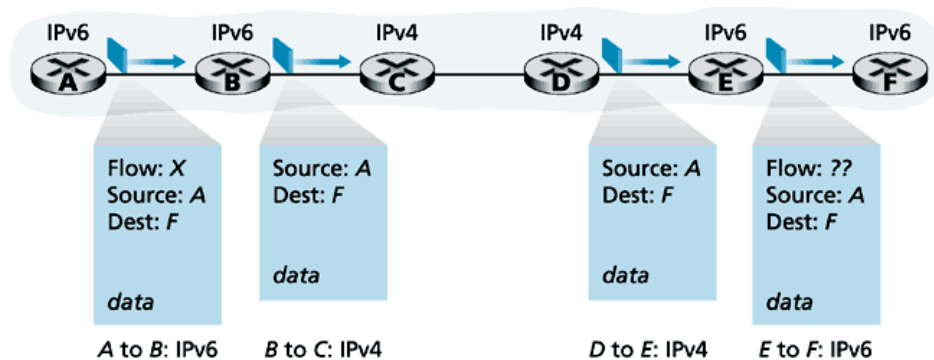
- **Unicast (Vienatipis)** – nurodo vienintelę sąsają. Paketas, pasiųstas šiuo adresu yra nukreipiamas trumpiausiu keliu į nurodytą sąsają.
- **Anycast** – nurodo keletą sąsajų (paprastai priklausančių skirtingiems mazgams). Paketas, pasiųstas šiuo adresu perduodamas artimiausiai (maršrutizavimo protokolo mažiausios „kainos“ atžvilgiu) sąsajai.
- **Multicast (Daugiatipis)** - nurodo keletą sąsajų (paprastai priklausančių skirtingiems mazgams). Paketas išsiųstas šiuo adresu perduodamas visoms sąsajoms su šiuo adresu.

Broadcast adreso funkcijos IPv6 versijoje pakeistos į multicast adresu.

Adresus IPv4 yra įprasta atvaizduoti dešimtainiu skaičiumi su tašku (dotted decimal notation). Kadangi IPv6 adresas turi 128 bitus, tai atvaizduoti 16 dešimtainių skaičių jau yra nebeįmanoma. Todėl IPv6 adresas yra užrašomas šešioliktainiu skaičiumi su dvitaškiais (*Colon Hexadecimal Notation*). Čia kiekviena 16 bitų grupė užrašoma šešioliktainiu skaičiumi, o grupės atskiriamos dvitaškiais. Žemiau pavyzdyje yra pateiktas IPv6 adresas užrašytas abiem būdais:

- 1) 105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255;
- 2) 69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF.

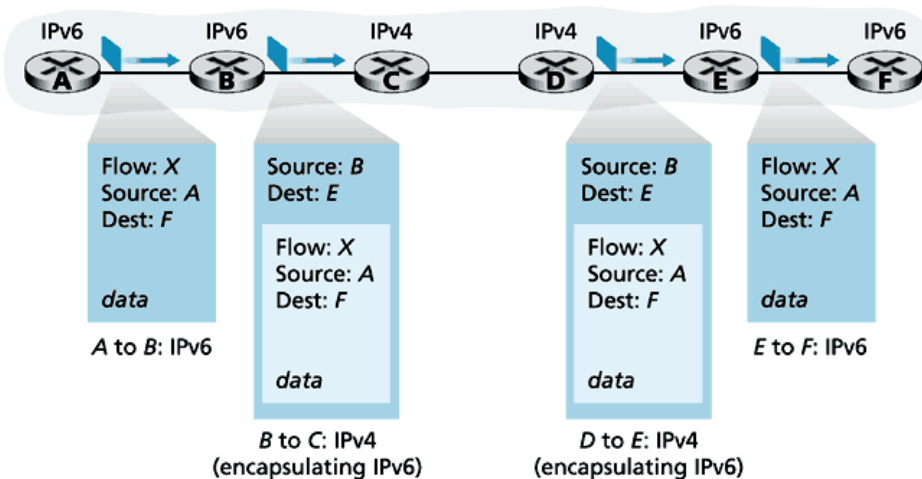
Iš senosios IPv4 versijos perėjimas į IPv6 vyksta palaipsniui. Galimi du IPv6 įdiegimo būdai: dvigubo steko ir tuneliavimo. Dvigubo steko atveju IPv6 mazgai turi ir senosios versijos palaikymą. Toks mazgas gali siųsti bei priimti abiejų tipų paketus bei konvertuoti paketus iš senosios versijos į naująją ir atvirkščiai. Tuneliavimo atveju visas IPv6 paketas yra įdedamas į IPv4 duomenų lauką jei persiuntimas vyksta tarp IPv4 mazgų.



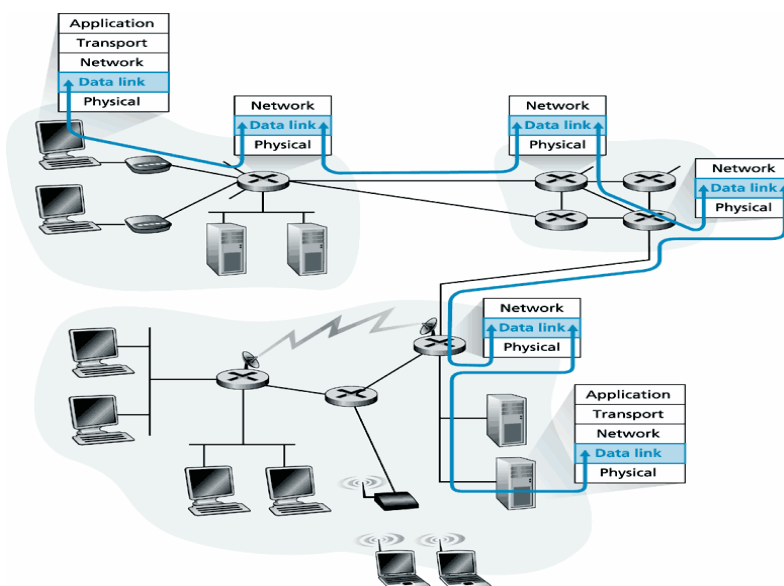
Logical view



Physical view



Kanalinis lygmuo



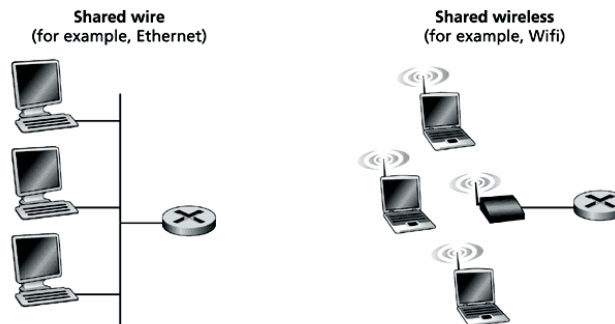
Šiame skyriuje tiek galines stotis, tiek maršrutizatorius vadinsime mazgais. Kanalinis lygmuo naudojamas IP paketų perdavimui tarp dviejų tiesiogiai sujungtų mazgų. Kanalinio lygmens protokolų pvz.: Ethernet, bevielis LAN, token ring. Kanalinio lygmens paketas vadinamas freimu.

Kanalinio lygmens galimos funkcijos: freimo formavimas; kanalo prieigos kontrolė (MAC Media Access Control); patikimas perdavimas; srauto kontrolė; klaidų aptikimas; klaidų taisymas.

Kanalinio lygmens protokolas yra įgyvendinamas tinklo plokštėje.

Kolektyvinio priėjimo protokolai

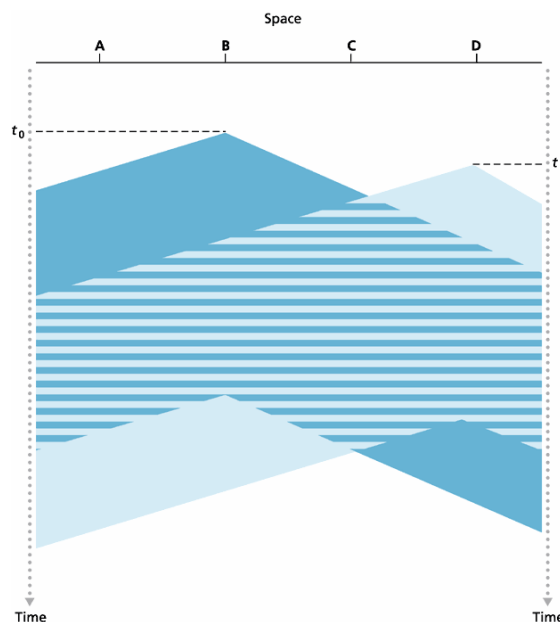
Egzistuoja dviejų rūšių kanalai: taškas-taškas, transliuojami. Taškas – taškas kanalai turi vieną siuntėją ir vieną gavėją. Pvz.: modemas ir ISP maršrutizatorius, maršrutizatorius –maršrutizatorius. Tokiems kanalams kolektyvinio priėjimo protokolai nėra reikalingi. Transliuojamuose kanaluose mazgai yra sujungti prie to paties bendro kanalo. Kai vienas mazgas išsiunčia freimą, jį gauna visi kiti mazgai.



Kai į kanalą tuo pačiu metu siunčia du ir daugiau mazgų įvyksta kolizija. Kolektyvinio priėjimo protokolai koordinuoja mazgų priėjimą prie bendrai naudojamo kanalo.

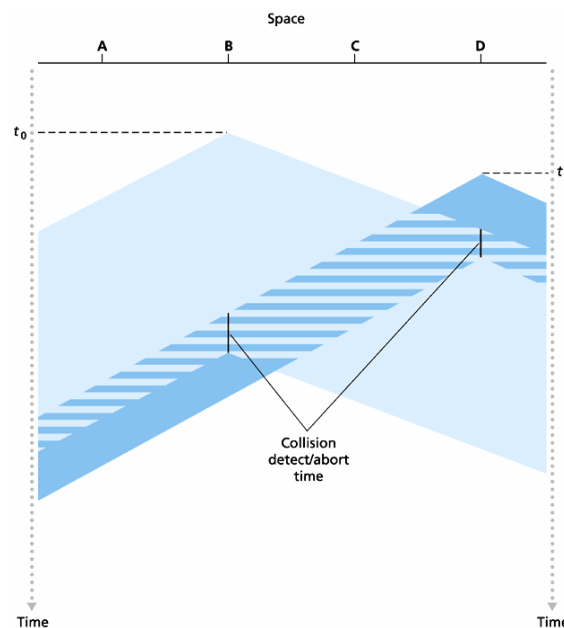
Trijų tipų kolektyvinio priėjimo protokolai: kanalo dalinimo (laikinis, dažninis, kodinis dalinimas); atsitiktinės prieigos; trumpalaikio resursų išskyrimo (taking turns).

CSMA (carrier sense multiple access) protokolai stebi kanalą. Jei kanalas laisvas, freimas yra siunčiamas. Jei užimtas, yra klausomasi kanalo ir jam atsilaisvinus, yra bandoma siųsti su tikimybe p . Kolizinė situacija gal susidaryti dėl sklaidimo vėlinimo. Mazgai gali negirdėti vienas kito. Pvz. erdvinė-laikinė diagrama.



Laiko momentu t_0 mazgas B pradeda siųsti. Išsiųsti bitai sklinda abejomis kryptimis. Laiko momentu t_1 , mazgas D taip pat pradeda siųsti, nes B bitai šio mazgo dar ne pasiekė. Po trumpo laiko įvyksta kolizija. Šiame paveiksle mazgai nedetektuoja kolizijos, ir išsiunčia pilnus freimus, nors ir įvyko kolizija.

CSMA/CD (Collision Detection) protokolas nutraukia siuntimą, jei buvo aptikta kolizija. Tai leidžia padidinti efektyvumą, kadangi nebeperduodami iškraipyti signalai.



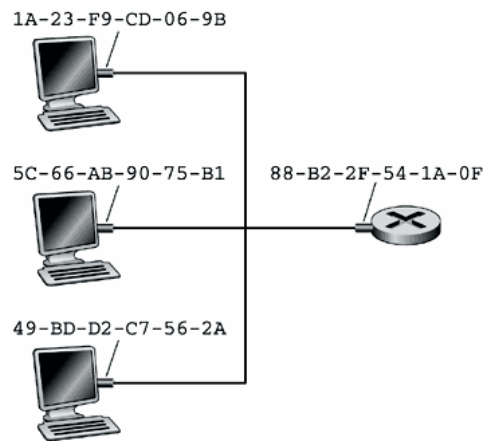
Trumpalaikio resursų išskyrimo protokolams priklauso apklausos (polling) protokolai, valdančiojo freimo (token-passing) bei protokolai su rezervavimu. Apklausos protokoluose valdantysis mazgas tam tikra tvarka apklausia visas stotis. Jei stotis turi freimų paruoštų siuntimui, ji siunčia max galimą freimų skaičių. Kai siuntimas baigiasi yra apklausiama sekanti stotis. Trūkumai: tinklas apkraunamas tarnybine informacija; vėlinimas; mažas patikimumas (valdantysis mazgas). Valdančiojo freimo protokoluose nėra valdančios stoties. Specialios paskirties freimas (token) keliauja tinklu iš vieno mazgo į kitą tam tikra tvarka. Mazgas, gavęs šį freimą užlaiko jį tik tuo atveju kai turi ką siųsti, jei ne persiunčia sekančiam. Siųsti leidžiama taip pat tik nustatytą max freimų skaičių. Po siuntimo token yra perduodamas kitam mazgui. Protokoluose su rezervavimu laikas yra dalinamas į n (stočių skaičius) intervalų. Jeigu n -toji stotis turi paruoštą siuntimui freimą, ji perduoda vienetinį bitą n -tojo intervalo metu.

Pvz iš lapų.

LAN adresai ir ARP

LAN Local Area Network : Ethernet, Token Ring, FDDI.

LAN adresais yra identifikuojamos tinklo plokštės. LAN adresai dar yra vadinami fiziniais adresais, Ethernet adresais ar MAC adresais. Daugumai LAN'ų (Ethernet, Token Ring) LAN adresas yra 6 baitų ilgio, užrašomas šešioliktaine forma. LAN adresas yra pastovus bei unikalus ir yra įrašomas į tinklo plokštės atmintį.

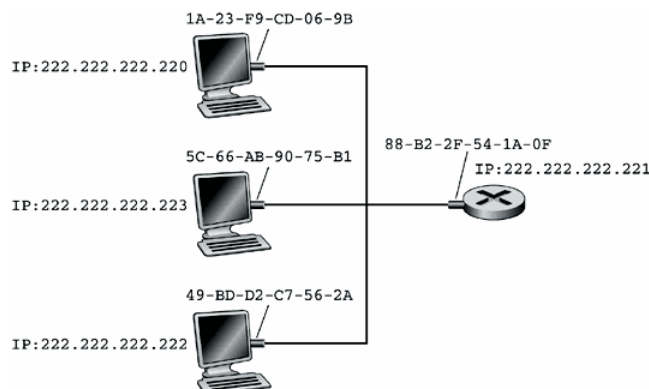


Kai mazgas išsiunčia freimą, jį gauna visi mazgai priklausantys tam pačiam LAN'ui. Jei freimo gavėjo LAN adresas sutampa su jį priėmusios stoties LAN adresu, tuomet iš freimo yra išskiriamas tinklinio lygmens paketas ir persiunčiamas aukščiau esančiam lygmeniui. Jei nesutampa – kanalinis lygmuo šį freimą atmeta.

LAN transliacijos visam tinklui adresas – FF-FF-FF-FF-FF-FF.

ARP (Address resolution protocol) RFC 826 susieja IP adresus su LAN adresais. Kiekviena LAN stotis ar maršrutizatorius turi ARP modulį. Pervedant IP adresą į LAN adresą siunčiantis mazgas kreipiasi į ARP modulį su IP adresu, o ARP atsako jį atitinkančiu LAN adresu. Analogišką funkciją atlieka DNS, kuris susieja stočių vardus su IP adresais. Skirtumas tas, kad DNS taikomas visame internete, o ARP tik to paties LAN ribose.

ARP modulis kiekvieno mazgo RAM'e turi ARP lentelę. Pvz.:



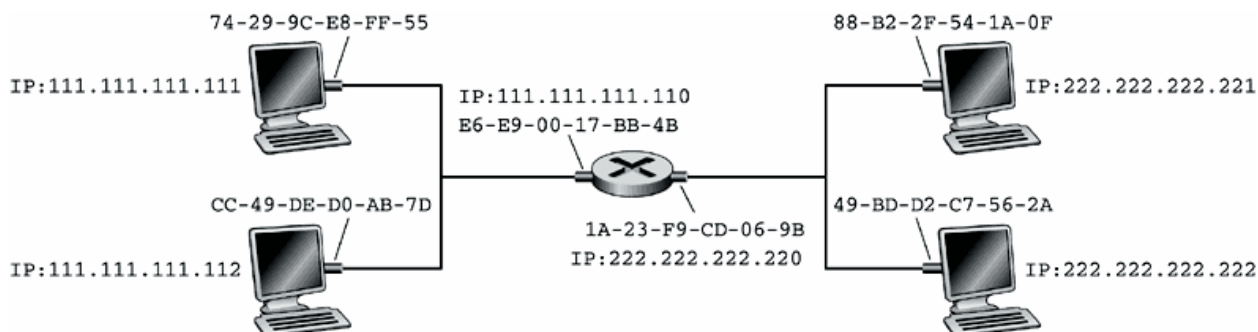
Mazgo 222.222.222.220 ARP lentelė:

IP Address	LAN Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Jei reikiamo įrašo ARP lentelėje nėra, mazgas naudoja ARP protokolą. Jis pirmiausiai suformuoja specialų ARP freimą-užklausą. Jame įrašomi siuntėjo IP ir LAN adresai bei IP adresas stoties, kurios LAN adresą reikia sužinoti. Jis siunčiamas į visas LAN stotis, t.y gavėjo LAN adreso vietoje įrašoma FF-FF-FF-FF-FF-FF. Stotis, kurios IP adresas sutampa su nurodytu užklausoje, siunčia atsakymo ARP freimą. Jo struktūra analogiška užklausiai. Tik LAN adreso lauke įrašomas IP adresą atitinkantis LAN adresas ir freimas adresuojamas mazgui, siuntusiam užklausą. Gavęs atsakymo freimą, mazgas papildo savo ARP lentelę ir siunčia duomenų freimą.

Deitagramos siuntimas už LAN ribų

Du tinklai sujungti maršrutizatoriumi.



Du mazgų tipai: stotys ir maršrutizatoriai. Kiekviena stotis turi vieną IP adresą bei vieną tinklo plokštę. Maršrutizatoriai turi IP adresus kiekvienam savo interfeisui, kurie savo ruožtu turi savo adapterius ir ARP modulius. Paveiksle M turi 2 interfeisus, 2 IP adresus, 2 ARP modulius, 2 tinklo plokštes, kurios turės skirtingus LAN adresus.

LAN1 IP adresas – 111.111.111.0/24; LAN2 IP adresas – 222.222.222.0/24.

Stotis 111.111.111.111 nori siųsti deitagramą stočiai 222.222.222.222.

Siuntėjas remdamasis maršrutizavimo lentele nustato, kad pasiekti gavėją 222.222.222.222, deitagrama iš pradžių turi būti nusiųsta maršrutizatoriaus interfeisui 111.111.111.110. Taigi freimo gavėjo LAN adrese bus įrašytas 111.111.111.110 interfeiso LAN adresas E6-E9-00-17-BB-4B, gautas iš ARP lentelės. Maršrutizatoriaus interfeisas priima freimą, išanalizavęs sužino kad jis yra skirtas būtent jam, tuomet išima deitagramą ir ją persiunčia tinkliniam lygmeniui. Naudojant maršrutizavimo lentelės maršrutizatorius nukreipia šią deitagramą į sąsają 222.222.222.220. Remdamasis ARP sužino gavėjo 222.222.222.222 LAN adresą, ir šiuo adresu išsiunčia freimą.

Ethernetas'as

Ethernet'as plačiausiai taikoma LAN technologija. Šiandieninis Ethernet'as turi daug pavidalų ir formų. Jo LAN tinklai gali turėti magistralės arba žvaigždės topologijas. Gali būti naudojami koaksialiniai, vytos poros ar optiniai kabeliai. Duomenų perdavimo greičiai 10 Mbps, 100 Mbps, 1 Gbps ar net 10 Gbps. Visos Ethernet'o technologijos turi bendras charakteristikas:

1. Etherneto freimo struktūra



Preamble (8 baitai). Ethernet'o freimas prasideda 8 baitų preamble. Kurioje pirmi 7 baitai turi reikšmes 10101010, o paskutinis aštuntasis baitas – 10101011.

Gavėjo adresas (6 baitai) – freimo gavėjo LAN adresas.

Siuntėjo adresas (6 baitai) – freimo siuntėjo LAN adresas.

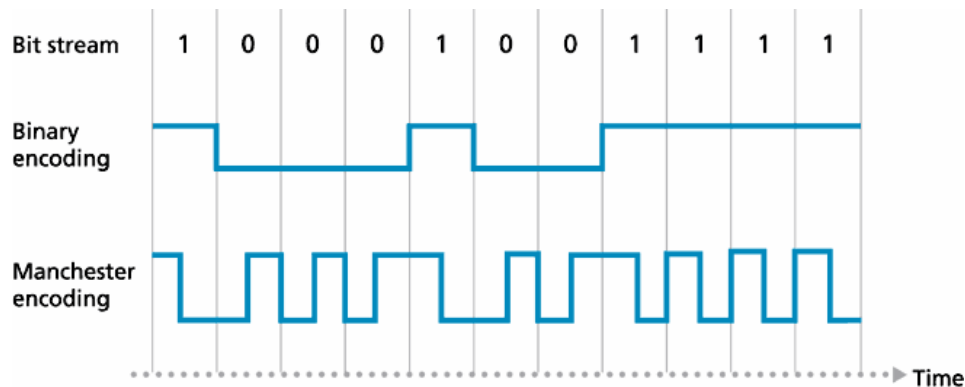
Tipas (2 baitai). Nurodo aukštesnio lygmens (tinklinio) protokolą. IP, IPX.

Duomenų laukas (46- 1500 baitų). Šiame laukelyje yra patalpina IP deitagrama. Etherneto MTU maksimalus perdavimo vienetas 1500 baitų. Jei IP deitagrama viršija 1500

baitų, ji turi būti fragmentuojama į atskiras deitagramas. Minimalus duomenų lauko dydis – 46 baitai. Jei IP deitagrama mažesnė nei 46 baitai, duomenų laukas yra papildomas iki 46 baitų.

CRC Cyclic Redundancy Check (4 baitai). Skirtas klaidų aptikimui.

2. Visos Ethernet'o technologijos neužtikrina patikimo duomenų perdavimo. Siuntėjas nežino ar jo siųstas freimas pasiekė gavėję be klaidų. Jei CRC baitai neatitinka gavėjo suskaičiuotos kontrolinės sumos, gavėjas šį freimą paprasčiausiai atmeta.
3. Tiesioginis perdavimas ir Mančesterio kodavimas. Ethernet'as naudoja tiesioginį perdavimą, tai yra Ethernet'o interfeiso plokštė siunčia skaitmeninį signalą tiesiai į ryšio liniją. Ethernet'as naudoja Mančesterio kodavimą, kur kiekvienas bitas turi perėjimą (transition); 1 turi perėjimą iš viršaus žemyn, o 0 – iš apačios į viršų.



4. Ethernet'as naudoja CSMA/CD kolektyvinio priėjimo protokolą.

Ethernet'o technologijos

Kartotuvas – tai fizinio lygmens įrenginys, turintis du ar daugiau interfeisų. Jis priimtą bitą viename interfeise sustiprina jį ir perduoda į visus kitus interfeisus. Kartotuvas nevykdo CSMA/CD protokolo.

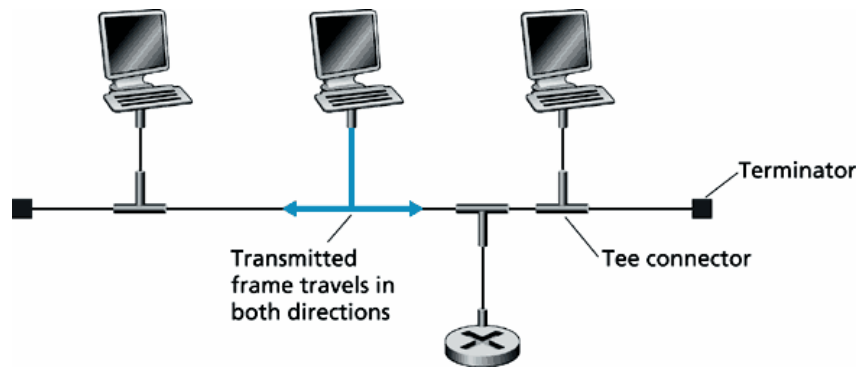
10Base5 10Base2

Technologija	Kabelis	Max. segmento ilgis be kartotuvo, m	Stočių skaičius
10Base5	Storas koaksialinis RG-8 RG-11	500	100
10Base2	Plonas koaksialinis RG-58	185	30

10 - 10 Mbps 5 – 500 m. 2 – 185 m apytiksliai 200.

10Base5 technologija dabar nebevartojama.

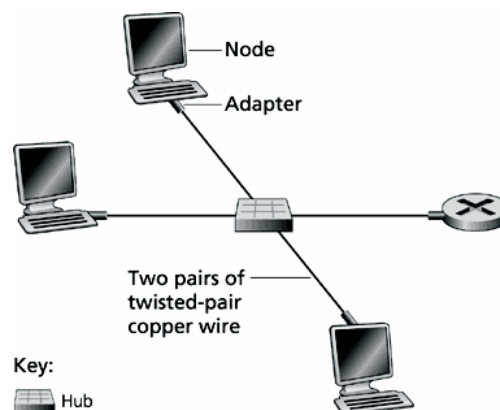
Šios Ethernet'o technologijos naudoja magistralės topologiją.



Gali būti panaudota iki 4 kartotuvų, taip sujungiant 5 kabelio segmentus. Tik 3 segmentai gali būti apkrauti, tai yra prie jų jungiami kompiuteriai. Šios technologijos dar apibūdinamos pagal taisyklę 5-4-3, t.y. 5 segmentai, 4 kartotuvai, 3 naudojami segmentai.

10BaseT 100BaseT

Šios dvi Ethernet technologijos yra populiariausios šiai dienai. Pagrindinis skirtumas tarp šių technologijų tas, kad 10BaseT duomenis perduoda 10Mbps greičiu, o 100BaseT – 100Mbps. T – twisted pair (vyta pora). Abi šios technologijos naudoja žvaigždės topologiją.



Žvaigždės topologijoje centrinis įrenginys yra vadinamas koncentratoriumi (hub). Kiekvienos stoties adapteris yra tiesiogiai sujungtas su koncentratoriumi. Sujungimui naudojamos RJ-45 jungtys. Maksimalus atstumas tarp stoties ir koncentratoriaus 100 m. Siekiant, kad tinklas patikimai dirbtų panaudojant CSMA/CD protokolą, koncentratorių kiekis tarp bet kurių dviejų tinklo kompiuterių neturi viršyti 4. Maksimalus kompiuterių skaičius – 1024.

Koncentratorius iš esmės yra kartotuvas: kai priima bitą viename interfeise, jį persiunčia į visus kitus interfeisus. Koncentratorius atlieka tinklo valdymo funkcijas: gali atjungti sugedusį interfeisą, kuris nuolatos siunčia freimus; atlikti tinklo monitoringą.

100BaseT technologija vietoje Mančesterio kodavimo naudoja efektyvesnį 4B5B kodavimą, kur per kiekvienus 5 taktus yra perduodami 4 bitai.

10 Mbps ir 100 Mbps Ethernet'o technologijos gali būti realizuotos optiniais kabeliais. Optinės sąsajos dažnai naudojamos LAN'ų sujungimui. Panaudojant optiką yra padidinamas max segmento ilgis.

Technologija	Kabelis	Max. segmento ilgis, m	Max. segmentų skaičius	Pastabos
10BaseT	3kat.vytos poros	100	1024	2 poros
10BaseF	Optinis kabelis	2000	1024	
100BaseT4	3 kat.vytos poros	100	1024	4 poros
100BaseTX	5 kat.vytos poros	100	1024	2 poros
100BaseFX	Optinis kabelis	2000	1024	

Gigabitinis Ethernet'as

Duomenų perdavimo sparta – 1 GBps. Naudoja standartinį Ethernet'o freimo formatą. Šį standartą galima įdiegti tiek taškas-taškas kanaluose, tiek transliuojamuose. Transliuojamuose kanaluose kaip ir jo pirmtakai naudoja CSMA/CD kanalo prieigos protokolą.

Technologija	Kabelis	Max. segmento ilgis, m
1000BaseSX	Optinis	550
1000BaseLX	Optinis	5000
1000BaseCX	2 poros STP	25
1000BaseT	4 poros 5 kat. UTP	100

LAN'ų jungimas tarpusavyje

Organizacijos paprastai yra sudarytos iš padalinių, turinčių ir prižiūrinčių savo LAN'us. Natūralu, kad atsiranda būtinybė šiuos LAN'us sujungti tarpusavyje. Kodėl ne vienas didelis LAN'as?

- LAN'e stotys dalinasi kanalo pralaidumu;
- Sistema, sudaryta iš kelių tinklų patikimesnė, negu vieningas tinklas, kuriame vieno mazgo gedimas gali nutraukti viso tinklo darbą;
- Limituotas maksimalus stočių skaičius;
- Limituoti maksimalūs atstumai tarp atskirų stočių;
- Didelė „kolizinė sritis“.

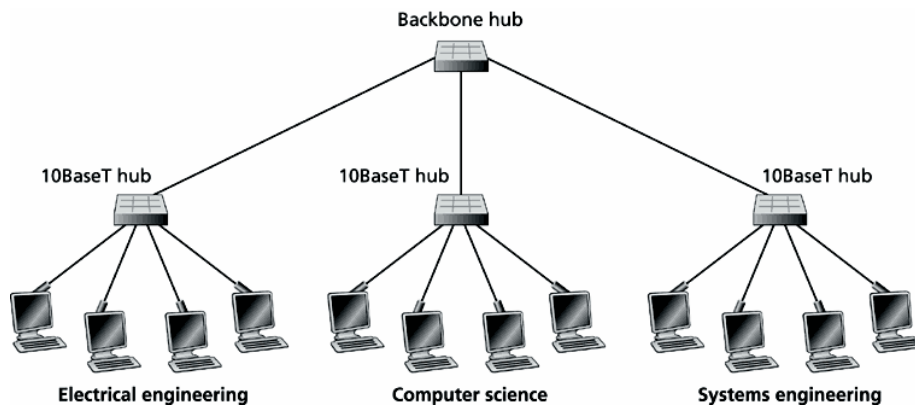
Kolizinė sritis – tai LAN'o dalis, kurioje visi LAN'o įrenginiai sugebės aptikti koliziją, tuo pačiu metu siunčiant dviems ar daugiau įrenginių.

LAN'ai tarpusavyje gali būti jungiami:

- Koncentratoriais (Hub);
- Tiltais (Bridge);
- Komutatoriais (Switch);
- Maršrutizatoriais (Router).

Koncentratoriai (Hubs)

LAN'ų jungimas koncentratoriais yra pats paprasčiausias. Kadangi koncentratoriai dirba bitų lygmenyje, o ne su freimais, jie yra fizinio lygmens įrenginiai. Paveiksle pavaizduotas universiteto fakultetų LAN'ų sujungimas koncentratoriumi.



Koncentratorius sujungiantis fakultetus, vadinamas centriniu koncentratoriumi (backbone hub). Čia pavaizduota struktūra yra hierarchinė. Visa tinklo struktūra laikoma kaip vieningas LAN'as, o kiekvieno fakulteto tinklas – LAN'o segmentais. Visi LAN'o segmentai priklauso tai pačiai kolizinei sričiai, t.y., jei du ar daugiau įrenginių siųs informaciją tuo pačiu metu, susidarys kolizija.

LAN'ų jungimo koncentratoriais privalumai:

- sudaro ryšio tarp padalinių galimybę;
- išplečia LAN sritį;
- padidina tinklo veikimo patikimumą. Sutrikus vieno tinklo segmento veikimui, centrinis koncentratorius gali atjungti sugedusį segmentą, o likusi tinklo dalis gali toliau sėkmingai funkcionuoti.

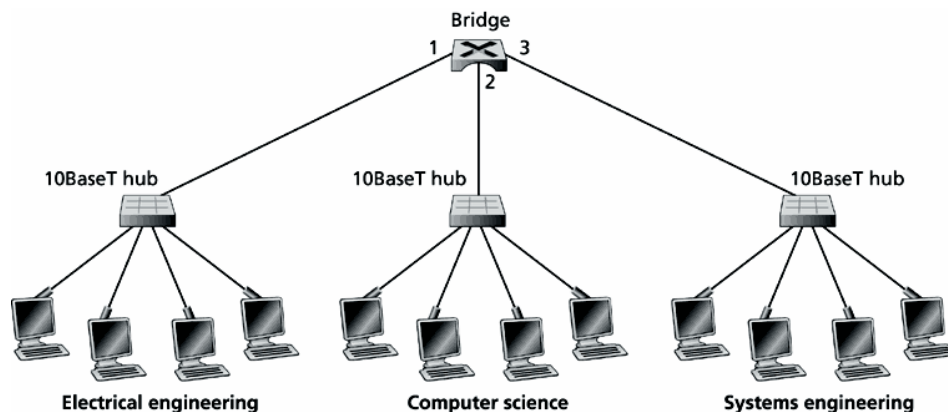
Trūkumai:

- kai LAN'ai yra sujungiami koncentratoriais, buvusios atskiros LAN'ų kolizinės sritys, tampa viena bendra kolizine sritimi, kas neleidžia padidinti bendro maksimalaus pralaidumo. Pvz. jei aukščiau pateiktame paveiksle LAN'ų pralaidumai buvo po 10 Mbps, tai suminis pralaidumas – 30 Mbps. Apjungus tinklus, dėl bendros kolizinės srities, bendras maksimalus pralaidumas išlieka 10 Mbps;
- Etherneto technologijos bendroje kolizinėje srityje negali viršyti maksimalaus stočių skaičiaus, maksimalaus atstumo tarp dvejų stočių, maksimalaus hierarchinės struktūros lygių skaičiaus. Visi šie apribojimai atsispindi bendroje LAN struktūroje;
- Koncentratoriais negalima sujungti skirtingų Ethernet technologijų (pvz. 10BaseT ir 100BaseT), kadangi jie yra tik fizinio lygmens įrenginiai. Skirtingų Ethernet technologijų LAN'ams sujungti reikalingas freimų apdorojimas.

Tiltai (Bridges)

Tiltai dirba su Ethernet'o freimais, todėl yra kanalinio lygmens įrenginiai. Tiltai filtruoja ir perduoda freimus pagal freimo gavėjo LAN adresą. Kai tilto interfeise priimamas freimas, jis neperduodamas į visus kitus, tačiau analizuojamas freimo gavėjo LAN adresas ir perduodamas į interfeisą, kuris veda gavėjo kryptimi.

Žemiau pateiktame paveiksle pavaizduotas LAN'ų sujungimas tiltu.



Šalia tilto interfeisų nurodyti jų numeriai. Skirtingai, nei jungiant koncentratoriumi, dabar kiekvienas LAN segmentas yra atskira kolizinė sritis.

Jungimo tiltais privalumai:

- leidžia sujungti LAN'us, išsaugant jų atskiras kolizines sritis, kas padidina bendrą maksimalų pralaidumą;
- galima sujungti skirtingų Ethernet technologijų tinklus, kadangi naudojamas sukaupti-ir-persiųsti perdavimo būdas (store-forward);
- nėra apribojimų stočių skaičiui ir LAN'o geografiniam dydžiui.

Tilto freimų filtravimas ir persiuntimas

Filtravimas – tai tilto sugebėjimas nustatyti, ar freimą reikia persiųsti į kitą interfeisą ar tiesiog sunaikinti. Jei freimo gavėjas priklauso tam pačiam LAN'o segmentui, iš kurio atėjo freimas, nėra tikslinga freimą perduoti į kitus interfeisus.

Persiuntimas – tai tilto galimybė nustatyti interfeisą, į kurį freimas turi būti nukreiptas, ir freimo persiuntimas į šį nustatytą interfeisą.

Filtravimas ir persiuntimas yra atliekami pasinaudojant filtravimo lentelę. Tiltų lentelėje yra įrašai LAN'o mazgams (nebūtinai visiems). Ši lentelė susideda iš:

- stoties LAN adreso;
- tilto interfeiso, kuris veda tos stoties kryptimi, numeris;
- laikas, kada informacija apie šį mazgą buvo įrašyta į lentelę.

Address	Interface	Time
62-FE-F7-11-89-A3	1	9:32
7C-BA-B2-B4-91-10	3	9:36
....

Filtravimo ir persiuntimo algoritmas:

1. Tarkime, kad tilto interfeisas x priima freimą, kurio gavėjo LAN adresas AA-AA-AA-AA-AA-AA-AA. Tiltas išanalizuoja lentelę, ir randa šį adresą atitinkantį interfeisą y.
2. Jei $x = y$, freimas atėjo iš LAN segmento, kuriame yra gavėjas. Tiltas atlieka filtravimo funkciją, pašalindamas freimą.
3. jei $x \neq y$, freimas turi būti perduotas į LAN segmentą, prijungto prie y interfeiso. Tiltas persiunčia freimą į interfeiso y išsiuntimo buferį.

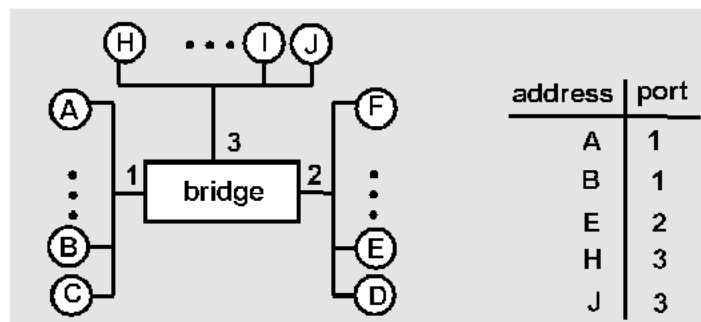
Šios paprastos taisyklės leidžia tiltui izoliuoti kolizines sritis. Šios taisyklės taip pat leidžia bendrauti tarpusavyje dviems mazgams iš to paties LAN segmento, kai tuo pačiu metu bendrauja kiti du kito LAN segmento mazgai.

Siųsdamas freimą į ryšio liniją, tiltas taiko CSMA/CD tinklo prieigos protokolą.

Tiltai pasižymi puikiai savybe – jie suformuoja ir atnaušina savo lenteles dinamiškai ir automatiškai be tinklo administratoriaus ar konfigūracijos protokolo įsikišimo. Tiltai yra savarankiška apsimokanti (self-learning) sistema. Ši savybė įgyvendinama sekančiai:

- 1) Inicializacijos metu tilto lentelė yra tuščia;
- 2) Kai vienu iš interfeisų yra priimamas freimas, o freimo gavėjo adreso nėra lentelėje, tiltas perduoda freimo kopijas į visų likusių interfeisų išsiuntimo buferius. Kiekvienas iš šių interfeisų naudoja CSMA/CD protokolą freimo perdavimui į LAN segmentą.
- 3) Kiekvienam priimtam freimui tiltas savo lentelėje įrašo: a) freimo siuntėjo LAN adresą b) interfeiso, kuriuo gautas freimas, numerį c) esamą laiką. Tokiu būdu tiltas užsirašo informaciją apie LAN segmentą, kuriame randasi siunčianti stotis. Jei kiekviena LAN stotis siunčia freimus, jie visi bus užrašyti lentelėje.
- 4) Kai gaunamas freimas, kurio gavėjo LAN adresas jau yra lentelėje, jis nukreipiamas į reikiamą interfeisą arba sunaikinamas.
- 5) Tiltas pašalina įrašą iš lentelės, jei tam tikrą laiką nėra gaunamas nei vienas freimas, kurio siuntėjo adresas sutaptų su adresu lentelėje. Tokiu būdu iš lentelės pašalinami neegzistuojantys (nebefunkcionuojantys) adresai.

Pavyzdys. C siunčia freimą D, ir D atsako C. Šalia tinklo topologijos pavaizduota tilto lentelė.



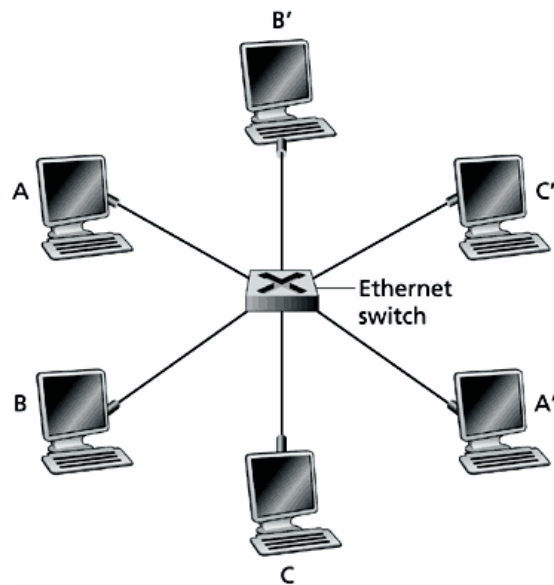
- Tiltas priima freimą iš stoties C:
 - Papildo lentelę įrašu, kad C pasiekiamas per 1 interfeisą;
 - Kadangi D nėra lentelėje, tiltas persiunčia freimą į 2 ir 3 interfeisus
- D priima freimą.
- D sugeneruoja atsakymą ir siunčia freimą C.
- Tiltas priima šį freimą:
 - Papildo lentelę įrašu, kad D pasiekiamas per 2 interfeisą;
 - Tiltas žino, kad C pasiekiamas per interfeisą 1, todėl freimą persiunčia tik į 1-ąjį interfeisą.

Komutatoriai (Switch)

Komutatoriai iš esmės yra didelio pralaidumo daugiainterfeisiai tiltai. Tiltai paprastai turi keletą interfeisų (2-4), o komutatoriai gali turėti dešimtis interfeisų. Komutatoriai, kaip ir tiltai dirba su Ethernet'o freimais (2-ojo lygmens įrenginiai): vykdo freimų persiuntimą bei filtravimą pagal LAN adresus. Komutatoriai gali būti naudojami su įvairiomis 10 Mbps, 100 Mbps ir 1Gbps interfeisų kombinacijomis. Pvz.: keturi po 100 Mbps ir vienas – 1Gbps interfeisai.

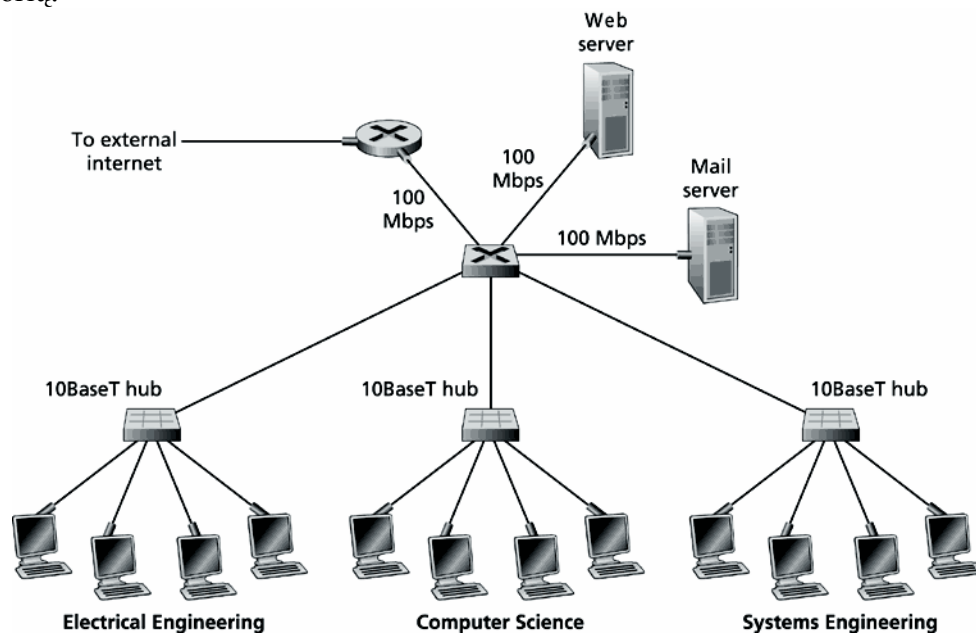
Šie įrenginiai gali dirbti pilno-duplekso režimu: vienu metu gali siųsti ir priimti freimus per tą patį interfeisą. Žemiau pateiktame paveiksle esant pilno duplekso režimui A galėtų siųsti duomenis A', tuo pačiu metu kaip ir A' siųstų A.

Kitas komutatorių privalumas tas, kad jie leidžia tiesioginį stočių prijungimą prie komutatorių. Stotys gali siųsti ir priimti duomenis pilnu greičiu, niekad nepatirdamos kolizijų. Toks jungimas vadinamas skirtine linija arba skirtiniu priėjimu (dedicated access). Pateiktame paveiksle A galėtų siųsti duomenis A' tuo pačiu metu kaip ir B – B', bei C – C'.



Komutatoriai naudoja ne sukaupti-ir-persiųsti freimo perdavimo būdą, bet perdavimą dalimis (cut-through). Jei nėra eilės išsiuntimo buferio, paketas perduodamas į buferį dar nepilnai gautas. Jo išsiuntimas pradedamas priėmus gavėjo LAN adresą, jį išanalizavus ir nukreipus į reikiamą interfeisą. Toks perdavimo būdas žymiai padidina paketo perdavimo greitį.

Žemiau pateikiamas universiteto tinklas, naudojantis koncentratorius, komutatorių ir maršrutizatorių.

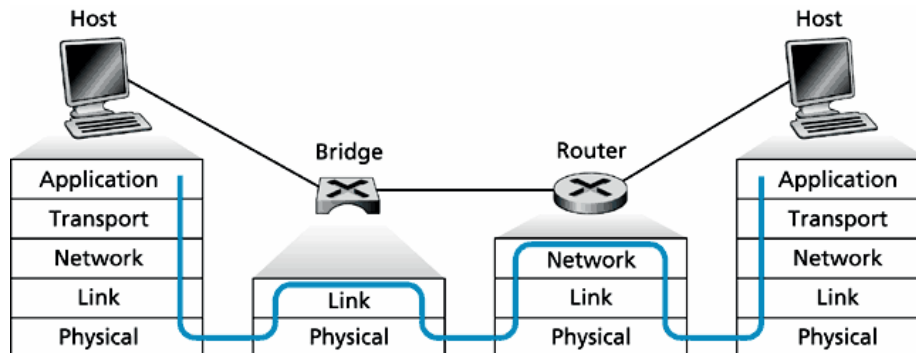


Įrenginių palyginimo lentelė:

	Koncentratoriai	Tiltai	Komutatoriai	Maršrutizatoriai
Srautų atskyrimas	N	T	T	T
Plug and Play	T	T	T	N
Optimalus maršrutizavimas	N	N	N	T
Cut-through perdavimas	T	N	T	N

Tiltai ar Maršrutizatoriai

Tinklo administratoriams dažnai tenka rinktis ką naudoti – tiltą ar maršrutizatorių. Maršrutizatoriai yra tinklinio lygmens įrenginiai (dirba su IP paketais). Maršrutizatoriai turi maršrutizavimo lenteles, juose įdiegti maršrutizavimo algoritmai. Tiltai yra kanalinio lygmens įrenginiai (dirba su freimais). Tiltai turi filtravimo lenteles, juose įgyvendinti filtravimo, savarankiško apsimokymo algoritmai.



Tiltų privalumai, trūkumai:

- + tiltų veikimas paprastesnis, reikalaujantis trumpesnio paketo apdorojimo laiko;
- + tiltų lentelės yra sudaromos automatiškai;
- freimai perduodami neoptimaliu maršrutu;
- tiltai neturi ugniasienių.

Maršrutizatorių privalumai, trūkumai:

- + optimalus maršrutizavimas;
- + gali būti alternatyvūs keliai, nuo paketų užsiciklinimo tinkle apsaugo TTL reikšmė;
- + turi ugniasienę;
- reikalingas rankinis konfigūravimas (ne plug&play);
- didesnis paketo apdorojimo laikas.

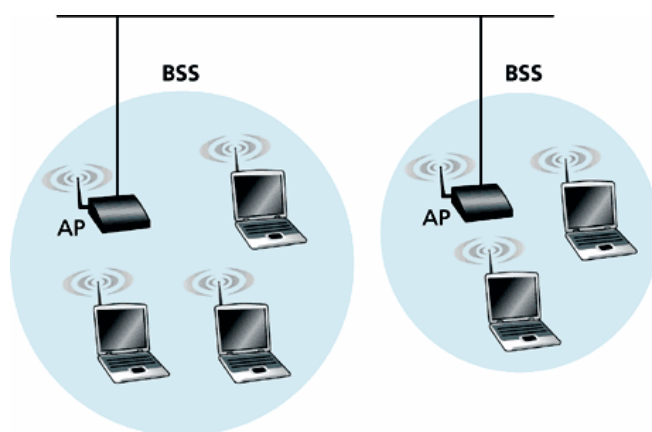
Paprastai maži tinklai (keli šimtai įrenginių) turi keletą LAN segmentų. Tokiems tinklams užtenka tiltų, kadangi jie izoliuoja kolizines sritis ir padidina maksimalų tinklo pralaidumą, nereikalaudami rankinio konfigūravimo. Didesni tinklai (iš tūkstančių stočių) be tiltų naudoja ir maršrutizatorius. Maršrutizatoriai griežčiau atskiria srautus, turi ugniasienes ir nustato optimalius maršrutus.

Bevieliai LAN'ai

Šiuo metu yra daug bevielių LAN'ų technologijų ir standartų. Labiausiai paplitęs yra IEEE 802.11b standartas, dar vadinamas bevieliu Ethernetu ar Wi-Fi. Šis standarto naudojamas dažnis 2,4 GHz, o duomenų perdavimo greitis iki 11 Mbps. 802.11b standartas aprašo fizinį lygmenį bei MAC (Media Access Control) lygmenį bevieliui vietiniam tinklui. Fizinis lygmuo naudoja DSSS (Direct Sequence Spread Spectrum) technologiją, kuri kiekvieną bitą verčia į tam tikrą bito šabloną, vadinamą kodu. Ši technologija yra panaši į CDMA (Code Division Multiple Access), tačiau skirtingai nei CDMA visos mobilios stotys (ir pagrindinės stotys) naudoja tą patį kodą. Taigi DSSS negalime vadinti kolektyvinio priėjimo protokolu, kadangi jis nekoordinuoja priėjimo prie bendrai naudojamo kanalo. DSSS yra tiesiog fizinio lygmens mechanizmas.

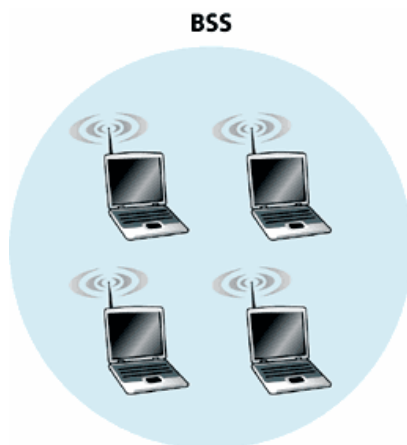
IEEE 802.11b standartas priklauso bevielių LAN'ų šeimai „IEEE 802.11“. Šiai šeimai taip pat priklauso 802.11a (perdavimo dažnis 5-6 GHz, vietoje DSSS naudoja OFDM (Orthogonal Frequency Division Multiplexing), perdavimo sparta iki 54 Mbps) bei 802.11g (perdavimo dažnis 2,4 GHz, perdavimo sparta iki 54 Mbps) standartai. Visi IEEE 802.11 šeimos standartai naudoja tą pačią LAN architektūrą bei MAC protokolą.

Žemiau pateiktame paveikslėlyje yra pavaizduoti visi pagrindiniai 802.11 bevielio LAN'o architektūros komponentai.



Fundamentalus architektūros blokas yra celė, vadinama BSS (Basic Service Set). Tipiškai BSS susideda iš kelių bevielių stočių ir centrinės bazinės stoties, vadinamos prieigos tašku (Access Point AP). Bevielės stotys ir AP komunikuoja tarpusavyje naudodami 802.11 bevielį MAC protokolą. Keletas AP gali būti sujungti tarpusavyje (pavyzdžiui, naudojant Ethernet'ą ar kitą bevielį kanalą), taip sudarant išskirstytas sistemas DS (Distribution Systems). Aukštesnio lygmens protokolams tokia išskirstyta sistema atrodo kaip vieningas LAN'as.

Žemiau pateiktas paveikslėlis vaizduoja bevielį LAN'ą be bazinės stoties.

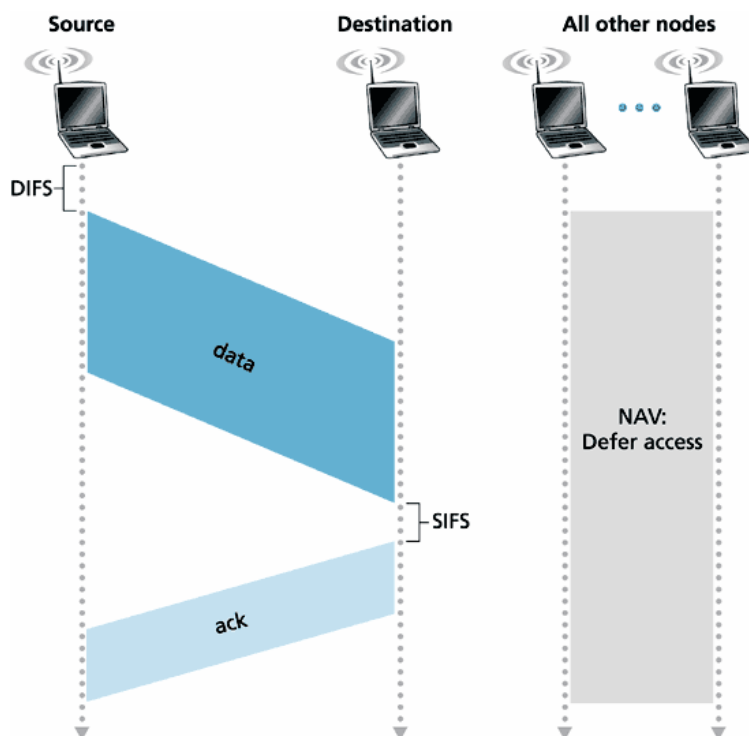


Tokiuose bevieliuose LAN'uose bevielės stotys bendrauja tik tarpusavyje, neturėdamos ryšio su „išoriniu pasauliu“. Toks tinklas susidarys tuomet, kai mobilūs įrenginiai norės apsikeisti duomenimis tokiose vietose, kur nėra sudaryta tinko infrastruktūra (pvz., toje vietoje nėra 802.11 BSS su AP). Pavyzdys galėtų būti nešiojamų kompiuterių „susitikimas“ konferencijų salėje traukinyje ar mašinoje.

Kaip ir 802.3 Ethernet'o tinkluose, taip ir bevielio LAN'o IEEE 802.11 stotys turi koordinuoti savo prieigą prie bendrai naudojamo kanalo (šiuo atveju radijo dažnis). Tai yra MAC (Medium Access Control) protokolo uždavinys. IEEE 802.11 MAC protokolas yra CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Tam, kad nustatyti ar kanalas laisvas, 802.11 fizinis lygmuo stebi signalo stiprumą tam tikrame dažnyje. Jei kanalas yra laisvas laiko intervalą lygų arba didesnį nei DIFS (Distributed Inter Frame Space), tuomet stotiai leidžiama siųsti. Kaip ir kituose atsitiktinės prieigos protokoluose, išsiųstas freimas bus teisingai priimtas gavėjo tik tuo atveju, jei siuntimo metu nesiuntė visos kitos likusios stotys.

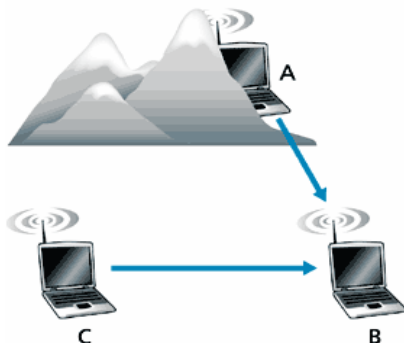
Kai gavėjo stotis pilnai ir teisingai priima freimą, ji po trumpo laiko intervalo (žinomo kaip SIFS – Short Inter Frame Spacing), išsiunčia siuntėjui patvirtinimą. Kadangi siuntimo metu siuntėjas

nevykdo kolizijos aptikimo (collision detection), šis patvirtinimas leidžia jam suprasti, kad freimas buvo teisingai priimtas gavėjo. Freimo ir patvirtinimo siuntimai grafiškai pavaizduoti paveiksle.



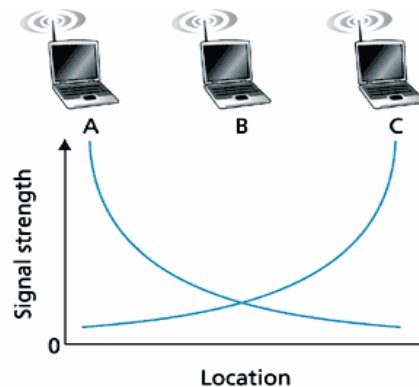
Pateiktame paveiksle pavaizduotas atvejis, kai siunčiančioji stotis aptiko, kad kanalas laisvas. Jei kanalas būtų užimtas, norinti siųsti stotis vykdytų eksponentinio atsitraukimo procedūrą. T.y. stotis, aptikusi užimtą kanalą, atideda siuntimą iki tol, kol kanalas taps laisvas. Kai kanalas laisvas laiko intervalą DIFS, stotis nesiunčia freimo iškart, tačiau vėl atideda siuntimą papildomam atsitiktiniam atsitraukimo laikui. Klausomasi kanalo ir jei šiam papildomam laikui pasibaigus, kanalas vis dar laisvas, siunčiamas freimas. Šis atsitiktinis atsitraukimo laikas padeda išvengti keleto stočių siuntimo iškart po DIFS laiko, taigi padeda išvengti kolizijų. Intervalas, iš kurio yra parenkamas atsitiktinis atsitraukimo laikas, yra dvigubinamas, po kiekvienos kolizijos, kurią sukėlė to paties freimo siuntimas. Sėkmingai išsiuntus freimą, intervalas atstatomas į pradinį.

Viena pagrindinių priežasčių, kodėl IEEE 802.11 MAC protokolas nevykdo kolizijos aptikimo, yra ta, kad jei siunčiantysis įrenginys neaptinka kolizijos, tai dar nereiškia kad kolizija negali susidaryti priimančiajame įrenginyje. Šią situaciją galime paaiškinti dviem scenarijais paslėptų stočių bei signalo slopinimo. Tarkime, kad stotis A siunčia stočiai B.



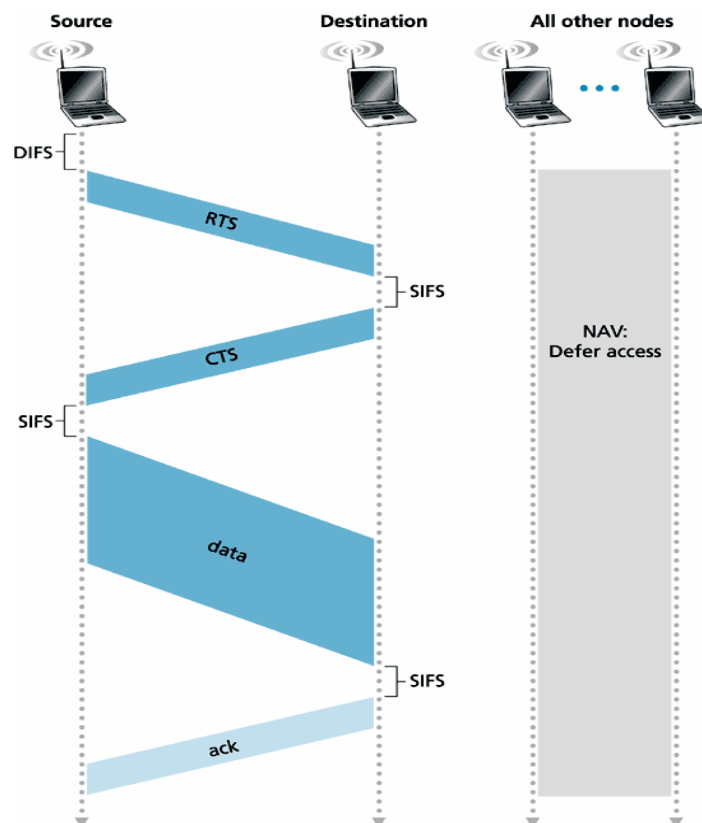
Stotis C nori siųsti freimą stočiai B, klausosi kanalo ir aptinka, kad kanalas laisvas. Stotys A ir C negirdi viena kitos siuntimo (paslėptos stotys), nes jas skiria objektas, kuriuo nesklinda radijo bangos. Taigi stotis C taip pat pradeda siuntimą. Stoties A ir B siuntimai interferuoja gavėjo B zonoje. Įvyksta kolizija.

Žemiau pateiktame paveiksle stotys negali aptikti kolizijos dėl signalo slopinimo sklindant perdavimo terpe. Stotys A ir C išsidėsčiusios taip, kad dėl signalo slopinimo jos negali aptikti viena kitos siuntimo. Tačiau signalo stiprumo užtenka stoties B zonoje, kad įvyktų signalų interferencija.



Taigi dėl išvardintų sunkumų aptinkant kolizijas bevieliose LAN'uose, IEEE 802.11 kūrėjai atsisakė CSMA/CD (aptikti kolizijas ir išeiti iš kolizinės būsenos) ir perėjo prie CSMA/CA (kolizijos vengimo). Visų pirma, IEEE 802.11 freimas turi trukmės laukelį, kuriame siuntėjas nurodo, kiek laiko truks freimo siuntimas į kanalą. Ši reikšmė visoms kitoms stotims leidžia nustatyti minimalų siuntimo atidėjimo laiką (NAV – Network Allocation Vector).

IEEE 802.11 protokolas taip pat gali naudoti ir specialius kontrolės freimus: RTS (Request To Send) ir CTS (Clear To Send), naudojamus kanalo rezervavimui. Kai stotis nori siųsti freimą, visų pirma ji gali siųsti RTS freimą gavėjui, jame nurodydama freimo ir patvirtinimo siuntimo trukmes. Gavėjas priėmęs RTS freimą, atsako su CTS freimu, suteikdamas siuntėjui teisę siųsti. Visos kitos stotys girdinčios RTS ir CTS freimus, sužino apie būsimą duomenų siuntimą, ir atideda savo siuntimus. RTS, CTS, duomenų bei patvirtinimo freimų siuntimas pateiktas žemiau esančiame paveiksle:



RTS ir CTS freimų naudojimo privalumai:

- Kadangi gavėjo išsiųstą CTS freimą girdės visos stotys gavėjo aplinkoje, CTS freimas padeda išvengti paslėptų terminalų bei signalo slopinimo problemų.
- Efektyvesnis kanalo išnaudojimas. Kolizija gali susidaryti tik siunčiant RTS ar CTS freimus. Kadangi šie freimai yra nedidelio dydžio, vadinasi ir kolizijos trukmė bus trumpesnė, nei susidūrus duomenų freimams.