

Ievads

Šis materiāls paredzēts skolotājam izmantošanai priekšmetā datoru tīkli, izglītības programmai “Datorsistēmas” 3. un 4. kursā. Mācību laikā audzēkņi iegūst jaunas zināšanas un iemaņas mācoties teoriju un izpildot dažādus praktiskos darbus profesionālajā mācību priekšmetā datoru tīkli.

Materiālā ir teorijas stundu konspekti, pārbaudes darbi, uzdevumu kopums ar vērtēšanas kritērijiem. Darbā ir konspekts 64 teorētiskajām stundām, 20 praktiskie darbi 64 stundām un 12 pārbaudes darbi teorētisko zināšanu nostiprināšanai.

Veiksmīgai mācību procesa realizācijai ir nepieciešams izmantot skolas materiālo bāzi teorētiskajās stundās demonstrējot praktiski ar piemēriem datortīklu aparatūru, programmu uzstādīšanu un konfigurēšanu.

Mācību procesa laikā audzēkņi apgūst teorētiski un praktiski ar datortīkliem saistītos jēdzienus, datortīklu veidus un to darbības principus. Iepazīstas ar svarīgākajiem tīkla protokoliem, topoloģijām un arhitektūrām, nepieciešamo aparatūru un programmatūru vienranga datortīklu izveidei un datortīklu uz servera pamata izveidei. Iemācās izveidot vienkāršu vienranga datortīklu. Apgūst praktiski veidot un lietot lokālos resursus. Izveidot un lietot FTP un Web serverus.

1. stunda

Stundas temats: Datortīklu būtība

Stundas mērķis: Iepazīties ar datortīklu būtību, to nozīmi informācijas apmaiņā.

Mācību uzdevumi:

1. Iepazīties ar datortīklu nepieciešamību.
2. Iepazīties ar datortīklu nozīmi informācijas apmaiņā.

Tīklu var definēt sekojoši: datoru, printeru, maršrutētāju, komutācijas mezglu un citu iekārtu kopa, kuras var apmainīties ar informāciju caur kādu pārraides vidi. Šī kopa darbojas kā vienots veselums, risinot datu vākšanas, apstrādes un pārraides uzdevumus. Visvienkāršākais tīkls sastāv kā minimums no diviem datoriem, kuri ir savienoti ar kabeļa palīdzību. Tas ļauj datoriem kopīgi izmantot datus. Visi tīkli neatkarīgi no sarežģītības balstās uz šo principu. Kaut gan ideja savienot datorus ar kabeļa palīdzību tagad neliekas mums sevišķi izcila, sava laikā tā bija nozīmīgs sasniegums komunikāciju jomā. Datoru tīklu rašanās bija izsaukta ar datu un citu tīkla resursu kopīgas izmantošanas praktisko nepieciešamību. Tīklā iekļautie datori var kopīgi izmantot: datus, ziņojumus, printerus, faksimilu aparātus, modemus un citus tīkla resursus.

Pašlaik lielāka organizāciju daļa glabā un kopīgi izmanto tīkla vidē svarīgu datu milzīgus apjomus. Tīkli tagad ir nepieciešami tāpat, kā vēl pavisam nesen rakstāmmašīnas un kartotēkas. Tātad, galvenais tīkla uzdevums ir kopīga resursu izmantošana un pastāvīga komunikācija (informācijas apmaiņa) reālā laika režīmā. Tīkla resursi ir dati, lietojumprogrammas vai lietojumprocesi, kas darbojas resursdatoros, un perifērijas ierīces, tādas kā printeris, modems vai skeneris. Kā lietojumprocesu piemērus var minēt tādus tīkla dienestus, kā datu un zināšanu bāzes, informācijas meklēšanas sistēmas, izziņu dienesti, apmācošas sistēmas, elektroniskais pasts, automatizētas projektēšanas sistēmas, telekonferences un citi.

Datoru tīkls ir nepieciešams, ja dokumentu, tabulu vai datu bāzu sagatavošanā vai izmantošanā vienlaikus piedalās vairāki cilvēki. Organizācijā, kurā ir vairāk nekā viens dators un nav tīkla, informācijas apmaiņa var notikt ar diskešu palīdzību. Šāds informācijas apmaiņas veids ir samērā neērts un lēns. Savukārt, ja organizācijā ir izveidots datortīkls, var organizēt kopēju disku lietošanu. Šajos koplietošanas diskos var izdalīt noteiktu apjomu katram lietotājam, kā arī veidot visiem lietotājiem vai tikai noteiktām lietotāju grupām pieejamas mapes un failus. Īpaši ērti tīklā ir strādāt ar datu bāzēm, jo tādā gadījumā lietotāji var strādāt vienlaikus arī tad, ja datu bāzē ir jāmaina informācija. Jaunās izmaiņas datu bāzē tūlīt ir redzamas arī pārējiem tās lietotājiem. Datortīklu parasti veido arī ekonomisko apsvēruma dēļ, piemēram, lai katram datoram nevajadzētu iegādāties savu printeri vai to pārmaiņus pārslēgt no viena datora pie otra, printeri pievieno vienam datoram un padara pieejamu visiem tīkla lietotājiem. Datoru tīklam var pieslēgt arī citas kopīgi izmantojamas ierīces.

2.stunda

Stundas temats: Datortīklu attīstības vēsture.

Stundas mērķis: Iepazīties ar datortīklu attīstības vēsturi.

Mācību uzdevumi:

1. Iepazīties ar datortīklu attīstības vēsturi.
2. Iepazīties ar datortīklu attīstības posmiem.

Datortīklu rašanās ir datortehnoloģijas evolūcijas loģiskais rezultāts. Pirmie 50.gadu datori bija lieli un dārgi, paredzēti nelielam skaitam lietotāju. Bieži šie monstri aizņēma veselas ēkas. Tādi datori tika izmantoti pakešu apstrādes režīmā. Pakešu apstrādes sistēmas tika veidotas uz lieldatora (*mainframe*) bāzes, t.i. jaudīga universālās nozīmes datora. Lietotāji gatavoja perfokartes, kuras saturēja programmu datus un komandas, un nodeva tās skaitļošanas centrā. Operatori ievadīja šīs kartes datorā, bet izdrukātus rezultātus lietotāji saņēma atpakaļ tikai nākošajā dienā. Tad viena nepareizi perforētā karte nozīmēja vismaz diennakts aizkavēšanos.

Lietotājiem interaktīvais darba režīms, kad no termināļa var operatīvi vadīt savu datu apstrādes procesu, būtu daudz ērtāks. Bet tolaik lietotāju intereses ignorēja, jo pakešu režīms ir visefektīvākais datora veikspējas izmantošanas režīms, tas ļauj izpildīt vienā laika vienībā vairāk lietotāju uzdevumu nekā jebkurš cits režīms. Tātad, šeit galvenais bija datora visdārgākās iekārtas, procesora, darbības efektivitāte, bet ne to izmantojošo speciālistu darba efektivitāte.

Daudztermināļu sistēmas - tīkla prototips

60.gadu sākumā, kad procesori kļuva lētāki, parādījās skaitļošanas procesa organizācijas jaunie paņēmieni, kas ļāva ievērot lietotāju intereses. Sāka attīstīties interaktīvās daudztermināļu laikdales sistēmas. Tad datoru izmantoja uzreiz vairāki lietotāji. Katra lietotāja rīcībā bija termināls, ar kura palīdzību viņš uzturēja dialogu ar datoru. Datora reakcijas laiks bija pietiekami mazs, lai lietotājam nebūtu manāms arī citu lietotāju paralēlais darbs ar datoru.

Tādas daudztermināļu centralizētas sistēmas ārēji jau bija ļoti līdzīgas lokālajiem datoru tīkliem. Termināļi izgāja aiz skaitļošanas centra robežām un izplatījās pa visu uzņēmumu. Un kaut skaitļošanas jauda palika pilnīgi centralizēta, dažas funkcijas, tādas, kā datu ievade un izvade, kļuva sadalītas. Ierindas lietotājs darbu pie lieldatora termināļa uztvēra apmēram tā pat, kā tagad viņš uztver darbu pie tīklam pieslēgta personālā datora. Lietotājs varēja dabūt pieeju kopējiem failiem un perifērijas iekārtām, pie tam viņam bija pilna ilūzija, ka viņš vienpersoniski pārvalda datoru, jo viņš varēja palaist vajadzīgo programmu jebkurā momentā un gandrīz uzreiz saņemt rezultātu.

Tādā veidā, daudztermināļu sistēmas, kuras strādā laikdales režīmā, kļuva par pirmo soli lokālo skaitļošanas tīklu radīšanas ceļā. Bet līdz lokālo tīklu rašanās vajadzēja vēl ilgākam laika

posmam, jo daudztermināļu sistēmas vēl saglabāja datu apstrādes centralizēto raksturu. No citas puses, uzņēmumu vajadzība pēc lokālajiem tīkliem vēl nebija nobriedusi: vienā ēkā vienkārši nebija ko apvienot tīklā, jo datoru augstās vērtības dēļ uzņēmumi nevarēja atļauties vairāku datoru iegādi. Tajā periodā darbojas tā saucamais "Groša likums", kurš empiriski atspoguļoja tā laika tehnoloģijas līmeni. Pēc šī likuma datora veikspēja bija proporcionāla tā vērtības kvadrātam. No tā izriet, ka par vienu un to pašu summu bija izdevīgāk nopirkt vienu jaudīgu mašīnu, nekā divas mazāk jaudīgas: to kopējā veikspēja bija daudz mazāka nekā dārgas mašīnas veikspēja.

Globālo tīklu rašanās

Vajadzība savienot datorus, kuri atrodas lielos attālumos viens no otra, šajā laikā jau bija pilnīgi nobriedusi. Viss sākās no vienkāršākā uzdevuma risinājuma: pieejas pie datora no termināļiem, kuri bija attālināti no tā uz daudziem simtiem vai pat tūkstošiem kilometru. Termināļi tika savienoti ar datoriem caur telefona tīkliem ar modemu palīdzību. Tādi tīkli atļāva daudziem lietotājiem gūt attālo pieeju vairāku spēcīgo superdatoru koplietojamiem resursiem. Parādījās sistēmas, kuros līdz ar attāliem savienojumiem tipa *termināls - dators* tika realizēti arī attālie savienojumi tipa *dators - dators*. Radās iespēja apmainīties ar datiem automātiskajā režīmā, kas ir jebkura datoru tīkla bāzes mehānisms. Izmantojot šo mehānismu, pirmajos tīklos tika realizēti dažādi pakalpojumi, tādi, kā:

- failu apmaiņa,
- datu bāžu sinhronizācija,
- elektroniskais pasts un citi pakalpojumi, kuri tagad kļuvuši ir tradicionāli.

Tāpat hronoloģiski pirmie parādījās globālie tīkli. Tieši, veidojot globālos tīklus, bija pirmo reizi piedāvātas un noslīpētas daudzas mūsdienu datortīklu pamatidejas un koncepcijas. Tādas, kā:

- komunikācijas protokolu daudzslāņu uzbūve,
- pakešu komutācijas tehnoloģija,
- pakešu maršrutēšana apvienotajos tīklos.

70.gadu sākumā parādījās jaunā tehnoloģija datorkomponentu ražošanā - lielās integrālās shēmas. To salīdzinoši nelielā cena un augstas funkcionālās iespējas noveda pie minidatoru radīšanas, kuri kļuva par lieldatoru reāliem konkurentiem.

Pat nelieli uzņēmumi un to nodaļas guva iespēju pirkt datorus. Minidatori pildīja tādus uzdevumus, kā tehnoloģisko iekārtu, noliktavu uzskaites vadība un citus uzdevumus uzņēmuma nodaļas līmenī. Datori ieviesās visā uzņēmumā, taču visi vienas organizācijas datori joprojām turpināja strādāt autonomi.

Ar laiku datoru lietotāju vajadzības izauga, parādījās datu apmaiņas nepieciešamība ar citiem blakus datoriem. Rezultātā uzņēmumi un organizācijas sāka savienot savus minidatorus un izstrādāt programmatūru to mijiedarbībai. Parādījās pirmie *lokālie datortīkli*. Agrāk tie atšķīrās no mūsdienu lokālajiem tīkliem, pirmām kārtām, ar savām saskarnes (interfeisa) iekārtām. No sākuma, lai savienotu datorus cits ar citu tika izmantotas nestandarta iekārtas katra ar savām datu attēlošanas veidiem, saviem kabeļu tipiem. Šīs iekārtas varēja savienot tikai tos datoru tipus, kuriem tās bija paredzētas.

Lokālo tīklu standarta tehnoloģiju radīšana

80.gadu vidū tika pieņemtas datoru apvienošanas tīklā standarta tehnoloģijas: Ethernet, Arcnet, Token Ring un stāvoklis lokālajos tīklos sāka kardināli mainīties. Spēcīgs stimuls to attīstībai bija uzradušies *personālie datori*. Šie masveida produkti kļuva par ideāliem elementiem tīklu uzbūvei: no vienas puses, tie bija pietiekami jaudīgi (veiktspējīgi) tīkla programmatūras darbībai, bet no otras puses - tiem vajadzēja apvienot savu skaitļošanas jaudu, lai risinātu sarežģītus uzdevumus, kā arī kopīgi lietot dārgas perifērijas iekārtas, piemēram, ietilpīgu disku masīvus. Personālie datori sāka dominēt lokālajos tīklos ne tikai kā klienta datori, bet arī kā datu glabāšanas un apstrādes centri, t.i. tīklu serveri, aizvietojoš šajās lomās minidatorus un lieldatorus. Standarta tīkla tehnoloģijas ieviešana pārvērta lokālā tīkla konstruēšanas procesu no mākslas rutīnas darbā. Lai radītu tīklu, bija pietiekami iegādāties attiecīga standarta tīkla adapterus, piemēram, Ethernet, standarta kabeli, pievienot adapterus kabelim ar standarta spraudņiem un uzstādīt datorā vienu no populārākajām operētājsistēmām, piemēram, *NetWare*. Tad tīkls bija gatavs strādāt, un katra jauna datora pievienošana neizraisīja nekādu problēmu.

3. – 4.stunda

Stundas temats: Datortīklu veidi.

Stundas mērķis: Iepazīties ar datortīklu veidiem.

Mācību uzdevumi:

1. Iepazīties ar datortīklu veidiem.
2. Iepazīties ar datortīklu sniegtajām priekšrocībām.
3. Izprast datu pārsūtīšanas jēdzienu.

Atkarībā no tīkla datoru izvietojuma, tos nosacīti var iedalīt vairākās grupās:

- lokālajā datoru tīklā (Local Area Network – LAN);
- pilsēttīkls (Metropolitan Area Network – MAN);
- teritoriālais tīkls (Wide Area Network – WAN);
- ar GAN (Global Area Network) apzīmē tīklu, kas savieno kontinentus.

Lokālais tīkls ir datoru tīkls, kas ir izvietots relatīvi nelielā teritorijā (līdz 1-2 km), parasti tā ir ierobežota ar vienu ēku, uzņēmumu, iestādi u.t.t. Vispārējā gadījumā lokālais tīkls pieder vienai organizācijai. Nelielo attālumu dēļ lokālajos tīklos ir iespēja izmantot relatīvi dārgas augstvērtīgas kabeļu sakaru līnijas, kuras ļauj, izmantojot vienkāršas datu pārraides metodes, sasniegt lielus datu apmaiņas ātrumus.

No sākuma lokālie datoru tīkli bija nelieli un apvienoja ne vairāk kā desmit viena veida datorus. Tehnoloģija ierobežoja tīkla izmērus, tas ir datoru skaitu un tīkla fizisko garumu. 80-to gadu sākumā vispopulārākais tīklu tips sastāvēja ne vairāk kā no 30 datoriem, bet kabeļa garums nepārsniedza 185m. Tādus tīklus varēja izvietot ēkas stāva vai nelielas organizācijas robežās.

Pirmie lokālo tīklu veidi neapmierināja to lielo uzņēmumu vajadzības, kuru ofisi atradās dažādās vietās. Tiklīdz datoru tīklu priekšrocības kļuva neapstrīdamas, korporācijām radās tīklu paplašināšanas problēma, lai saglabātu konkurētspēju. Tā uz lokālo tīklu bāzes radās lielākas sistēmas. Šodien, lai savienotu lietotājus no dažādām pilsētām un valstīm, lokālo tīklu ģeogrāfiskās robežas tiek paplašinātas. LAN pāraug globālajā tīklā (WAN), kur datoru skaits var variēt no desmit līdz vairākiem tūkstošiem.

Pilsēttīkls (MAN) ir paredzēts lielas pilsētas teritorijas apkalpošanai. Tas aptver lielāku ģeogrāfisko teritoriju nekā LAN, bet mazāku nekā WAN. *Pilsēttīkls* ir mazāk izplatīts tīklu tips, kas parādījās samērā nesen. Tajā laikā, kad LAN vislabāk der resursu koplietošanai īsos attālos un apraides pārraidēm, bet globālie tīkli nodrošina darbu lielos attālos, bet ar ierobežoto ātrumu, pilsēttīkli aizņem starpstāvokli. Tās izmanto kopnes sakaru ciparlīnijas, bieži optiskās, ar ātrumiem no 45 Mbit/s, un ir paredzētas, lai savienotu lokālos tīklu pilsētas mērogā un lokālos tīklus ar globāliem. Sākumā šos tīklus izstrādāja datu pārraidei, bet tagad tie uztur arī

tādus pakalpojumus, kā videokonferences un balss un teksta integrālā pārraide. Pilsētīklu attīstību parasti veic vietējās telefona kompānijas. Pilsētīkli ir publiskie tīkli, tāpēc to pakalpojumi ir lētāki, nekā privātīkla uzbūve pilsētas mērogā. Tātad pilsētīkliem ir diezgan lieli attālumi starp mezgliem (desmitiem kilometru), bet kvalitatīvas sakaru līnijas un augsti datu apmaiņas ātrumi, dažreiz pat augstāki nekā lokālajiem tīkliem. Kā arī lokālo tīklu gadījumā, veidojot pilsētīklus, esošas sakaru līnijas netiek izmantotas, bet tiek liktas no jauna. Var teikt, ka pilsētīklu rašanās ir viena no lokālo un globālo tīklu tuvināšanās izpausmēm.

Teritoriālais tīkls (Wide Area Network, WAN) ir datortīkls, kas nosedz plašu ģeogrāfisku platību, iesaistot lielu datoru daudzumu. Labākais teritoriālā tīkla piemērs ir Internets.

Teritoriālos tīklus izmanto lai savā starpā savienotu vairākus lokālos tīklus, ļaujot viena lokālā tīkla datoriem sazināties ar citu lokālo tīklu datoriem. Daudzi teritoriālie tīkli ir veidoti kādas organizācijas vajadzībām un ir privāti, savukārt citi, ko veido Interneta Pakalpojumu Sniedzēji nodrošina organizāciju lokālajiem tīkliem pieeju Internetam. Teritoriālos tīklus parasti veido izmantojot nomātās līnijas. Katras nomātās līnijas galā, maršrutētājs savieno vienas puses lokālo tīklu ar teritoriālā tīkla centrmezglu. Mūsdienās, kad Internets nodrošina lielas ātrdarbības teritoriālo tīklu, ir samazinājusies vajadzība pēc privātiem tīkliem, kas ir veidoti izmantojot organizācijai piederošas nomātās līnijas.

Lokālo tīklu resursi

Galvenais tīkla uzdevums ir kopīga resursu izmantošana un pastāvīga komunikācija (informācijas apmaiņa) reālā laika režīmā. Tīkla resursi ir:

- dati,
- lietojumprogrammas vai lietojumprocesi, kas darbojas resursdatoros,
- perifērijas ierīces, piemēram,
 - printeris;
 - modems;
 - skeneris.

Kā lietojumprocesu piemērus var minēt tādus tīkla dienestus, kā:

- datu un zināšanu bāzes,
- informācijas meklēšanas sistēmas,
- izziņu dienesti,
- apmācošas sistēmas,
- elektroniskais pasts,
- automatizētas projektēšanas sistēmas,
- telekonferences un citi.

Datu pārsūtīšanas ātrums ir, bitu, rakstzīmju vai datu bloku skaits, ko pārsūta laika vienībā starp divām iekārtām datu apstrādes sistēmā. Vidējo datu pārsūtīšanas ātrumu parasti nosaka ieraksta nolasīšanas ierīču ātrdarbība, bet momentāno - saskarnes vai kanāla caurlaidspēja.

5.stunda

Stundas temats: Lokālā datortīkla arhitektūra.

Stundas mērķis: Iepazīties ar lokālo datortīklu jēdzieniem – datortīklu arhitektūra, aktīvā un pasīvā tīkla aparatūra., .

Mācību uzdevumi:

1. Izprast lokālā datortīkla arhitektūras jēdzienu.
2. Izprast aktīvās un pasīvās tīkla aparatūras jēdzienu.
3. Iepazīties ar vienādranga datortīkliem.
4. Iepazīties ar tīkliem ar izdalītiem serveriem

Tīkla arhitektūra ir datoru tīkla uzbūves koncepcija un tā darbības principi. Tīkla arhitektūra nosaka datoru tīkla fiziskos parametrus un ir balstīta uz kādu no topoloģijām.

Datoru tīklā var izdalīt aktīvos un pasīvos elementus. Aktīvie elementi saņem un noraida datu paketes, kā arī aktīvi piedalās datu apmaiņas procesā. Aktīvās iekārtas ir:

- tīkla adapteri, kas atrodas datorā un ir informācijas raidītāji un tās saņēmēji;
- centrmezgli, komutatori un maršrutētāji, kas kalpo tam, lai no raidītāja informāciju nosūtītu adresātam.

Pasīvie komponenti ir kabeļi un to savienojumi, kas nodrošina, ka signāls no vienas aktīvās iekārtas nonāk citā.

Tīklu veidi

No tīklu organizācijas viedokļa, tīklus var iedalīt divās lielās grupās:

- vienādranga (*peer-to-peer*) tīkli;
- tīkli ar izdalītiem (*dedicated*) serveriem.

Vienādranga tīkls

Vienādranga tīklā katrs dators var būt gan klients, gan serveris vai apvienot abas šīs funkcijas. Šādā tīklā parasti tiek kopīgi izmantotas dažādas iekārtas, piemēram, CD-ROM, skeneri, printeri. Katrs vienādranga tīkla lietotājs var piešķirt tiesības citiem lietotājiem piekļūt noteiktiem sava datora resursiem jeb nodot tos kolektīvai lietošanai (*sharing*). Vienādranga tīklā parasti ir vairāki serveri, jo failus ir izdevīgāk glabāt tajā datorā, kurā tos visbiežāk lieto.

Lai izveidotu vienādranga tīklu, ir nepieciešami papild līdzekļi – katram datoram ir vajadzīga tīkla karte, bet datori savā starpā ir jāsavieno ar kabeļiem. Vienādranga tīkli ir piemēroti darbam nelielās grupās. Ja šādā tīklā esošo datoru skaits pārsniedz 10, tīkla darba ātrums jūtami samazinās

Vienādranga tīkla priekšrocības ir:

- lētums;
- vienkāršota vadība;

- elastīga struktūra.

Trūkumi:

- pieaugot lietotāju skaitam un darba intensitātei, vienādranga tīklu serveri kļūst arvien lēndarbīgāki.

Klients-serveris tipa tīkls

Klients-serveris arhitektūras tīkla centrā atrodas jaudīgs dators (serveris), kas ir savienots ar pārējām darba stacijām (klientiem). Izdalīti serveri parasti ir nepieciešami tīklos, kuros ir vairāk nekā 10 datoru. Izdalīts serveris, pateicoties tā specializācijai, ir ātrdarbīgāks, nodrošina augstāku slepenības pakāpi un darbībā ir stabilāks nekā vienādranga tīkla serveris. Izdalīts failu serveris ļauj uz kopējā diska glabāt ne tikai datus, bet arī izpildāmās programmas.

Tīkla vadību, t.i., atsevišķu darba staciju vadību un ārējo tīkla ierīču kontroli veic ar speciālas jaudīgas programmatūras palīdzību.

Resursu koplietošana

Serveris tiek projektēts tādā veidā, lai dotu pieejas iespējas failu un printeru kopai, pie tam nodrošinot augstu veiktspēju un aizsardzību. Datu pieejas vadība un administrēšana tiek veikta centralizēti. Resursi parasti tiek izvietoti arī centralizēti, kas atvieglo to meklēšanu un apkalpošanu..

Aizsardzība

Galvenais arguments, kas nosaka tīkla uz servera pamata izvēli, parasti ir datu drošība. Tādos tīklos, kā Windows NT, ar drošības problēmām var nodarboties viens administrators: viņš veido vienotu drošības politiku (security policy) un to pielieto attiecībā uz katru tīkla lietotāju.

Datu rezerves kopēšana

Tā kā vitāli svarīga informācija izvietota centralizēti, t.i., koncentrēta vienā vai vairākos serveros, nav grūti veikt tās regulāro rezerves kopēšanu (backup).

Redundance

Pateicoties sistēmu pārpilnībai, jebkurā serverī dati var tikt dublēti reālā laika režīmā, tāpēc jā tiks sabojāta informācijas galvenā krātuve, informācija nebūs pazaudēta – vienmēr varēs izmantot rezerves kopiju.

Lietotāju skaits

Tīkli uz servera pamata spēj uzturēt tūkstošus lietotāju. Vadīt tāda izmēra tīklus, ja tie būtu vienādranga, būtu neiespējams.

Aparatūra

Tā kā klienta dators nepilda servera funkcijas, tā raksturlielumu prasības nosaka pats lietotājs.

6. – 7.stunda

Stundas temats: Lokālo datortīklu topoloģijas.

Stundas mērķis: Iepazīties ar datortīklu topoloģijām.

Mācību uzdevumi:

1. Izprast jēdzienu datortīklu topoloģijas.
2. Iepazīties ar datortīklu topoloģiju veidiem..
3. Iepazīties ar vienādranga datortīkliem.
4. Iepazīties ar tīkliem ar izdalītiem serveriem

Termins “tīkla topoloģija” nozīmē datoru, kabeļu un citu tīkla komponentu fizisko izvietojumu.

Tīkla raksturojumi ir atkarīgi no topoloģijas tipa. Topoloģijas izvēle iespaido:

- nepieciešamās tīkla iekārtas sastāvu;
- tīkla iekārtas iespējas;
- tīkla paplašināšanas iespējas;
- tīkla vadības metodi.

Tīkla topoloģiju var definēt kā grafa konfigurāciju, kur virsotnēm atbilst datori vai citas iekārtas, piemēram, koncentratori, bet šķautnēm – fiziskās saites starp tiem. Tīklam pieslēgtos datorus bieži sauc par stacijām vai mezgliem.

Atzīmēsim, ka *fizisko saišu* konfigurāciju noteic datoru elektriskie savienojumi un tā var atšķirties no *loģisko saišu* konfigurācijas. Loģiskās saites ir datu pārraides maršruti starp tīkla mezgliem.

Bāzes topoloģijas

Visi tīkli tiek uzbūvēti uz triju bāzes topoloģiju pamata:

- maģistrāle jeb kopne (*bus*);
- zvaigzne (*star*);
- gredzens (*ring*).

Maģistrāles topoloģija

Kopnes topoloģija izmanto vienu kabeli, ko sauc par kopni (maģistrāli), vai segmentu, pie kura tiek pieslēgti visi tīkla datori un citas tīkla iekārtas. Tāda topoloģija ir visvienkāršākā tīkla realizācija.

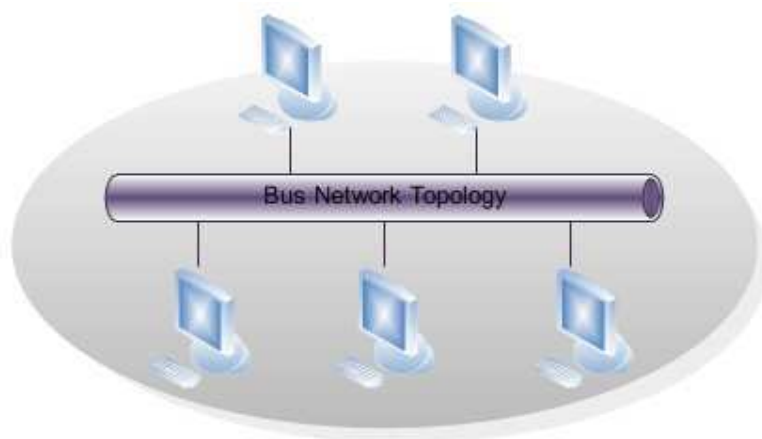
Tīklā ar kopnes topoloģiju datori adresē datus konkrētajam datoram, pārraidot tos caur kabeli elektrisko signālu veidā. Dati tiek pārraidīti visiem tīkla datoriem; bet informāciju pieņem tikai tas dators, kura adrese atbilst saņēmēja adresei, šifrētai šajos signālos. Pie tam katrā laika momentā pārraidīt datus var tikai viens dators.

Tā kā dati tiek pārraidīti tīklā tikai ar vienu datoru, tā veiktspēja ir atkarīga no datoru skaita, kuri ir pieslēgti maģistrālei. Jo vairāk datoru, jo lielāks datoru skaits gaida pārraidi un jo lēnāks ir tīkls.

Kopne ir pasīva topoloģija. Tas nozīmē, ka datori tikai “klausās” pārraidāmos datus, bet nepārvieta tos no avota līdz saņēmējam. Tāpēc, ja kāds dators izies no ierindas, tas neietekmēs tīkla darbību. (Aktīvās topoloģijās datori reģenerē signālus un pārraida tos tālāk.) Bet kabeļa pārrāvums pārtrauks tīkla funkcionēšanu.

Elektriskie signāli izplatās no viena kabeļa gala līdz otram. Ja netiek veikti nekādi speciāli pasākumi, signāls, sasniedzot kabeļa galu, atstarosies un radīs traucējumus, neļaujot citiem datoriem veikt pārraidi. Tāpēc kabeļa galos elektriskie signāli jādzēš. Šim nolūkam izmanto terminatorus, kuri absorbē šos signālus.

Lai savienotu divus kabeļa segmentus, izmanto atkārtotāju (*repeater*), kas pastiprina signālu pirms tā pārraides uz nākamo segmentu.



Priekšrocības:

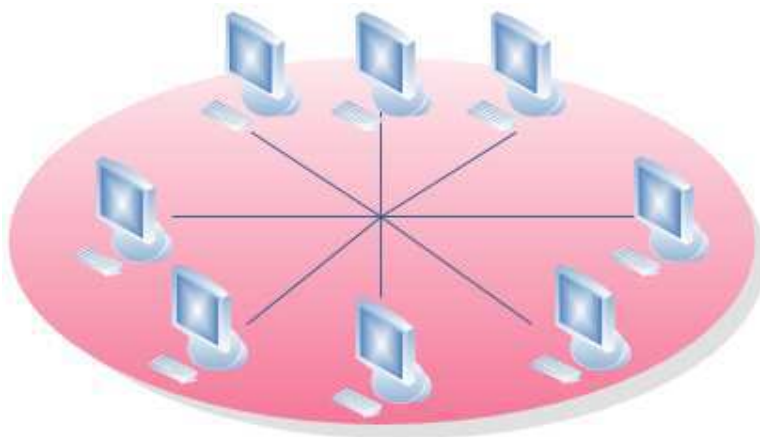
- lēts kabelis un spraudņi;
- vienkārša uzstādīšana (jebkurā brīdī darba staciju pie tīkla var pieslēgt vai atslēgt no tā, nepārtraucot visa tīkla darbu);
- darba stacijas ar informāciju var apmainīties bez servera starpniecības.

Trūkumi:

- kabeļa pārtrūkšanas gadījumā no ierindas iziet viss tīkls;
- grūti noteikt kabeļa bojājuma vietu;
- ierobežots kabeļa garums, kā arī pieslēdzamo staciju skaits;
- iespēja nesankcionēti pieslēgties tīklam, jo ir ļoti vienkārši tīklā ievietot kādu starpposmu.

Zvaigznes topoloģija

Zvaigznes topoloģijā visi tīklā ieslēgtie datori ir savienoti ar centrmezglu (*hub*), kas nodrošina kopējo savienojumu tā, lai katrs dators var apmainīties ar informāciju ar jebkuru citu tīkla datoru.



Šā slēguma tipa **priekšrocības**:

- kabeļa bojājums rada problēmas tikai vienam datoram un neietekmē pārējā tīkla darbu;
- viegli pieslēgt jaunu datoru, jo tas ir jāpieslēdz tikai centrmezglam;
- drošs aizsardzības mehānisms pret nesankcionētu piekļūšanu (iespējama centralizēta tīkla vadība un uzraudzība);
- liels datu pārraides ātrums no darba stacijas līdz serverim.

Trūkumi:

- ja centrmezgls neatrodas slēguma vidū, bet malā, darba staciju pievienošana var kļūt apgrūtināta un sadārdzināties;
- ja informācijas apmaiņa starp darba staciju un centrmezglu notiek ātri, tad starp atsevišķiem datoriem tā var notikt lēnāk;
- visa tīkla jauda ir atkarīga no centrmezgla jaudas;
- centrmezgla bojājums aptur visu tam pieslēgto staciju sakarus, jo bez tā palīdzības atsevišķas darba stacijas nevar kontaktēties.

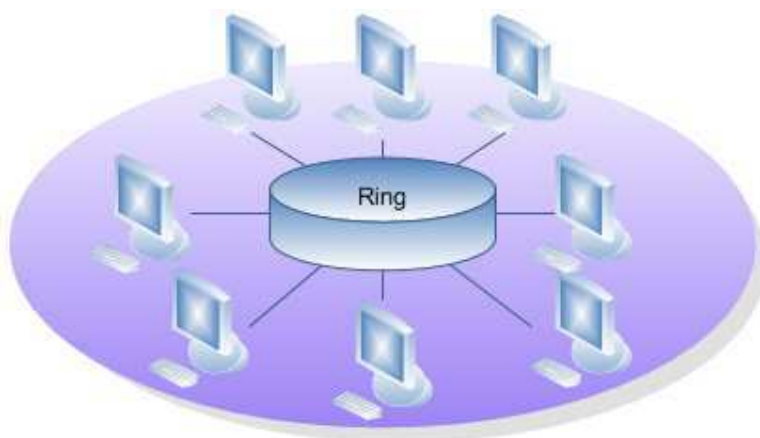
Gredzena topoloģija

Gredzena topoloģijā datori tiek pieslēgti kabelim, kurš ir saslēgts gredzenā. Tāpēc šim kabelim vienkārši nevar būt brīva gala, pie kura jāpieslēdz terminators. Signāli tiek pārraidīti pa riņķi vienā virzienā un iziet cauri katram datoram. Atšķirībā no pasīvas maģistrāles topoloģijas, šeit katrs dators izpilda atkārtotāja lomu, pastiprinot signālus un pārraidot tos nākamajam datoram. Tāpēc ja izies no ierindas viens dators, viss tīkls pārtrauks funkcionēt. Tīklos ar gredzena topoloģiju izmanto speciālus līdzekļus, lai sabojātais dators nepārtrauktu sakaru kanālu starp citiem datoriem. Gredzens ir ļoti ērta konfigurācija atgriezeniskās saites organizēšanai.

Dati, izdarijuši pilnu apgriezību, atgriežas pie datora-avota, kurš var kontrolēt datu piegādi adresātam.

Viens no datu pārraides veidiem pa riņķa tīklu tiek saukts par marķiera (*token*) nodošanu. Marķieris (neliels datu bloks) tiek secīgi pārraidīts no datora datoram, kamēr to saņems dators, kurš “grib” aizsūtīt datus. Pārraidošs dators pārveido marķieri, pievieno marķierim datus un saņēmēja adresi un aizsūta to tālāk pa riņķi. Dati iziet cauri katram datoram, kamēr sasniegs datoru, kura adrese atbilst saņēmēja adresei. Saņēmošs dators nosūta pārraidošam datoram ziņojumu, kur apstiprina datu saņemšanas faktu. Saņemis apstiprinājumu, pārraidošs dators veido jaunu marķieri un atgriež to tīklā.

Var likties, ka marķiera nodošana aizņem daudz laika, bet īstenībā marķiera virzīšanas ātrums ir salīdzināms ar gaismas ātrumu. 200 m diametra riņķī marķieris var cirkulēt ar frekvenci 10 000 apgriezienu sekundē.



Priekšrocības:

- tā kā informācija tīklā cirkulē pa riņķi starp virknē saslēgtiem datoriem, tad būtiski samazinās piekļūšanas laiks datiem;
- nav kopējā tīkla garuma ierobežojuma, jo noteicošais ir attālums starp diviem datoriem.

Trūkumi:

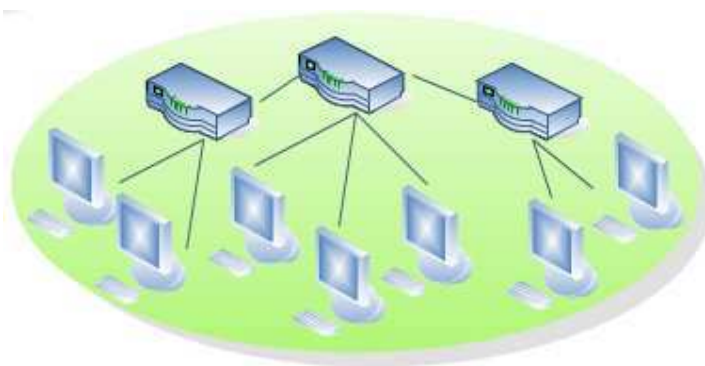
- datu pārraides laiks palielinās proporcionāli gredzenā savienoto datoru skaitam;
- datu pārraidē ir iesaistīta katra darba stacija. Ja nelieto speciālus pārejas savienojumus, vienas darba stacijas iziešana no ierindas var paralizēt visu tīklu;
- lai šādam tīklam pievienotu jaunu datoru, tīkla darbība uz laiku ir jāpārtrauc.

Gredzena topoloģiju izmanto specifiskos tīklu risinājumos, un tā nav sevišķi izplatīta.

Jaukta tipa topoloģijas

Praksē bieži lieto jauktu topoloģiju, apvienojot bāzes topoloģijas. Tādējādi pilnīgāk tiek izmantotas minēto topoloģiju priekšrocības un novērsti daži trūkumi. Piemēram, ja uzņēmums ir

izvietots vairākās ēkās, starp tām var izveidot optiskā kabeļa maģistrāli, bet ēku iekšienē veidot vītā pāra zvaigznes slēgumu.



8. – 9.stunda

Stundas temats: Tīkla kabeļi.

Stundas mērķis: Iepazīties ar tīkla kabeļiem.

Mācību uzdevumi:

1. Iepazīties ar koaksiālo kabeli.
2. Iepazīties ar vītā pāra kabeli.
3. Iepazīties ar optisko kabeli.

Šodien vairākums tīklu izmanto savienojumiem vadus, vai kabeļus. Tie ir starpdatoru signālu fizikālā pārraides vide. Pasaulē ir vairāk nekā 2200 kabeļu veidi. Praksē tiek izmantotas trīs galvenās kabeļu grupas:

- koaksiālais kabelis (*coaxial cable*);
- vītais pāris (*twisted pair*);
- optiskais kabelis (*fiber-optical*).

Koaksiālais kabelis



Koaksiālais kabelis sastāv no centrālā vara vada un ārējā ekrāna, starp kuriem atrodas izolējošs materiāls. Ārējais izolējošais slānis pasargā no ārējās vides ietekmes. Kabeli pārsvarā izmanto *Ethernet* tipa tīklos, tāpēc šo kabeļu veidu bieži vien dēvē par *Ethernet* kabeli. Pastāv divu veidu *Ethernet* kabeļi:

- tievais (*Thin Ethernet Cable*);
- resnais (*Thick Ethernet Cable*).



Tievā koaksiālā kabeļa pieslēgumam izmanto *BNC* standarta kontaktus. Ja tīklā izmanto papildu aparātūru, kopējais tīkla kabeļu garums var sasniegt 925 m.

Koaksiālā kabeļa izmantošanas **priekšrocības**:

- zemas apkalpošanas izmaksas;
- vienkārša uzstādīšana;
- laba noturība pret traucējumiem, nav nepieciešama papildu aparātūra.

Trūkumi:

- ierobežots segmenta garums (185 m) un pieslēdzamo datoru skaits (30);

- zema drošība – kabeļa bojājums izraisa traucējumus visā tīklā;
- sarežģīti mainīt tīkla topoloģiju;
- maksimālā tīkla caurlaidspēja – līdz 10 Mb/s.

Resnā koaksiālā kabeļa maksimālais segmenta garums starp divām darba stacijām var būt līdz 500 m, bet, izmantojot speciālu aparāturu, – 2500 m

Vītāis pāris



Vītā pāra kabelis sastāv no diviem savstarpēji savītiem izolētiem vara vadiem. Parasti vienā kabelī šādi vītā pāri ir vairāki. *Ethernet* tīklos izmanto 8 dzīslu kabeli (4 vītā pāri). Atkarībā no kabeļu viļņu parametriem tie ir sadalīti sešās kategorijās. 3. kategorijas vītā pāra kabeli izmanto līdz 10 Mb/s tīkliem, bet 5. kategorijas kabelus – 10, 100 un 1000 Mb/s tīklos. Tā kontaktligzdas standarts ir *RJ-45*.

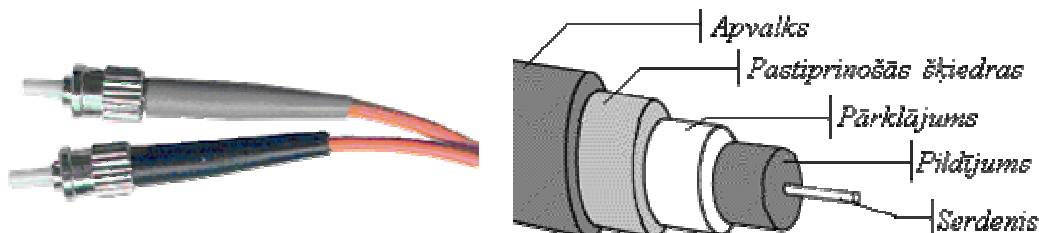
Vītā pāra kabeļa izmantošanas **priekšrocības**:

- lēts kabelis un spraudņi;
- vienkārši paplašināt tīklu;
- samērā augsta drošība – kabeļa bojājums pārtrauc tikai viena datora darbu;
- liels datu apmaiņas ātrums.

Trūkumi:

- sarežģīta instalācija;
- zema noturība pret traucējumiem;
- ierobežots segmenta garums (100 m);
- nepieciešama papildu aparātūra.

Optiskais kabelis



Optiskais kabelis pārvada gaismas viļņus. Modulētais (ar mainīgu intensitāti) gaismas stars optiskajā šķiedrā tiek raidīts (iespīdināts) ar speciāla lāzera vai gaismas diodes palīdzību. Kabelis sastāv no diviem vadiem, no kuriem katrs var pārraidīt datus tikai vienā virzienā. Katrā apvalkā plastikas kārtu veidā atrodas pastiprinošās šķiedras. Kabeļa garumam praktiski nav nekādas nozīmes. Pirmās problēmas datu pārraidē rodas tad, ja kabeļa garums sasniedz 50 kilometrus.

Optiskos kabeļus iedala:

- vienmoda (šķiedras izmērs $9/125\ \mu\text{m}$);
- daudzmodu ($50/125$; $62,5/125\ \mu\text{m}$).

Optisko kabeli parasti izmanto kā lielu tīklu mugurkaulu (*backbone*) vai arī lieljaudas serveru pieslēgšanai. Šis ir pats dārgākais kabeļu veids.

Optiskā kabeļa izmantošanas **priekšrocības**:

- ļoti liels datu apmaiņas ātrums ($>2\ \text{Gb/s}$);
- ļoti liels segmenta garums;
- augsta drošība un noturība pret traucējumiem.

Trūkumi:

- dārgs;
- sarežģīta instalācija;
- dārga papildu aparatūra.

10.stunda

Stundas temats: Kabeļu marķēšana.

Stundas mērķis: Iepazīties ar kabeļu marķējumiem.

Mācību uzdevumi:

1. Iepazīties ar kabeļu marķējumiem.
2. Iepazīties ar kabeļa izvēles kritērijiem.

Vītais pāris

Marķējums (Gauge) – tam nolūkam, lai kabeļus varētu salīdzināt vienu ar otru, pastāv standartizācijas un marķēšanas sistēma. Vislielāko izplatību ieguvusi sistēma American Wire Gauge (AWG). Praksē no visas šīs sistēmas ir vērts no galvas atcerēties tikai sekojošo: jo lielāks skaitlis atrodas aiz abreviatūras AWG, jo tievāku dzīslu nosaka šis numurs. Piemēram, ja kabelim ir marķējums, kura daļa sastāv no simbolu kopuma “AWG – 24” tad tam ir resnāka dzīsla, nekā kabelim, kura marķējuma daļu sastāda simbolu kopums “AWG-26”, bet attiecīgi tas nodrošina mazāku pretestību elektriskā signāla izplatībai, ļauj izveidot garākas pārvades līnijas. Atkarībā no aizsargātības līmeņa vītā pāra kabeļus iedala vairākās grupās:

- ekranētos (*Shielded Twisted Pair – STP*);
- neekranētos (*Unshielded Twisted Pair – UTP*);
- āra darbiem paredzētajos (*NYY*).

Speciālais standarts Electronic Industries Association and Telecommunications Industries Association (EIA/TIA) 568 Commercial Building Wiring Standard nosaka UTP septiņas kategorijas.

1. kategorija. Tradicionālais telefona kabelis, pa kuru var pārraidīt tikai runu, bet ne datus. Vairākums telefona kabeļu, kuri bija ražoti līdz 1983. gadam, attiecas uz 1. kategoriju.
2. kategorija. Kabelis, kurš ir spējīgs pārraidīt datus ar ātrumu līdz 4 Mbitiem/sek. Sastāv no četriem vītiem pāriem.
3. kategorija. Kabelis, kurš ir spējīgs pārraidīt datus ar ātrumu līdz 10 Mbitiem/sek. Sastāv no četriem vītiem pāriem. Paredzēts kā datu, tā arī balss pārraidei.
4. kategorija. Kabelis, kurš ir spējīgs pārraidīt datus ar ātrumu līdz 16 Mbitiem/sek. Sastāv no četriem vītiem pāriem.
5. kategorija. Kabelis, kurš ir spējīgs pārraidīt datus ar ātrumu līdz 100 Mbitiem/sek. Sastāv no četriem vītiem pāriem.
6. kategorija. Kabelis, kurš ir spējīgs pārraidīt datus ar ātrumu līdz 1000 Mbitiem/sek. Sastāv no četriem vītiem pāriem.

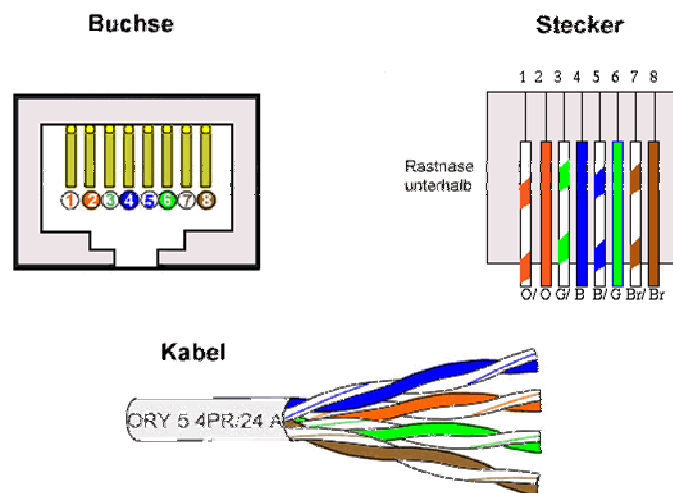
Vadu savīšana ļauj samazināt ārējo elektromagnētisko traucējumu iedarbību un vairāku vīto pāru gadījumā, samazina blakus vadu signālu inducēšanos, angliski dēvē - *crosstalk*. Vītais

pāris izveido samērā lētu informācijas pārraides vidi. Vijumu skaits ir svarīgs vīto pāri raksturojošs lielums, piemēram, 3. kategorijas vīto pāru kabelim ir 9 vijumi uz metru. Par labu vīto pāri uzskata tādu, kuram ir 12-22 vijumi uz pēdu (twists per foot). Lai droši aizsargātu kabeli pret traucējumiem, ko rada elektroniskās ierīces, kas atrodas kabeļa tiešā tuvumā, vītos pārus ietin folijā un ievieto vara vadu pinuma ekrānā. Šos kabelus sauc par ekranēto vīto pāri (*STP - Shielded Twisted Pair*) pretstatā parastam - neekranētam kabelim (*UTP - Unshielded Twisted Pair*). Ekranētie vītie pāri ir samērā dārgi un tos izmanto vietās ar paaugstinātu elektromagnētisko starojumu, piemēram, liftu šahtās, noliktavās, kurās strādā elektrokāri, jaudīgu transformatoru tuvumā u.c.

Vītais pāris tiek izmantots, ja ir nepieciešams ar nelieliem materiāliem ieguldījumiem organizēt LAN, pie kuras var viegli un ātri pieslēgt datorus. Vīto pāri nav ieteicams izmantot, kad jāpārraida dati lielos attālumos ar lieliem ātrumiem.

Lai pieslēgtu vīto pāri datoram, tiek izmantoti telefona savienotāji RJ-45. RJ-45 ir līdzīgi savienotājiem RJ-11, kuri ir izplatīti telefona tīklos, taču tiem ir būtiskas atšķirības. Pirmkārt, RJ-45 ir lielāki pēc izmēriem un neder RJ-11 ligzdai. Otrkārt, RJ-45 ir 8 kontakti, bet RJ-11 – tikai 4.

EIA/TIA 568B standarts



Kabeļa izvēle

Pirms izvēlēties Jums vispiemērotāko kabeļa tipu, atbildiet uz sekojošiem jautājumiem. Tie palīdzēs Jums noorientēties milzīgajā kabeļu produkcijas daudzveidībā.

- Kāda ir plānotā tīkla trafika intensitāte?
- Kādas ir prasības datu aizsardzībai?
- Uz kādu maksimālu garumu ir jāstiepj kabelis?
- Kādiem raksturojumiem ir jāatbilst kabelim?
- Cik daudz līdzekļu ir izsniegts projekta realizācijai?

11.stunda

Stundas temats: Atkārtotāji, pastiprinātāji.

Stundas mērķis: Iepazīties ar tīkla atkārtotājiem un pastiprinātājiem.

Mācību uzdevumi:

1. Iepazīties ar tīkla atkārtotājiem.
2. Iepazīties ar tīkla pastiprinātājiem.

Atkārtotājs (repeater) atjauno signālu līmeni (amplitūdu), kas samazinās, signālam izplatoties caur kabeļa vidi (faktiski atkārtotājs ir signālu pastiprinātājs). Tas savieno kabeļa segmentus, ļaujot palielināt pārraides tālumu vai tīklam pieslēgto datoru skaitu.

Piezīme. Atkārtotājs var savienot tikai viendabīgus tīklus ar vienādiem 2. slāņa protokoliem. Tas nepilda datu pārveidošanu vai filtrāciju.

Atkārtotājs ir vislētākais līdzeklis, kā paplašināt tīklu, bet tas nav ieteicams, ja tīkla trafiks ir intensīvs. Atkārtotājs pārsūta no segmenta uz segmentu katru datu bitu, pat ja dati ir kļūdaini vai nav paredzēti šim segmentam. Atkārtotāja galvenās īpašības:

- Atkārtotājs (repeater) ir iekārta, kas atklājot signālu vienā kabelī pārraida tā pastiprinātu kopiju uz otru kabeli.
- Atkārtotāji darbojas fizikālajā slānī un pastiprina visus pārraidāmos signālus tos nefiltrējot.
- Ar atkārtotājiem savienotie segmenti veido kopēju sadursmes apgabalu (collision domain).
- Atkārtotājs savieno 2 segmentus, kuru max garums <500m, piem., savienojot 3 segmentus ar 2 atkārtotājiem, var izveidot LT, kas aptver 1500m.
- Datori nevar noteikt, vai starp tiem atrodas atkārtotājs.
- Katrs atkārtotājs palielina aizkavi, tādēļ to skaits ierobežots
- Starp jebkurām tīkla stacijām nedrīkst būt vairāk kā 4 atkārtotāji.

Ethernet tīklā paketei, ko sūta viens dators, jāsasniedz saņēmējs pirms būs nosūtīts paketes pēdējais baits. Tādēļ aizkaves limita dēļ nevar lietot daudz atkārtotāju; 10Mbps Ethernet var būt 5 segmenti. un 4 atkārtotāji., bet Fast Ethernet līdz 2 atkārtotājiem.

Atsevišķu atkārtotāju lieto reti; tā funkcijas liek citās iekārtās piemēram komutatoros.

12.stunda

Stundas temats: Tīkla karte.

Stundas mērķis: Iepazīties ar tīkla karti.

Mācību uzdevumi:

1. Iepazīties ar tīkla kartes uzdevumiem.
2. Iepazīties ar tīkla kartes funkcijām.

Personālā datora izvērses karte, kas kopā ar tīkla operētājsistēmu vada informācijas plūsmu datoru tīklā. Tīklam darbojoties, šī karte ir tieši saistīta ar datu pārraides vidi (vīto pāri, koaksiālo vai optisko kabeli), kas, savukārt, saista savā starpā visas tīkla saskarnes kartes. Dažkārt šo karti sauc arī par tīkla adapteri.

Datoru tīklam pieslēdz, izmantojot tīkla karti (adapteri). Tīkla karte var būt arī integrēta sistēmplates sastāvā.

Tīkla kartes uzdevumi:

- sagatavot datus, kuri nāk no datora, pārraidei pa tīkla kabeli;
- pārraidīt datus citam datoram;
- vadīt datu plūsmu starp datoru un kabeli;
- pieņemt datus no kabeļa un pārvest formā, saprotamā datora centrālajam procesoram.

Tīkla karte sastāv no aparatūras daļas un lasāmatmiņā (ROM) ierakstītām programmām. Šīs programmas realizē OSI etalonmodeļa kanāla slāņa Loģiskā posma vadības un Vides pieejas vadības apakšslāņu funkcijas.

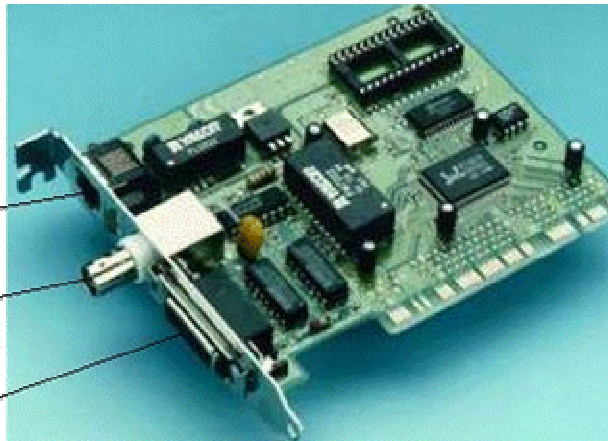
Pirms datu aizsūtīšanas tīklā tīkla kartei jāpārved tie no formas, kura ir saprotama datoram, formā, kurā tie var tikt pārraidīti pa tīkla kabeli.

Datorā dati tiek pārraidīti pa kopnēm (maģistrālēm). Kopne sastāv no vairākiem vadiem (8, 16, 32 vai 64), kuri iet paralēli viens otram. Datu biti tiek pārraidīti pa tiem ne secīgi, bet paralēli (*parallel*), kā 8, 16, 32 vai 64 bitu bloki. Tīkla kabeli datiem jāpārvietojas bitu plūsmas veidā: biti tiek pārraidīti secīgi (*serial*) viens aiz otra. Tīkla karte pieņem paralēlos datus un organizē tos secīgai pārraidei. Šis process beidzas ar datora cipardatu pārveidošanu elektriskos un optiskos signālos, kuri tiek pārraidīti pa tīkla kabeļiem. Par šo pārveidošanu atbild raiduztvērējs (*transceiver*).

Katrai tīkla kartei ir sava unikālā tīkla adrese (*network address*). Tīkla adreses ir IEEE komitejas pārziņā. Šī komitēja piešķir katram izgatavotājam adrešu intervālu. Pēc tam katrs izgatavotājs ieraksta plates lasāmatmiņā tās unikālo adresi.

*Tīkla karte ar pieslēgvietām
dažādu tipu kabeļiem:*

- RJ-45 (vītais pāris)
- BNC (tievais koaksiālais)
- D tipa 15 kontaktu
(resnais koaksiālais)



Parasti tīkla karte atbalsta vienu no lokālo tīklu arhitektūrām, piemēram, *Ethernet*, *LocalTalk*, *Token Ring* vai *Arcnet*. Pašlaik populārākā tīkla arhitektūra ir *Ethernet*. *Ethernet* tīkla adapteri atbilst vienai vai vairākām *Ethernet* specifikācijām:

- 10Base-2 (10 Mb/s tievais koaksiālais kabelis);
- 10Base-5 (10 Mb/s resnais koaksiālais kabelis);
- 10Base-T (10 Mb/s vītais pāris);
- 100Base-TX (100 Mb/s vītais pāris, 2 pāri);
- 100Base-T4 (100 Mb/s vītais pāris, 4 pāri);
- 100Base-FX (100 Mb/s optiskais kabelis);
- 1000Base-T (1 Gb/s vītais pāris);
- 1000Base-SX (1 Gb/s optiskais kabelis).

Tīkla kartes izvēle ir atkarīga no izvēlētās tīkla topoloģijas un aparatūras. Tīkla datoriem parasti izmanto 10 vai 100 Mb/s tīkla kartes. Lai tīkls strādātu efektīvāk, serverim izvēlas jaudīgāku tīkla karti.

Kartes ārpusē atrodas kabeļu pieslēgvietas. Lai karti varētu izmantot dažāda tipa kabeļu tīkliem, vienai kartei var būt vairākas pieslēgvietas. Lai izmantotu atšķirīgu tipu kabeļus, nav nepieciešams veikt kādas programmu vai aparatūras uzstādījumu maiņas.

13.stunda

Stundas temats: Bezvadu pieslēguma tīkla karte.

Stundas mērķis: Iepazīties ar bezvada tīkla kartes.

Mācību uzdevumi:

1. Iepazīties ar bezvadu tīkla kartes pielietojumu un nepieciešamību.
2. Iepazīties ar bezvadu tīkla priekšrocībām.
3. Iepazīties ar bezvadu tīkla kartes veidiem.

Bezvadu (wireless) tīklus izmanto gadījumos, kad kabeļu tīkla izveides vai pārkārtošanas izmaksas ir ļoti augstas. Otrs bezvadu tīklu attīstības virzītājspēks ir mobilo datoru lietotāji, kas izmanto portatīvos datorus un plaukstdatorus.

Viena no bezvadu tīklu priekšrocībām ir to relatīvi ātrā un vienkāršā uzstādīšana. Bezvadu tīklā datu pārraidei izmanto radioviļņus. Tīkla pamatelements ir šūna, kurā darbojas bezvadu savienojums (uztverams signāls). Katras šūnas iekšienē ir piekļuves (mezgla) punkts (access point), ko var uzskatīt par nelielu bāzes staciju, ar kuru sazinās visi šūnā esošie datori un/vai citas iekārtas. Savukārt datorā atrodas bezvadu tīkla adapteris ar nelielu antenu, kas sazinās ar piekļuves punktu. Katrs adapters ir līdzīgs mobilajam telefonam. Datu pārraidei tīklā pārsvarā izmanto radio frekvenču tehnoloģijas. Šādas tehnoloģijas ir vairākas: gan izmantojot noteiktu datu pārraides frekvenci (narrowband), gan plašu diapazonu (spread spectrum). Izplatītākie bezvadu tīkli ir bāzēti uz 802.11 a, b un g standartiem. b ir visvecākais standarts. B un g, darbojas 2,4GHz frekvencē (2400-2480 MHz). g atšķirībā no b lieto efektīvāku modulāciju, tāpēc var nodrošināt lielāku datu pārraides ātrumu. a darbojas 5GHz frekvencē, lieto to pašu modulāciju, ko g un nodrošina tādus pašus datu pārraides ātrumus.

Lai realizētu bezvadu tīklu ir nepieciešams bezvadu tīkla piekļuves punkts vai arī bezvadu tīkla maršrutētājs.



Kā arī datoram ir nepieciešams bezvadu tīkla adapteris. Bezvadu tīkla adapterus nosacīti var iedalīt pēc to pievienošanas veida datoram:

- PCI bezvadu tīkla kartes;



- PCMCIA bezvadu tīkla kartes;



- USB bezvadu tīkla konvertors;



14.stunda

Stundas temats: Koncentratori, komutatori.

Stundas mērķis: Iepazīties ar koncentratoriem un komutatoriem.

Mācību uzdevumi:

1. Iepazīties ar koncentratoriem.
2. Izprast kaskadēšanas nepieciešamību.
3. Iepazīties ar komutatoriem.

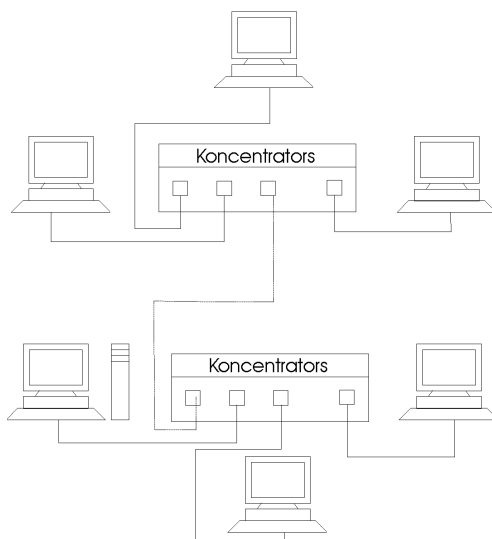
Koncentrators (hub)

Koncentratori (hub) – datu pārraides tīkla komunikācijas ierīce, kas modificē pārraidāmos signālus un ļauj pieslēgt datoru tīklam papildu darbstacijas. Koncentratori kļuvuši pazīstami sakarā ar lokālo tīklu *ARCnet* arhitektūru un dažādu datu pārraides tīklu (t.sk. arī optisko) plašu izplatību. Dažos zvaigžņtīklos koncentrators izpilda arī centrālās vadības ierīces funkcijas.

Koncentrators ir vītā pāra tīkla komponente, jo no tā ir atkarīgas tīkla darba spējas. Koncentratori tiek ražoti dažādiem tīkla ātrumiem (10 Mb/s, 100 Mb/s vai 10/100 Mb/s) un ar dažādu portu (pieslēgvieta) skaitu. To daudzums nosaka koncentratoram pieslēdzamo datoru skaitu.

Koncentratoru novieto uz galda, piestiprina pie sienas vai ievieto speciālā statīvā. Koncentratoram ir jābūt atbilstīgam pārējai tīkla aparātūrai. Ja tiek izmantots Fast Ethernet tīkls ar ātrumu 100 Mbit/s, tad arī koncentratoram un atbilstīgi tā portiem ir jābūt Fast Ethernet. Koncentratorus var savā starpā apvienot, pieslēdzot vienu pie otra, iegūstot kaskādes struktūru.

Šādus koncentratorus sauc par kaskadējamiem (*stack-able*). Veidojot ar tiem tīklu, jāuzmanās, lai neveidotos gredzena struktūra un ceļā no viena datora līdz otram neatrastos vairāk par četriem koncentratoriem.



Daudziem koncentratoriem ir arī vietas koaksiālo kabeļu pievienošanai. Šādi kļūst iespējams apvienot vītā pāra segmentus ar koaksiālajiem segmentiem. Vienam koncentratoram var pieslēgt tikai viena veida koaksiālo kabeli.

Parasti visiem koncentratoriem ir gaismas diožu indikatori, kas signalizē par portu stāvokļiem. Tas ļauj uzreiz redzēt, vai ports ir pieslēgts, vai notiek datu apmaiņa. Koncentratori bez gaismas diožu indikatoriem ir lietošanā neērti, jo nav iespēja kontrolēt stāvokli.

Ir gadījumi, ka gaismas diožu indikatoru sniegtā informācija ir nepietiekama, lai noteiktu dažāda rakstura problēmas. Ja koncentratoram ir kontroles un vadības iespējas caur tīklu (piemēram, izmantojot SNMP protokolu), tad tā stāvokli no savas darbstacijas var kontrolēt tīkla administrators. Parasti koncentratori ar vadības iespējām ļauj uzzināt konkrēto portu stāvokli, ļauj portus atslēgt un pieslēgt, ļauj uzkrāt statistiku par tīkla noslodzi un kolīziju skaitu tajā. Tīkla administratora darba programma bieži ir HP Open View, kam koncentratoru ražotāji pievienojuši nepieciešamos moduļus.

Komutators (Switch)

Komutators jeb slēdzis (angliski switch) ir līdzīgs koncentratoram, bet ir intelektuālāks par to. Tā funkcijas ir ātri komutēt datu paketes starp portiem. Komutators darbības sākumā iegaumē visu pieslēgto datortīkla adapteru fiziskās adreses. Saņemot datu paketi, tas šo paketi noraida tikai pa to kabeli, kas iet līdz šīs paketes adresātam. Līdz ar to samazinās tīkla noslodze un tīkla ātrums palielinās. Ar komutatoriem var atdalīt darba grupas vienu no otras.

Praksē ļoti perspektīvi ir slēdži, ar vienu vai diviem 1000 Mb/s portiem, kuriem pieslēdz serverus, un daudziem 100 Mb/s portiem. Serveru pieslēgumam lieto 1000 Mb/s portus, bet pārējiem tīkla segmentiem lieto 100 Mb/s portus. Šāds slēdzis kalpo kā tīkla mugurkauls, vienmērīgi sadalot slodzi visiem tīkla segmentiem. Šis varētu būt ideāls gadījums, kā maksimāli izmantot serveru jaudu.

Slēdžiem ļoti vēlama distances vadības un kontroles iespēja. Tas īpaši svarīgi ir lielos tīklos, jo tas ļauj sabalansēt tīkla slodzi pa tīkla segmentiem. Slēdžu ātrdarbību raksturo aiztures (angliski latency) lielums, kas nosaka, cik ilgi tiek apstrādāts signāls.

Jaudīgus slēdžus bieži veido universālā, viegli paplašināmā korpusā, kurā var ievietot daudzus nepieciešamus moduļus. Tas īpaši svarīgi lielās datorsistēmās, kuras paredzēts paplašināt un modificēt.

15.stunda

Stundas temats: Tilti, maršrutētāji

Stundas mērķis: Iepazīties ar tiltiem un maršrutētājiem.

Mācību uzdevumi:

1. Iepazīties ar tiltu pielietojumu.
2. Iepazīties ar maršrutētāju pielietojumu.

Tilts (*bridge*)

Atšķirībā no atkārtotāja atļauj sadalīt tīklu segmentos, tādā veidā izolējot trafika daļu vai radušās problēmas. Tilti strādā augstākā OSI slānī kā atkārtotāji. Tie ir “gudrāki” par atkārtotājiem, jo var izmantot plašāku informāciju. Piemēram, tilts pārbauda avota un saņēmēja fizikālās adreses katrā datu blokā un veido maršrutēšanas tabulu. Bet vienlaicīgi tilts var uzturēt tikai vienu maršrutu un nespēj to optimizēt. Slānis, kurā pielieto apvienošanu ar tiltu palīdzību (t.i. kanāla slānis):

- kontrolē informācijas plūsmu;
- apstrādā pārraides kļūdas;
- nodrošina fizisko (atšķirībā no loģiskās) adresāciju;
- pārvalda pieeju fiziskai videi.

Tilti nodrošina šo funkciju izpildi, atbalstot dažādus kanāla slāņa protokolus, kas noteic informācijas plūsmu, kļūdu apstrādi, adresāciju un pieejas pie nesēja algoritmus. Kā populārus kanāla slāņa protokolu piemērus var minēt *Ethernet*, *Token Ring* un *FDDI*.

Tilti nav sarežģītas iekārtas. Tie analizē pienākošos freimus, pieņem lēmumus par to virzīšanu, balstoties uz informāciju, ko satur freims, un pārsūta tos ierādītajā vietā. Dažreiz (piemēram, avota maršruta savienojums) katrs freims satur informāciju par visu ceļu uz gala punktu. Citos gadījumos (piemēram, caurspīdīgs savienojums) freimi tiek virzīti uz norādīto vietu ar atsevišķiem pārsūtījumiem, pa vienam katrā reizē.

Galvenā apvienošanas ar tiltu palīdzību priekšrocība ir augstāko slāņu protokolu caurspīdīgums. Tādēļ, ka tilti rīkojas kanāla slānī, no tiem netiek prasīta augstāko slāņu informācijas pārbaude. Tas nozīmē, ka tie var ātri virzīt trafiku, kas pārstāv jebkuru tīkla slāņa protokolu. Tilts ir parasta lieta *Apple Talk*, *DECnet*, *TCP/IP*, *XNS* un citu trafiku virzīšanā starp diviem vai vairākiem tīkliem.

Tilti spēj filtrēt freimus, balstoties uz jebkuriem 2. slāņa informācijas laukiem. Piemēram, tiltu var ieprogrammēt tā, lai tas aizliedz visus freimus, ko sūta no noteikta tīkla. Tā kā kanāla slāņa informācijā bieži iekļauj norādi uz augstākā slāņa protokolu, tilti parasti filtrē pēc šī parametra. Tāda filtrēšana ir lietderīga, lai aizliegtu neobligāto apraides pakešu informāciju un tātad samazinātu trafiku.

Dalot lielos tīklus autonomos blokos, tilti nodrošina virkni priekšrocību:

- Pirmkārt, tā kā tiek pārsūtīts tikai noteikts trafika procents, tīkli mazina trafiku, kas iet cauri visu savienoto segmentu iekārtām.
- Otrkārt, tilti darbojas kā nepārvarams šķērslis dažiem bojājumiem, kas ir potenciāli bīstami tīkliem.
- Treškārt, tilti ļauj uzturēt sakarus vairāku iekārtu starpā, nekā to varētu nodrošināt jebkurā tiltam pievienotā LAN, ja tā būtu patstāvīga.
- Ceturtkārt, tilti palielina LAN efektīvo garumu, ļaujot pieslēgt vēl nepieslēgtās attālās stacijas.

Maršrutētāji (router)

Bieži vien lokālo tīklu nākas pieslēgt globālajiem tīkliem (piemēram, internetam) vai arī apvienot vairākus attālinātus lokālos tīklus, izmantojot globālos tīklus. Šim nolūkam izmanto maršrutētājus.

Maršrutētājs (router) ir intelektuāls datu pakešu komunikators, kas nodarbojas ar pakešu nosūtīšanu starp tīkliem. Ja koncentratori, tilti, atkārotāji strādā izmantojot noteiktu tīkla standartu, piemēram, Ethernet, tad maršrutētāji ir augstāka līmeņa iekārtas, kas māk apstrādāt tikai konkrētus protokolus. To mērķis ir nodrošināt maksimāli efektīvu maršrutu starptīklu paziņojumiem un datu paketēm, vienlaicīgi veicot filtrāciju un nodrošinot tīklus pret nesankcionētu pieeju. Parasti visi maršrutētāji māk strādāt ar TCP/IP un IPX/SPX protokoliem (TCP/IP plaši lieto starptīklu savienojumos, bet IPX/SPX ir lokālajos tīklos visplašāk lietotie protokoli).

Maršrutētājos bez jau lokālā datortīkla portiem ir arī teritoriālo (WAN) tīklu porti. Tie parasti ir modemu pieslēgšanai. Ja lieto izdalītās telefonu līnijas, tad parasti lieto sinhronie WAN porti, kuri nodrošina labāku stabilitāti un lielāku darba ātrumu. Asinhronie porti paredzēti īslaicīgu sakaru nodibināšanai, izmantojot parastās telefonu līnijas un parastos portus. Maršrutētājos var būt arī radiosakaru porti, optisko kabeļu porti.

Maršrutētāja ātrdarbību raksturo tas, cik daudz pakešu tas ir spējīgs apstrādāt vienā sekundē. Arī maršrutētājos svarīgs ir aiztures ilgums. Tā kā darbs ar paketēm protokolu līmenī prasa lielus skaitļošanas resursus, tad aiztures laiks ir lielāks nekā slēdžiem. Nav ieteicams projektēt tīklus, kuros serveri pārējām tīkla daļām būtu pieslēgti caur maršrutētāju. Šī vieta ir paredzēta slēdzim. Maršrutētāji vislabāk noder, ja jāsavieno vairāki tīkli. Tas var būt caur telefona tīkliem, radiosakariem, optiskiem kabeļiem.

16. – 17.stunda

Stundas temats: Ethernet darbības princips

Stundas mērķis: Iepazīties ar Ethernet tehnoloģijas darbības principu.

Mācību uzdevumi:

1. Iepazīties ar Ethernet tehnoloģijas datortīklu standartu.
2. Iepazīties ar Ethernet tehnoloģijas darbības principu.

Ethernet datortīkli

Ethernet ir viens no populārākajiem lokālo datortīklu standartiem pasaulē un arī Latvijā. Šo tīklu 1972. gadā izstrādāja firma Xerox. 1985. gadā tīkla veids tika standartizēts un pašlaik ir pazīstams ar nosaukumu IEEE 802³. Šim standartam ir vairāki paveidi, no kuriem biežāk sastopamais ir IEEE 802.3.

Klasiskajā Ethernet tīklā izmanto koaksiālo kabeli ar 50 omu pretestību un maksimālais datu pārsūtīšanas ātrums ir 10 Mbit/s. Viens no būtiskākajiem raksturojošiem parametriem ir veids, kādā datori sazinās savā starpā. Literatūrā to sauc par piekļūšanas veidu. Problēmas būtība: kādā veidā nodrošināt, ka vienā laika sprīdī aktīvs ir tikai viens datu pārraidīšanas avots jeb dators. Ja kādā laika sprīdī datus raida divi datori, tad notiek datu sadursme jeb kolīzija (collision). Ethernet tīkla piekļūšanas principu sauc par CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) – piekļūšanas veids ar nesošas kontroli u kolīziju konstatēšanu.

CSMA/CD metodes pamatprincipi ir šādi:

- abonents, kurš vēlas nosūtīt datus, pārbauda, vai datu pārraides kanāls ir brīvs (pārbaude notiek, kontrolējot nesošo signālu (carrier);
- ja tīkls ir brīvs, tad sākas datu pārraide, vienlaikus tiek pārbaudīts tīkla stāvoklis (vai nav kolīziju). Ja kolīziju nav, tad datu sūtīšana tiek pabeigta;’
- ja kolīzija ir notikusi (kāds cits dators arī sāka sūtīt savus datus), tad datu raidīšana tiek pārtraukta. Analogiski rīkojas arī tas abonents, kurš izraisīja kolīziju;
- pēc datu kolīzijas katrs no abonentiem nogaida rakstura laika sprīdi un mēģina sūtīt tos pašus datus no sākuma.

Metodes priekšrocības ir tādas, ka tehniski to ir samērā vienkārši īstenot. Tāpēc Ethernet aparatūra ir diezgan lēta. Visi abonentu ir vienlīdzīgi, un tas nozīmē, ka nevienam no lokālā datortīkla abonentiem nevar būt īpašas prioritātes.

Ethernet tīklam ir arī nopietns trūkums: kolīziju dēļ nav garantēta ātrdarbība un, galvenais, ātrdarbība ir atkarīga no lokālā datortīkla noslogotības. Jo lielāka slodze tīklā, jo relatīvi biežāk notiek datu kolīzijas, jo vairāk samazinās datu pārraidīšanas ātrums. Piemēram, Ethernet tīklam ar maksimālo teorētisko ātrumu 10 Mbit/s reālais ātrums var samazināties praktiski līdz dažiem kilobitiem sekundē. Tas ir galvenais šā populārā tīkla trūkums.

Pašlaik lokālajos tīklos izmanto Fast Ethernet ar datu pārraides ātrumu 100 Mbit/s. Šajos tīklos izmanto vītā pāra vai optiskās šķiedras kabelus. Ir izstrādāts un jau tiek izmantots lokālajos tīklos jauns standarts Gigabit Ethernet ar datu pārraides ātrumu 1 Gbit/s.

18. – 19.stunda

Stundas temats: Ethernet datortīklu apzīmējumi, piemēri.

Stundas mērķis: Iepazīties ar Ethernet datortīklu apzīmējumiem.

Mācību uzdevumi:

1. Iepazīties ar Ethernet datortīklu apzīmējumiem.
2. Izprast Project 802 kategorijas.
3. Iepazīties ar lokālā tīkla piemēriem.

Katram Ethernet tīkla veidam ir šādi apzīmējumi:

- 10BASE5 – resnais koaksiālais kabelis, diametrs aptuveni 8 mm (pašreiz praktiski vairs neizmanto);
- 10BASE2 – tievais koaksiālais kabelis, diametrs aptuveni 5 mm;
- 10BASE-T – vītā pāra kabelis;
- 10BASE-F – optiskais kabelis;
- 100BASE-T4 – četrkārtīgais vītā pāra kabelis;
- 100BASE-TX – dubultais vītā pāra kabelis;
- 100BASE-FX – optiskais kabelis;
- 1000BASE-SX – optiskais kabelis ar gaismas viļņa garumu 850 nm;
- 1000BASE-LX - optiskais kabelis ar gaismas viļņa garumu 1300 nm;
- 1000BASE-CX – ekranētais vītā pāra kabelis;
- 1000BASE-T – četrkārtīgais ekranētais vītā pāra kabelis.

Apzīmējumu atšifrējums:

- 10,100,1000 – datu pārraides ātrums Mbit/s;
- BASE – Ethernet standarts;
- 5 – tīkla segmenta garums ir 500 m;
- 2 – tīkla segmenta garums ir 200 m (patiesībā ir 185 m);
- T – vītā pāra kabelis (twisted pair);
- F – optiskais kabelis (fiber optic).

Raksturojums	Ethernet	10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Ātrums, Mb/sek	10	10	10	10	10	100
Pārraides metode	Baseband	Baseband	Baseband	Baseband	Baseband	Baseband
Segmenta maks. garums, m	500	500	185	100	2000	100
Pārraides vide	50-Omu koaksiāls (resns)	50-Omu koaksiāls (resns)	50-Omu koaksiāls (tievs)	neekr. vītais pāris	optiskais kabelis	neekr. vītais pāris
Topoloģija	Kopne	Kopne	Kopne	Zvaigzne	Zvaigzne	Zvaigzne

Raksturojums	100BaseTX	100BaseFX	100BaseT4
Kabelis	5. kategorijas UTP vai STP	Optiskais	3., 4. vai 5. kategorijas UTP
Izmantojamo vīto pāru vai šķiedru skaits	2 pāri	2 šķiedras	4 pāri
Segmenta maks. garums	100 m	400 m	100 m
Tīkla maksimālais diametrs	200 m	400 m	200 m

LAN standarti, ko noteic Project 802, dalās 12 kategorijās; katrai savs numurs:

802.1 – Apvienotie tīkli (OSI modelis un tīkla pārvaldība).

802.2 – Loģiskā posma vadība (Logical Link Control – LLC).

802.3 – Ethernet (LAN ar daudzpieeju, nesēja jušanu un sadursmju atklāšanu – CSMA/CD).

802.4 – Token Bus (LAN ar topoloģiju “maģistrāle” un marķiera nodošanu).

802.5 – Token Ring (LAN ar topoloģiju “gredzens” un marķiera nodošanu).

802.6 – Pilsētītīkls (Metropolitan Area Network, MAN).

802.7 – Apraides tehnoloģijas konsultatīvā padome (Broadcast Technical Advisory Group).

802.8 – Optisko šķiedru tehnoloģijas konsultatīvā padome (Fiber-Optic Technical Advisory Group).

802.9 – Integrētie tīkli ar runas un datu pārraidi (Integrated Voice/Data Networks).

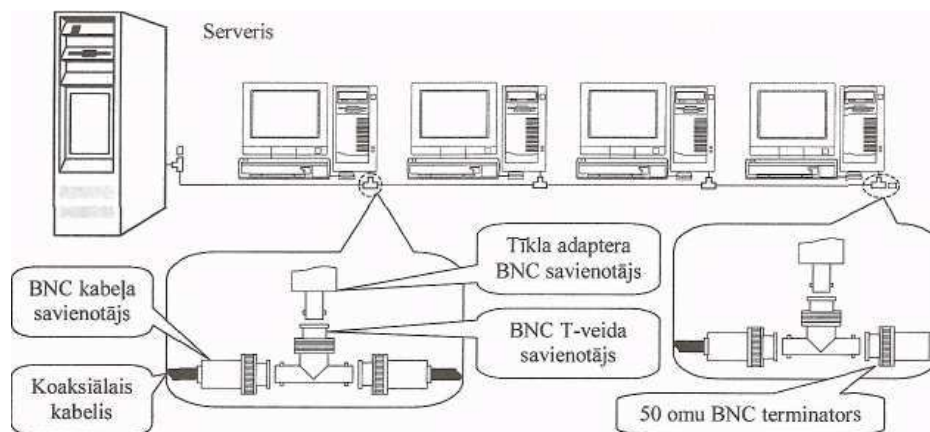
802.10 – Tīklu drošība.

802.11 – Bezvadu tīkli.

802.12 – LAN ar pieeju pēc pieprasījuma prioritātes (Demand Priority Access LAN, 100BaseVG-AnyLan).

Aparatūras izvēle Ethernet tīklam ir atkarīga no tīkla topoloģijas, datu pārraides vides (kabeļi) un no nepieciešamā datu pārraides ātruma.

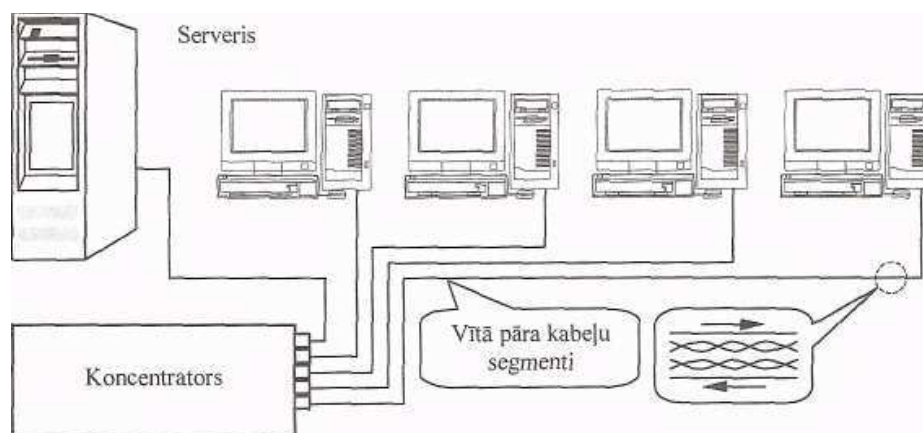
Lokālā tīkla piemērs uz koaksiālā kabeļa bāzes.



Tātad skatoties doto piemēru tīkla realizācijai ir nepieciešams:

- serveris, ja tīkls ir ar izdalītu serveri;
- pieci tīkla adapteri;
- četri 50 omu kabeļi;
- pieci BNC T - veida sadalītāji;
- astoņi BNC kabeļu savienotāji;
- divi 50 omu BNC terminatori.

Lokālā tīkla piemērs uz vītā pāra kabeļa bāzes.



Tātad skatoties doto piemēru tīkla realizācijai ir nepieciešams:

- serveris, ja tīkls ir ar izdalītu serveri;
- pieci tīkla adapteri;
- pieci vītā pāra kabeļi;
- desmit RJ-45 savienotāji;
- viens koncentrators.

20.stunda

Stundas temats: Token Ring, FDDI datortīkli

Stundas mērķis: Iepazīties ar Token Ring un FDDI datortīkliem.

Mācību uzdevumi:

1. Iepazīties ar Token Ring datortīklu attīstību, darbības principu, priekšrocībām un trūkumiem.
2. Iepazīties ar FDDI datortīklu darbības principu, priekšrocībām un trūkumiem.

Token Ring datortīkli

Token Ring lokālā datortīkla veidu firma IBM piedāvāja 1985.gadā. Token Ring tīkla uzdevums bija apvienot dažādus firmas IBM ražotos datorus lokālajā datortīklā. Pašlaik Token Ring tīklam atbilst starptautiskais standarts IEEE 802.5. Tas ierindo šo tīkla veidu vienā līmenī ar populāro Ethernet tīklu. Lai gan šo tīkla veidu izstrādāja ļoti liela un pazīstama datoru ražotāju firmā kāda ir IBM, Token Ring lokālais datortīkls nav tik plaši izplatīts pasaulē kā Ethernet tīkls – galvenokārt tā aparātūras lielo izmaksu dēļ.

Tīklam Token Ring ir „riņķa” topoloģija, kas izriet arī no tā nosaukuma, lai gan ārēji topoloģija atgādina „zvaigzni”. Tas saistīts ar to, ka visi abonenti (datori) tiek pieslēgti pie tīkla, izmantojot aparāturu, kas atgādina Ethernet koncentratorus. Token Ring tīklu tehnoloģijā šos koncentratorus sauc par MAU (Multistation Access Unit).

Informācija tiek sūtīta pa riņķi no viena datora uz nākamo, izmantojot speciālus marķierus. Marķieris cirkulē pa tīklu un katrs dators var pievienot marķierim savus pārsūtāmos datus, norādot, kuram datoram tie tiek sūtīti. Dators, kurš saņem šādu marķieri ar datiem, nolasa datus, kas ir domāti viņam, un sūta marķieri tālāk pa riņķi, šādu datu pārraidīšanas ir sarežģītāks nekā Ethernet tīklā, bet tam ir vairākas priekšrocības:

- tīklā nav kolīziju (konfliktu);
- ir garantēts datu pārsūtīšanas ātrums, kas praktiski nav atkarīgs no tīkla noslogotības, pretstatā Ethernet tīklam, kam pieaugot slodzei, samazinās datu pārsūtīšanas ātrums;
- viegli kontrolēt lokālā tīkla darbību, jo: ja marķieris neatgriežas datorā, kas to ir sūtījis, tad tīklā ir bojājumi (kabeļa pārrāvums, datora bojājums utt.).

Fiziskie datori tiek savienoti ar MAU ar vītā pāra kabeļiem. Pašlaik Token Ring tīklos lieto arī optiskos kabeļus. Maksimālais attālums starp datoru un koncentratoru (MAU) ir 45 metri. Ja izmanto ekranētā vītā pāra kabeli, tad šo attālumu var palielināt līdz 100 metriem. Datu pārraides ātrums ir 4 Mbit/s u 16 Mbit/s. No Token Ring trūkumiem var pieminēt galveno – diezgan dārga tīkla aparātūra un datortīkla adapteri.

FDDI datortīkli

FDDI (Fiber Distributed Data Interface) ir diezgan jauns datortīklu veids. Tīkls ir orientēts uz lielu datu pārsūtīšanas ātrumu 100 Mbit/s. Tīkla kabeļu sistēmā izmanto optiskās šķiedras kabeļus (gaismas viļņa garums – 850nm). Optisko kabeļu izmantošana nodrošina lielu izturību pret ārējiem traucējumiem, labu datora galvanisku atsaistīšanu un augstu datu pārsūtīšanas slepenību.

Tīkla topoloģija ir „riņķis”, un dati tiek pārsūtīti ar marķiera palīdzību. Datoru pieslēgums pie tīkla ir ļoti līdzīgs Token Ring tīklam. Pie katra datora ir pieslēgti divi optiskie kabeļi, kuros dati tiek pārsūtīti pretējos virzienos: pa vienu kabeli dati tiek saņemti, pa otru – sūtīti uz nākamo datoru. Optisko kabeļu lietošana nodrošina lielus ātrumus starp datoriem – līdz 2 km. Lai gan šim lokālajam datortīklam ir vairākas priekšrocības, FDDI datortīkli nav pārāk izplatīti, jo tīklu aparatūra ir ļoti dārga.

Kādos gadījumos rekomendē izmantot FDDI tehnoloģiju.

FDDI tehnoloģijas īpatnība: tā apvieno (ietver, nodrošina) dažas lokālajiem tīkliem ļoti svarīgas īpašības:

- ļoti augstu darba drošumu;
- spēju pārklāt (aptvert) ievērojamu teritoriju, piemēram, lielu pilsētu;
- liels datu apmaiņas ātrums;
- spēja nodrošināt sinhrono multimediju trafiku;
- gredzena caurlaides spējas sadalījums starp stacijām nav fiksēts, šis sadales mehānisms ir adaptīvs, tas piemērojas situācijai;
- tīkls spēj strādāt pie gredzena noslodzes koeficienta, kas tuvs vieniniekam;
- FDDI trafiku viegli translēt uz trafiku tādos populāros protokolos kā Ethernet un Token Ring jo staciju adrešu formāti ir saderīgi un var izmantot kopēju LLC apakšlīmeni.

21.stunda

Stundas temats: AnyLAN, Arcnet datortīkli

Stundas mērķis: Iepazīties ar AnyLAN, Arcnet datortīkliem.

Mācību uzdevumi:

1. Iepazīties ar AnyLAN datortīklu attīstību, darbības principu, priekšrocībām un trūkumiem.
2. Iepazīties ar Arcnet datortīklu attīstību, darbības principu, priekšrocībām un trūkumiem..

AnyLAN datortīkli

Firma AT&T un HP piedāvā jaunas tehnoloģijas projektu kā Fast Ethernet alternatīvu ar datu pārraides ātrumu 100 Mb/s -100 Base-VG. Šajā projektā ir uzlabota pieejas metode, ievērojot multimediju pielietojumu vajadzības. Bez tam nodrošināta paketes formāta saderība ar tīklu 802.3 paketes formātu. 1993. gada septembrī pēc IBM un HP iniciatīvas izveidoja komiteju IEEE 802.12, kura nodarbojās ar jaunās tehnoloģijas standartu. Šo projektu paplašināja, ievēdot jaunajā tīklā ne tikai Ethernet formāta kadrus, bet arī Token Ring formātus. Jauno tehnoloģiju nosauca *par 100VG -AnyLAN*, t.i., tehnoloģija jebkuriem tīkliem (AnyLAN = jebkuri tīkli), ievērojot, ka Ethernet un Token Ring tehnoloģijas izmanto gandrīz visos mezglos. 1995. gada vasarā šī tehnoloģija ieguva savu standartu IEEE 802.12.

100VG-Any LAN tehnoloģija atšķiras no klasiskā Ethernet ievērojami lielākā mērā nekā Fast Ethernet. Galvenās atšķirības ir sekojošas:

- Tiek izmantota cita vides pieejas metode Demand Priority, kura nodrošina taisnīgāku tīkla caurlaidspējas sadalījumu salīdzinājumā ar CSMA/CD un prioritātes pieeju laika jutīgiem lietojumiem.
- Kadri tiek pārraidīti ne visiem tīkla stacijām, bet tikai saņēmēja stacijai.
- Tīklā ir pieejas arbitrs – koncentrators.
- Tiek uzturēti divu tehnoloģiju freimi – Ethernet un Token Ring (no šejienes papildinājums AnyLAN tehnoloģijas nosaukumā).
- Dati tiek pārraidīti vienlaicīgi pa 3. kategorijas UTP 4 pāriem. Pa katru pāri dati tiek pārraidīti ar ātrumu 25 Mb/s, kas summā dod 100Mb/s.

100VG-AnyLAN tīkls sastāv no centrālā koncentratora, kuru sauc par saknes koncentratoru, un ar to savienotiem gala mezgliem un citiem koncentratoriem. Ir pieļaujami trīs koncentratoru kaskadēšanas līmeņi. Katram koncentratoram un tīkla adapteram jābūt uzstādītam darbībai vai nu ar Ethernet, vai Token Ring freimiem, vienlaicīgi tos izmantot nav atļauts.

Koncentrators cikliski izpilda portu aptauju. Stacija, kura grib pārraidīt datus, nosūta speciālo zemas frekvences signālu koncentratoram, pieprasot freima pārraidi un norādot tā

prioritāti. 100VG-AnyLAN tīklā tiek izmantoti prioritāšu divi līmeņi: zems un augsts. Zems prioritātes līmenis atbilst parastiem datiem (failu dienests, drukāšanas dienests u.t.t.), bet augsts prioritātes līmenis atbilst datiem, kuri ir jutīgi laika aizkavēs (piemēram, multimedija). Prioritātei ir statiskā un dinamiskā sastāvdaļa, t.i. stacija ar zemo prioritāti, kurai ilgi nav pieejas tīklam, saņem augsto prioritāti.

Ja tīkls ir brīvs, koncentrators atļauj freima pārraidi. Pēc freima saņēmēja adreses analīzes koncentrators automātiski nosūta freimu saņēmēja stacijai. Ja tīkls ir aizņemts, koncentrators nostāda pieprasījumu rindā, kura tiek apstrādāta atbilstoši pieprasījumu atnākšanas kārtībai un ievērojot prioritātes. Ja koncentratora portam ir pieslēgts cits koncentrators, tad aptauja tiek apstādināta kamēr zemāka līmeņa koncentrators pabeigs aptauju. Lēmums par pieejas piešķiršanu tiek pieņemts, kad visi koncentratori pabeigs visu savu portu aptauju.

Kā koncentrators uzzina, kādam portam ir pieslēgta saņēmēja stacija?

Lai atrisinātu šo uzdevumu, koncentrators uzzina stacijas MAC adresi stacijas fiziskās pieslēgšanas tīklam momentā un saglabā to MAC adresi tabulā, kura ir analogiska tilta/komutatora tabulai. 100VG-AnyLAN koncentratora atšķirība no tilta/komutatora ir tas, ka tam nav iekšēja bufera freimu glabāšanai. Tāpēc tas pieņem no tīkla stacijām tikai vienu freimu, nosūta to uz saņēmēja portu un, kamēr saņēmēja stacija pilnīgi pieņems šo freimu, jaunus freimus koncentrators nepieņem. Tātad šeit, kā arī citās vides pieejas metodēs, tikai viens dators katrā laika momentā var pārraidīt datus.

IEEE 802.12 nosaka sekojošus ierobežojumus kabeļu segmentu un tīkla garumiem. Segmenta maksimālais garums ir 100 m (3. kategorijas UTP) vai 150 m (5. kategorijas UTP). Tīkla maksimālais diametrs ir 600 m (3. kategorijas UTP) vai 900 m (5. kategorijas UTP). Neskatoties uz daudziem labiem tehniskajiem risinājumiem, 100Vg-AnyLAN tehnoloģija ir mazāk populāra nekā Fast Ethernet.

Arcnet datortīkli

Arcnet (Attached Resource Computer Net) lokālie datortīkli ir vieni no vecākajiem. Tie ir izstrādāti vēl 1977. gadā. Tīklu izstrādāja firma Datapoint Corporation. Lai gan nav starptautisko standartu šim lokālā datortīkla veidam, Arcnet ir diezgan populārs pasaulē (deviņdesmito gadu sākumā Arcnet produkcijas realizācija veidoja 30 % no kopējās lokālo tīklu produkcijas realizācijas).

Arcnet tīklos izmanto "maģistrāles" un „pasīvās zvaigznes” topoloģijas. No priekšrocībām var pieminēt diezgan nelielas izmaksas tīkla aparatūrai un kabeļu sistēmām, kas ir samērojamas ar Ethernet tīklu izmaksām. Var pieminēt lielu tīkla drošības pakāpi un elastīgumu, kā arī salīdzinājumā ar Ethernet tīklu mazākus ierobežojumus attiecībā uz kabeļu garumiem. No trūkumiem ir jāpiemin galvenais: zemais datu pārraides ātrums – 2.5 Mbit/s.

Pēc fiziskā izpildījuma Arcnet tīkls ir ļoti līdzīgs Ethernet tīklam, bet ir jāpiemin galvenā atšķirība. Arcnet tīklos izmanto koaksiālos kabeļus ar viļņu pretestību 93 omi, bet Ethernet tīklos kabeļi ir ar viļņu pretestību 50 omi. Tātad šo tīklu kabeļu sistēmas nav savienojamas un, pārejot no Arcnet tīkla uz Ethernet, visi kabeļi ir jānomaina.

Datu pārsūtīšanas protokols ir līdzīgs Token Ring tīklam, jo dati tiek sūtīti ar marķiera palīdzību. Tas nodrošina datu pārsūtīšanu bez kolīzijām un tāpēc labu noturību pret lielām slodzēm tīklā.

22. – 23.stunda

Stundas temats: ISO/OSI modelis.

Stundas mērķis: Iepazīties ar ISO/OSI modelis.

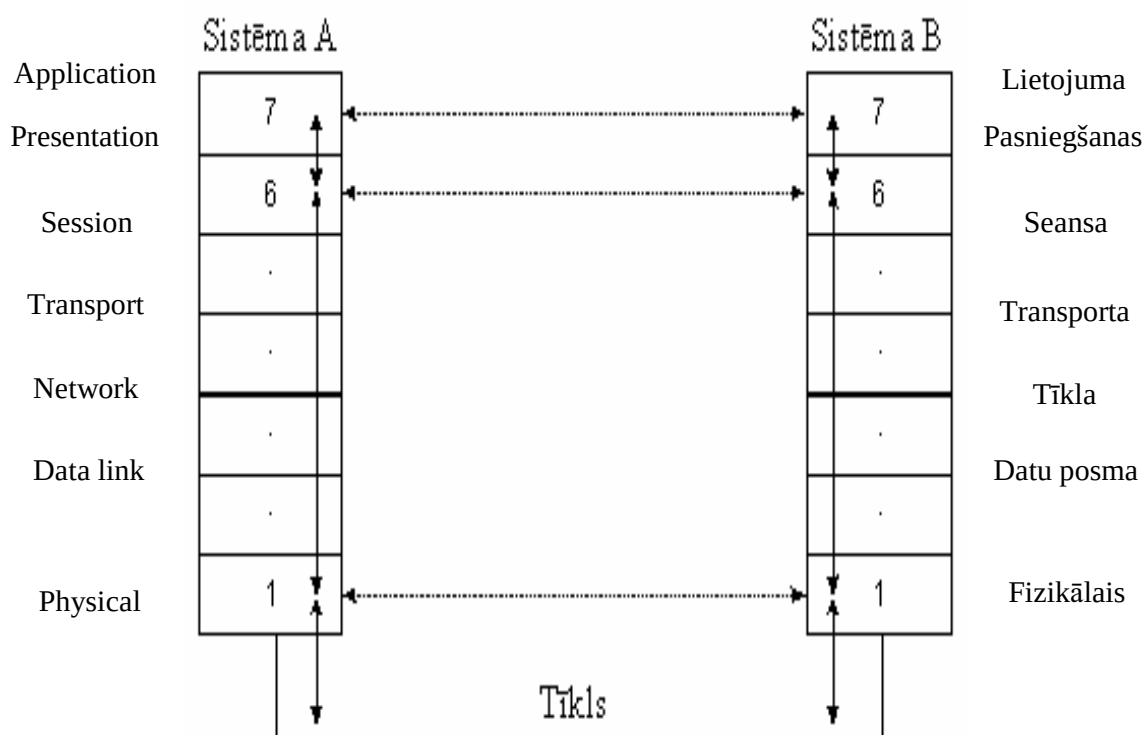
Mācību uzdevumi:

1. Iepazīties ar ISO/OSI modeļa nepieciešamību.
2. Iepazīties ar ISO/OSI modeļa slāņiem.
3. Izprast ISO/OSI modeļa slāņu nozīmi.

Atvērto sistēmu sadarbības modelis apraksta, kā informācija no programmatūras vienā datorā pārvietojas pa tīklu uz citu programmatūru citā datorā. Šis modelis angļiski pazīstams kā Open System Interconnection (OSI) Reference model. OSI modelis ir konceptuāls modelis, kas sastāv no septiņiem slāņiem. Katrs slānis nosaka specifiskas tīkla funkcijas.

Modeli izstrādāja Starptautiskā standartizācijas organizācija (ISO International Organization for Standardization) 1984. gadā, un pašlaik tas tiek uzskatīts par primāru arhitektūras modeli datoru savstarpējos sakaros.

OSI modelis sadala uzdevumus, kas saistīti ar informācijas pārvietošanu starp tīklā saslēgtiem datoriem septiņās smalkākās, daudz vieglāk vadāmās uzdevumu grupās. Katrs uzdevums vai uzdevumu grupa tiek piesaistīta kādam no septiņiem OSI modeļa slāņiem. Katrs slānis ir neatkarīgs tā, ka uzdevumi, kas piesaistīti vienam atsevišķam slānim var tikt implementēti neatkarīgi. Tas ļauj viena slāņa uzdevumus pārveidot, neizsaucot citu slāņu uzdevumu pārveidošanu.



Informācijai, kas tiek vadīta no programmatūras vienā datorā uz programmatūru otrā datorā ir jāiet cauri visiem OSI modeļa slāņiem.

Ja, piemēram, programmatūrai sistēmā A ir informācija, kas jānodod programmatūrai sistēmā B, programmatūra sistēmā A to nodos lietojumslānim (slānis Nr. 7) sistēmā A. Lietojumslānis šo informāciju nodos pasniegšanas slānim (slānis Nr. 6), kas savukārt to nodos tālāk savienojuma slānim (slānis Nr. 5), un tā tālāk lejup līdz fiziskajam slānim (slānis Nr. 1). Fiziskā slāņa līmenī informācija ar fiziskā mēdija palīdzību tiek nosūtīta uz sistēmu B. Sistēmas B fiziskais slānis nolasīs informāciju no fiziskā mēdija un nodos to datu posma slānim (slānis Nr. 2), kas savukārt to nodos tālāk tīkla slānim (slānis Nr. 3), un tā tālāk augšup, līdz informācija sasniegs sistēmas B lietojumslāni (slānis Nr. 7). Visbeidzot lietojumslānis nodos informāciju programmatūrai, tādējādi noslēdzot komunikācijas procesu.

Katrs OSI slānis pamatā komunicējas ar trijiem citiem slāņiem: ar slāni tieši virs tekošā, ar slāni tieši zem tekošā un ar savu vienranga slāni pretējā sistēmā.

OSI modeļa slāņi izmanto dažādas kontroles informācijas formas, lai komunicētos ar sava ranga slāni citā datorsistēmā. Šī kontroles informācija sastāv no specifiskiem pieprasījumiem un instrukcijām, ar kurām apmainās viena līmeņa OSI slāņi dažādā sistēmās.

Kontroles informācija parasti pieņem vienu no divām formām: *galvene* (ang. Header) vai *noslēgums* (eng. Trailer). Galvenes tiek pievienotas priekšā datiem, kas tiek nodoti no augstākiem slāņiem, savukārt noslēgumi tiek pievienoti beigās datiem, kas tiek nodoti no augstākiem slāņiem.

Galvene, noslēgums un dati ir relatīvi jēdzieni, atkarīgi no slāņa, kas analizē doto datu vienību. Piemēram, tīkla slānī informācijas vienība sastāv no šī paša slāņa galvenes un datiem.

Datu posma slānī visa informācija, kas tiek saņemta no tīkla slāņa (tīkla slāņa galvene un dati), tiek apstrādāta kā dati.

Tādējādi, informācijas apmaiņas procesā, slānis, kurš nodod datus nākamajam zemākajam slānim, pievieno kontroles informāciju, kas nepieciešama pretējās sistēmas tā paša ranga slānim. Savukārt, procesā, pirms informācija tiek nodota augstāka līmeņa slānim, tiek analizēta un aizvākta saņemtā kontroles informācija. Tātad, ejot cauri avota sistēmas OSI slāņiem nododamās informācijas apjoms nemitīgi pieaug, bet ejot cauri saņēmēja sistēmas slāņiem informācijas apjoms samazinās.

OSI modeļa Fiziskais slānis

Fiziskais slānis definē elektriskās, mehāniskās, procedurālās un funkcionālās specifikācijas, lai aktivizētu, uzturētu un ataktivizētu fizisko savienojumu starp sistēmām. Fiziskā slāņa specifikācijas definē tādas lielumus kā voltāžas stiprumu, voltāžas izmaiņu

laikietilpību, fiziskos datu pārsūtīšanas ātrumus, maksimālos pārraides attālumus, un fiziskos savienojumus. Fiziskā slāņa implementācijas var iedalīt LAN un WAN specifikācijās.

OSI modeļa Datu Posma slānis

Datu posma slānis nodrošina drošu datu pārraidi pa fizisko slāni. Dažādi datu posma slāņi definē dažādas tīkla un protokolu īpašības. Tās sastāda fiziskā adresācija, tīkla topoloģija, kļūdu apstrādes mehānismi, pārsūtīto kadru secība, un plūsmas kontrole.

Fiziskā adresācija (eng. physical addressing) nosaka, kā ierīces tiek adresētas datu posma slāņa līmenī. Tīkla topoloģija sastāv no datu posma slāņa specifikācijām, kas nosaka, kā ierīcēm jābūt fiziski saslēgtām. Kļūdu apstrādes mehānismi brīdina augstākus OSI slāņus par to, ka notikusi kļūda datu pārraides posmā. Kadru secības mehānisms sakārto datus, kas pie pārraides ir zaudējuši sākotnējo kārtību. Pārraides kontroles mehānisms seko lai ierīce, kas dotajā brīdī saņem datus, netiktu pārslogota ar lielāku datu daudzumu, kā tā spēj apstrādāt.

Elektrotehnikas un elektronikas inženieru institūtā (eng. IEEE - Institute of Electrical and Electronics Engineers) OSI datu posma slānis ir sadalīts divos apakšslāņos: Loģiskā posma vadības apakšslānī (eng. LLC – Logical Link Control) un medija pieejas vadības apakšslānī (eng. MAC – Media Access Control).

Loģiskā posma vadības apakšslānis (LCC) organizē savienojumus starp ierīcēm, kas ir savienotas ar vienu tīkla posmu. LCC ir aprakstīts IEEE 802.2 standartu specifikācijā un atbalsta gan bezsavienojuma, gan savienojumorientētus servisu, ko izmanto augstāka līmeņa slāņu protokoli.

Mēdiju pieejas kontroles apakšslānis vada protokolu pieeju fiziskajiem medijiem. IEEE MAC specifikācijās ir definētas MAC adreses, kas ļauj vairākām ierīcēm tīklā unikāli identificēt vienai otru datu posma slāņa līmenī.

OSI modeļa Tīkla slānis

Tīkla slānis nodrošina maršrutēšanu (eng. Routing) un ar to saistītas funkcijas, kas ļauj savienot daudzus datu posmus vienotā tīklā – internetā. Tas tiek veikts izmantojot ierīču loģisko adresāciju. OSI tīkla slānis atbalsta gan bezsavienojuma, gan savienojumorientētus servisu, ko izmanto augstāka līmeņa slāņi.

Tipiski tīkla slāņa protokoli ir maršrutēšanas protokoli (eng. Routing protocols), bet tīkla slānī ir implementēti arī citi protokolu tipi. Visizplatītākie maršrutēšanas protokoli ir:

- BGP – Border Gateway protocol;
- Internet Interdomain routing protocol;
- OSPF – open shortest path first;
- Link state;
- Interior gateway protocol developed for use in TCP/IP networks;

- RIP - Routing Information Protocol;

OSI modeļa Transporta slānis

Transporta slānis nodrošina drošus datu pārraides servissus, kas augstākiem OSI slāņiem ir caurspīdīgi. Transporta slāņa funkcijas iekļauj plūsmas kontroli (eng. Flow control), multipleksēšanu (eng. Multiplexing), virtuālo savienojumu vadību (eng. virtual circuit management) un kļūdu pārbaudes un labošanas mehānismus.

Plūsmas kontrole vada datu pārraidīšanu tā, lai raidošā ierīce nesūtītu vairāk datus, kā saņemošā ierīce var apstrādāt.

Multipleksēšana ļauj pārsūtīt datus no vairākām aplikācijām pa vienu fizisko savienojumu.

Transporta slānis vada virtuālo ķēžu izveidošanu, apkalpošanu un pārtraukšanu.

Kļūdu pārbaudes mehānismi nodarbojas ar dažādu pārraides kļūdu atklāšanu, savukārt pēckļūdu atkopšanās mehānismi nodarbojas ar uzdevumiem, tādiem kā, piemēram, pieprasījumi datus pārsūtīt vēlreiz, lai novērstu radušās kļūdas.

Dažas transporta slāņa implementācijas iekļauj pārraides vadības protokolu (eng. TCP Transmission Control Protocol), vārdu piesaistes protokolu (eng. Name Binding Protocol), kā arī

OSI transporta protokolus. Pārraides vadības protokols ir TCP/IP protokolu komplekta sastāvā un nodrošina drošu datu pārraidi. Vārdu piesaistes protokols – NBP ir protokols, kas asociē Apple Talk vārdus ar adresēm.

OSI modeļa Sesijas slānis

Sesijas slānis nodibina, vada un pārtrauc sesijas starp pasniegšanas slāņu vienībām. Komunikāciju sesijas sastāv no servisa pieprasījumiem un servisa atbildēm, kas norisinās starp aplikācijām dažādās tīklā saslēgtās ierīcēs. Daži sesijas slāņa implementāciju piemēri:

- ZIP – Zone Information Protocol;
- Apple Talk name binding protocol;
- SCP – Session Control Protocol;
- DECnet Phase IV session-layer protocol.

OSI modeļa Pasniegšanas slānis

Pasniegšanas slānis nodrošina lielu daudzumu dažādu kodēšanas un datu pārveidošanas funkciju, ko pielieto uz datiem no lietojumslāņa. Šo funkciju tiešais uzdevums ir nodrošināt, lai informācija, kas ir nosūtīta no vienas aplikācijas būtu saprotama un lasāma otras sistēmas aplikācijai. Pasniegšanas slāņa kodēšanas funkcijas sastāv no izplatītiem datu prezentēšanas formātiem, šo datu formātu konvertēšanas mehānismiem, plaši pielietotām datu saspiešanas un datu šifrēšanas shēmām.

Plaši pielietoti datu prezentēšanas formāti, tādi kā standarta attēlu, skaņas un video formātu pielietošana ļauj sazināties aplikācijām no dažādām datorsistēmām. Datu pārveidošanas

standarti ļauj sazināties sistēmām, kas izmanto dažādus datu reprezentēšanas mehānismus, tādus, kā, piemēram, EBCDIC un ASCII. Standarta datu saspiešanas shēmas garantē, ka sūtītāja sistēmas saspieštie dati ir pareizi dekompresēti saņēmēja sistēmā. Tāpat arī datu šifrēšanas standarti ļauj sūtītāja sistēmā šifrētos datus pareizi atšifrēt saņēmēja sistēmā.

Kā piemērus kodēšanas un kompresēšanas mehānismiem var minēt:

Video

- Quick Time – Apple Computer audio un video specifikācijas;
- MPEG - Motion Picture Experts Group;

Audio

- GIF - Graphics Interchange Format;
- JPEG - Joint Photographic Experts Group;
- TIFF - Tagged Image File Format;

Piemēram, MPEG, GIF un JPEG ir standarta audio/video saspiešanas mehānismi, savukārt Quick Time un TIFF ir audio/video kodēšanas mehānismi.

OSI Lietojumslānis

Lietojumslānis ir OSI modeļa slānis, kas atrodas vistuvāk gala lietotājam Gan gala lietotājs, gan lietojumslānis sadarbojas tieši ar aplikāciju.

Lietojumslānis tieši sadarbojas ar programmatūras aplikācijām, kas iekļauj savstarpējās komunikācijas. Pati programmatūra jau atrodas ārpus OSI modeļa. Lietojumslāņa funkcijas iekļauj savienojuma partneru identifikāciju, resursu pieejamības noskaidrošanu un savienojuma sinhronizāciju. Resursu pieejamības noskaidrošanas fāzē tiek noskaidrots, vai ir pietiekoši tīkla resursi, lai organizētu veiksmīgu datu pārraidi starp abām sistēmām. Sinhronizācijas fāzē visi nepieciešamie aplikāciju sadarbības uzdevumi tiek organizēti ar lietojumslāņa palīdzību.

Pastāv divi lietojumslāņa implementācijas līmeņi – TCP/IP aplikācijas, tādas kā Telnet, File Transfer protocol (FTP) un Simple Mail Transfer protocol (SMTP), un OSI aplikācijas, tādas kā File Transfer, Access, and Management (FTAM), Virtual Terminal Protocol (VTP), un Common Management Information Protocol (CMIP).

24.stunda

Stundas temats: TCP/IP protokolu steks

Stundas mērķis: Iepazīties TCP/IP protokola steku.

Mācību uzdevumi:

1. Iepazīties ar TCP/IP protokola steku.
2. Izprast atšķirības no ISO/OSI modeļa.

Transmission Control Protocol Internet Protocol (TCP/IP) – tas ir protokolu steka rūpnieciskais standarts, kas tika izstrādāts priekš globāliem tīkliem. TCP/IP standarti ir nopublicēti dokumentu sērijā, ko sauc par Request for Comment (RFC). Šie dokumenti apraksta Internet tīkla iekšējo darbu. Daži RFC apraksta tīkla servisu vai protokolu, kā arī to realizāciju, vai arī pielietošanas nosacījumus. TCP/IP standarti vienmēr tiek publicēti RFC dokumentu veidā, bet ne visi RFC nosaka standartus. Steks tika izstrādāts pēc ASV Aizsardzības ministrijas (Department of Defence, DoD) iniciatīvas vairāk nekā pirms 20 gadiem priekš eksperimentālā tīkla ARPAnet sakariem ar citiem satelītu tīkliem kā kopēju protokolu komplekts priekš dažādām skaitļojamām tehnikām. ARPA tīkls tika izmantots dažādās militārās sfērās. ARPA tīklā sakarus starp diviem datoriem nodrošina Internet Protocol (IP), kas arī mūsdienās ir viens no galvenajiem TCP/IP steka protokoliem, un tā nosaukums figurē steka nosaukumā. Liela daļa TCP/IP steka attīstībā pienākas arī Berklijas Universitātei, kas savā OS UNIX versijā realizēja steka protokolu. OS UNIX izplatīšanās veicināja arī IP un arī citu steka protokolu izplatīšanos. Izmantojot šo pašu steku, strādā arī vispasaules Internet tīmeklis. Šeit lielāko ieguldījumu steka standartu pilnveidošanā, ko publicē RFC specifikāciju formā, dod Internet Engineering Task Force (IETF). Līdz šim TCP/IP steks vairāk bija realizēts OS UNIX tīklos, bet tā parādīšanās pēdējos tīkla OS priekš personālajiem datoriem veicināja strauju TCP/IP steka izplatīšanos.

Tātad, TCP/IP steka līdera pozīcijas var izskaidrot ar sekojošām tā īpašībām:

- tas ir pilnīgākais un populārākais tīkla protokolu steks ar vairāku gadu vēsturi;
- gandrīz visi lielie tīkli lielāko trafika daļu pārsūta ar TCP/IP protokolu palīdzību;
- ar šo metodi var piekļūt Internet tīklam;
- šo steku izmanto par pamatu intranet – korporatīvais tīkls, kas izmanto Interneta transporta pakalpojumus un WWW hiperteksta tehnoloģiju, kas ir izstrādāta Internetā;
- visas mūsdienu OS atbalsta TCP/IP steku;
- tā ir elastīga tehnoloģija priekš dažādu sistēmu savienošanas gan transporta apakšsistēmu līmenī, gan pielikumu servisu līmenī;
- tā ir noturīga palielināma starpplatformu vide priekš klientu- serveriem.

Tā kā TCP/IP steks bija izstrādāts pirms parādījās atvērto sistēmu sadarbības modelis ISO/OSI, un, kaut arī tam bija daudzu līmeņu struktūra, atbilstība starp TCP/IP steka līmeņiem ar OSI modeļa līmeņiem ir diezgan nosacīta.

OSI modeļa slānis	IBM/Microsoft	TCP/IP	Novell	OSI steks	
7	SMB	Telnet, FTP, SNMP, SMTP, WWW	NCP, SAP	X.400 X.500 FTAM	
6				OSI pasniegšanas protokols	
5	NetBIOS	TCP		OSI seansa protokols	
4			SPX	OSI transporta protokols	
3			IP, RIP, OSPF	IPX, RIP, NLSP	ES-ES IS-IS
2	802.3(Ethernet), 802.5(Token Ring), FDDI, SLIP, Fast Ethernet, 100VG-AnyLAN, X.25, ATM, LAP-B,LAP-D, PPP				
1	Koaksiāls, ekranētais/neekranētais vītais pāris, Optiskais kabelis, Radioviļņi				

TCP/IP protokoli sastāv no 4 līmeņiem.

Zemākais līmenis (**IV līmenis**) atbilst OSI modeļa fiziskajam un kanālu līmenim. Šis līmenis TCP/IP protokolos netiek reglamentēts, bet atbalsta visus populāros fiziskā un kanālu līmeņa standartus: priekš lokālā tīkla tas ir Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG–AnyLAN, priekš globāliem tīkliem – “punkts–punkts” savienošanās protokoli SLIP un PPP, teritoriālo tīklu protokoli ar X.25 pakešu komutāciju, frame relay. Ir izstrādāta arī speciāla specifikācija, kas nosaka ATM tehnoloģijas izmantošanu kā kanālu līmeņa transportu. Parasti, parādoties jaunai lokālo vai globālo tīklu tehnoloģijai, tā ātri tiek iekļauta TCP/IP stekā, izstrādājot atbilstošu RFC, kas nosaka IP pakešu un kapsulācijas metodes kadrus.

Nākamais līmenis (**III līmenis**) – starptīklu sadarbības līmenis, kas nodarbojas ar pakešu pārsūtīšanu, izmantojot visdažādākās lokālā tīkla, teritoriālā tīkla u.t.t. transportēšanas tehnoloģijas. Kā tīkla līmeņa pamatu protokols (OSI modeļa terminos) stekā izmanto **IP** protokolu, kurš no sākuma tika projektēts kā pakešu pārsūtīšanas protokols saliktos tīklos, kas sastāv no liela skaita lokālo tīklu, kuri ir apvienoti gan ar lokāliem, gan globāliem sakariem.

Tādēļ IP protokols labi strādā tīklos ar sarežģītu topoloģiju, racionāli un ekonomiski patērējot mazo ātrumu sakaru līnijas. IP protokols ir datagramma protokols, jo tas negarantē pakešu nogādi līdz nozīmētajam mezglam, bet cenšas to izdarīt. Pie starptīklu sadarbības līmeņa var pieskaitīt arī visus protokolus, kas saistīti ar maršrutēšanas tabulu sastādīšanu un modifikāciju, piemēram, maršruta informācijas savākšanas protokoli **RIP** (Routing Internet Protocol) un **OSPF** (Open Shortest Path First), kā arī starptīklu vadošo ziņojumu protokols **ICMP** (Internet Control Message Protocol). Pēdējais protokols ir domāts, lai apmainītos ar informāciju par kļūdām starptīklu maršrutētājiem un mezglu – paketes nosūtītāju. Ar speciālu pakešu ICMP palīdzību tiek paziņots par neiespējamību nosūtīt paketi, paketes laika izbeigšanos, ieilgušu paketes salikšanu no fragmentiem, anomāliem parametriem, sūtīšanas maršruta un apkalpošanas tipa izmaiņām, sistēmas stāvokli u.t.t

Nākamo līmeni (**II līmenis**) saucas par pamata līmeni. Šajā līmenī funkcionē nosūtīšanas vadības protokols **TCP** (Transmission Control Protocol) un lietotāju datagramma protokols **UDP** (User Datagram Protocol). TCP protokols nodrošina drošu paziņojumu nogādi starptīklā attālinātiem pielikuma procesiem, izveidojot virtuālo savienojumu. UDP protokols nodrošina pielikuma pakešu nogādi ar datagrāmo metodi, tāpat kā IP, un izpilda tikai savienjošā posma funkciju starptīkla protokolos un daudzajiem pielikuma procesiem.

Augšējais līmenis (**I līmenis**) tiek saukts par pielikuma līmeni. Daudzo izmantošanas gadu laikā dažādās valstīs un organizācijās TCP/IP steks ir savācis lielu daudzumu pielikuma līmeņa protokolus un servisu. Pie tiem var pieskaitīt tāds plaši izmantots protokols, kā failu kopēšanas protokols FTP, termināla emulācijas protokols telnet, pasta protokols SMTP, ko izmanto Internet tīkla elektroniskajā pastā, hiperteksta servisi pieejai pie attālinātas informācijas, kā, piemēram, WWW un daudzi citi. Dažus no tiem apskatīsim tuvāk.

25.-28.stunda

Stundas temats: TCP/IP steka protokoli

Stundas mērķis: Iepazīties ar TCP/IP steka protokoliem.

Mācību uzdevumi:

1. Iepazīties ar TCP/IP steka protokolu veidiem.
2. Iepazīties ar protokolu pielietojumu.

Starptīklu līmeņa protokoli

- IP (Internet Protocol) – virza paketes no avota uz saņēmēju;
- ICMP (Internet Control Message Protocol) – kontrolē maršrutēšanu ar IP protokolu un tīkla uzvedību, informē avotu;
- PING (Packet Internet Network Grouper) – pārbauda piekļuvi no avota uz saņēmēju;
- ARP;
- RARP;
- BOOTP (Bootstrap Protocol) – DHCP priekštecis – IP-adrešu ielāde un konfigurēšana;
- RIP (Routing Information Protocol) – lokālo apv. tīklu maršrutēšana;
- BGP (Border Gateway Protocol) – starpdomēnu maršrutēšanas protokols;

Lai dators varētu uzturēt sakarus ar citu datoru, tam jāzina otra datora fizikālo (vai MAC) adresi. Internet protokolu komplekta ietilpst divi protokoli (*Address Resolution protocol - ARP* - Adreses noteikšanas protokols un (*Reverse Address Resolution Protocol - RARP* - Reversais adreses noteikšanas protokols), kuri dinamiski nosaka fizikālo (aparātūras) adrešu atbilstību IP adresēm un otrādi. ARP izmanto apraides paziņojumus aparātūras adreses noteikšanai (MAC slānis), kura atbilst konkrētai IP tīkla slāņa adresei. ARP protokolam ir pietiekoši universāls, lai ļautu izmantot IP ar praktiski jebkuru vides pieejas mehānisma tipu. RARP izmanto apraides paziņojumus IP adreses noteikšanai, kura saistīta ar konkrēto aparātūras adresi. RARP ir īpaši nozīmīgs mezgliem, kuriem nav diska un kuri var nezināt savu IP adresi, kad tie tiek sākotnēji iedarbināti. RARP paļaujas uz RARP servera esamību ar tabulas ierakstiem, kuri attēlo MAC apakšslāņa adreses IP adresēs.

Maršrutēšanas iekārtas Internet tīklā saucās par starptīklu interfeisiem (*gateway*), kas ir neveiksmīgs termins, jo tīklos ar šo terminu apzīmē iekārtu ar citādām funkcionālām iespējām.

Starptīklu interfeisi, ko saucim par maršrutētājiem, IP tīklā organizēti pēc hierarhijas –AS/AS apvienība- principa.

Dažus maršrutētājus lieto datu virzīšanai caur tīklu grupu, kuri atrodas zem vienas un tās pašas administratīvās vadības (to sauc par autonomo sistēmu – AS- *autonomous system*).

Maršrutētāji, ko lieto informācijas apmaiņai AS robežās, sauc par iekšējiem maršrutētājiem (*interior routers*); izmanto dažādus iekšējo maršrutētāju protokoli (*interior gateway protocol - IGP*) šī uzdevuma izpildīšanai.

Maršrutēšanas informācijas protokols (*Routing Information Protocol - RIP*) ir viens no tādiem protokoliem.

Maršrutētāji, kuri pārvieto datus autonomo sistēmu starpā, sauc par ārējiem maršrutētājiem (*exterior routers*); šī uzdevuma izpildīšanai tie izmanto ārējo maršrutētāju protokolus.

Robežas maršrutētāju protokols (*Border Gateway Protocol - BGP*) ir tādu protokolu piemērs IP maršrutēšana nosaka IP datagrammu pārvietošanas ceļu caur apvienotiem tīkliem (vienā pārsūtīšana reizē). Ceļojuma sākumā viss maršruts nav zināms.

Katrā pieturā tiek aprēķināts nākamais pieturas punkts, salīdzinot datagrammas sastāvā esošā saņēmēja adresi ar datu ierakstu katra mezgla maršrutu tabulā (MT).

Katra mezgla dalība maršrutēšanas procesā sastāv tikai no pakešu virzīšanas uz priekšu, balstoties tikai uz iekšējās informācijas, neatkarīgi no tā, cik veiksmīgs būs process un vai pakete sasniegs gala pieturas punktu.

IP nenodrošina paziņojumu par bojājumiem nosūtīšanu avotā, kad notiek maršrutēšanas anomālijas.

Šī uzdevuma izpildi veic cits Internet protokols - Internet vadības ziņojumu protokols (*Internet Control Message Protocol - ICMP*).

ICMP reaģē uz situācijām (piem., datu zudums) ģenerējot atbilstošus ziņojumus:

- Destination Unreachable,- saņēmējs nav sasniedzams;
- Echo Request and Reply, - atbalss pieprasījums/atbilde;
- Redirect,- pāradresēt;
- Time Exceeded - laiks pārsniegts un citus.

Ja ICMP ziņojumu nevar piegādāt, otru ziņojumu neģenerē, lai novērstu bezgalīgu ICMP ziņojumu plūsmu.

Ja maršrutētājs sūta ziņojumu *Destination Unreachable* (adresāts nav sasniedzams), tas nozīmē, ka maršrutētājs nespēj aizsūtīt paketi gala saņēmējam un noraida šo paketi.

Var būt 2 iemesli, kāpēc saņēmējs nav sasniedzams:

- avots noteica neeksistējošo adresi un (retāk);
- maršrutētājam nav attiecīga maršruta.

Jebkurš hosts var aizsūtīt ziņojumu *Echo Request* (atbalss pieprasījums), lai pārbaudītu vai mezgls ir pieejams caur tīklu.

Ziņojums *Echo Reply* (atbalss atbilde) rāda, ka mezglu var sekmīgi sasniegt.

Maršrutētājs sūta avotam ziņojumus:

- *Redirect* (pāradresēšana), lai stimulētu efektīvāku maršrutēšanu;
- *Time Exceeded* (laiks ir pārsniegts), lai norādītu, ja kāda pakete pārsniedz tai noteiktu eksistēšanas laiku (pārsūtījumos vai sekundēs).

Pēdējo ziņojumu sūta, ja IP paketes dzīves ilguma lauks TTL =0.

Pēc tam šo paketi noiet, lai novērstu nepārtrauktu paketes cirkulēšanu, ja tīklā izveidojas maršrutēšanas cilpa.

ICMP papildinājums nodrošina jauniem mezgliem apakštīkla maskas atrašanas iespēju, kuru izmanto apvienotajā tīklā dotajā momentā.

Kopumā ICMP ir jebkuru IP realizāciju integrālā daļa, it īpaši tādu, kuras izmanto maršrutētājus Transporta līmeņa protokoli

Tie uztur sakaru seansus starp datoriem un garantē drošu datu apmaiņu.

Populārākie transporta līmeņa protokoli:

- TCP (*Transmission Control Protocol*) – TCP/IP steka protokols datu, kuri ir sadalīti fragmentu secībā, garantētai piegādei;
- SPX – firmas Novell IPX/SPX (*Internetwork Packet Exchange/Sequential Packet Exchange*) protokolu komplekta daļa datiem, sadalītiem fragmentu secībā;
- NWLink – firmas Microsoft IPX/SPX protokola realizācija;
- NetBEUI (NetBIOS (*Network Basic Input/Output System*) *Extended User Interface* – lietotāja paplašinātais interfeiss) – uzstāda sakaru seansus starp datoriem (NetBIOS) un piedāvā augstākiem slāņiem transporta pakalpojumus (NetBEUI);
- ATP (*AppleTalk Transaction Protocol*, NBP (*Name Binding Protocol*) – firmas Apple sakaru seansu un datu transporta protokoli.

Transporta slāņa protokoli nodrošina mehānismus, kas nepieciešami jebkura daudzuma datu piegādei caur tīklu no avota saņēmējam.

Pārraidēšanas vadības protokols - TCP (Transmission Control Protocol), kas paredz iepriekšēju savienojumu nodibināšanu; tajā ir tādi drošas pārraidēšanas un **plūsmas vadības mehānismi** kā: slīdošais logs, taimauti, apstiprinājumi un atkārtotas pārraidēšanas.

Tas ir paplašinātais NetBIOS interfeiss. Sākotnēji, NetBIOS un NetBEUI uzskatīja kā vienu protokolu. Pēc tam LAN ražotāji tā nodalīja NetBIOS, seansa slāņa protokolu, ka to nevarēja izmantot kopā ar citiem maršrutējamiem transporta protokoliem.

NetBIOS (*Network Basic Input/Output System* – tīkla bāzes ievadizvades sistēma) – seansa slāņa IBM-interfeiss ar LAN, kurš darbojas kā lietojumu interfeiss ar tīklu. To lieto LAN zem MS-DOS, OS-2, **Windows** un dažu UNIX versiju vadības.

Protokols dod programmām līdzekļus sakaru seansu realizēšanai ar citām tīkla programmām. Tas ir ļoti populārs.

NetBEUI ir neliels, ātrs un efektīvs transporta slāņa protokols, ko piegādā visiem firmas Microsoft tīkla produktiem. Tas parādījās 80. gadu vidū pirmajā Microsoft tīkla produktā – MS®-NET.

NetBEUI priekšrocības:

- neliels steka izmērs (svarīgi MS-DOS-datoriem);
- augsts datu pārraides ātrums tīklā;
- saderība ar visiem Microsoft tīkliem.

Galvenais NetBEUI trūkums, ka neuztur maršrutēšanu (lieto LAN)

IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) -protokolu steks, ko lieto Novell tīklos. Neliels un ātrs protokols. Atšķirībā no NetBEUI, tas uztur maršrutēšanu. NWLink ir firmas Microsoft IPX/SPX realizācija.

AppleTalk ir firmas Apple Computer protokolu steks, kurš ļauj datoriem Apple Macintosh kopīgi lietot failus un printerus tīkla vidē. iekļauts OS Macintosh.

AppleTalk protokoli uztur protokolus LocalTalk, Ethernet (EtherTalk) un TokenRing (Token Talk).

Lietotāju datagrammu protokols – UDP (User Datagram Protocol), kas ļauj lietojumprogrammai nosūtīt ziņojumu vienam vai vairākiem lietojumiem. Ja, lietojot UDP, nepieciešama droša pārraide, tad augšējā programmā jāietver secības pārbaude un kļūdu atklāšana.

Failu pārsūtīšanas protokols **FTP** (File Transfer Protocol) realizē attālinātu piekļūšanu pie failiem. Drošas pārsūtīšanas nodrošināšanai, FTP transportēšanai izmanto saites izveidošanu protokolu – TCP. Bez failu pārsūtīšanas, FTP piedāvā arī citus pakalpojumus.

Lietotājs var uzsākt interaktīvu darbu ar attālinātu mašīnu, piemēram, viņš var izdrukāt tās kataloga saturu. Un visbeidzot, FTP veic lietotāju autentifikāciju. Pirms piekļūšanas pie faila, saskaņā ar protokolu, lietotājam ir jāievada savu vārdu un paroli. Lai piekļūtu pie publiskiem Interneta FTP arhīvu katalogiem, paroles autentifikācija netiek prasīta, un to var apiet ar, speciāli tādai pieejai domāto, lietotāja vārdu Anonymous. TCP/IP stekā FTP protokols piedāvā visplašāko pakalpojumu klāstu priekš darba ar failiem, bet tas ir arī visgrūtākais priekš programmēšanas. Pielikumos, kur nav nepieciešamas visas FTP iespējas, var izmantot vienkāršāko failu pārsūtīšanas protokolu TFTP (Trivial File Transfer Protocol), kas ir daudz ekonomiskāks. Šis protokols realizē tikai failu pārsūtīšanu, bez tam kā transports tiek izmantots daudz vienkāršāks protokols (nekā TCP) bez savienojuma uzstādīšanas – UDP.

Telnet protokols nodrošina baitu plūsmas starp procesiem, kā arī starp procesu un terminālu. Visbiežāk šo protokolu izmanto priekš attālināta datora termināla emulācijas. Izmantojot telnet servisu, lietotājs faktiski var vadīt attālinātu datoru tāpat, kā lokālais lietotājs, tādēļ šādam pieejas veidam ir nepieciešama laba aizsardzība. Šī iemesla dēļ, telnet serveri kā minimums vienmēr izmanto autentifikāciju pēc paroles, bet reizēm arī vēl spēcīgākus aizsardzības līdzekļus, piemēram, Kerberos sistēmu.

SNMP protokolu (Simple Network Management Protocol) izmanto tīkla līmeņa organizēšanai. No sākuma SNMP protokols tika izstrādāts priekš attālinātas Interneta maršrutizatoru, ko tradicionāli sauc par slūžām, kontroles un vadības. Palielinoties popularitātei, SNMP protokolu sāka izmantot arī priekš jebkura komunikācijas līdzekļa vadības – koncentratoriem, tiltiem, tīkla adapteriem u.t.t. SNMP protokola vadības problēma ir iedalīta divos uzdevumos. Pirmais uzdevums ir saistīts ar informācijas padošanu. Vadošās informācijas nodošanas protokoli nosaka SNMP–aģenta, kas strādā vadāmajā iekārtā, un SNMP–monitora, kas strādā uz administratora datora un ko bieži mēdz saukt arī par vadības konsoli, sadarbības procedūru. Nodošanas protokoli nosaka paziņojumu formātus, ar kuriem apmainās aģenti un monitors.

Otrais uzdevums ir saistīts ar kontrolējamajiem mainīgajiem, kas raksturo vadāmās iekārtas stāvokli. Standarti reglamentē, kādiem datiem ir jāsaglabājas un jāsakrājas iekārtā, kā arī šo datu nosaukumus un nosaukumu sintaksi. Standartos SNMP ir noteikta tīkla vadības informacionālās datu bāzes specifikācijas. Šī specifikācija, pazīstama kā MIB (Management Information Base) datu bāze, nosaka datu elementus, kurus vadāmajai iekārtai ir jāsaglabā, kā arī iespējamās operācijas ar tiem.

29.stunda

Stundas temats: TCP/IP komandrindas utilitās.

Stundas mērķis: Iepazīties ar komandrindas tīkla utilitām.

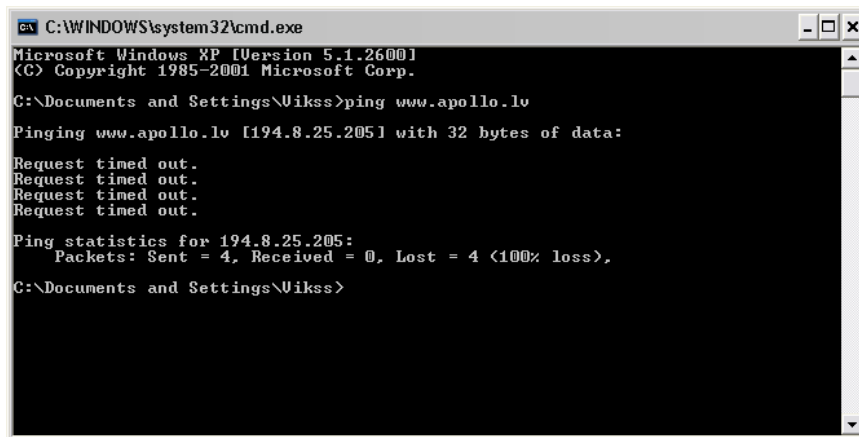
Mācību uzdevumi:

1. Iepazīties ar komandrindas tīkla utilitām PING, ROUTE, IPCONFIG, TRACERT, NETSTAT.
2. Izprast utilītu pielietojumu.

Startēt komandrindas utilitās var, ja piemēram Windows XP operētājsistēmas vidē tiek startēta utilīta CMD.

ping

Utilītprogramma, kas nosaka, vai kāda noteikta tīkla Internet IP adrese ir sasniedzama. Pārbaudi veic, nosūtot paketi uz šo adresi un sagaidot uz to atbildi. Sākotnēji utilītprogramma PING tika izmantota, lai pārbaudītu tīkla Internet savienojumus.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Uikss>ping www.apollo.lv

Pinging www.apollo.lv [194.8.25.205] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 194.8.25.205:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

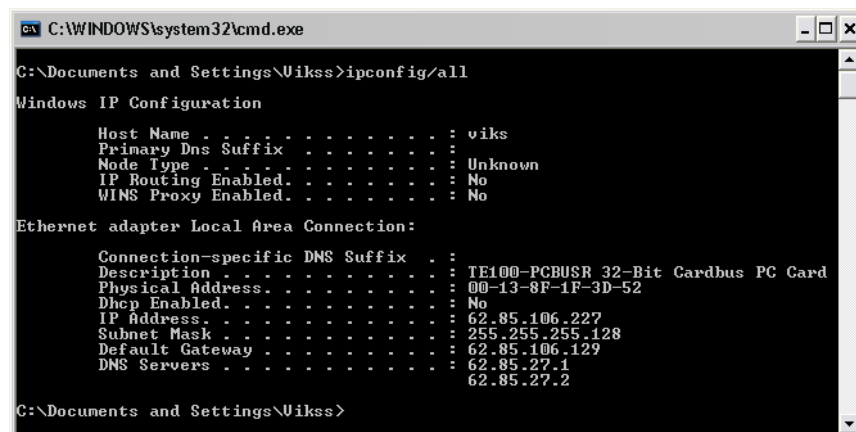
C:\Documents and Settings\Uikss>
```

route

Datu bloka (paketes) pārraides ceļš datu pārraides tīklā.

ipconfig

sniedz ziņas par sava datora tīkla elementiem, TCP/IP uzstādījumiem, ieskaitot DHCP un WINS serverus tīklā.



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Uikss>ipconfig/all

Windows IP Configuration

    Host Name . . . . . : viks
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

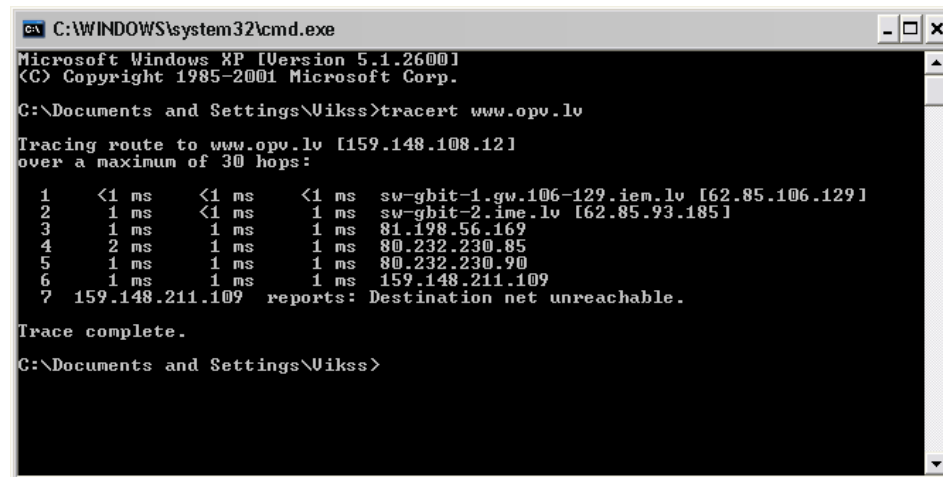
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    Description . . . . . : TE100-PCBUSR 32-Bit Cardbus PC Card
    Physical Address. . . . . : 00-13-8F-1F-3D-52
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 62.85.106.227
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 62.85.106.129
    DNS Servers . . . . . : 62.85.27.1
                           62.85.27.2

C:\Documents and Settings\Uikss>
```

tracert

Komanda ļauj reģistrēt pakešu maršrutu līdz konkrētam datoram globālajā tīklā un spriest par pakešu noraides ātrumu attiecīgajos tīkla posmos



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Vikss>tracert www.opv.lv

Tracing route to www.opv.lv [159.148.108.12]
over a maximum of 30 hops:

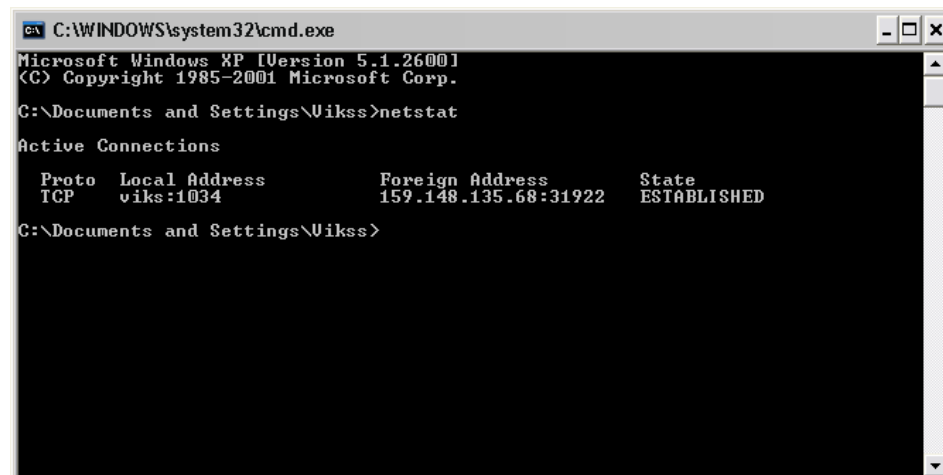
  1  <1 ms    <1 ms    <1 ms    sw-gbit-1.gw.106-129.iem.lv [62.85.106.129]
  2  1 ms     <1 ms    1 ms     sw-gbit-2.iem.lv [62.85.93.185]
  3  1 ms     1 ms     1 ms     81.198.56.169
  4  2 ms     1 ms     1 ms     80.232.230.85
  5  1 ms     1 ms     1 ms     80.232.230.90
  6  1 ms     1 ms     1 ms     159.148.211.109
  7  159.148.211.109 reports: Destination net unreachable.

Trace complete.

C:\Documents and Settings\Vikss>
```

netstat

Attēlo TCP/IP tīkla protokola aktivitātes un statistiku.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Vikss>netstat

Active Connections

   Proto Local Address          Foreign Address         State
   TCP    viks:1034              159.148.135.68:31922    ESTABLISHED

C:\Documents and Settings\Vikss>
```

30. – 31.stunda

Stundas temats: IP klases. IP adresu binārā un decimālā formas.

Stundas mērķis: Iepazīties ar IP klasēm un IP adresu formām.

Mācību uzdevumi:

1. Iepazīties ar IP klasēm.
2. Iepazīties ar IP adresu bināro un decimālo formu.
3. Izprast, kas ir lokālās adreses un simboliskie domēnu vārdi.

Protokolu stekā TCP/IP tiek lietoti 3 adresu tipi:

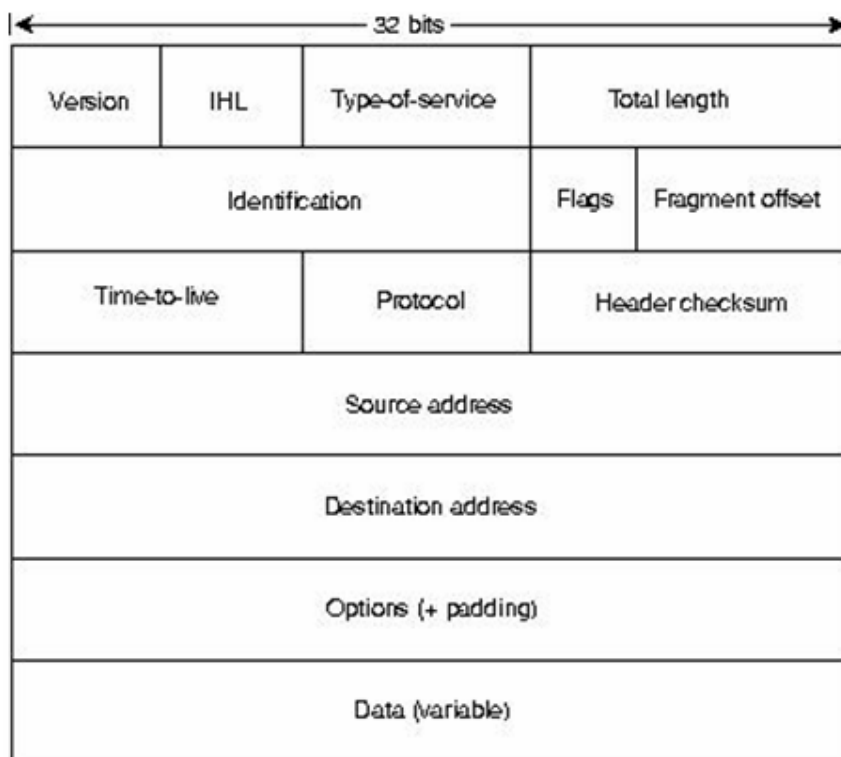
- lokālās adreses, ko sauc arī par aparātadresēm jeb MAC-adresēm;
- IP-adreses;
- simboliskie domēnu vārdi.

TCP/IP-terminoloģijā ar vārdu lokālā adrese saprot tādu adresi, ko lieto datu nogādei tāda apakštīkla ietvaros, kas ir intertīkla sastāvdaļa. Dažādos apakštīklos ir pieļaujamas dažādas tīklu tehnoloģijas un dažādi protokolu steki, tādēļ veidojot TCP/IP tīklu tika paredzēta dažādu tipu lokālo adresu eksistence. Ja apakštīkls ir lokālais tīkls, tad lokālā adrese ir MAC-adrese. To piešķir tīkla adapteriem un maršrutētāju tīkla interfeisiem šo iekārtu ražotāji. Piešķiršana notiek centralizēti un tādēļ šīs adreses ir unikālas.

MAC-adresēm ir 6 baitu formāts, piemēram, 11-A0-17-3D-BC-01.

Tāpat kā citiem tīkla slāņa protokoliem, IP adresācijas shēma ir IP datagrammu maršrutēšanas procesa caur apvienotu tīklu neatņemama daļa. IP adreses garums sastāda 32 bitus, kuri ir sadalīti divās vai trijās daļās. Pirmā daļa nozīmē tīkla adresi (to nosaka Internet tīkla informācijas centrs (Network Information Center - InterNIC), ja tīkls ir Interneta daļa, otrā (ja tā eksistē) - apakštīkla adresi, un trešā - resursdatora adresi (to nosaka tīkla administrators). Apakštīkla adreses ir tikai tajā gadījumā, ja tīkla administrators pieņēma lēmumu par tīkla sadalīšanu apakštīklos. Tīkla, apakštīkla un resursdatora adreses lauku garumi ir mainīgi lielumi.

IP paketes formāts



IP iesākums sākas no versijas numura (version number), kas norāda izmantojamās IP versijas numuru. Iesākuma garuma lauks (IHL) apzīmē datagrammas iesākuma garumu 32 bitu vārdos. Servisa tipa lauks (type-of-service) norāda, kādā veidā jāapstrādā tekošā datagramma saskaņā ar konkrēta augstāka slāņa protokola norādījumiem. Ar šī lauka palīdzību datagrammām var tikt piešķirti dažādi nozīmības līmeņi.

Kopējā garuma lauks (total length) nosaka visas IP paketes garumu baitos, ieskaitot datus un iesākumu. Identifikācijas lauks (identification) satur veselu skaitli, kurš nozīmē tekošu datagrammu. Šis lauks tiek izmantots datagrammas fragmentu savienošanai. Karogu lauks (flags) ir 3 bitu lauks, kurš nosaka, vai var tikt fragmentēta dotā datagramma un vai tekošais fragments ir pēdējais.

Fragmenta pārbīdes lauks (fragment offset) norāda fragmenta pozīciju pret datu sākumu oriģinālajā datagrammā, kas ļauj IP saņēmēja procesam pareizi rekonstruēt oriģinālo datagrammu. Dzīves ilguma lauks (time-to-live) uztur skaitītāju, kura vērtība pakāpeniski samazinās līdz nullei; šajā momentā datagramma tiek noraidīta. Tas novērš pakešu ieciklēšanos. Protokola lauks (protocol) norāda, kurš augstākā slāņa protokols pieņems ieejošās paketes pēc IP apstrādes pabeigšanas. Iesākuma kontroles summas lauks (header checksum) palīdz nodrošināt IP iesākuma veselumu. Avota un saņēmēja adresu lauki (source and destination address) nozīmē nosūtīšanas un pieņemšanas mezglus. Opcijas lauks (options) ļauj IP nodrošināt fakultatīvās iespējas, tādas, kā datu aizsardzība. Datu lauks (data) satur augstāko slāņu informāciju.

IP adrešu struktūra:

Decimālais pieraksts x.x.x.x

32 biti sadalīti 4 oktetos (astoņu bitu skaitļos,

piem., 192.5.5.1 = binārie

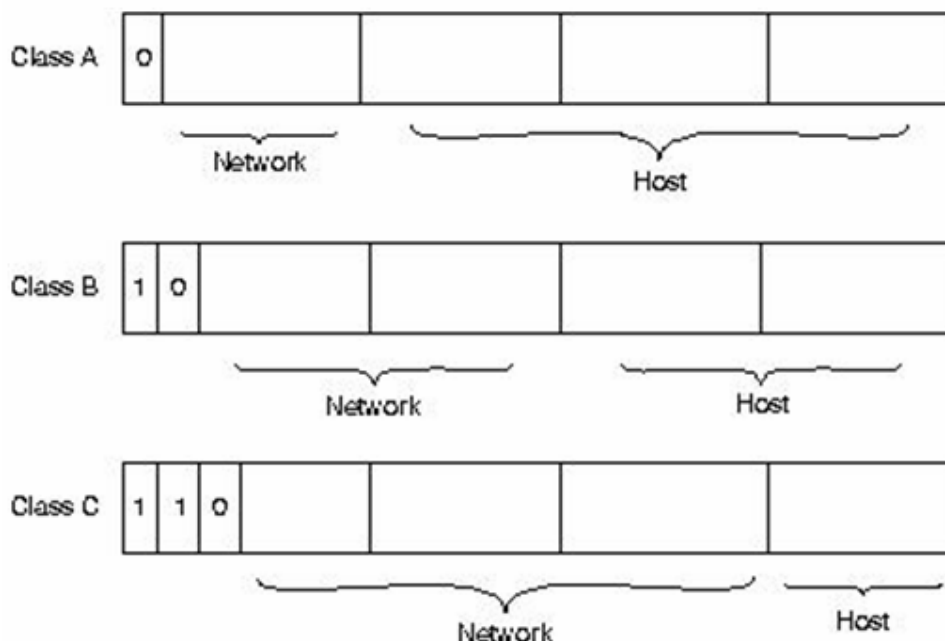
11000000.00000101.00000101.00000001)

IP adresācija nodrošina piecas dažādas adrešu klases. Paši galējie kreisie biti nozīmē adreses klasi.

- **A klases adreses** galvenokārt paredzēts izmantošanai ļoti **lieliem tīkliem**, jo tie nodrošina tikai 7 bitus tīkla adreses laukam, pārējos - hostiem
- **B klases adreses – vidējiem tīkliem** - izdala 14 bitus tīkla adreses laukam un 16 bitus resursdatora adreses laukam. Nodrošina kompromisu starp tīkla un hosta adreses telpu.
- **C klases adreses – maziem tīkliem** - izdala 22 bitus tīkla adreses laukam. C klases adreses nodrošina tikai 8 bitus hosta adreses laukam, tāpēc resursdatoru skaits vienā tīklā var kļūt par ierobežojošu faktoru.
- **D klases adreses** tiek rezervētas **grupām ar vairākpunktu adresāciju – grupu apraidei** - D klases adresēs četri augstākās kārtas biti tiek uzstādīti uz vērtībām 1,1,1 un 0.
- IP nosaka arī **E klases adreses**, bet tās ir rezervētas izmantošanai nākotnē. E klases adresēs visi četri augstākās kārtas biti tiek uzstādīti uz 1.

IP (Internet protocol) ir 3.slāņa galvenais protokols Internet protokolu komplektā. Tas ir aprakstīts RFC 791 un kopā ar TCP protokolu veido Internet protokolu kodolu. IP nodrošina datagrammu piegādi bez savienojuma nodibināšanas ar vismazākām pūlēm (best effort), kā arī datagrammu fragmentēšanu un reasamblēšanu, lai uzturētu datu kanālus ar dažādiem maksimālo pārraides bloku (maximum-transmission unit - MTU) izmēriem.

Katrs baits 32 bitu IP adresē tiek pasniegts decimālskaitļa formātā un tiek atdalīts no citiem baitiem ar punktu (dot) palīdzību (dotted decimal notation), piemēram, 34.0.0.1. ir parādīti IP adrešu formāti A, B un C klasēm.



Rezervētās IP adreses

IANA – Internet Assigned Numbers Authority (RFC 1918)

- 10.0.0.0 - 10.255.255.255 10.0.0.0/8
- 172.16.0.0 - 172.31.255.255 172.16.0.0/12
- 192.168.0.0 - 192.168.255.255 192.168.0.0/16

Domēnu simbolu vārdus IP tīklos sauc par domēniem un tie ir konstruēti pēc hierarhijas principa.

Domēnu vārdu sastāvdaļas tiek atdalītas viena no otras ar (.) un tās nolasa tā, ka paša augstākā slāņa – saknes – domēna vārds atrodas labajā pusē. Tātad no sākuma (kreisā pusē) atrodas gala mezgla vārds, tad mezglu grupas vārds (piemēram, organizācija), tad lielākas grupas – apakšdomēna – vārds (ja tāds ir). Piemērs: www.opv.lv

Jāuzsver, ka starp domēna vārdu un mezgla IP-adresi nav nekādas algoritmiskas atbilstības, tādēļ nepieciešams izmantot papildus tabulas vai servisu, lai tīkla mezglu varētu viennozīmīgi noteikt kā pēc domēna vārda tā arī pēc IP-adreses. TCP/IP tīklos šim nolūkam lieto speciālu izklaidētu servisu – domēnu vārdu sistēma (*Domain Name System –DNS*), kas nodibina šo atbilstību balstoties uz tīkla administratora izveidotajām atbilstības tabulām. Tādēļ domēna vārdus sauc arī par DNS-vārdiem.

32.stunda

Stundas temats: Apakštīkli un maskas

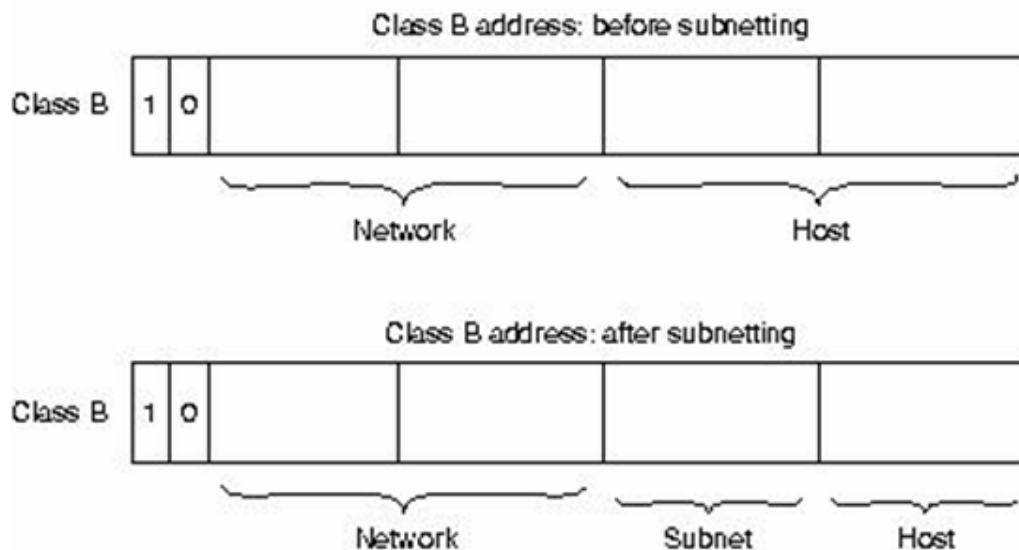
Stundas mērķis: Iepazīties ar apakštīkliem.

Mācību uzdevumi:

1. Iepazīties ar tīklu apakštīkliem.
2. Iepazīties ar tīkla maskām.

IP tīkli var arī būt sadalīti mazākās vienībās, kuras sauc par apakštīkliem (subnets). Apakštīkli nodrošina papildus elastību tīkla administratoram. Piemēram, pieņemsim, ka kaut kādam tīklam ir noteikta B klases adrese, un ka visi mezgli tīklā dotajā brīdī atbilst B klases adreses formātam. Tālāk pieņemsim, ka šī tīkla adrese ir 128.10.0.0 (visas nulles resursdatora adreses laukā norāda uz visu tīklu). Administrators var sadalīt tīklu, izmantojot apakštīklu organizēšanu. Tas tiek izpildīts, aizņemoties bitus no adreses daļas, kura pieder resursdatoram, un izmantojot tos kā apakštīkla adreses lauku.

Apakštīklu organizēšana.



Ja tīkla administrators nolēma izmantot astoņus bitus apakštīkla organizēšanai, tad trešais IP B klases adreses baits nodrošina šī apakštīkla numuru. Mūsu piemērā adrese 128.10.1.0. attiecas uz tīklu 128.10, apakštīklu 1; adrese 128.10.2.0. attiecas uz tīklu 128.10, apakštīklu 2, u.t.t.

Bitu skaits, kuri ir aizņemti ar apakštīkla adresi, ir mainīgs lielums. Izmantojamo bitu skaita uzdošanai IP nodrošina apakštīkla masku. Apakštīkla maskas izmanto to pašu adreses izteiksmes formātu un tehniku, kā IP adreses. Apakštīkla maskas satur vieniniekus visos bitos, izņemot tos, kuri nosaka resursdatora lauku. Piemēram, apakštīkla maska, kura uzdod 8 apakštīkla organizēšanas bitus A klases adresei 34.0.0.0, ir izteiksme 255.255.0.0. Apakštīkla

maska, kura nosaka 16 apakštīkla organizēšanas bitus A klases adresei 34.0.0.0, ir izteiksme 255.255.255.0.

Lai dators varētu uzturēt sakarus ar citu datoru, tam jāzina otra datora fizikālo (vai MAC) adresi. Internet protokolu komplektā ietilpst divi protokoli (Address Resolution protocol - ARP - Adrešes noteikšanas protokols un (Reverse Address Resolution Protocol - RARP - Reversais adrešes noteikšanas protokols), kuri dinamiski nosaka fizikālo (aparātūras) adrešu atbilstību IP adresēm un otrādi. ARP izmanto apraides paziņojumus aparātūras adrešes noteikšanai (MAC slānis), kura atbilst konkrētai IP tīkla slāņa adresei. ARP protokolam ir pietiekoši universāls, lai ļautu izmantot IP ar praktiski jebkuru vides pieejas mehānisma tipu. RARP izmanto apraides paziņojumus IP adrešes noteikšanai, kura saistīta ar konkrēto aparātūras adresi. RARP ir īpaši nozīmīgs mezgliem, kuriem nav diska un kuri var nezināt savu IP adresi, kad tie tiek sākotnēji iedarbināti. RARP paļaujas uz RARP servera esamību ar tabulas ierakstiem, kuri attēlo MAC apakšslāņa adrešes IP adresēs.

Class A address	00100010	. 0 ,	. 0 ,	. 0 ,	34.0.0.0	
Subnet mask: 8 subnet bits		. 1 ,	. 1 ,	. 0 ,	. 0 ,	255.255.0.0
Class A address	00100010	. 0 ,	. 0 ,	. 0 ,	34.0.0.0	
Subnet mask: 16 subnet bits		. 1 ,	. 1 ,	. 1 ,	. 0 ,	255.255.255.0