ო. ნატროშვილი

მონაცემთა მიღება-გადაცემის მართვისა და დიაგნოსტირების ალგორითმები კომპიუტერულ ქსელებში

„ტექნიკური უნივერსიტეტი”

საქართველოს ტექნიკური უნივერსიტეტი

ო. ნატროშვილი

მონაცემთა მიღება-გადაცემის მართვისა და დიაგნოსტირების ალგორითმები კომპიუტერულ ქსელებში

დამტკიცებულია სტუ-ს
სარედაქციო-საგამომცემლო
საბჭოს მიერ

თბილისი
2009

უაკ 681.3

წინამდებარე სახელმძღვანელო წარმოადგენს ერთ-ერთ ძირითად კურსს კომპიუტერული სისტემებისა და ქსელების მიმართულების მაგისტრანტებისათვის. მასში განხილული საკითხებით შეიძლება ისარგებლონ 2201 სპეციალობის ბაკალავრიატის უფროსი კურსის სტუდენტებმა და დოქტორანტებმაც შესაბამისად საკურსო და სადისერტაციო ნაშრომების შესასრულებლად.

რეცენზენტები: სრული პროფესორი ზ. წვერაიძე
სრული პროფესორი კ. კამკამიძე

ISBN 978-9941-14-601-5
http://www.gtu.ge/publishinghouse/

შინაარსი

წინასიტყვაობა

წარმოდგენილი სახელმძღვანელო განკუთვნილია ძირითადად კომპიუტერული სისტემებისა და ქსელების მიმართულების მაგისტრანტებისათვის, რომლებსაც უკვე გააჩნიათ სათანადო საბაკალავრო მომზადება 2201 – სპეციალობაში. ყურადღება გამახვილებულია თანამედროვე კომპიუტერული ქსელების ძირითად სახეებზე და მათი მეშვეობით მონაცემთა პაკეტების მიღება – გადაცემების ალგორითმების თავისებურებებზე. სახელმძღვანელოში გაშუქებულია ცენტრალიზებული და დეცენტრალიზებული ქსელების აგებისა და მუშაობის პრინციპები, მოცემულია OSI – შვიდდონიანი ეტალონური მოდელის თითოეული დონის დახასიათება, შესაბამისი პროტოკოლების როლი და მნიშვნელობა ქსელის გამგზავნ და მიმღებ კომპიუტერებს (ე.წ. ჰოსტის მუშა სადგურებს) შორის მონაცემთა პაკეტების ფორმირებისა და მათი ელექტრონული ტრანსპორტირებისათვის, განხილულია კომპიუტერული ქსელების ტოპოლოგიური სტრუქტურები, შემადგენელი ქსელური კომპონენტები, მათი მახასიათებლები და ამ სტრუქტურებში მონაცემთა მიღება-გადაცემის ალგორითმები. წიგნში განხილულია ქსელების ფიზიკური გარემოს საკაბელო სისტემები, მათი გავლენა

მონაცემთა პაკეტების მიღება-გადაცემის სიჩქარეებზე. ამჟამად მომქმედი სტანდარტების მიხედვით მიმოხილულია პაკეტების ფორმირებისა და მათი ელექტრონული ტრანსპორტირებისათვის საჭირო კადრის სტრუქტურები. განხილულია მონაცემთა მიღება-გადაცემების თავისებურებები საერთო სალტური და რგოლური სტრუქტურის კომპიუტერული ქსელებისათვის. მოცემულია CSMA/CD პროტოკოლზე დაფუძნებული მონაცემთა მიღება-გადაცემის ალგორითმები და შესაბამისი ბიჯების მიხედვით მათი სარეალიზაციო პროცედურები. ქსელის მართვისა და დიაგნოსტირების მიზნით დახასიათებულია ქსელში გამოყენებული პროტოკოლების ანალიზატორები, გაშუქებულია მათ მიერ რეალიზებული ქსელური ოპერაციების კონტროლის საკითხები. აღნიშნულია და ღრმად გაანალიზებული პაკეტებს შორის კოლიზიური მოვლენების შემთხვევები, ქსელის სეგმენტების მუშაობის გადატვირთული რეჟიმების აღმოჩენა-აღმოფხვრის პრობლემები. მოცემულია გრძელი და მოკლე ზომის (სიგრძის) კადრების დახასიათება. განხილულია ქსელის მონიტორინგის და მართვის საკითხები, მოცემულია შესაბამისი პროტოკოლების მუშაობის პრინციპების დეტალური განხილვა. ამ მიზნით ნაჩვენებია ქსელის მართვის NMS-სისტემის ზოგადი სქემა MIB-შემადგენელი ელემენტებით. ყურადღებაა გამახვილებული სახელწოდებათა გლობალური "ხის" აგების საბაზო ალგორითმზე SNMP-აგენტების გამოყენებით. სახელმძღვანელოში ცალკე

თავადაა გამოყოფილი კომპიუტერული ქსელის სადიაგნოსტიკო პაკეტების სტრუქტურების შექმნისა და ქსელის მიმღებ-გადამცემ მუშა სადგურებს შორის კორექტული შეერთების ტესტირების საკითხები Diagnostic Responder სადიაგნოსტიკო ”კითხვა-პასუხების” წარმოების თანამედროვე ტექნოლოგიებით.

შესავალი

ნებისმიერი ტიპისა და დანიშნულების კომპიუტერულ ქსელებში ოპერატორის (წარმოდგენილ სახელმძღვანელოში ყველგან ოპერატორში ვგულისხმობთ როგორც მომხმარებელს, ისე მომსახურე პერსონალს: ქსელის ადმინისტრატორს, მიმღებ-გადამცემი საკომუნიკაციო არხების ინტეგრატორს, კავშირის ხაზების უსაფრთხოების დაცვის ინსპექტორს და ა.შ.). კომპიუტერულ ქსელში მუშაობის სპეციფიკა მნიშვნელოვნად განსხვავდება ცალკეულ პერსონალურ (ქსელთან არა მიერთებულ) კომპიუტერზე მუშაობისაგან. კომპიუტერული ქსელით მონაცემთა მიღება-გადაცემებისათვის საჭიროა სასიცოცხლო მნიშვნელობის სხვადასხვა მოწყობილობების გამოყენება. ასეთ მოწყობილობებს პირველ რიგში წარმოადგენენ მომხმარებელთა მუშა სადგურები (უმეტესწილად პერსონალური კომპიუტერები) და კავშირგაბმულობის საკომუნიკაციო ხაზები, რომლებიც რეალიზებული არიან საკაბელო სისტემებით ან მონაცემთა მიმღებ-გადამცემი რადიო სიხშირული არხების გამოყენებით. საკაბელო სისტემას, როგორც წესი, თან ახლავს აუცილებელი აღჭურვილობა, კერძოდ, სიგნალების მიმღებ-გადამცემი კავშირგაბმულობის მოწყობილობები, რომლებიც მთლიანობაში ქმნიან ინფორმაციის მიმღებ-გადამცემ არხებს. ქსელის დანიშნუ-ლებისა

და მისი მასშტაბებიდან გამომდინარე საკაბელო სისტემასთან მიერთებულია სხვადასხვა რაოდენობის კომპიუტერული ტექნიკა. ისინი იწოდებიან ქსელის კვანძებად ან სადგურებად, ხოლო მომხმარებლები კი - ქსელის აბონენტებად. კომპიუტერულ ქსელში მონაცემების გაცვლა საკაბელო სისტემასთან მიერთებული ერთი სადგურიდან მეორეში სწარმოებს საკომუტაციო პროტოკოლების მიხედვით, რომლებიც ჰოსტის ან სატრანზიტო დანიშნულების კომუტატორებში არეგულირებენ ურთიერთშეთანხმებებს ქსელის მიმღებ-გადამცემ კვანძებს შორის.

საკომუტაციო თანამედროვე ტექნოლოგიებში დღეს-დღეობით დომინირებს IP (Internet Protocol) ტექნოლოგია, რის გამოც ტექნიკურ ლიტერატურაში შესაბამისი კომპიუტერული ქსელები მოიხსენებიან, როგორც IP-ქსელები. სხვადასხვა სტანდარტებისა და მუშაობის პრინციპების მიხედვით IP-პროტოკოლები გაერთიანებული არიან პროტოკოლების ერთიან ოჯახში TCP/IP(Transmission Control Protocol/Internet Protocol- მონაცემთა გადაცემის მართვის პროტოკოლები). ხშირად მას (ოჯახს) მოიხსენიებენ როგორც პროტოკოლების "სტეკს". ამ ოჯახის პროტოკოლები და სტანდარტები წარმოადგენენ იმ ძირითად ბირთვს, რაზედაც დაფუძნებულია ის ინსტრუმენტი, რომელთანაც ჩვენ გვაქვს ყოველდღიური შეხება კომპიუტერულ-ქსელურ საქმიანობაში.

ქსელების მუშაობის პრინციპები და სტანდარტების აღწერა კოორდინირებულია RFC-ით (Requests For Comments)-ქსელის

მუშაობის პრინციპებისა და TCP/IP ქსელური პროტოკოლების სტანდარტების სპეციფიკაციებით. ამჟამად RFC - აერთიანებს 5000-ზე მეტი სტანდარტების აღწერილობებს, რომელთაგან თითოეული წარმოადგენს საშუალოდ 2-დან 200 გვერდამდე მოცულობის ტექნიკურ ტექსტებს ინგლისურ ენაზე (მაგალითად, TCP პროტოკოლის ერთ-ერთი აღწერა იმყოფება RFC-793-ში). პროტოკოლები, რომლებიც ძირითადად ემსახურება ქსელის მთავარ მიზანს, მონაცემთა პაკეტების მანძილზე ეფექტურ გადაცემებს, განისაზღვრება RFC მუშა დოკუმენტებით. ისინი პერიოდულად (ყოველი ახალი ვერსიის შემუშავებისას) ქვეყნდება, საყოველთაოდ რეცენზირდება და ანალიზირდება Internet-ის სპეციალისტების მიერ. ამ უკანასკნელთა მხრიდან დადებითი შეფასებების საფუძველზე ისინი ფიქსირდება (რეგისტრირდება) ISO-სტანდარტიზაციის საერთასორისო კომიტეტის ქვედანაყოფების მიერ შემდგომში მათი მასობრივი გავრცელებისა და გამოყენების მიზნით. RFC-დოკუმენტების რაოდენობა თანდათანობით იზრდება (ქსელური ტექნიკის განვითარებასთან ერთად), რაც დაკავშირებულია ძველი სტანდარტების განუწყვეტელ მოდერნიზაციასთან და ახალი სტანდარტების შექმნასთან (როგორც აღვნიშნეთ, ვერსიების მიხედვით). მათი გაცნობით პირველ რიგში დაინტერესებული არიან კომპიუტერული ქსელების ინტეგრატორები და

ადმინისტრატორები თავიანთ დაქვემდებარებაში მყოფ ქსელებში უახლოესი ტექნიკის დანერგვის მიზნით.

საკომუტაციო ქსელური რესურსების (როგორც ტექნიკური მოწყობილობების და მის პარალელურად პროგრამული უზრუნველყოფის) დაპროექტებითა და წარმოებით ამჟამად დაკავებულია მრავალი წამყვანი ფირმა თუ ცალკეული ორგანიზაცია. საკომუტაციო პროდუქციის მწარმოებლები ერთმა-ეთის მიმართ მკაცრი კონკურენციის პირობებში ცდილობენ მაქსიმალური ოპერატიულობით მოახდინონ რეალიზაცია IP-ტექნოლოგიებისა და მათი მუდმივად ცვალებადი, თანდათან უფრო სრულყოფილი, თვისებებით. თუ დღევანდელ მდგომა-რეობას შევაფასებთ მონაცემთა მიღება-გადაცემებისათვის საჭირო აღჭურვილობას ხარისხის კუთხით, თანამდეროვე კომუტატორები, მარშრუტიზატორები და სხვა ქსელური აპარატულ-პროგრამული მოწყობილობები ასრულებენ ძირითადად უკვე დაჩქარებული მარშრუტიზაციის ფუნქციებს, რომლებიც ექვემდებარება IP ბოლო უახლოეს ვერსიებს. ისინი მართავენ მომსახურების ხარისხს QoS (Quality of Service), რომელშიც პირველ რიგში იგულისხმება მონაცემთა ეფექტური მიღება-გადაცემის თვალსაზრისით ისეთი მახასიათებლები, როგორიცაა ქსელის სწრაფქმედება, მისი წარმადობა (გადაცემული მონაცემების რაოდენობა დროის ერთეულში) და მისი გამოყენების საიმედოობა.

ძალზე აქტუალური და სასარგებლოა QoS მართვის ახალ-ახალი პროტოკოლების შესწავლა და მათი გამოყენება, მაგალითად, RSVP (Reservation Protocol-რესურსების რეზერვირების) პროტოკოლის. ადმინისტრატორების გარდა უახლოესი პროტოკოლების დანერგვით დაინტერესებული არიან სახალხო (მასობრივი მოხმარების) ქსელების პროვაიდერებიც, რომელთა დაქვემდებარებაშიც იმყოფება მონაცემთა მიმღებ-გადამცემი კავშირგაბმულობის საკომუნიკაციო ხაზები.

კომპიუტერულ ქსელებში მონაცემთა მიმღებ-გადამცემი უახლოესი აღჭურვილობის შეძენა და დამონტაჟება (მასში იგულისხმება ქსელის მართვისა და დიაგნოსტიკის საშუალებებიც) საკმაოდ ძვირადღირებული საქმიანობაა, ამიტომ მათი მუშაობის სავარაუდო ხანგრძლიობის წინასწარი ანალიზის დროს ქსელის ადმინისტრატორები უნდა სერიოზულად დაფიქრდნენ რა გავლენას მოახდენს მონაცემთა მიღება-გადაცემის მართვისა და დიაგნოსტიკის ყოველი ახალი ტექნოლოგიების შემოსვლა თავიანთ ქსელზე უახლოეს მომავალში. პასუხების გაცემა მსგავს კითხვებზე აუცილებელია იმ შემთხვევაშიც კი, თუ ამა თუ იმ ორგანიზაციის მონაცემთა მიღება-გადაცემის IP-ტექნოლოგიების ახალი შესაძლებლობების გამოყენება ჯერ-ჯერობით მათ არ სჭირდებათ. თუმცა დაბეჯითებით შეიძლება იმის მტკიცება, რომ მონაცემთა (შეტყობინებათა) მიღება-გადაცემის ახალი ტექნოლოგიების მთელი რიგი პერსპექტიული შესაძლებლობები, როგორიცაა, მაგალითად,

IP-ტელეფონია, ვიდეოკონფერენციები, ჯგუფური გადაცემები რეალურ დროში და სხვა, მათ აუცილებლივ დასჭირდებათ უახლოეს მომავალში. ამის უგულველყოფა კი ქსელის ორგანიზაციისა და მონტაჟის დროს შეიძლება ძვირად დაუჯდეს მატერიალური დანახარჯების თვალსაზრისით ქსელის რესურსების შემდგომი, კვლავ მოდერნიზაციისათვის.

იმისთვის, რომ კარგად გავერკვეთ მონაცემთა მიღება-გადაცემის ახალ-ახალ ტექნოლოგიებში, საჭიროა საფუძვლიანად შევისწავლოთ ის ფუძემდებლური პრინციპები, რომლებიც საერთოა ამ ტექნოლოგიებისათვის. ეს წარმოადგენს წინამდებარე სახელმძღვანელოს ძირითად მიზანს. ამასთან, იმისთვის რომ სწორად გამოვიყენოდ ესა თუ ის ახალი შესაძლებლობების მქონე ქსელური მოწყობილობები, მეტად საჭიროა აღნიშნული სახელმძღვანელოდან იმ ცოდნის მიღებაც, თუ როგორ ურთიერთმოქმედებენ ეს მოწყობილობები სხვა საკომუნიკაციო აღჭურვილობასთან მიმართებაში ერთი დასრულებული ქსელური გადაწყვეტის ფარგლებში.

თავი 1

ზოგადი ცნობები კომპიუტერული ქსელების შესახებ

1.1. ძირითადი ცნებები. კომპიუტერული ქსელების სახესხვაობები

კომპიუტერული ქსელები წარმოადგენენ გამოთვლითი ტექნიკის მოწყობილო-ბებისა და კავშირგაბმულობის საკომუნი-კაციო საშუალებების ბრწყინვალე ურთიერთ შერწყმას, რომლის მიზანია მონაცემთა პაკეტების სახით ფორმირებული შეტყობინე-ბების მიღება-გადაცემის პროცედურების რეალიზება (უმეტეს წილად სასურველ, მიმდინარე რეალურ დროში).

სახალხო მომსახურების ნებისმიერი ტიპის გამომთვლელი ქსელი წარმოადგენს პერსონალური კომპიუტერებისა (ქსელის კლიენტებისთვის) და დიდი წარმადობის მეინფრეიმების (ქსელის სერვერული ნაწილისათვის), უპირველეს ყოვლისა მეხსიერე-ბის დიდი მოცულობის მქონე კომპიუტერების ბაზაზე შექმნილი კვანძების ღია (გახსნილ) სისტემას, რომელშიც გამოყენებულია ამ კვანძების ერთმანეთთან დაკავშირებული მონაცემთა პაკეტების მიმღებ-გამცემი არხები კვანძის სადგურებს შორის ინფორმაციების ეფექტური ურთიერთ გაცვლების საწარმოე-ბლად.

ინფორმაციის გადაცემის უშეცდომო და მაქსიმალური მოხერხებულობის უზრუნველსაყოფად ყველა ქსელური ოპერა-

ცია რეგულირდება გარკვეული წესებისა და შეთანხმებების ერთობლიობით (კრებულით), რომლებიც ცნობილია ქსელური პროტოკოლების (protocols) სახელწოდებით. თითოეული პროტოკოლი ასახავს როგორც მონაცემთა მიღება-გაცემის (ასევე ოპერაციების კორექტულობის დიაგნოსტიკის) ალგორითმების პროგრამულ მხარეს, ასევე ამ ალგორითმების სარეალიზაციო აპარატურის ტექნიკურ მხარესაც, ე.ი. პროტოკოლი განსაზღვრავს ზოგადი გაგებით მომხმარებელთა პერსონალური კომპიუტერების, კაბელების, მათთან ამ მუშა სადგურების შემაერთებელი საკონტაქტო ჩანგლების ტიპებს, მონაცემთა მიღება-გადაცემებისთვის გამოყენებული სიგნალების სახეებს, მონაცემთა ფორმატებს, პაკეტების გადაცემებისას წარმოქმნილი შეცდომების აღმოჩენის (და აღმოფხვრის) ხერხებს და ა.შ.

გარდა ზემოთ ჩამოთვლილი კომპონენტებისა, ქსელის პროტოკოლები განსაზღვრავენ, აგრეთვე, ქსელური მოწყობილობების მუშაობის (ფუნქციონირების) ალგორითმებს ქსელის დონეებს შორის (OSI ეტალონური მოდელის შვიდდონიან საფეხურებს შორის) ინტერფეისებისთვის ამ ინტერფეისული მოწყობილობების თავისებურებების გათვალისწინებით, ეყრდნობა რა სტანდარტულ მონაცემებს გარკვეული ტიპისა და დანიშნულების ქსელის საზღვრებში. ისინი (პროტოკოლები) ასახავენ შეტყობინებების მომზადების პრინციპებს, პაკეტების მიღება-გადაცემისა და ანალიზის (ასევე კონტროლის) სახეებს მათი დეტალიზაციის სხვადასხვა დონეზე.

კომპიუტერულ ქსელებს ერთმანეთისგან განასხვავებენ მათი დანიშნულების (საინფორმაციო-საკომუნიკაციო და მმართველი

მიზნებისათვის განკუთვნილი ქსელები), ქსელის გეოგრაფიული ტერიტორიების გადაფარვის მასშტაბების, ანუ ქსელის ზომების (კორპორაციული-ლოკალური ან გლობალური ქსელები), მონაცემთა გადაცემის პრინციპებისა და ქსელის მართვის სახეობის (ცენტრალიზებული და დეცენტრალიზებული ქსელები) და სხვა პარამეტრების მიხედვით.

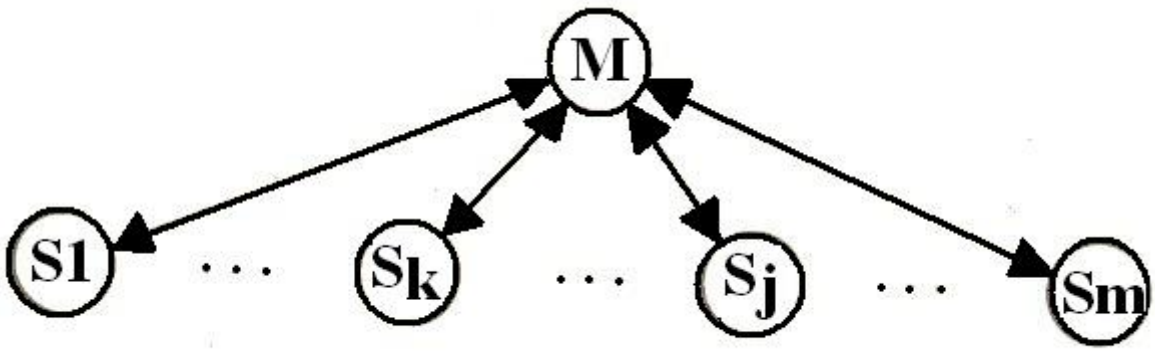
ზემოთ ჩამოთვლილი განსხვავებები დაკავშირებულია როგორც საკუთრივ ქსელის მუშაობასთან, ასევე მონაცემთა მიმღებ-გადამცემი არხებისა და იმ ფიზიკური მოწყობილობების სახესხვაობებთან, რომლებიც გამოიყენება მთლიანობაში გარკვეული ქსელური გარემოს შესაქმნელად.

კომპიუტერულ ქსელურ სისტემებს შორის ხაზგასასმელია ორი ძირითადი სახე-სხვაობა: ცენტრალიზებული და დეცენტრალიზებული ქსელური სტრუქტურები. ქსელის მართვის თავლსაზრისით ისინი დიდ გავლენას ახდენენ მონაცემთა მიღებასა და გადაცემის პრინციპებზე და ამ პრინციპებზე დაფუძნებული მეთოდების სარეალიზციო ალგორითმებზე.

ცენტრალიზებულ ქსელში წამყვან ნაწილს წარმოადგენს “მთავარი” კვანძი-ქსელური კონტროლერი (ან ცენტრალური სადგური), რომელიც მართავს მონაცემთა ნებისმიერ გადაცემებს ქსელის ყველა კვანძს შორის (ე.ი. როგორც კლიენტებისათვის, ასევე სერვერებისათვის, რომლებიც აკმაყოფილებენ (უზრუნველყოფენ) ამ კლიენტების საინფორმაციო მოთხოვნილო-ბებს). ყველა მონაცემმა (პაკეტებმა) ასეთი ტიპის ქსელის ყველა კვანძებს შორის უნდა იმოძრაოს ცენტრალური კვანძის (მმართველი სადგურის ან მისი შემადგენელი ნაწილის-

კონტროლერის) გავლით იმ შემთხვევაშიც კი თუ საინფორმაციო გაცვლა წარმოებს ორ მეზობელ პერიფერიულ (თუნდაც ერთმანეთთან ძალზე ახლოს მდებარე) კვანძს, კონკრეტულ შემთხვევაში მომხმარებელთან ორ მუშა სადგურს, ე.ი. ჰოსტის კომპიუტერებს, შორის.

ცენტრალიზებული ქსელის მაგალითი წარმოდგენილია ნახ.1.1–ზე.



ნახ.1.1. ცენტრალიზებული ქსელის მაგალითი. M-წამყვანი კვანძი; S1...Sk...Sj...Sm - მიმღებ-გადამცემი კვანძები

როგორც ნახ. 1.1–დან ჩანს, აქ განასხვავებენ ორი ტიპის ქსელურ კვანძებს: წამყვან M კვანძს (მაგალითად, ქსელურ კონტროლერს) და მიმღებ Sj კვანძებს. ამ მოდელში ყველა შეტყობინება გადაიცემა M – წამყვანი (მთავარი) კვანძის

გავლით. მაგალითად, თუ K-ურ კვანძს სურს გადასცეს შეტყობინება (პაკეტის სახით) J-ურ მიმღებ კვანძს, მაშინ შეტყობინება ჯერ გადაეცემა M წამყვან კვანძს, ხოლო ეს უკანასკნელი გაუგზავნის J-კვანძს.

ცენტრალიზებული სტრუქტურის ქსელში წამყვანი M კვანძი მუშაობს შემდეგი ალგორითმით:

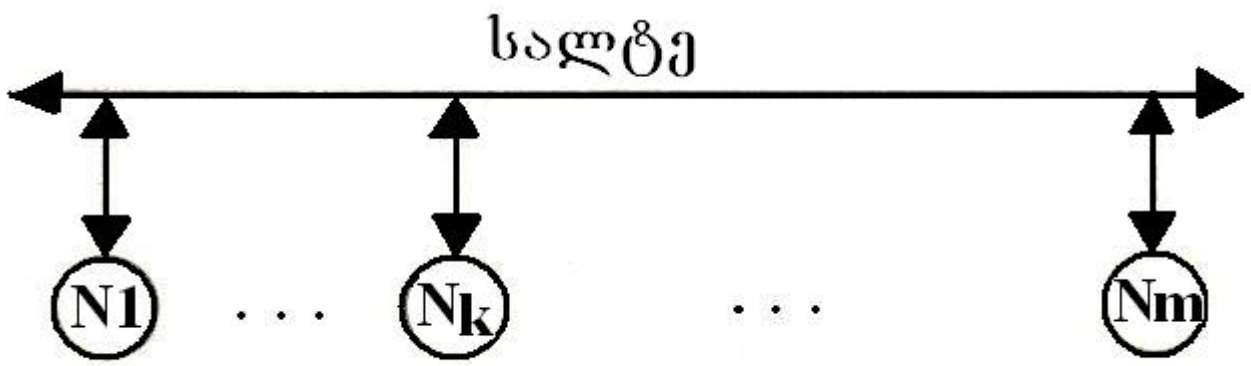
```
repeat
    k : = 1
    repeat
     if  there is message  for  k-thnode  then
        send  message  to the  k-th node
     endif
     inquire the k-th  node  for message
     if the k-th  node  has  a messageto send  then
     grant  permission  to  transmit  for  the  k-th node
     accapt  message  from the  k-th  node
     endif
     k : = k + 1
    until  k : = m + 1 (*m – number of  slave  nodes  on the network*)
    until  power down.
```

ხოლო თითეული მიმღები კვანძისათვის მუშაობის ალგორითმს აქვს შემდეგი სახე:

```
repeat
 wait  for the message  or  inquiry  from  master  node
 if  message  then
   accept  message  from  master  node
 elseif  inquiry  then
   if  there  is a message  to be  transmitted  then
     send  request  for  permission  to  transmit
     wait  for permission  to  transmit
     transmit  message  to  master  node
   endif
```

```
  endif
until power down.
```

ჩენტრალიზებული ქსელებისაგან განსხვავებით დეცენტრალიზებულ ქსელში ყველა კვანძს გააჩნიათ თანაბარი უფლებები ქსელის არხების გამოსაყენებლად და ისინი იმართებიან ერთი და იმავე წესით (მონაცემთა მიღება-გაცემის ალგორითმით). ასეთ ქსელში არ არსებობს მკვეთრად გამოხატული წამყვანი მოწყობილობა ან წამყვანი დამაკავშირებელი არხი, ისე როგორც ამას ადგილი აქვს ცენტრალიზებულ ქსელში. ანუ სხვა სიტყვებით რომ ვთქვათ, ქსელის არხებში შეღწევის მართვა განაწილებულია ყველა კვანძებს შორის თანაბრად. დეცენტრალიზებული ქსელის მაგალითი ნაჩვენებია ნახ. 1.2–ზე:



ნახ. 1.2 დეცენტრალიზებული ქსელის მაგალითი. N1..., N2..., Nk..., Nm-ქსელის შემცველი კვანძები

თუ დეცენტრალიზებულ ქსელს აქვს რგოლური (ჩაკეტილი) სტრუქტურა, მასში გამოიყენება მონაცემთა გადაცემის მეთოდი, დაფუძნებული მმართველი კადრის მოძრაობასთან (ხშირად უწოდებენ მარკერს). ასეთ სტრუქტურაში თითოეულ კვანძს ეძლევა მონაცემთა გადაცემის უფლება მაშინ, როცა ის მიიღებს (დაიჭერს) ქსელში მოძრავ მარკერს (როგორც აღვნიშნეთ, მმართველ კადრს), რომელიც თავისუფლად მოძრაობს (ცირკულირებს ჩაკეტილ წრეში) ქსელთან მიერთებულ შუალედურ სადგურებს შორის. ამგვარად, მარკერი წარმოადგენს მმართველი დანიშნულების შეტყობინებას (მმართველ კადრს), რომელიც მოძრაობს ჩაკეტილი რგოლის გარშემო ქსელის კვანძებს შორის (უფრო ზუსტად ამ კვანძების გავლით). როგორც კი რომელიმე კვანძი მიიღებს მარკერს (ხშირად ამბობენ დაეუფლება ამ მმართველ კადრს), ის კვანძი გააქტიურდება და იღებს დეტერმინირებულ უფლებას კონკრეტული შემთხვევისათვის თავისი საჭიროებისამებრ გამოიყენოს მონაცემთა მიმღებ-გამცემი არხი. გააქტიურებული კვანძი, თავის მონაცემებს (რგოლთან მიერთებულ თითოეულ სადგურს (კომპიუტერს) გააჩნია კონკრეტული საკუთარი MAC მისამართი) მიმღები კვანძისაკენ, აგზავნის ქსელის სხვა კვანძების გავლით. ეს უკანასკნელები თუკი მათი აპარატურული მისამართები (MAC–მისამართები) არ ემთხვევა პაკეტების გამგზავნი კომპიუტერის კვანძის მიერ (ხშირად მოიხსენიებენ მას, როგორც წყარო–კომპიუტერს) მარკერში (მმართველ კადრში) მითითებულ კონკრე-ტულ მიმღები კომპიუტერის მისამართს (ან მისამართებს

პაკეტების ფართო სამაუწყებლო დაგზავნის რეჟიმებისათვის), მაშინ დანარჩენი ყველა კვანძი გვევლინება გამმეორებლის (Repeator) როლში, რომლებიც დაუბრკოლებლად გაატარებენ წყარო–კომპიუტერიდან გამოგზავნილ შეტყობინების პაკეტს. გადაცემის სეანსის დამთავრების შემდეგ (ე.წ. დასტურის სიგნალის მიღების შემდეგ, როცა მიმღები კომპიუტერი ჩაიბარებს წყარო-კომპიუტერიდან გამოგზავნილ პაკეტს), წყარო–კომპიუტერი ან მიმღები–კომპიუტერი (ტრეილერის მიღების შემთხვევაში) ათავისუფლებენ მარკერს, რომელიც დაიწყებს ხელახალ თავისუფალ ცირკულაციას ქსელის კვანძებს შორის.

დეცენტრალიზებული ქსელის ყველა კვანძი მუშაობს ერთი და იგივე ალგორითმით, რომელსაც აქვს შემდეგი სახე:

```
repeat
  wait for token or message
  if message then
     accept message
  elseif token then
     if there is a message to be sent then
     transmit message
  endif
  transmit token to the next node
 endif
until power down.
```

ზემოთ განხილული ცენტრალიზებული და დეცენტრალიზებული ქსელების, ერთმანეთთან შედარებისას აღვნიშნოთ, რომ ცენტრალიზებული ქსელი უფრო ნაკლებ საიმედოა მუშაობაში (თუმცა გადაცემის ალგორითმი მარტივია) დეცენტრალიზებულ ქსელთან შედარებით, ვინაიდან ცენტრალიზებულ

ქსელში წამყვანი M კვანძის მწყობრიდან გამოსვლა იწვევს მთელი ქსელის პარალიზებას, ეს იმ დროს, როცა, დეცენტრალიზებულ ქსელში რომელიმე კვანძის (ან კვანძების) მწყობრიდან გამოსვლა გავლენას არ ახდენს ქსელის სხვა კვანძების ნორმალურ ფუნქციონირებაზე.

როგორც ზემოთ აღვნიშნეთ, კომპიტერულ ქსელებს განასხვავებენ, აგრეთვე, კვანძების გეოგრაფიული განაწილების მიხედვითაც (მათი გადაფარვის ზონის ზომების მხედველობაში მიღებით), რომელთაგან ძირითადად აღსანიშნავია ქსელების ორი კატეგორია: ლოკალური ქსელები და გლობალური ქსელები. ეს უკანასკნელი წარმოადგენს ლოკალური ქსელების გაერთიანებას (ამის მაგალითია ყველასათვის ცნობილი და ამჟამად ფართოდ გავრცელებული Ethernet-ქსელი).

ლოკალური ქსელის შემცველი კვანძები განთავსებული არიან ერთმანეთისგან დაშორებული შედარებით მცირე მანძილებით. ქსელის ზომიდან გამომდინარე ლოკალურ ქსელებს განასხვავებენ კორპორაციული დანიშნულების (ქსელის ყველა კვანძი, ე.ი. მომხმარებლის პერსონალური კომპიუტერი განლაგებულია ერთი კონკრეტული დაწესებულების–კორპორაციის შიგნით), საქალაქო ქსელებს (ხშირად მოიხსენიებენ მეგაპოლისებად), კამპუსის ტიპის ქსელებად (გადაფარული, მაგალითად, მეგაპოლისის ერთ რომელიმე მცირე ნაწილში (მცირე დასახლებაში)), რეგიონალურ ქსელებად (საქალაქთაშორისო ქსელებად) და ა.შ. ყველა სახის ზემოთ ჩამოთვლილ ლოკალურ ქსელებში მათი განთავსების საზღვრები (სადგურებს შორის მანძილები) არ აღემატება

რამდენიმე კილომეტრს (თანამედროვე ტექნოლოგიებით კი რამოდენიმე ასეულ კილომეტრს).

გლობალური ქსელები, როგორც აღვნიშნეთ, წარმოიქმნება ლოკალური ქსელების გაერთიანებით, რომლებიც ერთმანეთთან დაკავშირებულია ე.წ. ხიდების (Bridges) დახმარებით. თუმცა აქვე უნდა აღინიშნოს ისიც, რომ ხშირად გლობალური და ლოკალური ქსელების ცნებები (ისევ და ისევ თავიანთი ზომებიდან გამომდინარე) პირობითია. Internet-ის გარდა თანამედროვე გაგებით გლობალური ქსელის სახესხვაობას წარმოადგენს, მაგალითად, ავიახაზების დამაკავშირებელი საკომუნიკაციო ქსელები, ასევე მაგალითად, სხვადასხვა ქალაქებში, ქვეყნებში ან სხვადასხვა კონტინენტებზე განლაგებული ობიექტების დამაკავშირებელი ქსელები.

როგორც ცენტრალიზებული ისე დეცენტრალიზებული ქსელები შეიძლება რეალიზებული იქნენ ლოკალური გამომთვლელი ქსელების სახით. მაგალითად, ფირმა Intel-ის BITBUS კავშირგაბმულობა წარმოადგენს ცენტრალიზებული ლოკალური კომპიუტერული ქსელის ტიპიურ მაგალითს, ეს იმ დროს, როცა Ethernet-ქსელები წარმოადგენენ დეცენტრალიზებულ კომპიუტერულ ქსელებს. ცენტრალიზებული გამომთვლელი ქსელები გამოიყენება ძალზე დიდი ხანია.

ერთ-ერთ პირველ ქსელურ სტანდარტს წარმოადგენს კავშირგაბმულობის ხაზები, შექმნილი IEEE-488 სალტის ბაზაზე. ასეთი ქსელი იყო ტიპიური ცენტრალიზებული ქსელი, რომელიც აწარმოებდა (ხშირად ხმარობენ ტერმინს მხარს უჭერდა)

სადგურებს შორის ინფორმაციის სწრაფ ურთიერთ გაცვლას ერთმანეთისგან მცირე მანძილებით დაშორებულ კომპიუტერებს შორის.

დეცენტრალიზებული ლოკალური კომპიუტერული ქსელი წარმოიქმნა გასულ საუკუნეში (კერძოდ 1970-იან წლებში). პირველ ასეთ ქსელებს წარმოადგენენ Datapoint ფირმის მიერ შემუშავებული ქსელი-Arcent და ფირმა Xerox-ის მიერ შექმნილი Ethernet-ქსელი.

ამჟამად არსებობს ლოკალური გამომთვლელი ქსელების მრავალნაირი სახეობა. მათთვის დამუშავებულია პროტოკოლების მრავალი სტანდარტი, რომლებიც დროის მსვლელობასთან ერთად თანდათან მოდერნიზდება (აქედან გამომდინარე პროტოკოლებს ყოფენ სხვადასხვა ვერსიებად), თუმცა აქვე შევნიშნოთ ისიც, რომ ამჟამად შემუშავებული სატანდარტული ნორმები ჯერ კიდევ ამომწურავად არ მოიცავენ ლოკალური ქსელების ფუნქციონირების ყველა ასპექტს. არსებობს სტანდარტული მოთხოვნები ქსელებისა და მათი კომპონენტების მიმართ, რომლებსაც არეგულირებენ სტანდარტიზაციის საერთაშორისო კომიტეტები. მათგან გამოირჩევა ISO და IEEE. ამ უკანასკნელმა ლოკალური ქსელებისთვის გამოაქვეყნა სამი ფუძემდებლური სტანდარტი, რომლებიც ეხება ლოკალური ქსელების პროტოკოლებს (ძირითადად OSI მოდელის ქვედა დონეების) დეცენტრალიზებული სტრუქტურებისათვის. ეს პროტოკოლები ახდენენ ქსელის კვანძების მიერ მონაცემთა

გადამცემი გარემოს ერთდროულად გამოყენების სხვადასხვა მეთოდების ფორმალიზაციას.

ერთ-ერთი ფართოდ გავრცელებული სტანდარტი Ethernet 802.3 (იგი ციფრებით იშიფრება, როგორც 1980 წლის 2 თებერვალს გამოქვეყნებული Ethernet-ქსელის მე-3 ვერსია). ამ ვერსიის ყველა პროტოკოლი დაფუძნებულია ქსელში სიმრავლითი (კოლექტიური) შეღწევის (ქსელის რესურსებზე წვდომის) მეთოდზე წარმტანის კონტროლითა და კოლიზიების (გადაცემულ პაკეტებს შორის კონფლიქტის) აღმოჩენით– CSMA/CD (Carrier Sense Multiple Access with Collision Detection). ამ მეთოდზე (პროტოკოლზე) არის დაფუძნებული ამჟამად ყველაზე ფართოდ გავრცელებული და პოპულარული ქსელური Ethernet-ტექნოლოგიები. (AT&T ფირმის Starlan ქსელიც ასევე დაფუძნებულია CSMA/CD პრინციპებზე).

შედარებით ახალ სტანდარტს წარმოადგენს Ethernet 802.5. ამ სტანდარტით გათვალისწინებულ მოწყობილობებს აწარმოებს ფირმა IBM, ლოკალური ქსელების, ჩვენს მიერ ზემოხსენებული რგოლური სტრუქტურებისათვის, რომლებიც მუშაობენ მარკერის გადაცემის პრინციპით (ასეთი ტიპის ქსელებს შორის ამჟამად ყველაზე პოპულარულია Token Ring 802.5 ქსელები, რომლებიც მხარს უჭერენ მე-5 ვერსიის ტექნოლოგიას 1980 წლის თებერვალში გამოქვეყნებულ სტანდარტში). ზემოთ აღნიშნულ ძირითად სტანდარტებს შორის პოპულარობის თვალსაზრისით მესამე ადგილზეა Ethernet 802.4, რომლის სალტურ სტრუქტურაში გამოყენებულია მარკერული გადაცემა. ამ სტანდარტის

სწრაფად გავრცელებად დამატებას (გამოყენებით პროგრამულ დამატებას) წარმოადგენს MAP (Manufacturing Automation Protocol). ამ ტექნოლოგიის ქსელებს მართვის ავტომატიზებული სისტემებისათვის წარმატებით იყენებს კომპანია General Motors-ი.

1.2. Ethernet – ტექნოლოგიების ქსელების დადებითი მხარეები და ნაკლოვანებები

კომპიუტერული ქსელების საერთო დადებითი მხარეები და მათი ნაკლოვანე-ბები მოკლედ ჩამოვთვალოთ Ethernet – ტექნოლოგიებით აგებული ქსელების ორ, ამჟამად სხვა ტექნოლოგიებთან შედარებით ფართოდ გავრცელებული, საერთო სალტური და რგოლური სტრუქტურების მაგალითზე.

ტექნიკურ და სამომხმარებლო ფაქტორების გათვალი-სწინებით Ethernet – ქსელების, რომლებსაც გააჩნიათ საერთო სალტური სტრუქტურა, ძირითადად დადებით მხარეებს წარმოადგენენ:

– ქსელის დაყენებისა და გამართვის სიმარტივე, ე.ი. ქსელის მონტაჟისა და ქსელური პროგრამული ინსტალაციის სიმარტი-ვე. ეს გამოიხატება იმაში, რომ ქსელის ყველა მუშა სადგური შესაძლებელია ადვილად მიუერთდეს ნებისმიერი სეგმენტის კაბელს (T-ს მაგვარი მისაერთებლით ან ტრანსივერით). მუშა სადგურის Ethernet ლოკალურ გამომთვლელ ქსელთან მისა-

ერთებლად არ არის აუცილებელი ცალკე კონცენტრატორების გამოყენება (Token Ring ქსელებისაგან განსხვავებით);

– საკმაოდ კარგად შესწავლილი და დახვეწილი ტექნოლოგია (ქსელების ამჟამად არსებული სხვა ტექნოლოგიებთან შედარებით). მრავალი წლის განმავლობაში Ethernet – ლოკალური ქსელები წარმოადგენენ ყველაზე ფართოდ გავრცელებულ სამრეწველო ქსელებს;
– ქსელური ბარათების (რუქების) ხელმისაწვდომობა (Ethernet – ქსელური რუქები ბოლო პერიოდში მნიშვნელოვნად გაიაფდა);
– შესაძლებელია გამოყენებული იქნას სხვადასხვა კონფიგურაციის საკაბელო სისტემა. Ethernet–ი შეიძლება აგებული იქნეს სხვადასხვა ტიპის (და გაყვანილობის სხვადასხვა სქემით) საკაბელო სისტემით.

სალტური სტრუქტურის Ethernet – ქსელების ნაკლოვანებად უნდა ჩაითვალოს:

– ქსელის გამტარუნარიანობის მნიშვნელოვანი კლება, თუ კი ლოკალური ქსელი ძლიერ დატვირთულია. ეს ნიშნავს იმას, რომ ლოკალურ ქსელებში, რომლებიც მუშაობენ ქსელში შეღწევის CSMA/CD მეთოდით, მათი წარმადობა ქვეითდება (ეცემა) ქსელის დატვირთვის გაზრდასთან ერთად.
– უწესივრობის ძებნის სირთულე. ეს ნაკლოვანება მდგომარეობს იმაში, რომ მაგალითად, Ethernet – ქსელის საერთო საკაბელო სისტემის გაყვანილობის დროს გამოიყენება “სქელი” და “წვრილი” (ან მათი კომბინაცია) Ethernet –

კაბელი, რის გამოც ზოგიერთ სიტუაციაში ქსელში უწესივრობის ძებნა გაძნელებულია. კაბელის გაწყვეტის დროს მწყობრიდან გამოდის ქსელის მთლიანი სეგმენტი და ქსელის იმ კვანძის ლოკალიზება, რომლის მიზეზითაც წარმოიქმნება შეცდომები და მტყუნებები, ასევე საკმაოდ რთულია. თუმცა უახლოეს ტექნოლოგიებში (თანამედროვე ქსელებში, სადაც გამოიყენება გასაჭიმი სპილენძის წყვილი), ამ სიძნელეების ნაწილი დაძლეულია.

– კოლიზიების წარმოქმნისას პაკეტების გადაცემის დრო იზრდება, რაც საკმაოდ ხშირად ხდება სხვადასხვა კლიენტებიდან პაკეტური შეტყობინებების დიდი რაოდენობის გადაცემების დროს.

ახლა, რაც შეეხება Ethernet 802.5 რგოლური სტრუქტურის (ხშირად მას მოიხსენიებენ Token Ring 802.5 ქსელურ სტრუქტურებად) ქსელებს, მათ გააჩნიათ შემდეგი დადებითი მხარეები:

– მაღალი გამტარუნარიანობა. ასეთი ტიპის ქსელში ყველა მოწყობილობა მუშაობს რიგ-რიგობით (დეტერმინირებული დროის განმავლობაში), რითაც გამორიცხულია მონაცემთა მიღება-გადაცემისათვის შეჯიბრი პირველობისათვის და შესაბამისად თითქმის არ არსებობს კოლიზიებიც (ერთდროულად გადაცემული პაკეტების ერთმანეთთან შეჯახება – დაზიანებაც). აღნიშნული თვისებები საშუალებას იძლევა დაკავებული (დაუფლებული) იქნეს გატარების ზოლის მნიშვნელოვანი ნაწილი (80%-ზე მეტი) გამტარუნარიანობის

დანაკარგების გარეშე იმ შემთხვევაშიც კი, როდესაც რგოლში ბევრია გადამცემი მოწყობილობები.

– დეტერმინირებული შეღწევისას ქსელის საკაბელო სისტემაში რგოლური ტიპის Token Ring – ქსელში თითოეული მოწყობილობა (მაგალითად, მომხმარებლის მუშა სადგური) გარანტირებულად იღებს შესაძლებლობას მონაცემთა გადაცემისათვის. ეს განსაკუთრებული თვისება გადამცემ სადგურებს აძლევს შესაძლებლობას შეაღწიონ ქსელში (დაეუფლონ ქსელის საკაბელო სისტემას მონაცემების გადაცემისათვის) დროის რეგულარულ ინტერვალებში, რაც იდეალურია MISSION – CRITICAL გამოყენებითი პროგრამებისათვის, რომლებიც საჭიროებენ ქსელში დეტერმი-ნირებულ შეღწევას.

– გაადვილებული პროცედურები უწესივრობების ძებნისა და მართვისათვის. Token Ring ქსელს გააჩნია მართვის ჩაშენებული საშუალება, რომელიც იძლევა ინფორმაციას უწესივრობების მოსაძებნად, ასევე ინფორმაციას როგორც მთლიანი რგოლის, ისე რგოლის ცალკეული მოწყობილობების მართვისათვის.

– მაღალი მტყუნებადმდგრადობა. Token Ring – ქსელს გააჩნია შესაძლებლობა მოახდინოს აპარატურის უწესივრობათა სიმრავლის დინამიური ლოკალიზაცია და აღმოჩენის შემდეგ აღადგინოს მათი ნორმალური ფუნქციონირება.

Token Ring - რგოლური ტიპის კომპიუტერული ქსელების ნაკლოვანებად უნდა ჩაითვალოს:

– საკმაოდ მაღალი ღირებულება. ასეთი ტიპის ქსელის გამოყენების დროს საჭიროა სპეციალური აღჭურვილობის შეძენა და, თუმცა მათი ფასი თანდათან მცირდება, მაინც ჯერ-ჯერობით ისინი საკმაოდ ძვირადღირებულია.
– ქსელის დაყენების (გაყვანილობის) სირთულე. მანამდე, სანამ დაიწყებდეთ აღჭურვილობის ყიდვასა და საკაბელო სისტემის გაბმას, საჭიროა მკაცრად დააგეგმაროთ ქსელის კონფიგურაცია (რისთვისაც საჭიროა გამოყენებული იქნას საკმაოდ რთული საანგარიშო ფორმულები). ქსელის დაყენების დროს სპეციფიკაციების დარღვევისას (განსაკუთრებით ისეთი რგოლისათვის, სადაც გამოყენებულია არაეკრანირებული გამტარების წყვილები), წარმოიქმნება სიძნელეები, წინააღმდეგ შემთხვევაში ქსელი შეიძლება გახდეს მუშაუუნარო.
– საკმაოდ მაღალია დანახარჯები ქსელის ნორმალური ფუნქციონირების აღდგენაზე და მისი მართვისათვის. მტყუნების მიმართ მდგრადობა შეიძლება ჩაითვალოს ნაკლად, თუ ქსელის ადმინისტრატორს არ გააჩნია შესაბამისი სადიაგნოსტიკო აპარატურა და საკმაო გამოცდილება წარმოქმნილი არამდგრადი უწესივრობების აღმოსაჩენად და მათ გამოსასწორებლად. ნაკლოვანებად უნდა ჩაითვალოს ისიც, რომ ქსელში ცალკეული უწესივრობების აღმოჩენა და ქსელის კორექტული მუშაობის რეჟიმის აღდგენა მნიშვნელოვნად ანელებს ქსელის მიმდინარე წარმადობას.

1.3. ქსელის კომპონენტები და ძირითადი მახასიათებლები

ლოკალური ან გლობალური ქსელები, აგებული Ethernet – ტექნოლოგიებით, წარმოადგენენ მონაცემთა გადაცემის ღია (გახსნილ) სისტემებს, რომლებიც მათთან მიერთებულ ძირითად კომპონენტებს – მუშა სადგურებს (ქსელის მომხმარებელთა პერსონალურ კომპიუტერებს) საშუალებას აძლევენ ერთმანეთისგან დამოუკიდებლივ გადასცენ და მიიღონ ინფორმაციები მეტად ეფექტურად, იაფად და ნაკლები დროითი დანახარჯებით. ამასთან, ეს ინფორმაციები შეიძლება იყვნენ რთული ბუნების, მაგალითად, მულტიმედიური ხასიათის (ტექსტი, გამოსახულება, ხმის თანხლებით). გლობალურისგან განსხვავებით ლოკალური ქსელის ძირითად განსაკუთრებულობას წარმოადგენს მისი განთავსება შეზღუდულ ტერიტორიებზე. ეს შეიძლება იყოს დაწესებულების (ფირმის, კომპანიის) შენობა ან შენობის ერთი რომელიმე სართული, შენობათა კომპლექსი, მაგალითად, პროდუქციის მწარმოებელი ქარხნის ტერიტორიის ფარგლები, რომელთა დამამზადებელი საამქროები დაკავშირებული არიან ერთმანეთთან ამ ქსელით, საუნივერსიტეტო კომპლექსის ქსელი (წოდებული კამპუს-ქსელად) და ა.შ. ასეთი ტიპის (ლოკალური, კორპორაციული დანიშნულების) ქსელი მომსახურებას უწევს მასთან მიერთებული, ასევე შეზღუდული რაოდენობის მუშა სადგურებს, ხოლო საკუთრივ ქსელი მთლიანობაში იმყოფება ერთი ორგანიზაციის კონტროლის ქვეშ (ამ ფუნქციას, როგორც წესი, ასრულებს ქსელის ადმინისტრატორი).

ფიზიკური გაგებით მომხმარებლის პერსონალური კომპიუტერების გარდა ქსელის ძირითად კომპონენტებს წარმოადგენენ მონაცემთა გადამცემი გარემო (საკაბელო სისტემა თავისი მიმღებ – გადამცემ მოწყობილობებთან ერთად, ან გადამცემი გარემო რადიო – სიხშირული კავშირის ან ლაზერული კავშირის მოწყობილობებთან ერთად) და დამატებითი სატერმინალო მოწყობილობები (სხვადასხვა ტიპისა და რაოდენობის, გამომდინარე ქსელის დანიშნულებიდან).

აპარატურულ–პროგრამული უზრუნველყოფის გაგებით ქსელურ ლიტერატურაში ზოგიერთი ავტორი ქსელის კომპონენტებში გულისხმობს, აგრეთვე, ჰოსტებზე (Hosts) არსებულ პერიფერიულ მოწყობილობებს, სერვერული დანიშნულების აპარატურას, კონცენტრატორებს (Hubs), მარშრუტიზატორებს (Routers) და სხვა. ჰოსტის კომპიუტერებში (რომლებთანაც მუშაობენ უშუალოდ ქსელის მომხმარებლები) და განსაკუთრებით კი სერვერებში შესაძლებელია დიდი რაოდენობის (მოცულობის) ინფორმაციის განთავსება. ისინი დახარისხებული არიან კატალოგებად, ფაილებად ან ფაილების ერთობლიობებად – მონაცემთა ბაზებად.

სიტყვა “სერვერი” ქსელურ ტექნიკაში გამოიყენება ორგვარი გაგებით: პირველი სერვერი (Server) – ეს არის მძლავრი (ჰოსტ–კომპიუტერებთან შედარებით) და გაფართოებული მოცულობის მეხსიერების მქონე კომპიუტერი, რომელსაც ხშირად მიმართავენ ქსელის მომხმარებლები. ნებისმიერი ჰოსტი შეიძლება წარმოადგენდეს სერვერსაც (და არა პირიქით); მეორე

სერვერი – ეს არის პროგრამა, რომელიც მომსახურეობას უწევს სხვა პროგრამებს (რომლებსაც ხშირად მოიხსენიებენ, როგორც კლიენტ–პროგრამებს).

კონკრეტული გაგებით, Ethernet შედგება უამრავი რაოდენობის ასეთი სერვერებისაგან. მაგალითად, თუ რომელიმე კომპიუტერი ინტერნეტში ინახავს რაიმე შინაარსის (მისი დანიშნულებიდან გამომდინარე) Web – დოკუმენტს, მაშინ იგი წარმოადგენს Web – სერვერს და მან უნდა უზრუნველყოს ამ Web – დოკუმენტის კლიენტებზე გადაცემა, რომლის მართვას აწარმოებს ბროუზერი. ამგვარად, ბრაუზერის (Brauzer) დახმარებით (ფაქტიურად იგი წარმოადგენს საძიებო დანიშნულების პროგრამას WWW – საინფორმაციო სივრცეში) კლიენტებს წარედგინება ნებისმიერი ტიპის შესაბამისი დოკუმენტი: ტექსტი, სურათი, ხმა, ანიმაცია, ვიდეო და ა.შ. ამგვარად, ბროუზერს შეუძლია არა მარტო "წაიკითხოს" ნებისმიერი Web – დოკუმენტი, არამედ მოძებნოს კიდეც ინფორმაცია ინტერნეტის ნებისმიერი სამსახურიდან (უფრო ზუსტად, ნებისმიერი მომსახურებიდან), მიიღოს და დაამუშაოს ეს ინფორმაცია და გადაუგზავნოს კლიენტს მისგან მითითებულ გარკვეულ მისამართზე. ამას გარდა ბროუზერის დახმარებით ძალზე მარტივად სწარმოებს გადასვლა ერთი რომელიმე Web – დოკუმენტიდან სხვა Web – დოკუმენტზე, მიუხედავად მისი ადგილმდებარეობისა (ინტერნეტის WWW – საინფორმაციო სივრცეში). ასეთ გადასვლას უწოდებენ სერფინგს (Surfing),

რომელიც WWW – სივრცეში სწარმოებს ჰიპერ–კავშირებით (იგულისხმება საინფორმაციო სივცეში გლობალური კავშირებით).

ნებისმიერი დანიშნულებისა და ტიპის ლოკალური კომპიუტერული ქსელის ძირითად მახასიათებლებს წარმოადგენენ:

- ქსელის ზომა;
- გამოყენებული მოწყობილობები;
- ინფორმაციის გადაცემის სიჩქარე;
- ქსელის ტოპოლოგია;
- ინფორმაციის გადამცემი ფიზიკური გარემო;
- გამოყენებული პროტოკოლები და ქსელში შეღწევის მეთოდები;
- ქსელის მმართველი კვანძი (ავტონომიური ან ჩაშენებული ქსელის სხვა მოწყობილობებში).

ვინაიდან ლოკალური კომპიუტერული (გამომთვლელი) ქსელები ვითარდება სწრაფად, ცხადია, რომ ზემოთჩამოთვლილი მახასიათებლებიც შეიძლება შეიცვალონ მონაცემთა გადაცემის სხვადასხვა მეთოდებთან ან პროგრამულ დამატებებთან დამოკიდებულებით. რაც შეეხება დანარჩენ კომპონენტებსა და მახასიათებლებს (მათ შორის ქსელურ ტოპოლოგიებს, მონაცემთა მიმღებ – გადამცემ ფიზიკურ გარემოს – საკაბელო სისტემებს, მონაცემთა მიღება – გადაცემებისათვის გამოყენებული კადრის სტრუქტურებს და ა.შ), მოკლედ შევეხებით მათ მომდევნო თავში).

თავი 2

კომპიუტერული ქსელების აგების სტრუქტურულ–ორგანიზაციული მიდგომები და მათი გავლენა მონაცემთა მიღება–გადაცემებზე

2.1. კომპიუტერული ქსელის ტოპოლოგიის განმარტება

კომპიუტერული ქსელის ტოპოლოგიის ცნების ქვეშ იგულისხმება ქსელის კომპიუტერებს შორის ფიზიკური კავშირების ორგანიზაცია. ქსელის ტოპოლოგიას განსაზღვრავს ქსელში კომპიუტერების განლაგების კონფიგურაცია. ეს კონფიგურაცია მეტად მოსახერხებელია გამოხატული იქნეს გრაფ-სქემის სახით, რომლის წვეროები შეესაბამება კომპიუტერებს (როგორც წინა თავში ავღნიშნეთ, მათ ხშირად უწოდებენ ქსელის მუშა სადგურებს, კვანძებს ან აბონენტებს), ხოლო წვეროების შემაერთებელი ხაზები კი აღნიშნავენ კომპიუტერებს შორის კავშირებს.

ქსელის ტოპოლოგიის შესაბამისი კონფიგურაციების ანალიზის დროს საჭიროა განვასხვაოთ ორი ერთმანეთისაგან შინაარსობრივად განსხვავებული ცნებები: ფიზიკური კავშირების კონფიგურაცია და ლოგიკური კავშირების კონფიგურაცია. პირველი გულისხმობს კომპიუტერების ელექტრულ შეერთებებს კავშირის ხაზებით (მაგალითად, საკაბელო სისტემებით), ხოლო

მეორე წარმოადგენს ქსელში მონაცემთა ელექტრონული ტრანსპორტირების (პაკეტების გადაადგილების), ე.ი. კავშირის ხაზებით ქსელის კვანძებს შორის მონაცემების გადაცემის მარშრუტებს. ლოკალურ კომპიუტერულ ქსელში ერთი ტოპოლოგიის ფარგლებში კვანძებს შორის ლოგიკური კავშირები შეიძლება იყოს სხვადასხვა. ხშირად ქსელურ ლიტერატურაში ლოგიკურ კავშირებს უწოდებენ ვირტუალურ კავშირებს, ხოლო ლოგიკური კავშირების ტოპოლოგიას მთლიანობაში – ვირტუალურ ქსელს.

2.2. კომპიუტერული ქსელის ტოპოლოგიების სახესხვაობები

კომპიუტერული ქსელების ასაგებად არსებობს ფიზიკური კავშირების ტოპოლოგიების მრავალნაირი სახეობა. მათი კონფიგურაციების შერჩევა დიდ გავლენას ახდენს ისეთ მახასიათებლებზე, როგორიცაა პირველ რიგში ქსელის წარმადობა, ქსელის საიმედოობა და ქსელის ცალკეული სეგმენტების ბალანსირებული დატვირთვა. ეს უკანასკნელი თავის მხრივ დიდ გავლენას ახდენს წინა ორ მახასითებელზე. ამ მახასიათებლების გარდა ქსელის ასაგებად, ამა თუ იმ შერჩეული ტოპოლოგიის ავკარგიანობას (ქსელის ეფექტური ორგანიზაციისთვის) აფასებენ, აგრეთვე, ისეთი პარამეტრებით, როგორიცაა კავშირის ხაზების ჯამური სიგრძე, ქსელის სტრუქტურაში ახალი კვანძების, ე.ი. ახალი აბონენტებისათვის კომპიუტერების მიერთების სიადვილე, ქსელის რესურსებზე შეღწევის სიმარტივე და სხვა.

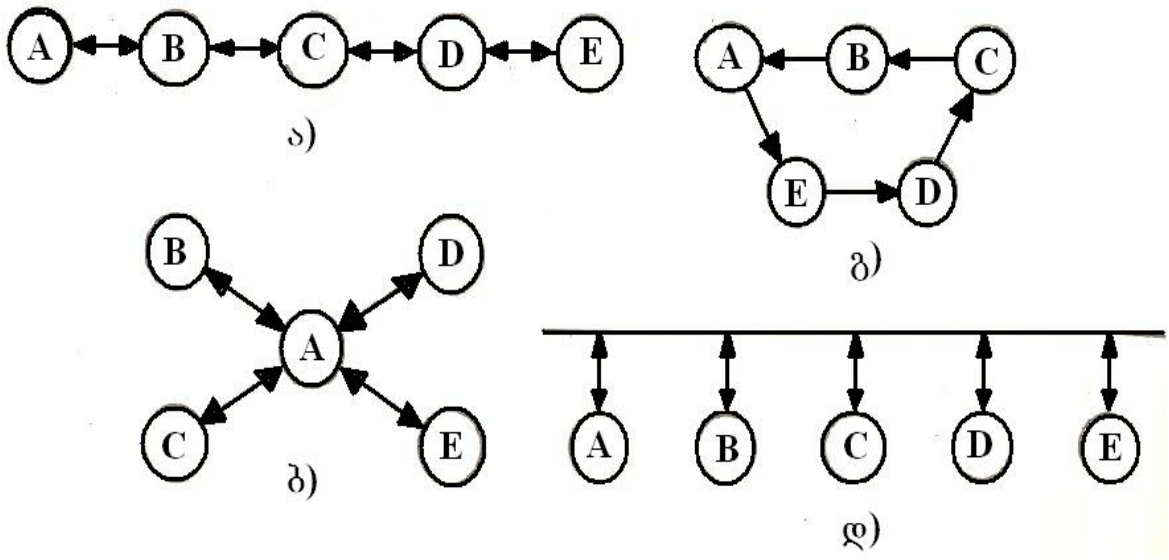
გამოვიყენებთ რა ქსელის ტოპოლოგიის მარტივი გამოხატვის ზემოთ ნახსენებ წესს (გრაფების სახით), შეიძლება ვაჩვენოთ ამჟამად ყველაზე ფართოდ გავრცელებული სახეები. ნახ. 2.1-ზე წარმოდგენილია შემდეგი ტოპოლოგიური სტრუქტურები:

— წრფივი (ხაზოვანი) სტრუქტურები (ნახ. 2.1. ა);

— ვარსკვლავისებრი სტრუქტურები (ნახ. 2.1. ბ);

— რგოლური სტრუქტურები (ნახ. 2.1. გ);

— საერთო სალტის მქონე სტრუქტურები (ნახ. 2.1. დ);



ნახ. 2.1 ქსელების ძირითადი ტოპოლოგიები

მოკლედ განვიხილოთ თითოეული მათგანი. როგორც ნახ. 2.1-დან ჩანს, ყველა სტრუქტურები საერთო სალტური სტრუქტურის გარდა წარმოადგენს ორწერტილოვანი არხების ნაკრებს და უმეტეს შემთხვევებში წყარო-სადგურიდან (ე.ი. მონაცემთა გადამცემი კომპიუტერიდან) გაგზავნილმა შეტყობი-

ნებამ უნდა გაიაროს რამოდენიმე კვანძი, სანამ მიაღწევდეს დანიშნულების ადგილს (ე.ი. მიმღებ სადგურამდე). მაგალითად, წრფივ სტრუქტურაში (ნახ. 2.1. ა) შეტყობინებამ (პაკეტის სახით) A კვანძიდან, რომელიც დამისამართებულია E კვანძზე, უნდა გაიაროს B, C და D კვანძები. ასეთი ტოპოლოგიის დადებითი მხარეა ის, რომ გაადვილებულია მარშუტიზაცია და B, C და D კვანძები გვევლინებიან შეტყობინებების გამმეორებლები (ხშირად გამმეორებლებს უწოდებენ რეპიტერებს, ინგლისური სიტყვიდან repeat – გამეორება). ეს ნიშნავს იმას, რომ თუ გაგზავნილ შეტყობინებაში (პაკეტის მისამართში) ნაჩვენები მისამართი არ დაემთხვევა ქსელის სხვა კვანძების საკუთარ მისამართებს (ჩვენს მაგალითში ასეთებია B, C და D), ისინი შეუფერხებლად გაატარებენ ამ შეტყობინებას დანიშნულების (E) კვანძისკენ. დადებით მხარესთან ერთად ასეთ ტოპოლოგიას გააჩნია უარყოფითი მხარეც. კერძოდ, თუ რომელიმე კვანძი დაზიანებულია (ან დაზიანებულია კვანძებს შორის შემაერთებელი რომელიმე კაბელი), მაშინ გაგზავნილი შეტყობინება (პაკეტი) დანიშნულების ადგილს ვერ მიაღწევს.

ვარსკვლავისებრ სტრუქტურაში (ნახ. 2.1. ბ) ერთ-ერთი კვანძი ასრულებს ცენტრის როლს (კვანძი A), რაც ნიშნავს იმას, რომ კვანძის ყველა შეტყობინებამ (პაკეტებმა) უნდა შეასრულონ აუცილებელი პირობა. მათ უნდა გაიარონ ეს კვანძი, რომ მიაღწიონ დანიშნულების ადგილს. ცენტრალურ კვანძს ხშირად უწოდებენ ქსელის აქტიურ კონცენტრატორს. მისი ძირითადი ფუნქციაა რომელიმე წყაროდან წამოსული

ინფორმაცია გადაუგზავნოს ერთ რომელიმე სხვა კვანძს (შეტყობინების ინდივიდუალური მიღება). ორ ან რამოდენიმე კვანძს (ჯგუფური მიღება) ან უკლებლივ ყველა კვანძს (ფართოსამაუწყებლო მიღება) ცხადია, თუ ეს კვანძი (ცენტრალური) რაიმე მიზეზით დაზიანდა, ირღვევა მონაცემთა მიღება-გადაცემის კორექტული (სწორი) რეჟიმები, ხოლო მისი მწყობრიდან გამოსვლისას კი მთელი ქსელი წყვეტს მუშაობას. ეს უკანასკნელი წარმოადგენს სტრუქტურა – ვარსკვლავის ძირითად ნაკლს.

ყველა ზემოთ მოხსენიებული რეჟიმები (ინდივიდუალური, ჯგუფური და ფართოსამაუწყებლო გადაცემები) განისაზღვრება წყარო-კომპიუტერის მიერ გასაგზავნი შეტყობინების მისამართით (მიეთითება გასაგზავნი პაკეტის კადრების სამისამართო ველებში). წინა (ნახ. 2.1. ა-ზე ნაჩვენები) ტოპოლოგიისგან განსხვავებით ამ ტოპოლოგიას (ნახ. 2.1. ბ) გააჩნია საიმედოობის შედარებით მაღალი მაჩვენებელი. მაგალითად, კაბელის დაზიანება გავლენას ახდენს მხოლოდ იმ კომპიუტერის მუშაობაზე, რომლითაც იგი მიერთებულია კონცენტრატორთან (ვარსკვლავის ცენტრთან). ასეთი კონცენტრატორები (პასიურ კონცენტრატორებთან შედარე-ბით) საკმაოდ ძვირადღირებულია და მათგან მოითხოვება მაღალი ინტელექტუალური დონეც. ასეთი ტოპოლოგიის უარყოფით მხარეს, როგორც ზემოთ აღვნიშნეთ, არის ის, რომ კონცენტრატორის მწყობრიდან გამოსვლა იწვევს მთელი ქსელის პარალიზებას. ამ ნაკლოვანე-ბისაგან თავის დასაღწევად იყენებენ რამოდენიმე კონცენტრა-ტორს, რომლებიც განლაგებული არიან იერარქიულად.

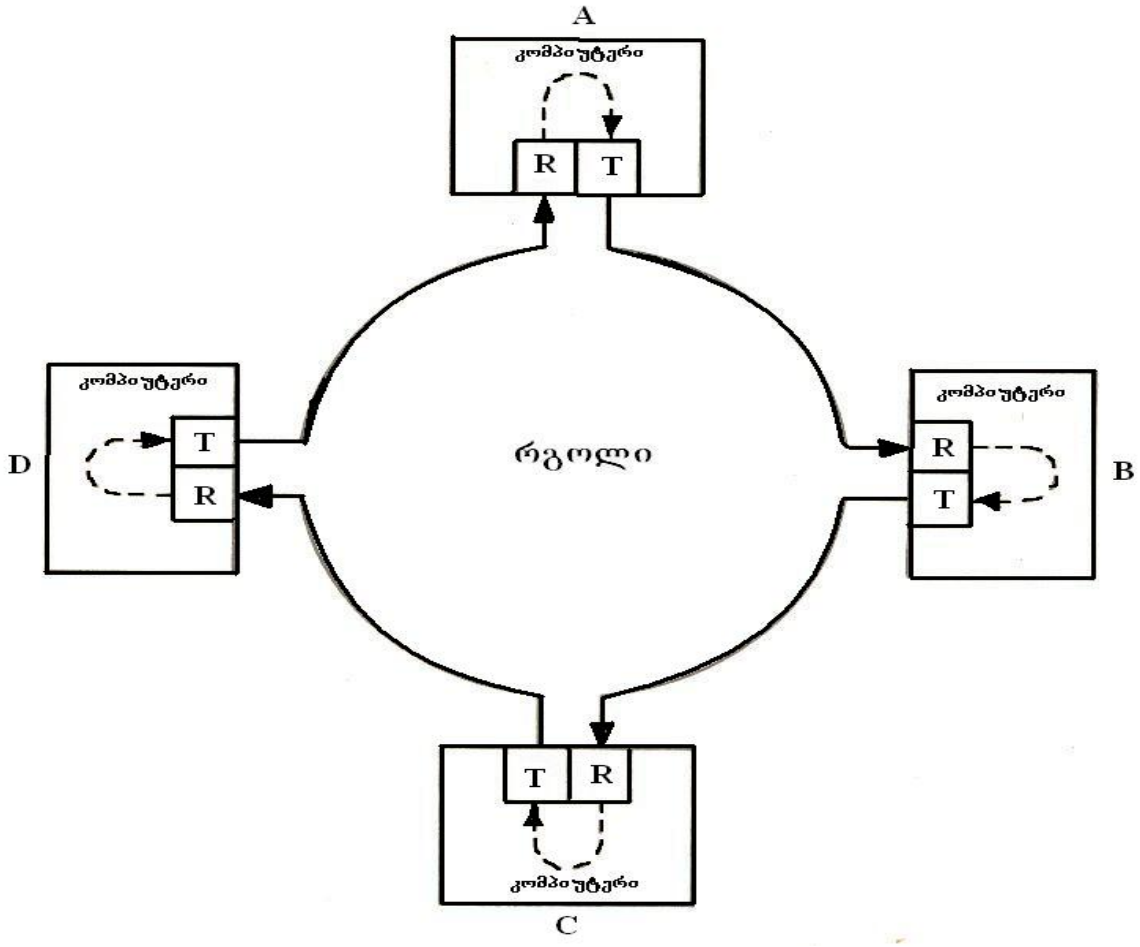
ამჟამად იერარქიული ვარსკვლავის ტოპოლოგია წარმოადგენს ყველაზე ფართოდ გავრცელებულ სტრუქტურას როგორც ლოკალური, ისე გლობალური ქსელებისათვის.

რგოლურ ტოპოლოგიურ სტრუქტურას (ნახ. 2.1. გ) გააჩნია მეტად საინტერესო თვისება. მის მიერ შეიძლება რეალიზებული იქნეს ერთმიმართულებიანი კავშირები. ასეთ სტრუქტურაში ნებისმიერ ადგილას ერთმანეთის მეზობლად მდებარე კვანძების წყვილი წარმოადგენენ მიმღებ-გადამცემებს. კვანძების ასეთი შეერთების დროს, მაგალითად, შეტყობინებამ, რომელსაც აგზავნის A-წყარო B-მიმღებისაკენ (ნახ. 2.1. გ), მან ჯერ უნდა გაიაროს E, D და C კვანძები (რომლებიც ასრულებენ ზემოთხსენებული რეპიტერების როლს).

ასეთი ტოპოლოგიური სტრუქტურის დადებითი მხარეა ის, რომ გამგზავნი კვანძი (წყარო – კომპიუტერი) წინასწარ ამყარებს ვირტუალურ (ლოგიკურ) კავშირს მიმღებ კვანძთან, რაც უზრუნველყობს შეტყობინებათა პაკეტების კონფლიქტების გარეშე გადაცემას. ამგვარი გადაცემა – მიღება გარანტირებულია, ვინაიდან გადამცემი კვანძი ისე არ დაიწყებს თავისი მონაცემების გადაცემას, თუ იგი არაა დარწმუნებული, რომ მიმღები კვანძი მზადაა მიიღოს მისი შეტყობინება. ამას იგი ახერხებს დამხმარე წინასწარი შეტყობინების პაკეტით, რომელსაც ხშირად მარკერს უწოდებენ (ზოგჯერ კი კონტეინერსაც). ამგვარად, სანამ A კვანძი (ნახ. 2.1. გ) გადაუგზავნის შეტყობინებას B კვანძს, ჯერ მან უნდა "დაიჭიროს" მარკერი, რომელიც თავისუფალ დროს ცირკულირებს რგოლის გარშემო,

მიუთითოს მიმღების მისამართი, სპეციალურად ამღნიშვნელ ველში (ხშირად მას უწოდებენ ალამს), გააკეთოს სამისამართო ჩანაწერი (ამ ველს ზოგჯერ “დასტურის მოთხოვნის” ველსაც უწოდებენ) და ამგვარი ინფორმაციით “შეიარაღებულ” მარკერს გააგზავნის ქსელში. ამით იგი (ქსელის A კვანძი) მონაცემთა გადასაცემად “გაკვალავს” გზას მიმღებამდე, ანუ დაამყარებს მასთან (ჩვენს შემთხვევაში B კვანძთან) ვირტუალურ კავშირს. სხვა სიტყვებით რომ ვთქვათ, “გაასუფთავებს” ტრაფიკს ქსელის გადამცემ და მიმღებ კომპიუტერებს შორის. მონაცემთა გადაცემა-მიღების სეანსის დასამყარებლად თუ მარკერში ნაჩვენები მიმღების მისამართი არ ემთხვევა სხვა კვანძების (ჩვენს შემთხვევაში E, D, C კვანძების) მისამართებს, ისინი შეუფერხებლად გაატარებენ მას, ე.ი. გამოვლენ მხოლოდ ამ მარკერის რეპიტერების როლში. როგორც კი მიმღები კვანძი (B) “დაიჭერს” მარკერს, რაც ნიშნავს მისი მისამართების დამთხვევას მარკერში მითითებულ მისამართთან, ეს უკანასკნელი გააკეთებს შესაბამისი “დასტურის” აღნიშვნას მარკერის სათანადო ველში (ე.წ “დასტურის” ალამში), რომ ეს მმართველი – სამომსახურეო კადრი (მარკერი) მისია და დაუბრუნებს მას ისევ გამგზავნ წყარო – კომპიუტერს. ამრიგად, შეიკვრება რგოლი (როგორც ავღნიშნეთ ვირტუალური, ანუ ლოგიკური რგოლი. აქედანაა სახელწოდება – ქსელის რგოლური ტოპოლოგია). ამის შემდეგ წყარო – კომპიუტერი გადააქცევს მარკერის კადრს მონაცემთა კადრად და დაიწყებს გადაცემის სეანსს მიმღებისაკენ. ამ სეანსის

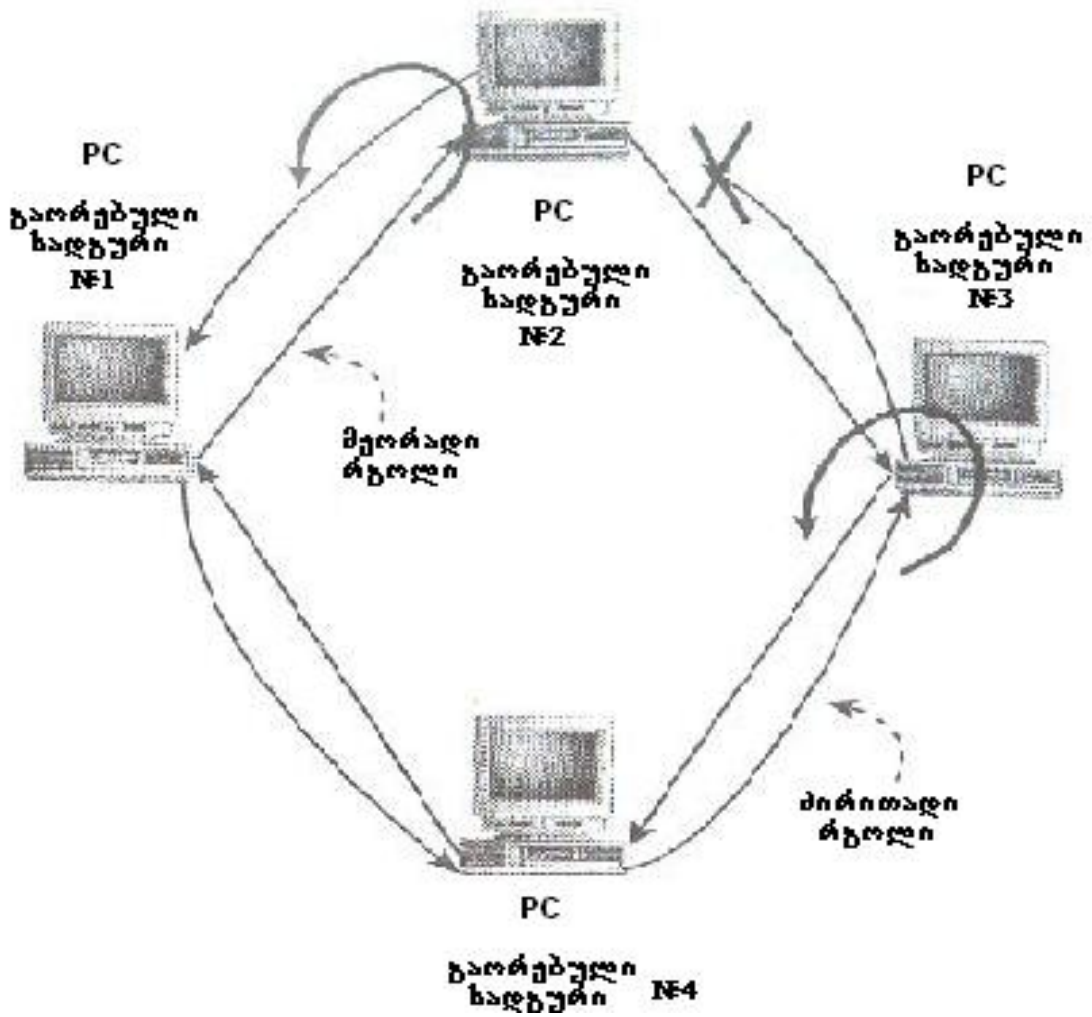
დამთავრების შემდეგ ათავისუფლებს მარკერს, რის შემდეგაც ეს უკანასკნელი კვლავ დაიწყებს ცირკულირებას (ე.ი. დაიწყებს რგოლში ჩართული ყველა კომპიუტერის გარშემოვლას) რგოლის ირგვლივ და მისცემს საშუალებს აწარმოონ მიღება-გადაცემები იმავე წესით რგოლში ჩართულმა სხვა კომპიუტერებმა. ფიზიკური რგოლის ტოპოლოგიას კარგად ასახავს ნახ. 2.2-ზე ნაჩვენები სტრუქტურა.



ნახ.2.2. კომპიუტერული ქსელის რგოლური სტრუქტურა

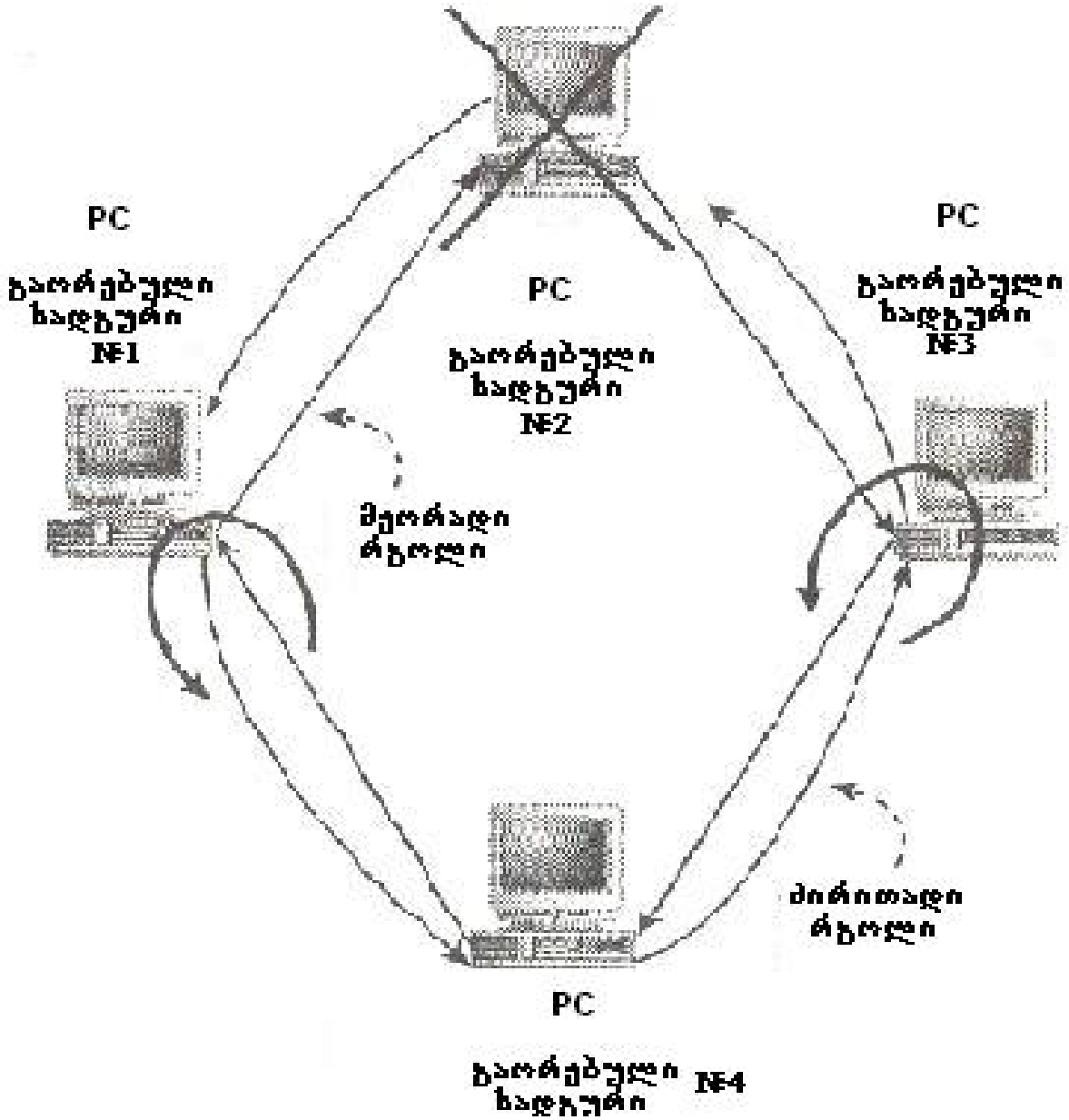
ასეთი (რგოლური) ტოპოლოგიური სტრუქტურების დადებით მხარედ ითვლება ის, რომ ისინი გამორიცხავენ პაკეტების შეჯახებასა და გაფუჭებას. ასეთი შემთხვევები, როგორც ზემოთ აღვნიშნეთ, ცნობილია გადაცემულ პაკეტებს შორის კონფლიქტების, ანუ კოლიზიების სახელწოდებით. უარყოფითი მხარე კი არის ის, რომ რომელიმე კვანძის მწყობრიდან გამოსვლა იწვევს რგოლის გაწყვეტას და ქსელის მუშაობის შეფერხებას, თუმცა თანამედროვე სტრუქტურებში (IBM–ფირმის **Token Ring** – ქსელებში) ეს ხარვეზი გამოსწორებულია ორი გზით. ჯერ ერთი, დამუშავებულია ინტელექტუალური სპეციალური მოწყობილობები (ცნობილი **MSAU**–ს სახელწოდებით), რომლებიც არ წყვეტენ ვირტუალურ რგოლურ კავშირს რომელიმე კვანძის მწყობრიდან გამოსვლის შემთხვევაშიც კი (**MSAU**–ებით აღჭურვილია ქსელის თითოეული კვანძი), ხოლო მეორე, თანამედროვე რგოლურ სტრუქტურებში დანერგილია მარკერის მოძრაობის ორმიმართულებიანობა, ე.ი. დამუშავებულია ორმაგი რგოლის მქონე ტოპოლოგიები, რომლის ერთი რგოლი ძირითადია, მეორე კი სარეზერვო.

ნახ. 2.3 ა,ბ-ზე ნაჩვენებია ასეთი ორმაგი რგოლის მქონე სტრუქტურები, რომლებზედაც ასახულია, რგოლის დაზიანების შეთხვევებიც.



ნახ. 2.3 ა. გარშემოვლითი რგოლი (კაბელი გაწყვეტილია)

კაბელის გაწყვეტამ, როგორც ნახ. 2.3 ა-დან ჩანს, იმოქმედა №2 სადგურზე. მისი მეზობელი №1 და №3 სადგურები გადასცემენ მონაცემებს ამ უწესივრობის გვერდის ავლით (გარშემოვლით) მეორადი რგოლით, რითაც შენარჩუნებულია რგოლის მთლიანობა. თუ ნახ. 2.3 ა) –ზე №2 სადგური მთლიანად გამოვა მწყობრიდან, მაშინ მისი გვერდის ავლით განახლდება რგოლი (ნახ. 2.3 ბ). ამ მიზნით ორმაგი რგოლების მქონე სტრუქტურები (ისინი ISO სტანდარტიზაციის კომიტეტებში რეგისტრირებულია საერთო სახელწოდებით, როგორც **FDDI** – ქსელები)



ნახ. 2.3 ბ. გარშემოვლითი რგოლი (სადგურის მტყუნება)

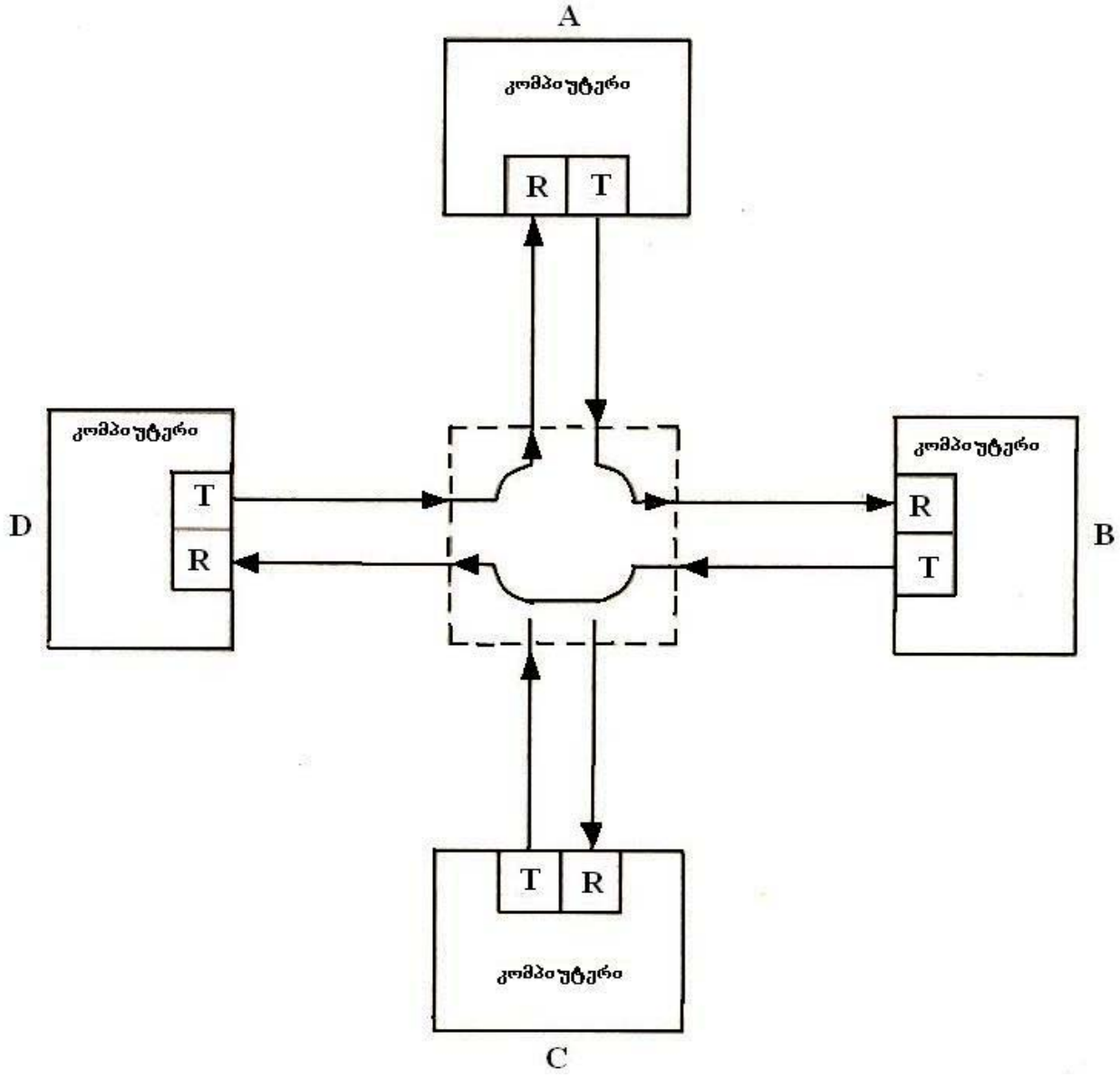
აღჭურვილია მოწყობილობებით, ე.წ. "გარშემოვლითი ოპტიკური კომუტატორებით (Optical bypass switches). ამგვარი მოწყობილობები ყენდება სადგურებსა და კონცენტრატორებს შორის. რომელიმე სადგურის (ჩვენს მაგალითში №2 კვანძის) მტყუნების დროს ამგვარი კომუტატორები მონაცემთა მიღება-გადაცემების

დროს უნარჩუნებენ რგოლს მარშრუტის მთლიანობას დაზიანებული სადგურის გვერდის ავლით.

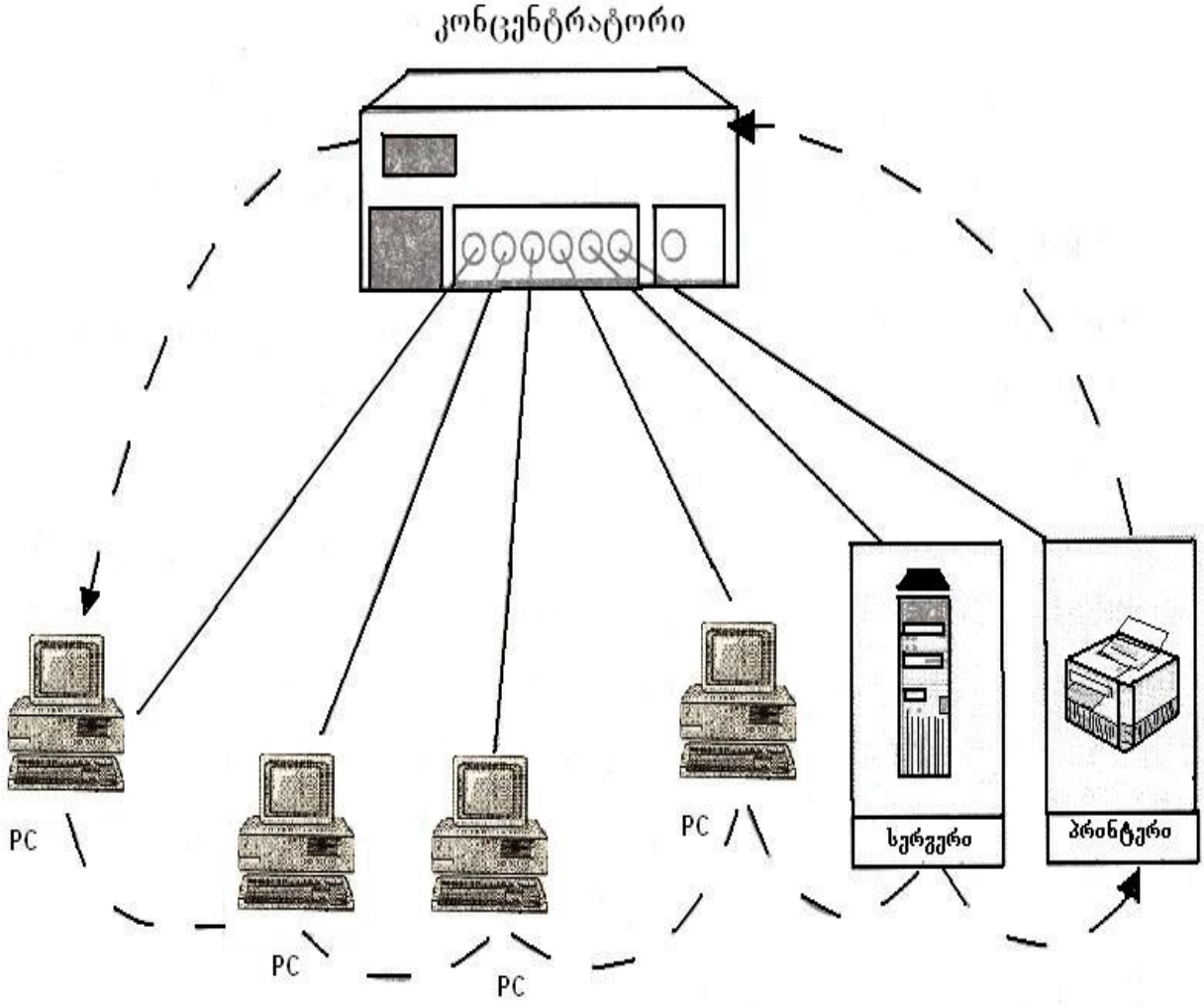
ამჟამად, რგოლურმა სტრუქტურებმა მეტად ფართო გავრცელება ჰპოვეს მცირე ზომის ქსელებში, განსაკუთრებით კი სამრეწველო ობიექტებში საწარმოო – ტექნოლოგიური პროცესების რეალურ დროში მართვისათვის.

ზემოთ განხილული ვარიანტების გარდა, როგორც აღვნიშნეთ, არსებობენ ქსელური სტრუქტურების სხვა კონფიგურაციებიც. მათ შორის "საერთო-სალტე", ასევე "მარყუჟი" და სხვა კომბინირებული სტრუქტურებიც, რომლებსაც აქვთ, აგრეთვე, თავიანთი დადებითი და უარყოფითი მხარეები. მაგალითად "მარყუჟის" ტოპოლოგიაში ყველა კვანძი ერთმანეთთან შეერთებულია რგოლად, რომელთაგან ერთ-ერთს დაკისრებული აქვს დანარჩები კვანძების მართვა (მმართველ კვანძს ხშირად უწოდებენ ქსელის კონტროლერს).

ბოლო პერიოდში ფეხს იკიდებს ე.წ. "ვარსკვლავ – რგოლური" ტოპოლოგიები, რომლებსაც ასახავენ ნახ. 2.4 და ნახ. 2.5-ზე ნაჩვენები ილუსტრაციები.



ნახ. 2.4 ვარსკვლავ–რგოლური ტოპოლოგია

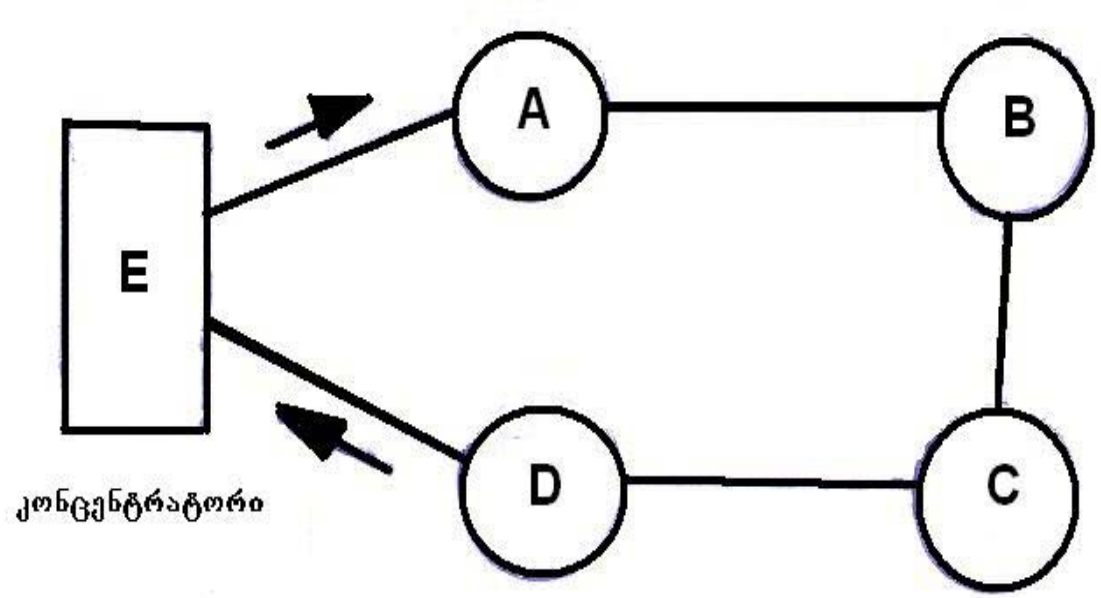


ნახ. 2.5 ვარსკვლავ–რგოლურ სტრუქტურაში გამოყენებული კონცენტრატორი

რგოლის თითეული სადგური (ნახ. 2.4-ზე ნაჩვენებია ოთხი ასეთი მუშა სადგური **A, B, C, D)** შეიცავს გადამცემ (**T**) და მიმღებ (**R**) მოწყობილობებს. რგოლის ამგვარ სტრუქტურაში ("ვარსკვლავის" ცენტრში) არსებობს საერთო კვანძი (ნახ. 2.4-ზე ნაჩვენებია ის წყვეტილი ხაზებით), რომელიც ცნობილია კონცენტრატორის –**Hub** სახელწოდებით. ამ "ცენტრის" გავლით

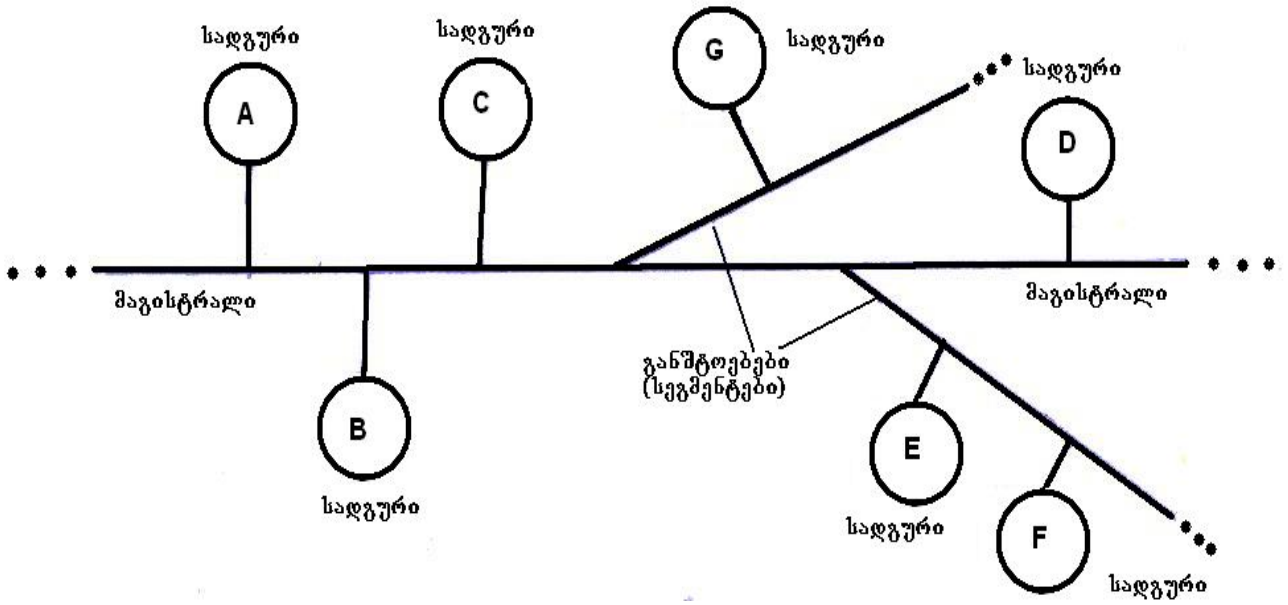
მყარდება რგოლის ყველა კვანძებთან საკომუნიკაციო კავშირები.

ზემოთ ნაჩვენები ტოპოლოგიების გარდა, როგორც ზემოთ ვახსენეთ, გვხვდება აგრეთვე, "მარყუჟის" ტიპის სტრუქტურები, სადაც ცალკე კვანძის სახით გამოკვეთილია სადგურების დამაკავშირებელი კონცენტრატორი. ნახ.2.6-ზე ნაჩვენებია კომპიუტერული ქსელის ტოპოლოგია "მარყუჟი".



ნახ.2.6. ტოპოლოგია "მარყუჟი". E – დამაკავშირებელი კონცენტრატორი

Ethernet-ქსელურ სტრუქტურებში, ამჟამად ყველაზე ფართოდ გავრცელებულია "ხის-მსგავსი" ტოპოლოგიები (ნახ. 2.7).

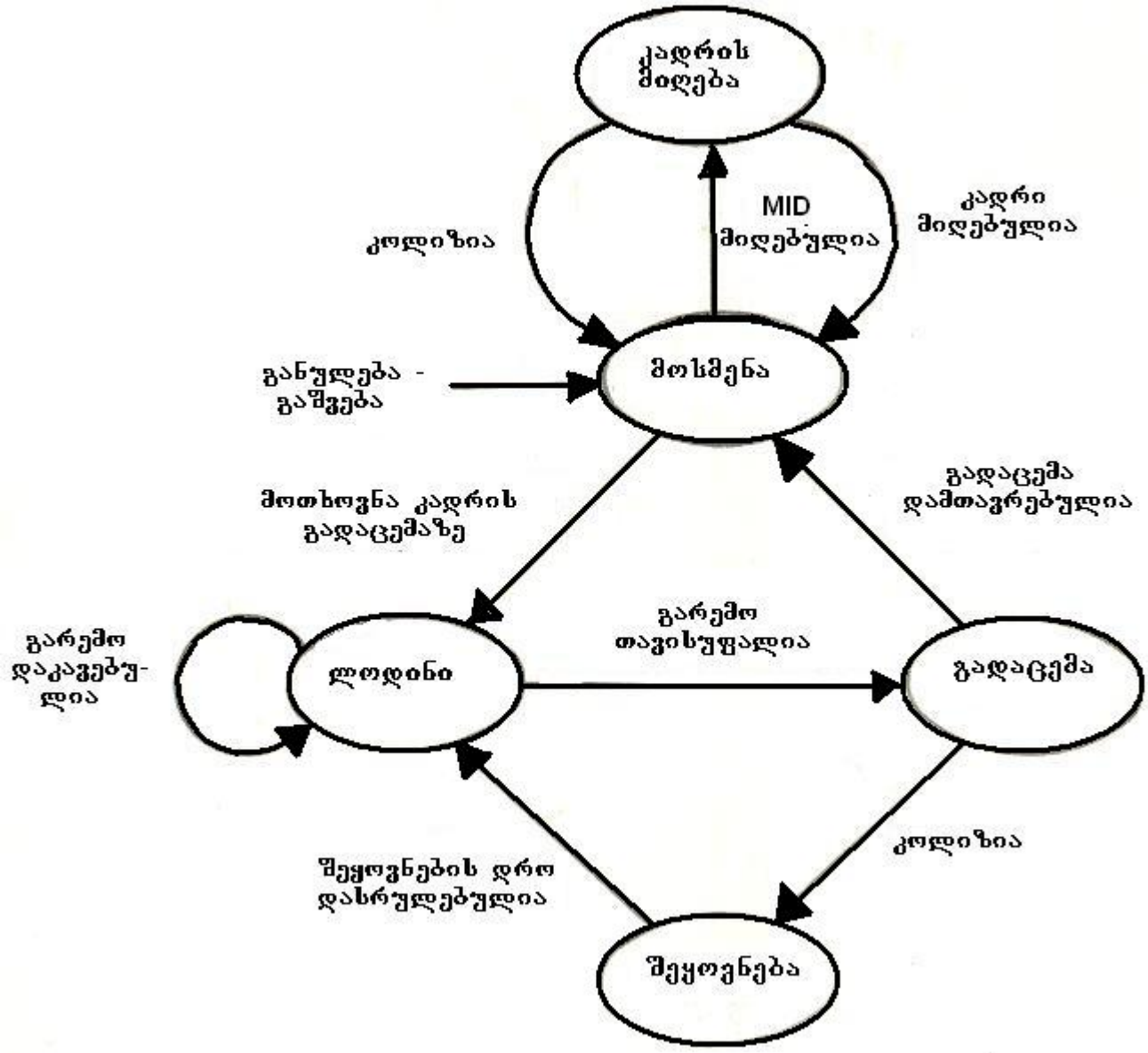


ნახ. 2.7 “ხის-მსგავსი” სალტური ტოპოლოგია

ისინი წარმოადგენენ სალტური სტრუქტურის სახესხვაობას, რომელსაც გააჩნია ერთი ცენტრალური მაგისტრალური ხაზი და მისგან განშტოებული ერთი ან რამოდენიმე სეგმენტი (მუშა სადგურები – მომხმარებელთა პერსონალური კომპიუტერები ნახ. 2.7 –ზე ნაჩვენებია პატარა წრეხაზებში ჩაწერილი ასოებით). წინა სტრუქტურებისგან განსხვავებით ასეთ სტრუქტურებში ნებისმიერი გადამცემი კვანძი დროის ნებისმიერ მომენტში აგზავნის პაკეტებს საერთო სალტეში (ე.ი მაგისტრალში და მასთან მიერთებულ სეგმენტებში-განშტოებებში). მიმღები სადგურები “უსმენენ” ქსელს და იღებენ მხოლოდ იმ პაკეტებს, რომელთა კადრების სამისამართო ველში ნაჩვენები მისამართი ემთხვევა თავიანთ მისამართებს. ასეთი ტოპოლოგია მუშაობს **CSMA/CD** პროტოკოლით (მონაცემთა გადაცემა და მიღება

CSMA/CD პროტოკოლის მეთოდებით დაწვრილებით განხილულია მომდევნო თავში).

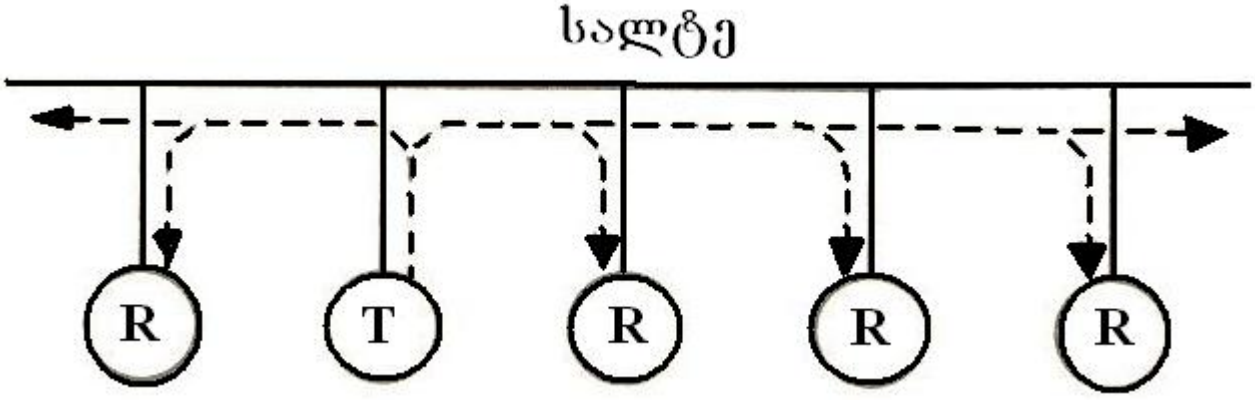
მონაცემთა მიღება-გადაცემის CSMA/CD ზოგადი ალგორითმი ნაჩვენებია შემდეგ ბლოკსქემაზე (ნახ. 2.8):



ნახ. 2.8. პაკეტების მიღება-გადაცემის CSMA/CD ალგორითმი

ვინაიდან მონაცემთა მიღება-გადაცემის ასეთი ალგორითმის დროს თეორიულად შესაძლებელია გადაცემები დაიწყოს ქსელის ყველა სადგურმა ერთდროულად, შესაძლებელია კოლიზიების, ე.ი. პაკეტების შეჯახების შემთხვევები (როგორც ადრე შევნიშნეთ კონფლიქტების დროს გადაცემული პაკეტები ფუჭდება და ისინი მოითხოვენ განმეორებით გადაცემების პროცედურების ჩატარებას).

საერთო სალტით (მაგისტრალით) მონაცემთა მიღება-გადაცემის მიმართულებები (მიმღებ–**R** და გადამცემ–**T** კვანძებს შორის) ნაჩვენებია ნახ. 2.9-ზე.



ნახ. 2.9. ფართო-სამაუწყებლო გადაცემა საერთო მაგისტრალით. **T**-გადამცემი სადგურები, **R**- მიმღები სადგურები

კოლიზიური მოვლენა, დამახასიათებელი ორ სადგურს შორის მონაცემთა გადაცემების დროს **CSMA/CD** ალგორითმით, ნაჩვენებია ნახ. 2.10-ზე.

ნახ. 2.10. პაკეტების კოლიზია ორ გადამცემ სადგურს შორის

ამგვარად, საერთო-სალტური სტრუქტურების მქონე ქსელში კოლიზია წარმოიქმნება ყოველთვის, როდესაც ერთდროულად დაიწყებს გადაცემას თუნდაც მინიმუმ, ორი გადამცემი მაინც. კოლიზიების გამო დამახინჯებული შეტყობინებების გაშიფვრა მიმღები სადგურების მიერ ძალიან ძნელია და ხშირ შემთხვევებში შეუძლებელიც, თუმცა მათი (კოლიზიური მოვლენების) აღმოჩენა არ წარმოადგენს სიძნელეს. ამ ფუნქციას წარმატებით ართმევენ თავს ქსელის პროტოკოლების ანალიზატორები (მათ შესახებ ინფორმაციები წარმოდგენილია ასევე აღნიშნულ სახელმძღვანელოში, კერძოდ მე-8 თავში).

ზემოთგანხილული სტრუქტურების გარდა, როგორც ზემოთ შევნიშნეთ, სხვადასხვა ქსელურ გადაწყვეტებში გხვდება შერეული (კომბინირებული) ტოპოლოგიებიც, სადაც მთლიანი ქსელის ფარგლებში, როგორც შემადგენელი ნაწილები (როგორც მთლიანი დიდი ზომის ქსელის ფრაგმენტები ქვექსელების სახით), შედიან სალტური, ვარსკვლავური და რგოლური სტრუქტურებიც.

თავი 3
ლოკალური კომპიუტერული ქსელის სტრუქტურიზაციისა და დამისამართების პრობლემები მონაცემთა გადაცემა-მიღების ოპერაციების შესასრულებლად

3.1 კომპიუტერული ქსელის კავშირის ხაზების ერთდროული გამოყენების იდეა მონაცემთა გადაცემა-მიღებისათვის ჰოსტის კომპიუტერებს შორის

კომპიუტერულ ქსელებში მონაცემთა გადაცემა – მიღების ოპერაციების შესასრულებლად მომხმარებელთა მუშა სადგურების ერთმანეთთან საკომუნიკაციო გაერთიანების ორი გზა არსებობს. პირველი – კომპიუტერების ერთმანეთთან დაკავშირება საკუთარი წყვილებით, ხოლო მეორე – კავშირის ხაზების გამოყენება საერთო სარგებლობისათვის.

კავშირის ხაზების ერთდროული გამოყენების იდეა ძალზე პერსპექტიულია, ვინაიდან იგი უპირველეს ყოვლისა ხელს უწყობს ქსელების თვითღირებულების შემცირებას. ეს იდეა მისაღებია უმეტესწილად საერთო სალტიან ქსელურ სტრუქტურებში. ეს იდეა ძირითადად დაფუძნებულია იმაზე, რომ ქსელის არც ერთ კომპიუტერს (კვანძს) პრინციპში არ შეუძლია გადამცემი არხის გამოყენება ინდივიდუალურად, ე.ი. ქსელის სხვა კომპიუტერების გარეშე. ეს ნიშნავს იმას, რომ ქსელის რომელიმე საგდურს არ შეუძლია იყოს “მონოპოლისტი” შეტყობინებათა პაკეტების გადაცემების ან მიღების დროს. ამას

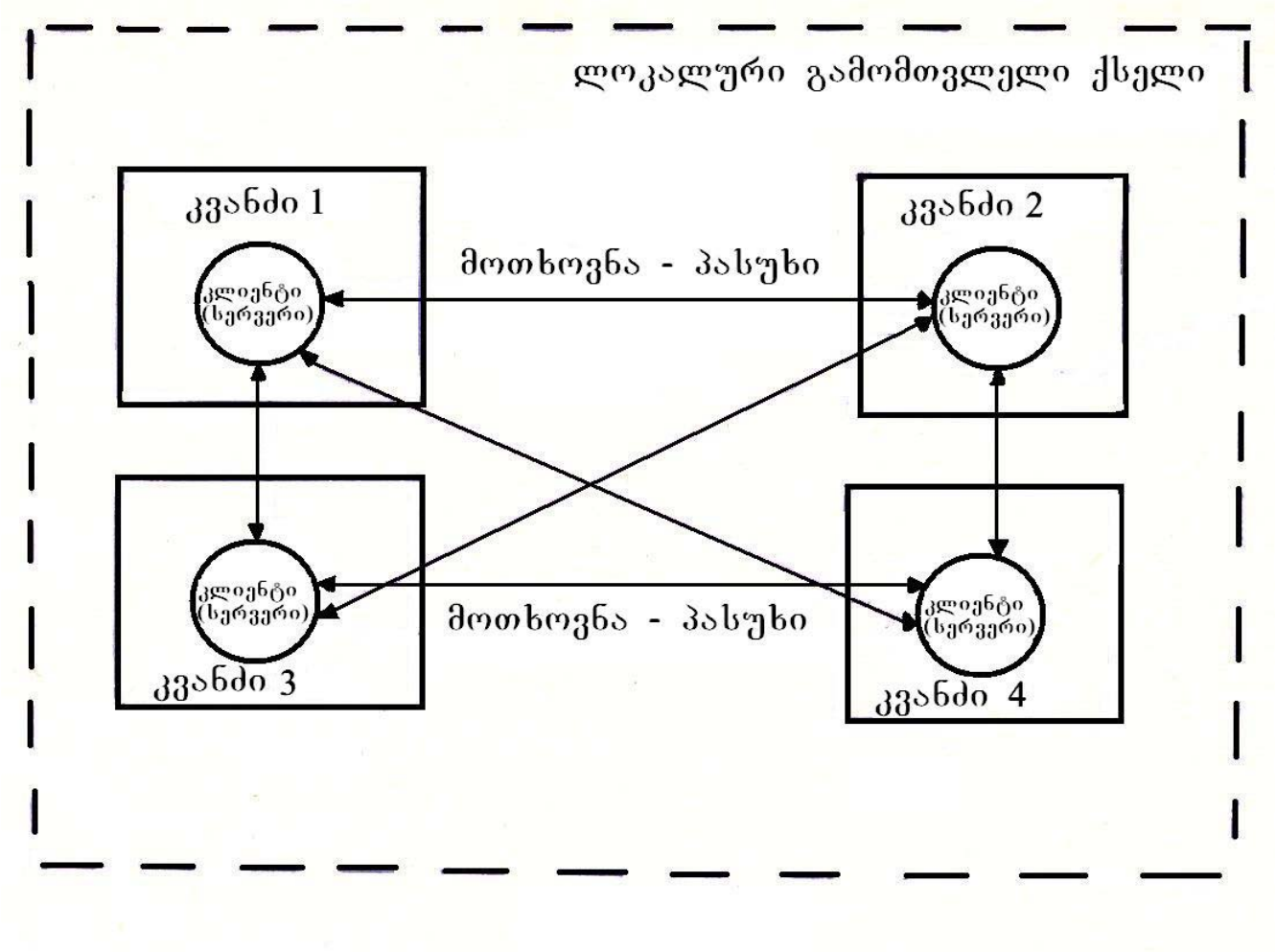
იგი ახერხებს სხვა კომპიუტერებთან "კომპრომისის" გზით. მაგალითად, რგოლურ სტრუქტურებში ერთ რომელიმე კვანძის კომპიუტერი უცდის სხვა კვანძის კომპიუტერს, სანამ იგი არ დაამთავრებს გადაცემის სეანსს მიმდებ კომპიუტერთან, ხოლო ამის შემდეგ იწყებს იგი გადაცემას.

ამჟამად არსებობს სხვადასხვა ხერხები კავშირის ხაზების ერთდროული გამოყენების პრობლემების გადასაჭრელად. ერთ-ერთ ასეთ ხერხს წარმოადგენს ლოკალურ ქსელებში კავშირის გამოყოფილი ხაზების გამოყენება, თუმცა იგი იწვევს ქსელის წარმადობის შემცირებას. ამგვარად, გამოყოფილი კავშირის ხაზის (Shared) დროს კავშირგაბმულობის ერთი ხაზი გამოიყენება რამოდენიმე კომპიუტერის მიერ.

კავშირის ხაზების როგორც ინდივიდუალურ, ისე ერთდროულ გამოყენებას ქსელის სადგურებისათვის უზრუნველყოფს სპეციალური მოწყობილობა, რომელსაც კომუტატორი ეწოდება. ამჟამად არც თუ ისე იშვიათად გამოიყენება კომპიუტერულ ქსელებში "კომუტატორი – კომუტატორი" ტიპის კავშირის ხაზები, რომლებიც წარმატებით წყვეტენ ხაზების ერთდროული გამოყენების ორგანიზაციის პრობლემებს.

მომხმარებლის მუშა სადგურებს – პერსონალურ კომპიუტერებს ამჟამად საკმაოდ გაფართოებული ფუნქციონალური შესაძლებლობები გააჩნიათ (მათ შორის მეხსიერების საკმაოდ დიდი მოცულობაც). ქსელის ჰოსტების კომპიუტერების აპარატურულ – პროგრამული შესაძლებლობები ბოლო წლებში ისე გაიზარდა, რომ ხშირად აღარც კი არსებობს ფუნციონალური დანიშნულების თვალსაზრისით "სერვერსა" და "კლიენტს"

შორის საზღვარი. ეს იმას ნიშნავს, რომ კომპიუტერი შეიძლება იყოს ქსელის როგორც სერვერი, ისე კლიენტი. ეს კარგად ჩანს ნახ. 3.1 - დან, სადაც ნაჩვენებია 4 კვანძიანი ქსელის ფრაგმენტი.



ნახ.3.1. კვანძის კომპიუტერები ასრულებენ როგორც კლიენტის, ისე სერვერის ფუნქციებს

ქსელის ამ ფრაგმენტიდან ჩანს, რომ თითოეული კვანძის კომპიუტერს (იგულისხმება წრეხაზში მდებარე კომპიუტერი) მონაცემთა ურთიერთ გაცვლების დროს შეუძლია შეასრულოს როგორ სერვერის, ისე კლიენტის ფუნქციებიც, ე.ი. ინფორმაციის გაცემის დროს იგი გვევლინება სერვერის როლში, ხოლო ინფორმაციის მიღების დროს კი კლენტის როლში.

ქსელური სამსახურები მუშაობენ განაწილებული პროგრამებით, ამასთან ერთი კვანძის სერვერი ფლობს ერთი გარკვეული სახის მომსახურებას (სერვისს), ხოლო სხვა კვანძის სერვერი – სხვა დანიშნულების სერვისს (რომელსაც უზრუნველყოფს სხვა სახის პროგრამა).

ზოგადად თუ შევაფასებთ, სერვერების არსებობა თანამედროვე ლოკალურ ქსლებში ძალზე მნიშვნელოვანია, ვინაიდან ისინი ასრულებენ მომსახურების საკმაოდ დიდ რაოდენობას. კვანძის კომპიუტერებს შეთავსებული აქვთ ქსელური მართვის სხვადასხვა ფუნქციებიც. მაგალითად, მათი საშუალებით შესაძლებელია ლოკალური ტრაფიკის მართვა, მონაცემთა ბაზების მართვა (მათ შორის ძალზე დაშორებული სხვა ჰოსტის კომპიუტერებზე ასრებული მონაცემთა ბაზების მართვა), მათ შეუძლიათ საჭიროების შემთხვევაში მარშრუტიზატორის ფუნქციების თავის თავზე აღებაც (მაგალითად, ელექტრონული ფოსტის სერვერი) და ა.შ.

ამგვარად, კომპიუტერული ქსელები წარმოადგენენ მონაცემთა დამუშავების განაწილებული სისტემების ლოგიკურ განვითარებას, რომლებსაც გააჩნიათ ასევე შესაძლებლობა ამ მონაცემების ნებისმიერ მანძილზე გადაცემაც (კავშირგაბმულობის საკომუნიკაციო საშუალებების გამოყენებით). აქვე აღვნიშნოთ, რომ პირვანდელი ქსელების უმრავლესობა საინფორმაციო მომსახურებისათვის იყენებდა კვანძებს შორის კომუტაციას არხების დონეზე, ვინაიდან ისინი დაფუძვნებული იყვნენ სატელეფონო კავშირებზე, სატელევიზიო კომუნიკაციებზე და ა.შ., სადაც დომინირებდა არხების კომუტაცია.

ამჟამად კი (და მომავალშიც), როგორც ცნობილია რაც დრო გადის, მონაცემთა მიღება-გადაცემებისათვის სულ უფრო და უფრო ფართოდ ინერგება საკომუნიკაციო ტექნოლოგია პაკეტების კომუტაციის სახით. ქსელური ტექნიკის წამყვანი სპეციალისტების აზრით კი უახლოეს 10-25 წელიწადში მთლიანად მოხდება ყველა ტექნოლოგიის (გამომთვლელი, სატელეფონო, სატელევიზიო და ა.შ.) შერწყმა ერთ ტექნოლოგიად (ამის ნიშნები უკვე სახეზეა, მაგალითად IP – ტელეფონია), რომელსაც საფუძვლად დაედება პაკეტების კომუტაცია (ე.ი. მოხდება როგორც ფაილური კორესპონდენციის ტრანსპორტის ტრაფიკის, ასევე ხმისა და მოძრავი გამოსახულების ტრაფიკების სინთეზი).

3.2. კვანძის კომპიუტერების კომუნიკაციური დაკავშირება მონაცემთა ურთიერთ გაცვლის მიზნით

იმისათვის, რომ განვიხილოთ კომპიუტერების კომუნიკაციურ ქსელში გაერთიანების საკითხები, საჭიროა უპირველეს ყოვლისა გავერკვიოთ თუ რა აპარატურულ – პროგრამული საშუალებებია საჭირო კომპიუტერების ერთმანეთთან დასაკავშირებლად. განასხვავებენ კომპიუტერების კომუნიკაციური გაერთიანების მარტივ და შედარებით რთულ შემთხვევებს. ამ საკითხებში გარკვევა გაგვიადვილდება თუ ვიცით როგორ ურთიერთქმედებენ თვით კომპიუტერები (უფრო ზუსტად მათი პროცესორული ნაწილები) თავიანთ პერიფერიულ მოწყობილობებთან. პერიფერიულ მოწყობილობებში იგულისხმება უპირველეს ყოვლისა გარე მეხსიერების მოწყობილობები (მაგნიტური

დისკები, დ ა.შ.), საბეჭდი მოწყობილობები (ლაზერული, ან სხვა ტიპის პრინტერები), გრაფოამგებები (მათ შორის ფოტოგრაფიული მიზნებისათვის), მანიპულიატორები (ძირითადად "თაგვის" ტიპის) და სხვა. პერიფერიული მოწყობილებები თავის მხრივ იმართებიან სპეციალური აპარატურულ-პროგრამული საშუალებებით, რომლებსაც გარე მოწყობილობების კონტროლერები ეწოდებათ (მაგალითად, დისკის კონტროლერი, რომელიც მართავს მაგნიტური თავაკის დისკის შესაბამის ბილიკებზე მოძრაობას; პრინტერის კონტროლერი, რომელიც ამოწმებს ქაღალდის შეტანა-გამოტანას საბეჭდ მოწყობილობაში და ა.შ.). საინტერესოა, აგრეთვე, რა ტექნიკურ-პროგრამული საშუალებებით ამყარებს კავშირს ქსელის კომპიუტერის შიგა „ორგანიზმი" ზემოთ აღნიშნულ კონტროლერებთან. ქსელის კვანძის თითეულ კომპიუტერს ჩვენთვის კარგად ცნობილი პროცესორული ნაწილისა და შიგა მეხსიერების (ოპერატიული მეხსიერების) მოწყობილობების გარდა, გააჩნია მართვის მოწყობილობა, რომელიც ფუნქციონირებს შიგა ოპერაციული სისტემის პროგრამებით. იგივე ტერმინოლოგიას თუ ვიხმართ, ქსელის კვანძის თითეულ კომპიუტერს თავის მხრივ გააჩნია „საკუთარი კონტროლერები". მათგან ზოგიერთი აწარმოებს ურთიერთქმედებას ზემოთ ნახსენებ პერიფერიულ მოწყობილობებთან თავისი მმართველი პროგრამებით – დრაივერებით. დრაივერი მჭიდრო ურთიერთობაშია კომპიუტერის საერთო ოპერაციულ სისტემასთან (მათ შორის ქსელურ ოპერაციულ სისტემასთანაც), რომლის მითითებითაც იგი მართავს ქსელის პერიფერიულ მოწყობილობებში მონაცემების შეტანა-გამოტანის

პროცესებს. ქსელის კვანძის კომპიუტერის კონტროლერები პროცესორების გარდა შეიცავენ მეხსიერების რეგისტრებს, რომლებიც ხშირად მოიხსენიებიან, როგორც პორტებად. ამგვარად, დრაივერის მითითებით სრულდება კვანძის პროცესორის ორი ძირითადი სახის ბრძანება: „ჩაიტვირთოს მონაცემები პორტში” და „ამოღებული იქნეს მონაცემები პორტიდან”. თითოეულ პორტს გააჩნია თავისი საკუთარი ნიშნები, რომლის მიხედვითაც სწარმოებს მონაცემების პორტებში მიღება-გაცემის პროცედურების მართვა. ამ მიზანს ემსახურება აპარატურულ-პროგრამული საშუალებები, რომლებსაც უწოდებენ კვანძის ინტერფეისს. ინტერფეისებს შორის პროცესებს ძირითადად არეგულირებს აპარატურულ-პროგრამული საშუალებები – პროტოკოლები.

ზოგადად თუ ვიმსჯელებთ, არსებობს შიგა და გარე ინტერფეისები, რომლებიც მუშაობენ პარალელურად (Centronics interfase) და მიმდევრობით (Consistent interface). ეს უკანასკნელი (მაგალითად, RS–232 C–ტიპის ინტერფეისი) მუშაობს ადაპტერის ფუნქცი-ების შესასრულებლად, ე.ი. მუშაობს კვანძის მიმღებ-გადამცემ მოწყობილობებთან ერთად, რომლებსაც ხშირად მოდემებად (Modulator – demodulator) მოიხსენიებენ.

ბოლო თაობის ქსელურ ადაპტერებს გააჩნიათ საკუთრივ როგორც პროცესორი, ისე შიგა მეხსიერება. ეს პროცესორი ახორციელებს შიგა მეხსიერებაში ფორმირებული მონაცემების (მათ შორის მისი მეხსიერების რეგისტრები გამოიყენება ჭარბი პაკეტების დროებით შესანახადაც) გაცვლას ქსელის სხვა

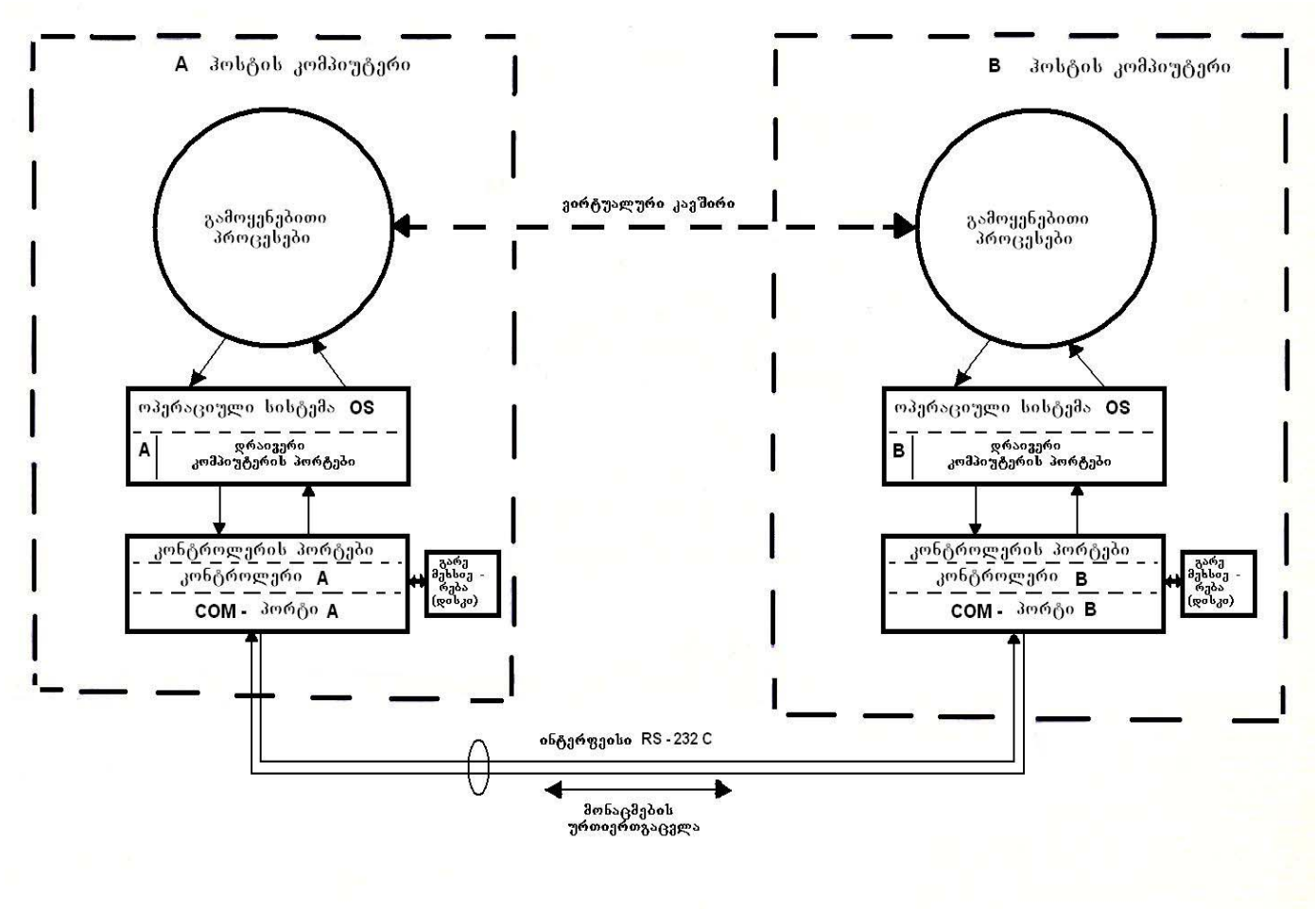
კვანძების ადაპტერებთან, ჰოსტის კომპიუტერების ერთმანეთთან კავშირის დროს.

გარე ინტერფეისი შედარებით უფრო რთულია, ვინაიდან მას აქვს საქმე არა ერთ, არამედ ორ ან მეტ ურთიერთმომქმედ პროგრამებთან. მათ შორისაა ისეთი პროგრამებიც, რომლებიც მართავენ ქსელის სხვა კომპიუტერების რესურსებს (მეხსიერების დაშორებულ ფაილებს, დისკებს, პრინტერებს და ა.შ.). უფრო ზუსტად რომ ვიმსჯელოთ დამაკავშირებელმა ინტერფეისმა შემაერთებელი არხით უნდა გადაუგზავნოს შესაბამისი შეტყობინება ქსელის სხვა კომპიუტერის იმ პროგრამას, რომელიც განაგებს თავის საკუთარ რესურსებს რათა მიიღოს თანხმობა ამ რესურსებში შესაღწევად და სამუშაოდ.

ნახ. 3.2–ზე ნაჩვენებია მონაცემთა ურთიერთ გაცვლის მიზნით ქსელის ორი კომპიუტერის კომუნიკაციური გარეთიანების (დაკავშირების) ზოგადი სქემა.

როგორც ნახ. 3.2-დან ჩანს, A და B კომპიუტერები ურთიერთ საკომუნიკაციოდ გაერთანებული არიან თავიანთი კონტროლერის პორტებისა და COM – პორტების გავლით ინტერფეისით (RS-232 C). ჰოსტის თითეულ კომპიუტერს გააჩნია თავისი ოპერაციული სისტემა (OS), რომელიც დრაივერით მართავს კომპიუტერის შიგა პორტებს, კონტროლერის პორტებს და კომპიუტერის COM – პორტებს მონაცემების შეტანა-გამოტანისათვის.

შევეცადოთ მოკლედ და ზოგადი ფორმით აღვწეროთ ის პროცედურა, როდესაც ქსელის ერთ კომპიუტერს სურს გამოიყე-



ნახ. 3.2. კვანძის კომპიუტერების კომუნიკაციური დაკავშირება მონაცემთა ურთიერთ გაცვლის მიზნით

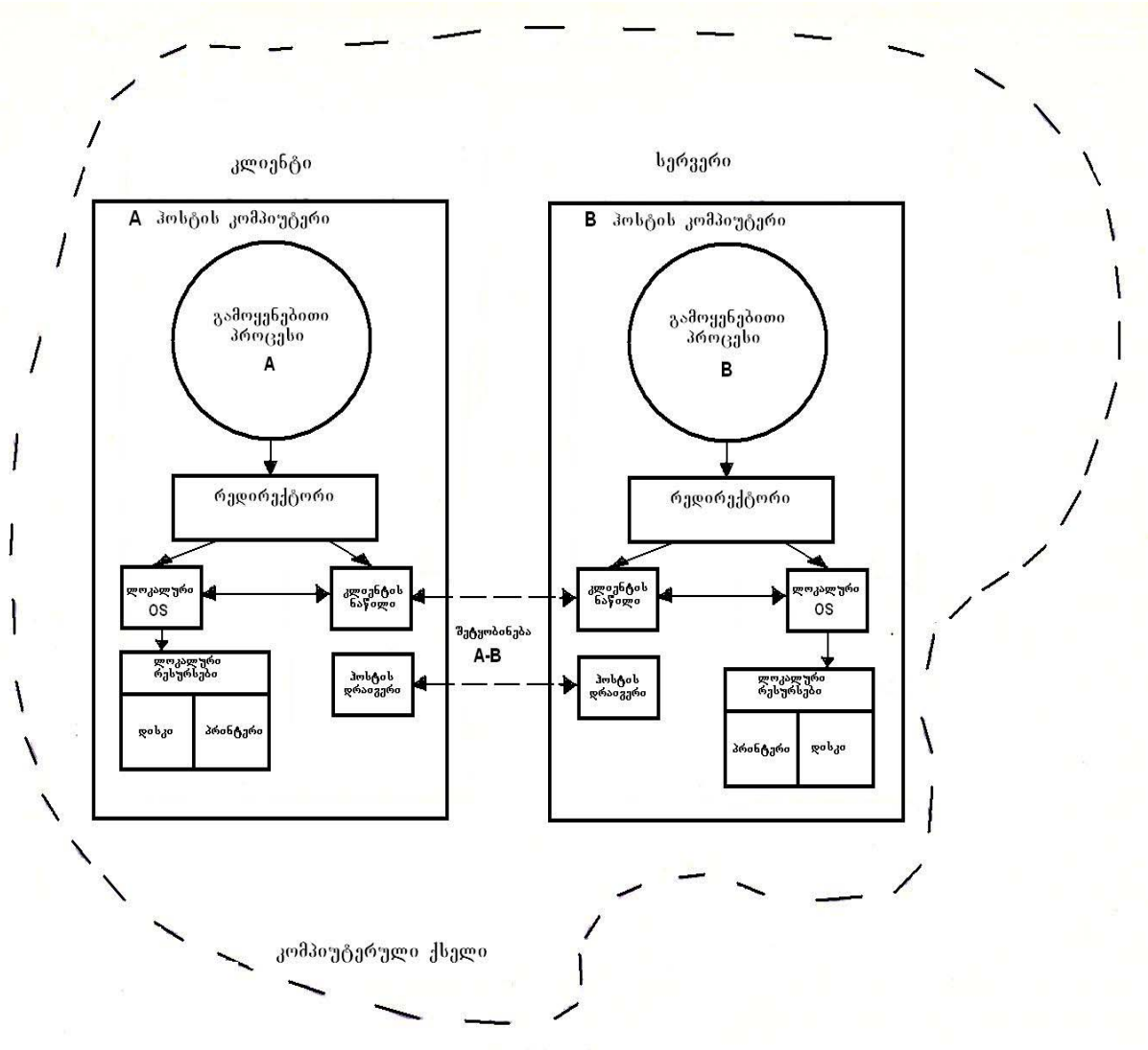
ნოს ქსელის მეორე კომპიუტერის რესურსები (მაგალითად, მათ მეხსიერებაში ჩაწერილი მონაცემთა ფაილები). ვთქვათ, ქსელის ერთ მხარეს მდებარე (A ჰოსტის) კომპიუტერის სურს მოახდინოს შეღწევა ქსელის მეორე მხარეს მდებარე (B ჰოსტის) კომპიუტერის ფაილებზე. ამგვარი საჭიროება იბადება A კომპიუტერის გამოყენებითი პროცესიდან, რომელიც ამ გამოყენებითი პროცესის შესაბამისი პროტოკოლის დახმარე-ბით ვირტუალური კავშირით ატყობინებს B კომპიუტერის გამოყენებით პროცესს.

A კომპიუტერის გამოყენების პროცესი „უსაბუთებს” რა თავის ოპერაციულ სისტემას (OS) B კომპიუტერის დიკზე

(ვინჩესტერზე) არსებული მონაცემების გამოყენების საჭიროებას თავისი საქმიანობისათვის, OS აძლევს მითითებას A დრაივერს, რომელიც თავის მხრივ ამზადებს კომპიუტერის შიგა პორტებს და ასევე „ავალებს" A კონტროლერს გაანთავისუფლოს მიმღები A პორტი მეორე B კომპიუტერიდან ფაილების მისაღებად. მსგავს პროცედურას აწარმოებს მეორე, B ჰოსტის კომპიუტერიც, რომლის გამოყენებითი პროცესი, რომელმაც იცის უკვე A ჰოსტის გამოყენებითი პროცესის „თხოვნა". იგი თავისი ოპერაციული სისტემით B დრაივერის გავლით უგზავნის B კონტროლერს გაანთავისუფლოს თავისი პორტები. ონტრო-ლერი B ამოიკითხავს რა სათანადო ფაილს (ფაილებს) B კომპიუტერის დისკიდან, მოათავსებს მას თავის პორტებში, ხოლო შემდეგ გადაწერს გამავალ B COM –პორტში. ეს უკანა-სკნელი გამოფენს რა თავის "ალამს" იმის შესახებ, რომ გასაგზავნი ფაილის გადმოწერა დასრულდა, B დრაივერი უბრძანებს B კონტროლერს გადასცეს მონაცემები ინტერფეისს RS-232 C, რომელიც თავისი არხით გაუგზავნის A ჰოსტის კომპიუტერს. მონაცემები ჯერ თავსდება A COM-პორტში (რომელიც, როგორც ვთქვით, უკვე თავისუფალია), ხოლო შემდეგ A ჰოსტის კომპიუტერის OS სისტემის მითითებით და A დრაივერის მმართველი სიგნალებით A კონტროლერი A COM-პორტიდან გადაწერს მიღებულ შეტყობინებებს თავის შიგა პორტში და იგივე A ჰოსტის კომპიუტერის ოპერაციული სისტემა გადაწყვეტს გაუგზავნოს მიღებული მონაცემები თავის

გამოყენებით პროცესს თუ A კონტროლერს დაავალოს ეს მონაცემები მოათავსოს თავის დისკზე. ანალოგიური პროცესები სწარმოებს იმ შემთხვევებშიც, როცა წარმოიქმნება საჭიროება პირიქით, ე.ი. როცა B ჰოსტის კომპიუტერს სურს A ჰოსტის კომპიუტერის რესურსების გამოყენება. ამგვარად, ორი კომპიუტერის კომუნიკაციური გაერთიანების დროს საქმე გვაქვს ორ მოდულთან, რომელთაგან ერთს (ჩვენს მაგალითში A ჰოსტის კომპიუტერის რესურსებს) უწოდებენ როგორც კლიენტს, ხოლო მეორეს (B ჰოსტის კომპიუტერის რესურსებს) – სერვერს. ორივე პროგრამული მოდული ასრულებენ სისტემურ ფუნქციებს A კომპიუტერის გამოყენებითი პროცესის განაცხადის (მოთხოვნის) დასაკმაყოფილებლად (დაშორებული B ჰოსტის კომპიუტერის სერვერიდან საჭირო ფაილის მისაღებად).

ნახ. 3.2-ზე ნაჩვენები იყო კომპიუტერების მეტად მარტივი აპარატურული კავშირი. ხშირ შემთხვევებში კლიენტისა და სერვერის ურთიერთქმედება (მითუმეტეს მაშინ, თუ ისინი ერთმანეთისაგან ძალზე დაშორებულნი არიან) გაცილებით რთულია ვინაიდან ზემოთ აღნიშნული პროცედურების წარმატებით ჩასატარებლად საჭიროა სხვა ქსელური კომპონენტებისა და ქსელური ოპერაციული სისტემის გამოყენებაც (როგორიცაა მაგალითად, ხიდების, მარშრუტიზატორების, კონცენტრატორების და ა.შ. საქმეში ჩართვა და გამოყენება).



ნახ.3.3. პროგრამული კომპონენტების ურთიერთქმედება A ჰოსტის კომპიუტერების კავშირის დროს

ნახ. 3.3-ზე ნაჩვენებია A და B ჰოსტის კომპიუტერების პროგრამული კომპონენტების ურთიერთქმედების სქემა. როგორც აღნიშნული სქემიდან ჩანს კლიენტსა და სერვერს შორის არსებობს ორმხრივი კავშირები. ხშირ შემთხვევებში საჭიროა კლიენტის პროგრამებს გააჩნდეთ უნარი გაარჩიონ ერთმანეთი-საგან დაკავშირებული ფაილი და ლოკალური ფაილი (ამას აკეთებს პროგრამული საშუალება, რომელსაც რედირე-ქტორი ეწოდება). თუ იგი გამოიცნობს, რომ საჭიროა დაშორებული

ფაილის მიღება, ამას ქსელური ოპერაციული სისტემის კლიენტის ნაწილის (ნახ.3.3) მეშვეობით გადაუგზავნის დაშორებული ჰოსტის კომპიუტერს.

3.3. დამისამართების პრობლემები მონაცემთა გადაცემა-მიღების ოპერაციებისათვის

ლოკალურ კომპიუტერულ ქსელში ჩართულ კოპიუტერებს შორის ბუნებრივია ზოგი მათგანი წარმოადგენს ინფორმაციის (მონაცემთა პაკეტების) გადამცემს, ზოგი მიმღებს. მონაცემთა პაკეტების ურთიერთ გაცვლა, ე.ი. ურთიერთ გადაგზავნა შეუძლებელია, თუ არ არიან ისინი ერთმანეთთან დამისამართებულნი. ისეთი კომპიუტერის (ე.წ. ჰოსტის კომპიუტერის) არსებობა ქსელში, რომელსაც არ გააჩნია თავისი საკუთარი მისამართი, შეუძლებელია. ამგვარად, დამისამართებული კვანძების (მუშა სადგურების) გარეშე ქსელის არსებობა წარმოუდგენელია.

დამისამართების პრობლემები მაშინვე წარმოიქმნება, თუ ქსელში ჩართულია მინიმუმ სამი (ან სამზე უფრო მეტი) კომპიუტერი მაინც. ადვილი მისახვედრია, თუ ქსელი შედგება მხოლოდ ორი კომპიუტერისაგან (ყველაზე მარტივი შემთხვევა), მაშინ მათი დამისამართება არავითარ პრობლემას არ წარმოადგენს. ისინი ერთმანეთთან დაკავშირებული იქნებიან უშუალოდ ორმხრივი ფიზიკური არხებით (კავშირის ხაზებით).

იმის და მიხედვით, თუ რა ტოპოლოგიის (ტოპოლოგიებთან დაკავშირებული საკითხები საკმაოდ დაწვრილებით განხილული

გვქონდა წინა თავში) და დანიშნულების ქსელებთან გვაქვს საქმე, მათში კომპიუტერების დამისამართების პრობლემებსაც გააჩნიათ სხვადასხვა ხასიათი. თუმცა მათ (მისამართებს) კომპიუტერებთან მიმართებაში უნდა გააჩნდეთ საერთო თვისებებიც. ეს თვისებებია:

1. მისამართების ინდივიდუალურობა. ეს იმას ნიშნავს, რომ ქსელთან მიერთებულ ნებისმიერ კომპიუტერს უნდა ჰქონდეს თავისი საკუთარი მისამართი. ამ მისამართმა გარანტირებულად უნდა უზრუნველყოს ნებისმიერი მასშტაბისა (ზომისა) და სირთულის ქსელში ყველაზე მარტივ შემთხვევაში ორ კომპიუტერს, ე.ი. ქსელის ორ აბონენტს შორის საიმედო კავშირი (შეიძლება ეს კავშირი იყოს ცალმხრივი – სიმპლექსური ან ორმხრივი – დუპლექსური). სხვა სიტყვებით რომ ვთქვათ, ნებისმიერი მისამართი უნდა იყოს უნიკალური ქსელში მკაცრი პერსონალური იდენტიფიცირების თვალსაზრისით მონაცემთა მიღება-გადაცემების სარეალიზაციოდ. საჭიროა აქვე აღვნიშნოთ ისიც, რომ ქსელის გადამცემ სადგურებს უნდა შეეძლოთ (ეს თვისება უნდა გააჩნდეს მიმღებ სადგურებსაც) გადასაცემი მონაცემები დაამისამართონ ერთი (ინდივიდუალური დამისამართება), ორი ან რამოდენიმე ოღონდ შეზღუდული რაოდენობით (ჯგუფური დამისამართება), ანდა ერთდროულად ქსელის უკლებლივ ყველა კომპიუტერი (ფართოსამაუწყებლო დამისამართება). მისამართების ინდივიდუალობამ მაქსიმალურად უნდა გამორიცხოს მათი დუბლირება, ვინაიდან ორი ერთნაირ მისამართიანი კვანძის (მუშა სადგურის ან სერვერული

კომპიუტერის) არსებობა ქსელში გამოიწვევს გაუგებრობას და სირთულეებს მონაცემთა მიღება-გადაცემების დროს.

2. მისამართების იერარქიულობა. მისამართების იერარქი-ული სტრუქტურის გარეშე შეუძლებელია დიდი ქსელების აგება. იერარქიულობის არსი ძალზე წააგავს ჩვეულებრივ საერთაშო-რისო (საქალაქთაშორისო ანდა შიგა საქალაქო) საფოსტო მეურნეობის პრინციპს: თუ ჩვენ გვინდა წერილი გავუგზავნოთ სხვა ქვეყანაში მცხოვრებ მეგობარს, მისამართში აუცილებლად უნდა მივითითოთ ქვეყანა, ქალაქი (ან დასახელება), ქუჩის და საცხოვრებელი ბინის ნომრები. ანალოგიურია ქსელების დამისამართებაც. იგი მოითხოვს ქსელის ჰოსტ-კომპიუტერებს შორის შეტყობინებების (დიდი ზომის პაკატების) მიღება-გადაცემის პროცედურების განხორციელებისას მარშრუტიზა-ციის პრობლემების გადაჭრას. ყველზე მარტივ შემთხვევას წარმოადგენს დამისამართების ორდონიანი იერარქიულობა: ქსელის ნომერი და კვანძის ნომერი. რთული ქსელების შემთხვევაში დამისამართების ორი დონე უკვე აღარაა საკმარისი და მისამართის იერარქია უნდა შედგებოდეს შემდეგი კომპონენტებისაგან: ქსელის, მაგისტრალის, სეგმენტებისა, და თვით სადგურების ნომრებისაგან (მისამართებისაგან). ასეთ შემთხვევებში ქსელს საკომუნიკაციო მოწყობილობები, რომელთა რაოდენობა თანამედროვე ქსელებში (ქსელების გაერთიანებებში) მილიონობითაა, ერთმანეთთან უნდა დაკავში-რდეს სხვადასხვა მეთოდებით, მათ შირის მისამართების ცხრი-ლების გამოყენებით.

3. მისამართების სიმარტივე. ეს თვისება მისამართს უნდა ხდიდეს ძალზე მოხერხებულს და რაც შეიძლება მარტივად დასამახსოვრებელს ქსელის თითოეული მომხმარე-ბლისათვის. ამ მიზნით მისამართები შეიძლება შეიცავდნენ როგორც სიმბოლურ, ასევე რიცხვითი ფორმის ჩანაწერებსაც. მომხმარებლების (იგულისხმება ადამიანები) გარდა ადვილი მისახვედრია, რომ მისამართები დამახსოვრებული და შენახული უნდა იქნენ ამ მიზნებისათვის განკუთვნილ სპეციალური საკომუნიკაციო აპარატურის მეხსიერებაში, ისეთებში, როგორიცაა მაგალითად, ქსელის ადაპტერები (რომლებითაც აღჭურვილია ქსელთან მიერთებული თითოეული კომპიუტერი), მარშრუტიზატორები, რომლებსაც, როგორც აუცილებელ კომპონენტებს, უნდა შეიცავდნენ ქსელის მაგისტრალები და ცალკეული სეგმენტებიც, ამ სეგმენტების დამაკავშირებელი კომუტატორები და ა.შ. იმისათვის, რომ ზემოთ ნახსენები საკომუნიკაციო ტექნიკური აღჭურვილობების მეხსიერება არ გადაიტვირთოს და შესაბამისად მისამართების ძებნა მონაცემთა მიღება-გადაცემების დროს გაადვილდეს, საჭიროა მისამართებს ჰქონდეთ მარტივი სტრუქტურა, რათა მათ შესახებ გაკეთდეს შესაბამის მეხსიერებებში რაც შეიძლება მოკლე ჩანაწერები.

თანამედროვე კომპიუტერულ ქსელებში გამოიყენება სხვადასხვა სახისა და შინაგანი სტრუქტურის მქონე მისამართები. მათგან ძირითადად აღსანიშნავია აპარატურული მისამართები (ფიზიკური მისამართები), სიმბოლური მისამართები (სახელწოდების მქონე მისამართები) და რიცხვითი მისამართები (ე.ი. მისამართები, რომლებიც შედგენილია ციფრებით). მოკლედ

დავახასიათოდ თითეული მათგანი და ამასთან შევნიშნოთ, რომ ქსელების საკომუნიკაციო საშუალებები აღჭურვილი არიან სპეციალური პროტოკოლებით, რომლებიც „არკვევენ ურთიერთობებს" ზემოთ ჩამოთვლილ სხვადასხვა სახის მისამართებს შორის.

აპარატურული მისამართები (Hardware address). ასეთი სახის მისამართები გამოიყენება შედარებით მცირე ზომის ქსელებში, რომლებიც აკავშირებენ ერთმანეთთან კომპიუტერების შეზღუდულ რაოდენობას.

აპარატურულ მისამართს ხშირ შემთხვევებში მიუთითებენ გარკვეული სიგრძის თექვსმეტობითი ჩანაწერით (მაგალითად, ასე: 098001e508a4, რომლის სიგრძე დამოკიდებულია ქსელის ზომაზე და მასში ჩართული ფიზიკური აპარატურის რაოდენობაზე. ასეთი სახის მისამართზე (ე.წ. MAC – მისამართზე) ოპერირებას ახდენს მხოლოდ აღჭურვილობა და მას ანიჭებს აპარატურის დამამზადებელი ფირმა.

აპარატურულ დამისამართებას გააჩნია ის ძირითადი ნაკლი, რომ აპარატურის შეცვლის შემთხვევაში (მაგალითად, თუ მწყობრიდან გამოვიდა ძველი და იგი უნდა შეიცვალოს ახლით) საჭიროა აუცილებლივ შეიცვალოს შესაბამსი ადაპტერების აპარატურული მისამართებიც, რაც ხშირად მოუხერხებელია.

სიმბოლური მისამართები. ასეთი სახის მისამართებს გააჩნიათ აზრობრივი (შინაარსობრივი, ე.წ. სემენტიკური) დატვირთვა და ამიტომ მათი დამახსოვრება შედარებით უადვილდებათ ქსელის მომხმარებლებს. ისინი აპარატურული

მისამართებისაგან განსხვავებით შეიძლება გამოყენებული იქნენ ნებისმიერი ზომის კომპიუტერულ ქსელებში, ე.ი. ქსელში ჩართული კომპიუტერების ნებისმიერი რაოდენობის დროს. თუმცა მათ ნაკლად უნდა ჩაითვალოს ის, რომ მათი ფორმატი (ე.ი. ასეთი სახის მისამართებში გამოყენებული სიტყვების რაოდენობა) ძალზე ცვალებადია და გრძელი ჩანაწერების ქსელში გადაცემა-მიღება კი, ცხადია, საჭიროებს დროის გარკვეულ დანახარჯებს.

<u>რიცხვითი მისამართები.</u> მისამართების ჩაწერის რიცხვითი ფორმები სხვა ფორმებთან შედარებით ფართოდ გამოიყენება, ვინაიდან ისინი ძალზე მოსახერხებელია და მათი მეხსიერებაში ჩაწერა საშუალებას იძლევა გამოყენებული იქნეს მარტივი და ფიქსირებული ფორმატები. ჩაწერისას ასეთი ფორმები გამოიყენება, მაგალითად Ethernet-ში (IP ან IPX/SPX მისამართები ბოლო ვერსიის IPv6 პროტოკოლებში). ასეთი სახის მისამართების ჩაწერა სწარმოებს ორდონიანი იერარქიით (ქსელისა და კვანძის ნომრების მითითებით). ამჟამად მათ გარდა გამოიყენება ასევე მისამართების უფრო რთული ციფრული სტრუქტურებიც.

საჭიროა ხაზი გავუსვათ ერთ მნიშვნელოვან გარემოებასაც. თანამედროვე კომპიუტერულ ქსელებში მეტ-ნაკლები წარმატებით გადაწყვეტილია დამისამართების ავტომატიზაციის პრობლემები, სადაც გამოყენებულია ყველა ზემოთ ჩამოთვლილი აპარატურული, სიმბოლური და რიცხვითი (ციფრობრივი) მისამართების სახეები. სპეციალიზებულ მოწყობილობებში, რომლებითაც აღჭურვილია თანამედროვე ქსელები, ჩატვირთული ოპერაციული სისტემები უზრუნველყოფენ ზემოთხსენებული მისამარ-

თების ერთი ფორმიდან მეორე ფორმაში გარდაქმნას. აგალითად, მომხმარებლები ქსელის კომპიუტერების დასამისამართებლად დასაწყისში გამოიყენებენ სიმბოლურ სახელებს (ვთქვათ, ელექტრონული ფოსტის E-mail მისამართს lona@informat.ge), რომლებიც ავტომატურად გარდაიქმნებიან რიცხვითი ნომრებით წარმოდგენილ შეტყობინებაში. ამ ნომრებით გადაიცემა ისინი ერთი ქსელიდან მეორეში და მერე ასეთი შეტყობინებები ქსელის მიმღები სერვერების მიერ იშიფრებიან კომპიუტერის აპარატურულ მისამართებში.

კომპიუტერების ქსელში დამისამართების ასეთ განაწილებულ მიდგომას აქვს თავისი როგორც დადებითი, ასევე უარყოფითი მხარეებიც. კერძოდ, დადებითი მხარეა ის, რომ არაა საჭირო ამ მიზნისათვის სპეციალური კომპიუტერის მიმღებ კვანძში ცალკე გამოყოფა, რომელიც გაერკვევა მისამართების ცხრილებში, ხოლო უარყოფით მხარეს კი წარმოადგენს ის, რომ წარმოიქმნება მისამართების ფართოსამაუწყებლო გადაცემის საჭიროება, რომელმაც შეიძლება თავის მხრივ გამოიწვიოს ქსელის გადატვირთვა, ვინაიდან ასეთ დროს მისამართები უნდა დაამუშაოს უკლებლივ ყველა კვანძმა და არა მხოლოდ მიმღებმა კვანძმა. დიდი ზომის ქსელებში გადასაცემი პაკეტების დამისამართების მიზნით ფართოსამაუწყებლო დაგზავნა სეგმენტებისა და კვანძების დიდი რაოდენობის გამო დიდ სირთულეებთან არის დაკავშირებული. ამ მიზნით თანამედროვე კომპიუტერულ ქსელებში გათვალისწინებულია სპეციალური სამსახური. მაგალითად Ethernet-ში DNS (Domain Name System – სახელების ნებადართვის – დომენების სისტემა) სამსახური.

თავი 4

კომპიუტერული ქსელის სტრუქტურიზაცია და მისი გავლენა მონაცემების გადაცემა – მიღების ალგორითმების ეფექტურობაზე

4.1. ფიზიკური და ლოგიკური სტრუქტურიზაციის განმარტება

ქსელური სტრუქტურების აგების, ასევე მათი ექსპლუატაციის დროს კომპიუტერული ტრაფიკის ოპტიმიზაციისათვის (ტრაფიკის ოპტიმიზაციაში იგულისხმება საინფორმაციო პაკეტებით კავშირის არხების დატვირთვის ნორმალური დონის შენარჩუნება მონაცემთა გადაცემა-მიღების სეანსების რეალიზაციისას), აუცილებელია გათვალისწინებული იქნეს ქსელების სტრუქტურიზაციის გარკვეული სახის პრობლემები. სტრუქტურიზაციის ნებისმიერი პრობლემა განიხილება ძირითადად ფიზიკურ და ლოგიკურ დონეებზე.

ფიზიკური სტრუქტურიზაციის ქვეშ იგულისხმება ქსელის ძირითადი კვანძებისა (მათ შორის მომხმარებელთა მუშა სადგურების – პერსონალური კომპიუტერების და სერვერული მეინფრეიმების) და დამხმარე საკომუნიკაციო მოწყობილობების: კომუტატორების, მარშრუტიზატორების, ხიდების, რაბების (შლიუზების) და ა.შ. ქსელში ფიზიკური განლაგებისა და მათი ერთმანეთთან ოპტიმალური შეერთების პრობლემების გადაწყვეტა მონაცემთა გადაცემა-მიღების ალგორითმების გამარტივებისა და საიმედოობის გაზრდის მიზნით.

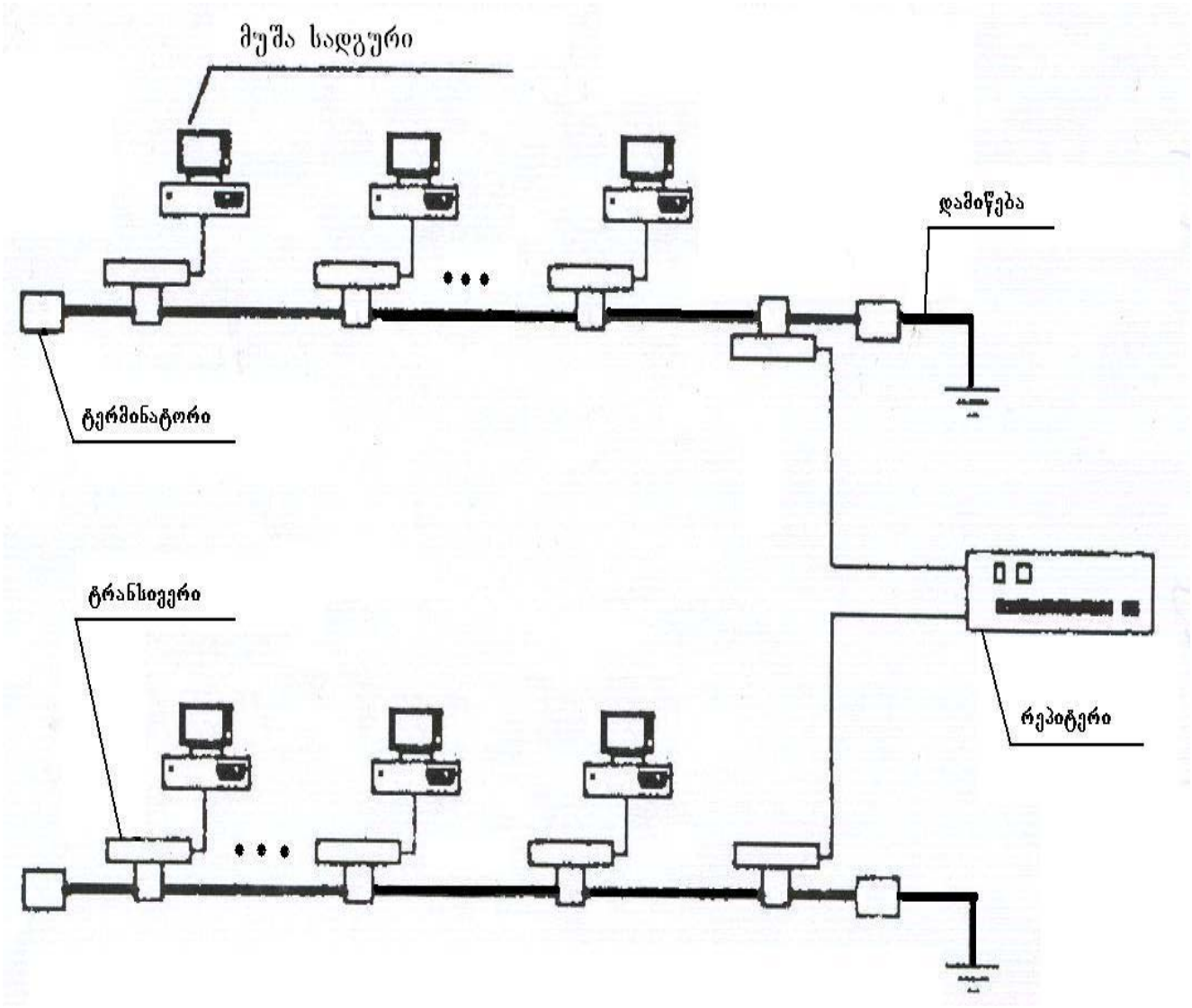
ლოგიკურ სტრუქტურიზაციაში კი, უპირველეს ყოვლისა, გულისხმობენ ქსელის ტრაფიკის ლოგიკურ განაწილებას (ან გადანაწილებას) სხვადასხვა ფიზიკურ სეგმენტებზე არსებულ ქსელურ, აპარატურულ რესურსებს შორის. ლოგიკურ სტრუქტურიზაციაში ოპტიმალური მიდგომების დანერგვას ხშირ შემთხვევაში გადამწყვეტი მნიშვნელობა ენიჭება ქსელში განსაკუთრებით ჭარბი დატვირთვების არსებობის დროს (მაგალითად, ქსელის მუშაობისას პიკის საათებში).

ფიზიკური სტრუქტურიზაციის დროს ქსელური აღჭურვილობის, ისეთების როგორიცაა კვანძების მოწყობილობები (მუშა სადგურები – მომხმარებლის პერსონალური კომპიუტერები ქსელის კლიენტებისათვის, ასევე მძლავრი კომპიუტერები – მეინფრეიმები ქსელის სერვერებისათვის), საკაბელო სისტემები, ასევე დამხმარე კომპონენტები, რომლებიც მუშაობენ გამმეორებლების (Repeators), კონცენტრატორების (Hubs) და ა.შ. რეჟიმებში (ამ უკანასკნელის ქვეშ გულისხმობენ ქსელში ფუნქციონალური აპარატურის განლაგების მთავარ ცენტრებს), მათი ფიზიკური განლაგება და ერთმანეთთან შეერთება სწარმოებს ჩვენს მიერ წინა თავებში განხილული ტოპოლოგიების მიხედვით. ტოპოლოგიურმა სტრუქტურებმა უნდა უზრუნველყოფენ ძირითადი მოთხოვნა – ქსელური აღჭურვილობის ერთგვაროვნება. ამას გარდა დიდი მნიშვნელობა ენიჭება იმას, რომ ქსელებს უნდა გააჩნდეს ფიზიკური გაფართოების ტექნიკური შესაძლებლობები. ფიზიკური სტრუქტურიზაციის დროს ერთგვაროვნებაში იგულისხმება ქსელის სეგმენტებზე არსებული კვანძების (ძირითადად მუშა სადგურების) თანაბარი უფლებები მონაცემთა

გადაცემა-მიღების ალგორითმების რეალიზიციის დროს. ასევე მათ უნდა გააჩნდეთ ერთგვაროვანი ტექნიკური საშუალებები (სტანდარტიზირებული საერთაშორისო კომიტეტების მიერ) ქსელის სადგურებს შორის ფიზიკური კავშირების დასამყარებლად.

აღსანიშნავია ისიც, რომ დიდი ქსელების აგების დროს ერთგვაროვნობის (ასევე თანაბარუფლებიანობის) მოთხოვნები ყოველთვის ვერ ხორციელდება სხვადასხვა მიზემების გამო, რომელთაგან პირველ რიგში აღსანიშნავია ფიზიკურად არსებულ (განლაგებულ) კვანძებს შორის მანძილი (მაგალითად სხვადასხვა სპეციფიკაციის საკაბელო სისტემებს გააჩნიათ სხვადასხვა დასაშვები ფიზიკური სიგრძე, ერთი სეგმენტის ფარგლებში, კერძოდ, რამდენიმე მეტრიდან რამოდენიმე ათეულ კილომეტრამდე), რაც იწვევს შერჩეული სპეციფიკაციების არაერთგვაროვნობის გამოყენების საჭიროებას. დიდ გავლენას ახდენს ქსელში განლაგებული კვანძების შესაძლო მაქსიმალური რაოდენობაც, რის გამოც კვანძების მიერ შექმნილი ტრაფიკის ინტენსიურობა ატარებს ცვალებად ხასიათს (წარმოიქმნება ტრაფიკის ე.წ. პულსაციები).

მაგალითისათვის (ნახ.4.1) შეიძლება აღვნიშნოთ, რომ ქსელის მაგისტრალის 10Base5 სპეციფიკიაციის კოაქსიალური კაბელით (ხშირად მოიხსენიებენ, როგორც სქელ კოაქსიალურ კაბელს), უზრუნველყოფის დროს ქსელის ფიზიკური სტრუქტურიზაცია ექვემდებარება შემდეგ შეზღუდვებს: მასზე (კაბელზე) მიერთებული კომპიუტერების მაქსიმალური რიცხვი კორპორაციული ქსელისათვის შეადგენს 100.



ნახ. 4.1. Ethernet – ქსელის ფრაგმენტი სქელ კოაქსიალურ კაბელზე

კვანძების დაყოფა შესაძლებელია მხოლოდ 5 სეგმენტად. შესაძლებელია ასევე მხოლოდ 4 რეპიტერის გამოყენება. სეგმენტის მაქსიმალური სიგრძე შეადგენს 500 მეტრს, ხოლო ქსელის საერთო სიგრძე კი 2,5 კმ-ს. ტრანსივერებს შორის მინიმალური სიგრძე უნდა იყოს 2,5 მეტრი, ხოლო მაქსიმალური – 50 მეტრი.

აქვე შევნიშნოთ ისიც, რომ ქსელის ტრაფიკის ინტენსიობა და ქსელში არსებული კომპიუტერების (კვანძების) რიცხვი

ერთმანეთთან არიან უკუპროპორციულ დამოკიდებულებაში. რას ნიშნავს ეს? ეს ნიშნავს, რომ თუ საქმე გვაქვს ისეთ ქსელებთან, რომლეთა კომპიუტერებს შორის მონაცემთა ურთიერთ გაცვლის ინტენსიურობა ძალზე მაღალია, მაშინ ქსელის ადმინისტრატორი იძულებულია მონაცემთა გადაცემა-მიღების ნორმალური რეჟიმის უზრუნველსაყოფად 100 კომპიუტერის რაოდენება (ზემოთ მოყვანილი მაგალითისათვის) სეგმენტზე შემციროს (სხვა სიტყვებით რომ ვთქვათ, მოახდინოს ქსელის ფიზიკური სტრუქტურიზაცია) მხოლოდ 30-40–მდე, რათა თითოეულ კომპიუტერს "ეყოს" ქსელის საჭირო გამტარუნარიაონობა.

კომპიტერული ქსელების ფიზიკური და ლოგიკური რაციონალური (ოპტიმალური) სტრუქტურების შექმნისა და სხვადასხვა შეზღუდვების შემცირებას ხელს უწყობს ზემოთ ხსენებული ისეთი საკომუნიკაციო საშუალებების გამოყენება, როგორიცაა გამმეორებლები, კონცენტრატორები, ხიდები, შლიუზები და მარშრუტიზატორები.

4.2. ქსელების ფიზიკური სტრუქტურიზაცია

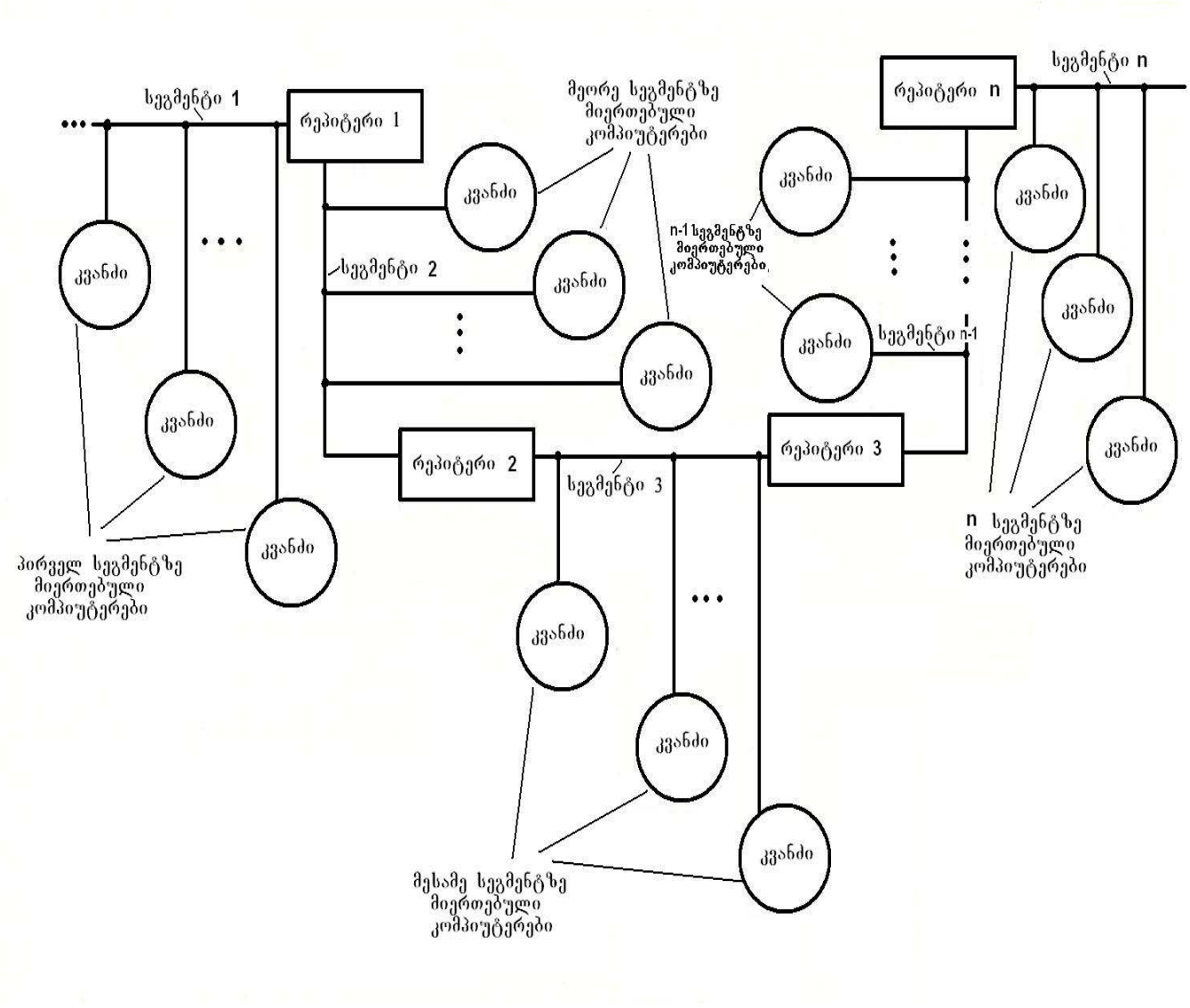
ლოკალური კომპიუტერული ქსელების სტრუქტურიზაციის დროს საკომუნიკაციო მოწყობილობების გამოყენება ემსახურება შემდეგ ძირითად მიზნებს: მონაცემთა მიმღებ-გადამცემი ქსელური სტრუქტურების ტექნიკური შესაძლებლობების გაზრდას, ამ სტრუქტურების გაფართოებასა და მასში მომსახურების ხარისხის გაუმჯობესებას. ამ მიზნებს ემსახურება

სხვადასხვა ფიზიკური დანიშნულების ქსელური საკომინიკაციო კომპონენტების გამოყენება, რომლებიც ჩამოვთვალეთ წინა პარაგრაფში. აღნიშნული კომპონენტებიდან ყველაზე მარტივ საკომუნიკაციო მოწყობილობას წარმოადგენს გამმეორებლები ანუ რეპიტერები (ინგლისური ტრანსკრიპტაციიდან repeators), რომელთა ძირითადი დანიშნულებაა კომპიუტერული ქსელის სხვადასხვა მონაკვეთების (სეგმენტების) ფიზიკური შეერთება და ამ სეგმენტების საკაბელო სისტემის საერთო სიგრძის გაზრდა, რაც თავის მხრივ ხელს უწყობს ქსელის გაფართოებას.

რეპიტერების გამოყენება ქსელის სიგრძის გაზრდის მიზნით ნაჩვენებია ნახ.4.2-ზე გამოსახულ ქსელის ფრაგმენტზე.

ქსელის სეგმენტების რაოდენობის გაზრდის გარდა რეპიტერების, როგორც ტექნიკური მოწყობილობების, დანიშნულებაა აგრეთვე კაბელებში გადაცემული სიგნალების ისეთი მახასიათებლების რეგულირება, როგორიცაა: სიგნალის სიმძლავრე, ამპლიტუდა, ფრონტები და ა.შ. დანიშნულებიდან გამომდინარე რეპიტერებს ხშირად აიგივებენ ქსელის კომუტატორებსა და ჰაბებთან (კონცენტრატორებთან). განსხვავება მათ განკარგულებაში მყოფი პორტების რაოდენობაშია. ონცენტრატორებს აუცილებლივ გააჩნიათ რამოდენიმე პორტი, რომლებიც აერთიანებენ (ე.ი. ერთმანეთთან აკავშირებენ) ანუ კონცენტრაციას უკეთებენ რამოდენიმე ფიზიკურ სეგმენტს (აქედან გამომდინარეობს მათი სახელწოდებაც – კონცენტრატორები).

ისინი აღჭურვილი არიან კავშირის ყველა პროგრამულ-ტექნიკური (ე.ი. პროგრამულ–აპარატურული) საშუალებებით, რომლებიც ახდენენ ქსელის სხვადასხვა სეგმენტების თავმოყ –



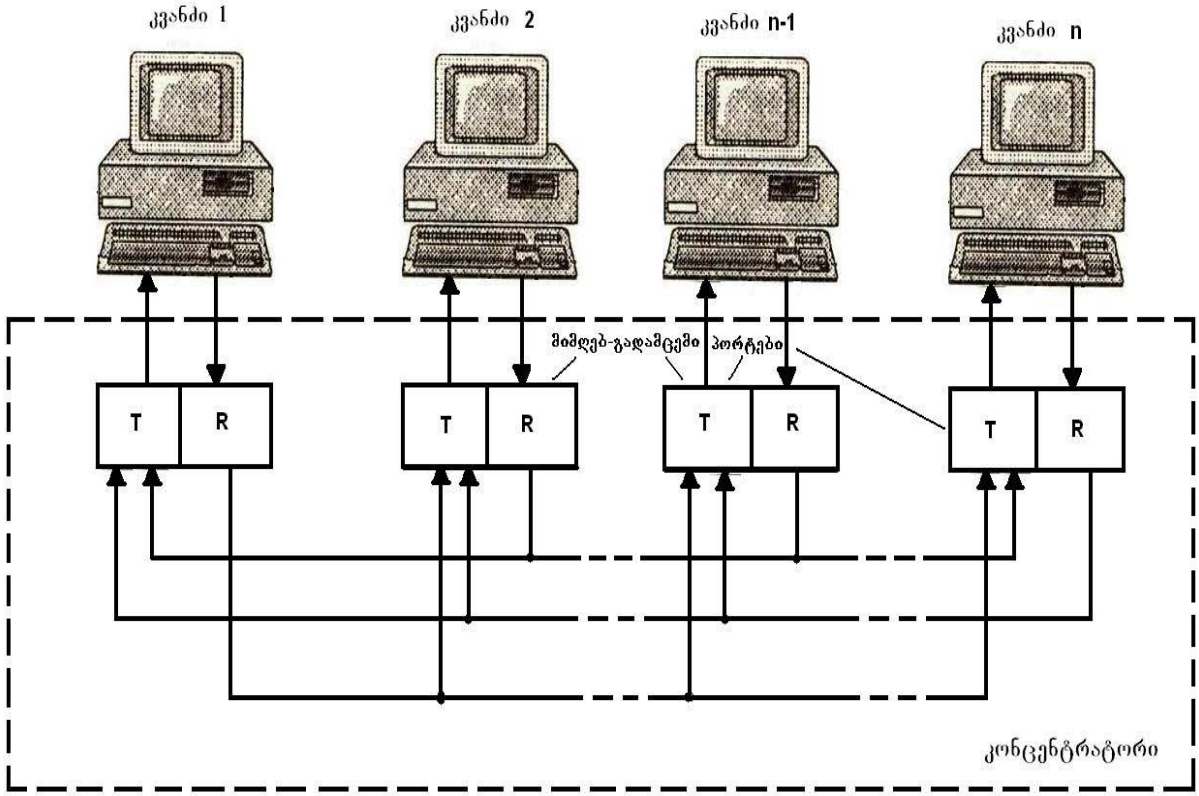
ნახ.4.2. ქსელის ფიზიკური სტრუქტურიზაციის დროს რეპიტერები ზრდიან სეგმენტების რაოდენობას

რასა და ამ სეგმენტებს შორის კავშირების რეგულირებას.

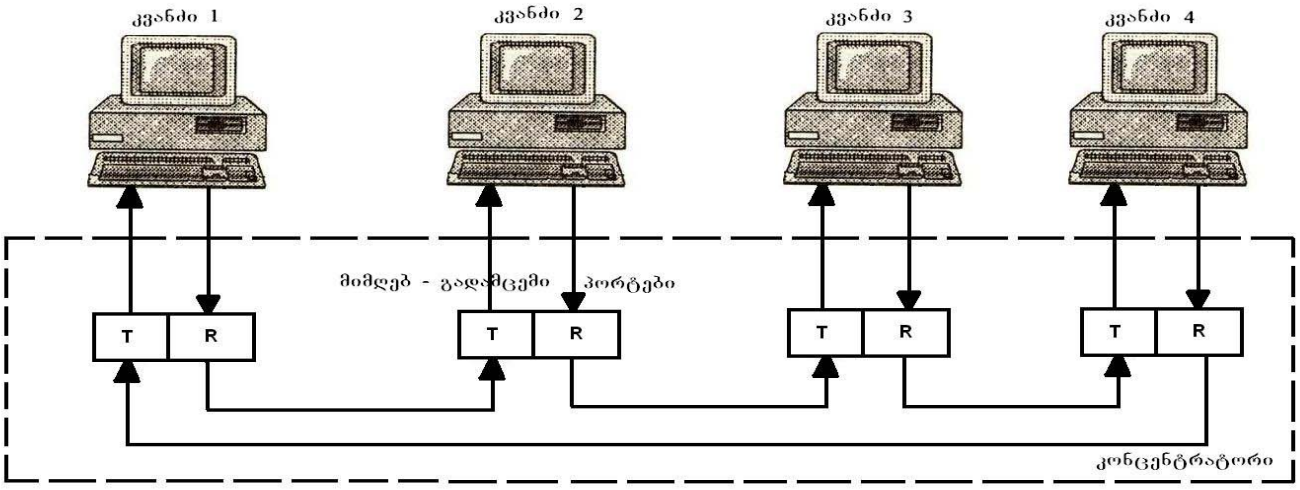
ამრიგად, ქსელის ფიზიკური სტრუქტურიზაციის დროს კონცენტრატორების ძირითადი ფუნქციაა სხვა პორტებიდან სიგნალების თავის პორტებში თავმოყრა და შემდეგ სხვა პორტებში მათი გადანაწილება სიგნალების ელექტრული მახასიათებ-ლების შეცვლის გარეშე, რაც ნიშნავს იმას, რომ ისინი აწარმოებენ არა სიგნალების ფიზიკური მახასიათებლების გარდაქმნას, არამედ მხოლოდ იმეორებენ მათ.

იმის და მიხედვით თუ როგორი საბაზო ტექნოლოგიებითაა ორგანიზებული ქსელი, რეპიტერებისა და კონცენტრატორების გამოყენების ტექნოლოგიებიც სხვადასხვაა Ethernet, Token Ring, FDDI, Fast Ethernet და 100 VG – AnyLAN და ა.შ. სხვადასხვა სიჩქარის ლოკალურ კომპიუტერულ ქსელებში.

მაგალითების სახით ნახ. 4.3 და 4.4-ზე ნაჩვენებია კონცენტრატორის პორტების ორგანიზაცია კონცენტრატორებში შესაბამისად Ethernet და Token Ring ქსელებისათვის.



ნახ 4.3. კონცენტრატორის პორტებს შორის კავშირი
Ethernet ქსელებისათვის

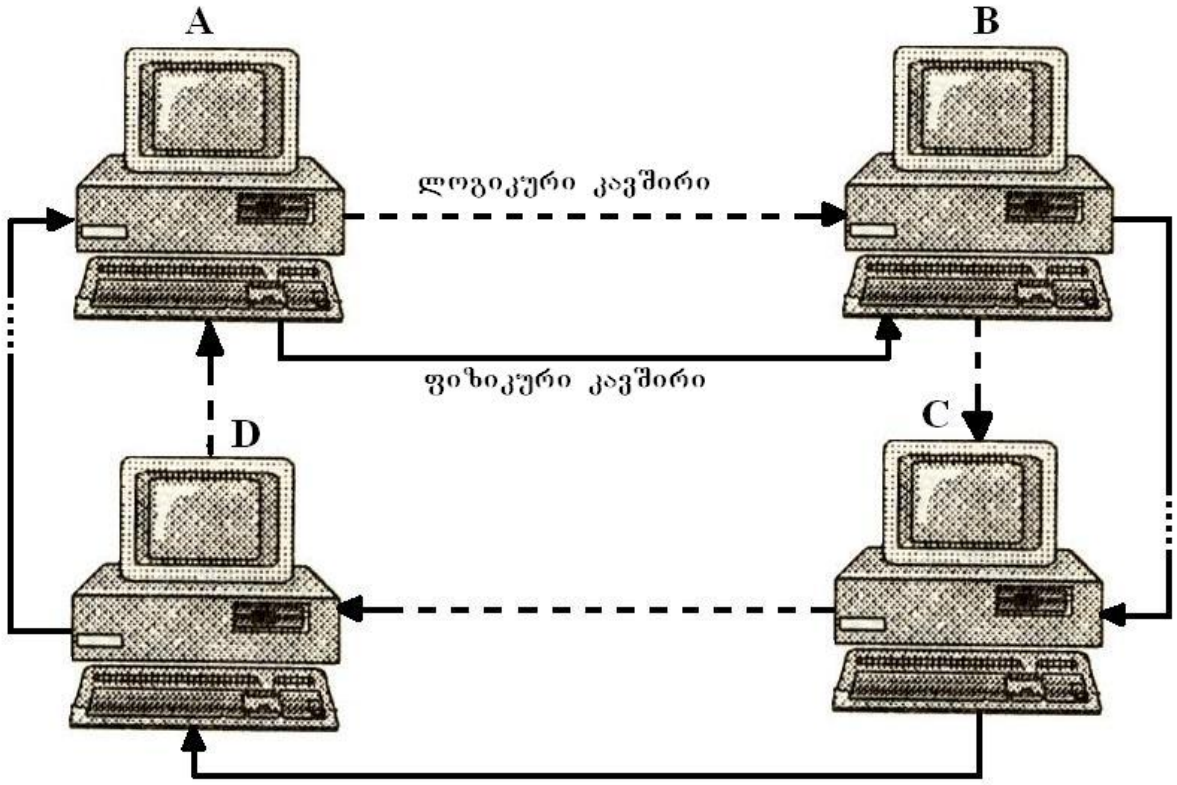


ნახ 4.4. კონცენტრატორის პორტებს შორის კავშირი

Token Ring ქსელებისათვის.

ფიზიკური სტრუქტურიზაციის დროს, როგორც ზემოთ აღვნიშნეთ, ქსელის ტოპოლოგია (სტრუქტურა) იქმნება ფიზიკური კავშირების გარკვეული კონფიგურაციით, ხოლო მისგან განსხვავებით ლოგიკური სტრუქტურიზაცია კი განისაზღვრება ქსელის კვანძებს შორის საინფორმაციო ნაკადების მოძრაობის კონფიგურაციით. ეს ორივე სახის კონფიგურაციები კონცენტრატორების სხვადასხვა ტექნოლოგი-ებში გამოყენების დროს შეიძლება დაემთხვნენ ან არ დაემთხვნენ ერთმანეთს.

ნახ. 4.5 –ზე ნაჩვენებია მაგალითი (ერთი ფრაგმენტი) რგოლური სტრუქტურის ქსელის ოთხკომპიუტერიანი ტოპოლო-გიისა, სადაც ფიზიკური და ლოგიკური კავშირები ემთხვევიან ერთმანეთს.

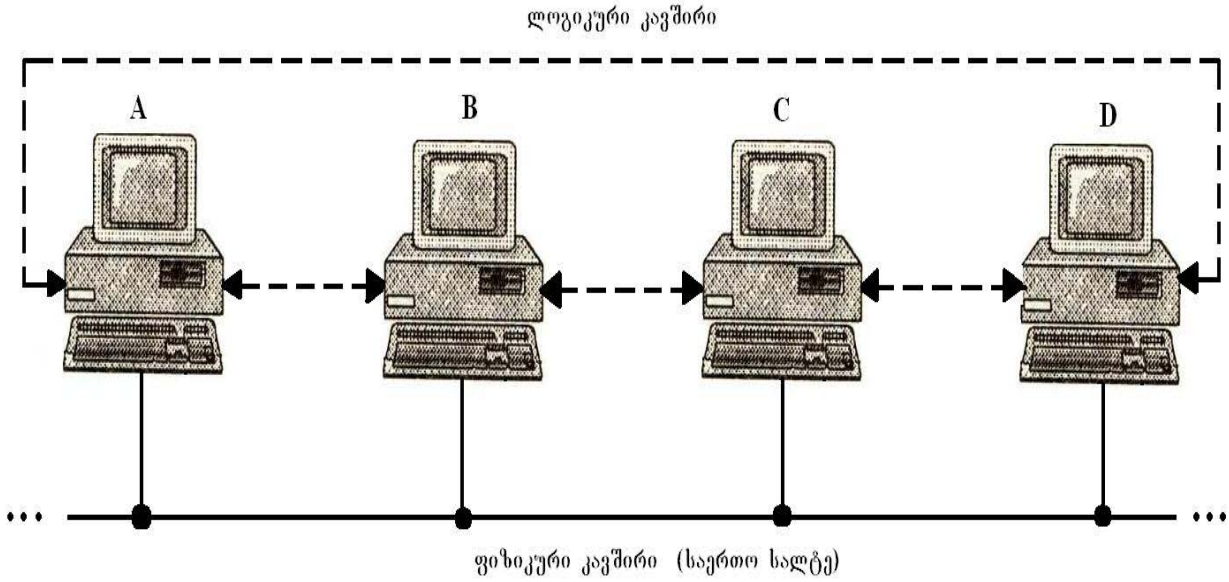


ნახ. 4.5. რგოლური სტრუქტურა, სადაც ქსელის ფიზიკური (⟶) და ლოგიკური (- - →) კავშირები ემთხვევა ერთმანეთს

ნახ.4.5–ზე გამოხატული ფრაგმენტის მიხედვით მისი კომპიუტერები ურთიერთქმედებენ (აწარმოებენ ერთმანეთს შორის მონაცემების მიღება-გადაცემებს) შემაერთებელ კაბელებში მარკერის ერთი კომპიუტერიდან მეორეში გადაცემის გზით. კერძოდ, A კომპიუტერი გადასცემს B კომპიუტერს, B – C კომპიუტერს, C – D – კომპიუტერს და D კომპიუტერი კი A – კომპიუტერს, რითაც იკვრება როგორც ფიზიკური ასევე ლოგიკური რგოლი.

ნახ.4.6–ზე კი ნაჩვენებია ქსელი (დამახასიათებელი Ethernet ტექნოლოგიებისათვის), სადაც კომპიურტერებს შორის

ფიზიკური და ლოგიკური კავშირების სტრუქტურები არ ემთხვევიან ერთმანეთს.



ნახ 4.6. ქსელის სალტური სტრუქტურა, სადაც ფიზიკური (⟶) და ლოგიკური (- - →) კავშირები არ ემთხვევიან ერთმანეთს

როგორც ამ ნახაზიდან ჩანს ეს კომპიუტერები ერთმანეთთან შეერთებული არიან საერთო სალტით, ხოლო მარკერის გადაცემა კი სწარმოებს რგოლური ტოპოლოგიით (ამ შემთხვევაში საუბარია ისეთი სალტური ტოპოლოგიის ქსელზე, სადაც პაკეტების გადაცემის დროს გამოიყენება სპეციალური კადრი–მარკერი).

ქსელის ასეთი სტრუქტურიზაციისას (ნახ.4.6.), როგორც ვხედავთ, მონაცემების გადაცემის დროს კომპიუტერებს შორის კავშირები არ იცვლება. ეს იმ დროს, როცა თითოეული კომპიუტერის ქსელური ადაპტერის დრაივერებს შეუძლიათ შეცვალონ ლოგიკური კავშირების კონფიგურაცია (ე.ი.

მოახდინონ ქსელის ლოგიკური სტრუქტურიზაცია) და ინფორმაციების კომპიუტერებს შორის ურთიერთ გაცვლა შეიძლება მოხდეს ნებისმიერი თანმიმდევრობით (ე.ი. შესაძლებელია გადაცემის მრავალი ვარიანტის განხორციელება).

ამგვარად, ქსელის ფიზიკური სტრუქტურიზაცია რეპიტერების ან კონცენტრატორების დახმარებით არა მარტო აფართოებს ქსელის მასშტაბებს, არამედ ზრდის მის (ქსელში პაკეტების გადაცემის) საიმედოობასაც, მონაცემთა გადაცემის ლოგიკური (ვირტუალური) კავშირების სხვადასხვა ვარიანტების წარმოქმნით.

4.3. ქსელების ლოგიკური სტრუქტურიზაცია

ლოგიკური სტრუქტურიზაცია, როგორც ეს §4.1–ში აღვნიშნეთ, გულისხმობს ქსელის სეგმენტებს შორის ტრაფიკის განაწილებას (სხვა სიტყვებთ რომ ვთქვათ, წყარო-კომპიუტერიდან მიმღებ-კომპიუტერამდე მონაცემების გადაცემა-მიღების პროცედურებს ახორციელებს სხვადასხვა გზებით, ანუ მარშრუტებით), რომელიც ვერ ხორციელდება ქსელის ფიზიკური სტრუქტურიზაციის დონეზე. როგორც ცნობილია, დიდი და საშუალო ზომის ქსელები შედგებიან ქვექსელების გარკვეული სიმრავლეებისაგან, რომლებიც ხასიათდებიან მონაცემთა გაცვლის ინტენსიობების არათანაბრობით.

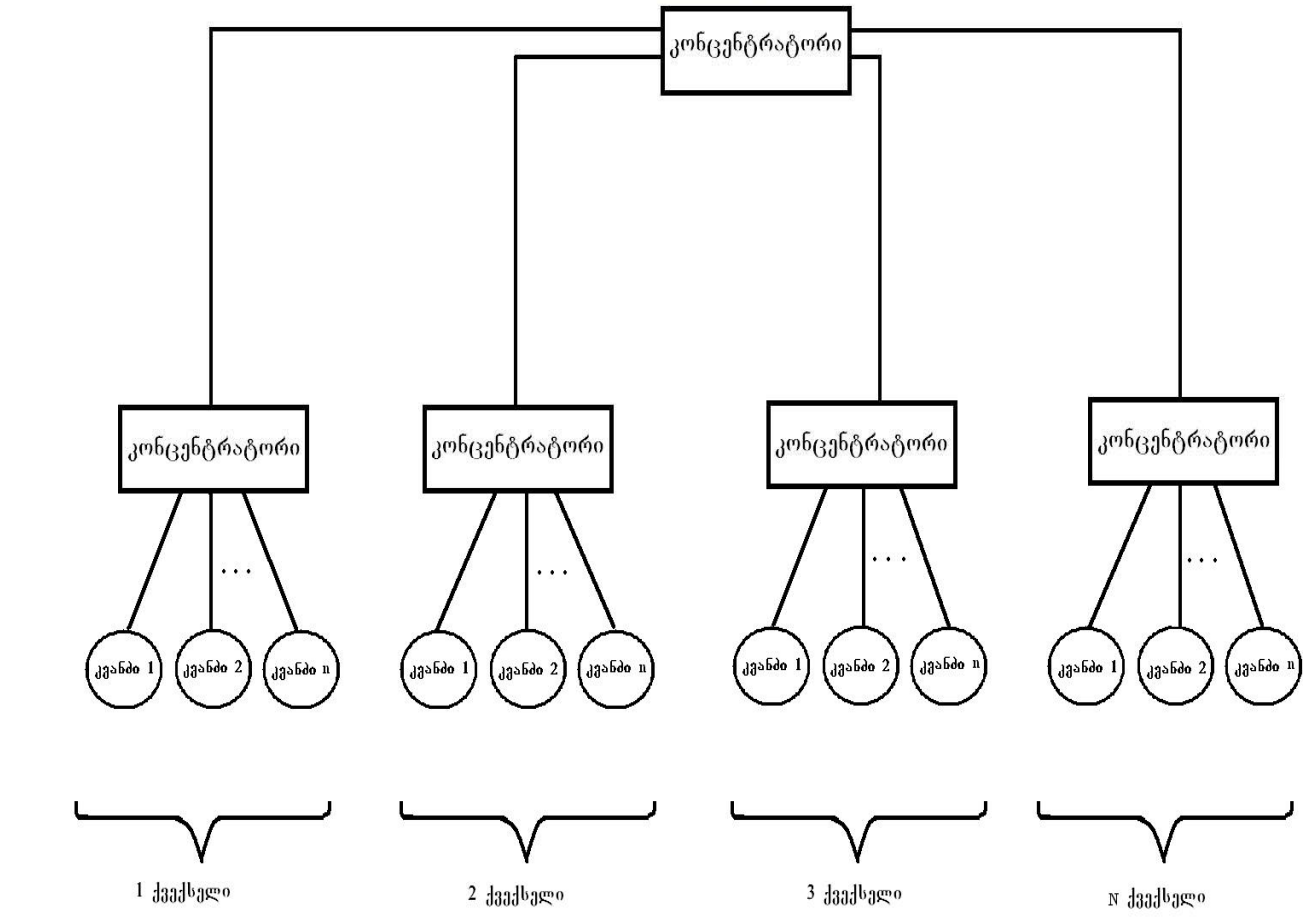
განასხვავებენ ტრაფიკის ლოგიკური განაწილების ორ სახეს:

– ტრაფიკის განაწილებას ქვექსელის შიგნით არსებულ კომპიუტერებს შორის (შიგა ტრაფიკი);

– ტრაფიკის განაწილებას თვით ქსელებს შორის (გარე ტრაფიკი).

ტექნიკური ლიტერატურიდან ცნობილია, რომ სულ ახლო წარსულში სამართლიანად თვლიდნენ ტრაფიკების თანაფარდობას 80/20 – თან (ე.ი. 80% მონაცემების გადაცემებისა მოდიოდა შიგა ტრაფიკზე, ხოლო 20% - გარე ტრაფიკზე). თუმცა ამჟამად ასეთი თანაფარდობის სამართლიანობა უკვე ეჭვის ქვეშ დგება ქვექსელების საკომუნიკაციო მასშტაბებისა და დატვირთვების გაზრდის გამო.

ამჟამად ფართოდ ინერგება Internet – ტექნოლოგიები და ზემოთ მოყვანილი თანაფარდობა იცვლება გარე ტრაფიკის სასარგებლოდ. დიდი ზომის ქსელებში კომპიუტერებს შორის ურთიერთქმედებისას მხოლოდ ფიზიკურ კავშირებზე ორიენტაცია აღარ არის საკმარისი, ვინაიდან კომპიუტერების რაოდენობის გაზრდის დროს საერთო სალტები ვეღარ უზრუნველყოფენ გამტარუნარიანობის საჭირო დონეს თუნდაც კონცენტრატორების დახმარებით ფიზიკური სტრუქტურიზაციის საკმაოდ მაღალი ხარისხის დროსაც კი (ნახ 4.7.). ამასთან ერთი ქვექსელის კომპიუტერები იძულებულები არიან დაელოდონ, სანამ რომელიმე წყვილი სხვა ქვექსელში არ დაამთავრებს მონაცმების გაცვლას, ვინაიდან კონცენტრატორები ნებისმიერ კადრს ავრცელებენ ყველა ქვექსელის სეგმენტებზე. ეს კი თავის მხრივ უარყოფით გავლენას ახდენს ქსელის საერთო წარმადობაზე. მაგალითად, თუ პირველი ქვექსელის კვანძს 1 და კვანძს 2 სურთ ერთმანეთში მონაცემების გაცვლა (რაც შეესაბამება შიგა ტრაფიკის გამოყენებას) კონცენტრატორების



ნახ 4.7. მაღალი დონის ფიზიკური სტრუქტურიზაცია კონცენტრატორების გამოყენებით

მუშაობის ლოგიკიდან გამომდინარე ამ მონაცემებმა უნდა გაიარონ მე-2, 3, 4 ქვექსელების სეგმენტებიც და სანამ ყველა კონცენტრატორი არ მისცემს თანხმობას კვანძს 2, ე.ი. სანამ არ მიიღებს კვანძი 2–ის კომპიუტერი მასზე დამისამართებულ კადრს, ქსელის სხვა კომპიუტერებს არ შეუძლიათ გადასცენ თავიანთი მონაცემები. ეს ნიშნავს იმას, რომ ტრაფიკის განაწილების ლოგიკური სტრუქტურა ერთგვაროვიანია და კომპიუტერის ყველა წყვილს (მიმღებ-გადამცემს) გააჩნიათ მისით სარგებლობის თანაბარი უფლებები. აღნიშნული

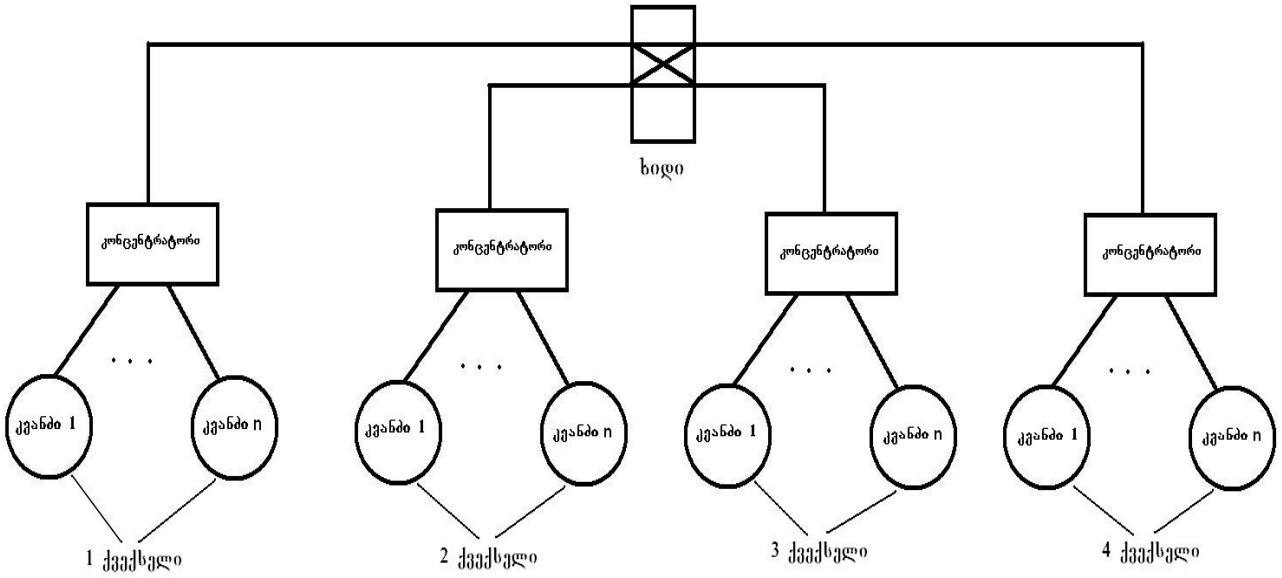
პრობლემიდან თავის დასაღწევად გაჩნდა იდეა ქსელის ტრაფიკის არაერთგვაროვანად გამოყენებისა ქსელის სხვადასხვა სეგმენტების მიერ, ანუ სხვა სიტყვებით რომ ვთქვათ, მონაცემები არ უნდა გავიდეს ქვექსელის გარეთ (ნახ 4.7 მაგალითისათვის) თუ კი გადაცემული კადრები არ ეკუთვნიან მის გარეთ არსებული ქვექსელების (ჩვენს შემთხვევაში მე-2, 3,4 ქვექსელების) კვანძებს (კომპიუტერებს).

ამ პრობლემიდან თვის დასაღწევად გამოყენებულია ქსელების ლოგიკური სტრუქტურიზაციის მეთოდები, რომლებიც რეალიზებულია ისეთი საკომუნიკაციო მოწყობილობების დახმარებით, როგორიცაა კომუტატორები (Switching hubs) , ხიდები (Bridges) და მარშრუტიზატორები (Routers).

მაგალითად, ხიდი ჰყოფს ქვექსელის გადამცემ გარემოს რამოდენიმე ნაწილად (ე.წ. ლოკალიზებულ ტრაფიკებად). ხიდი ერთი ქვექსელის რომელიმე სეგმენტიდან მონაცემებს გადასცემს მეორე ქვექსელში (რომელიმე სეგმენტს), თუ დამისამართებული კომპიუტერი მდებარეობს ამ უკანასკნელში.

ამრიგად, ხიდები აწარმოებენ ერთი ქვექსელის ტრაფიკის იზოლაციას მეორე ქვექსელის ტრაფიკისაგან, რითაც მნიშვნელოვნად მცირდება არასანქცირებული შეღწევები და იზრდება ქსელის საერთო წარმადობაც.

ნახ.4.8.-ზე ნაჩვენებია ფრაგმენტი, სადაც ქსელის ლოგიკური სტრუქტურიზაციისათვის გამოყენებულია ხიდი.



ნახ 4.8. ქსელის ლოგიკური სტრუქტურიზაცია ხიდის დახმარებით

ადვილი მისახვედრია, რომ ხიდს აუცილებლივ უნდა გააჩნდეს ინტელექტუა-ლური უნარი დაიმახსოვროს თუ რომელი პორტის გავლით მიეწოდა მას მონაცემთა კადრი ქსელის თითოეული კომპიუტერიდან, რათა უზრუნველყოს მან მონაცემთა ურთიერთ გაცვლა მხოლოდ დამისამართებულ კომპიუტერებს შორის.

ლოგიკური სტრუქტურიზაციისას ხიდების გამოყენების უარყოფით მხარედ უნდა ჩაითვალოს ის, რომ იგი მნიშვნელოვნად ზღუდავს ქსელში კავშირების კონფიგურაციას, თანაც სეგმენტები ისე უნდა მიუერთდნენ მას, რომ არ წარმოიქმნას ჩაკეტილი კონტურები.

ხიდების ლოგიკურ განვითარებას მოჰყვა ქსელის კომუტატორების შექმნა, რომლებიც წარმოადგენენ ერთგვარ საკომუნიკაციო მულტიპროცესორებს. კომუტატორის პორტები უფრო “ინტელექტუალურია”, ვინაიდან ისინი აღჭურვილნი არიან საკუთარი სპეციალიზებული პროცესორებით, რომლებსაც ხიდის მუშაობის საერთო ალგორითმის მიხედვით სხვა პორტებისაგან დამოუკიდებლივ შეუძლიათ დაამუშაონ დამისამართებული კადრები (და თანაც პარალელურ რეჟიმში).

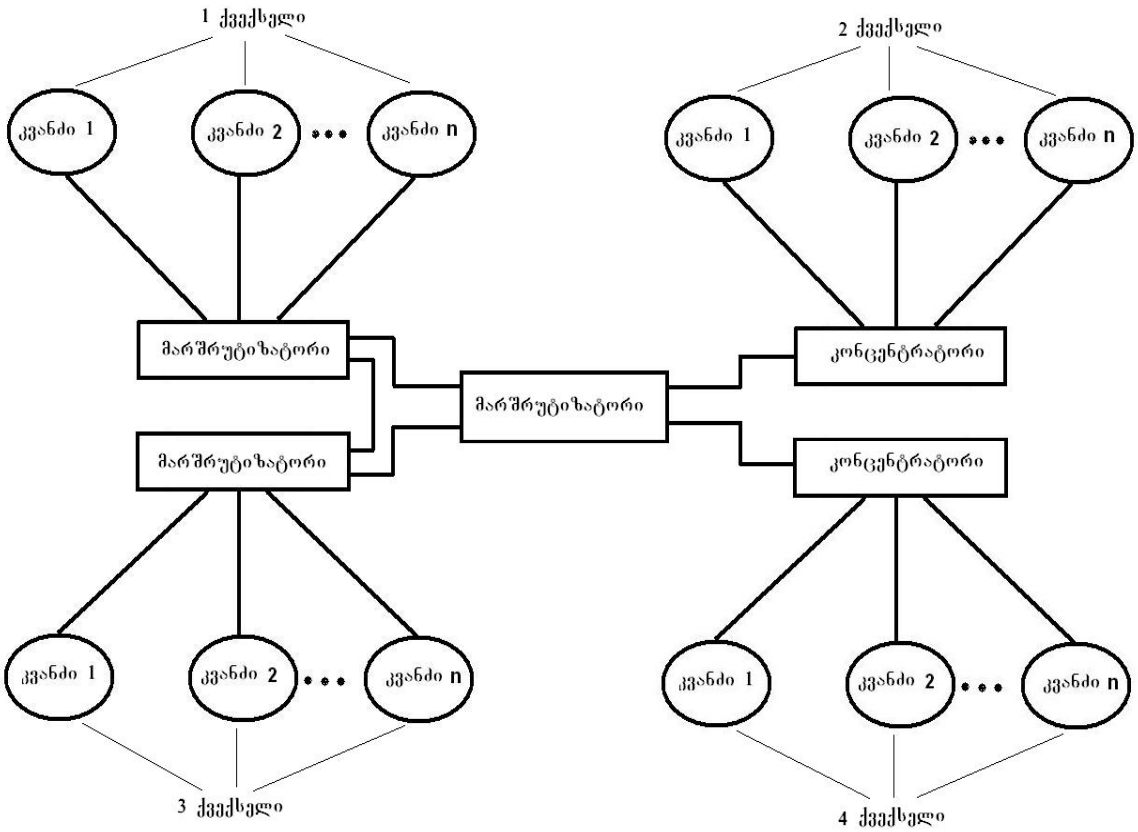
ხიდებისა და კომუტატორების გარდა ქსელის ლოგიკურ სტრუქტურიზაციას ახორციელებენ სპეციალიზირებული საკომუნიკაციო მოწყობილობები – მარშრუტიზატორებიც.

მონაცემების გადაცემა-მიღების ალგორითმების რეალიზაციის დროს მარშრუტიზატორების გამოყენება ხშირ შემთხვევებში უფრო ეფექტურია, ვიდრე ხიდებისა და კომუტატორების გამოყენება. იგი (მარშრიტიზატორი) ამასთანავე უფრო საიმედოა ქსელის ცალკეული ნაწილების (ე.ი. ქვექსელების) ტრაფიკის იზოლაცი-ისათვის, ვინაიდან იგი სეგმენტებისათვის იყენებს შედგენილ რიცხვით მისამართებს. ამ მისამართებში გამოყოფილა ცალკე ველი ქსელის ნომრისათვის. ასე რომ, თუ კომპიუტერების რომელიმე ჯგუფს გააჩნია ამ ველის ერთნაირი მნიშვნელობა, ეს მიუთითებს იმაზე, რომ ისინი ეკუთვნიან ერთ სეგმენტს, რომელიც შეიძლება იყოს როგორც ერთი ქვექსელი (Subnet).

ტრაფიკის ლოკალიზაციის გარდა ხიდებსა და მარშრუტიზატორებთან შედარებით მათ (მარშრუტიზატორებს) გააჩნიათ კიდევ ის უპირატესობა, რომ რამოდენიმე შესაძლო ვარიანტიდან

მათ შეუძლიათ ამოარჩიონ უფრო მოკლე (რაციონალური) მარშრუტები პაკეტების გადაცემებისას, ან/და "შეგნებულად" გვერდი აუარონ ისეთ მარშრუტებს, რომელთა სეგმენტებიც გადატვირთულია ქსელის პიკურ მომენტებში აქტიური დატვირთვების დროს.

ლოკალური კომპიუტერული ქსელების წარმადობასა და საიმედოობის გაზრდის მიზნით შესაძლებელია მარშრუტიზატორებისა და კონცენტრატორების ერთდროული გამოყენებაც (ნახ 4.9).



ნახ 4.9. ქსელის ლოგიკური სტრუქტურიზაცია მარშრუტიზატორებისა და კონცენტრატორების გამოყენებით

მარშრუტიზატორების გამოყენების ერთ-ერთი უპირატესობა მგდომარეობს კიდევ იმაში, რომ მათ გააჩნიათ შესაძლებლობა ერთმანეთთან დააკავშირონ სხვადასხვა ტექნოლოგიებით აგებული ქვექსელები (მაგალითად Ethernet –ი დააკავშირონ X . 25 ქსელებთან). ამას კი ძალზე დიდი მნიშვნელობა ენიჭება, ვინაიდან X . 25 საკომუნი-კაციო პროტოკოლებზე რეალიზებული კავშირგაბმულობის სატელეფონო ხაზებით თითოეულ ორგანი-ზაციასა და ოჯახსაც კი შეუძლიათ ჩართონ თავიანთი კომპიუტერები Ethernet –ის ქსელში.

ადვილი მისახვედრია, რომ მონაცემთა შეუფერხებელი გადაცემა – მიღებისათვის ცალკეული ქსელების ერთმანეთთან დაკავშირებას ძალზე დიდი მნიშვნელობა ენიჭება, რადგან ხშირად ეს ქსელები (შესაძლოა ქვექსელებიც) ერთმანეთისაგან განსხვავდებიან იმითაც, რომ მათ გააჩნიათ სისტემური და გამოყენებითი პროგრამული უზრუნველყოფის სრულიად განსხვავებული ტიპები. ასეთ შემთხვევებში ქსელების (ან ქვექსელების) ერთმანეთთან დასაკავშირებლად იყენებენ სპეციალიზირებულ საკომუნიკაციო საშუალებებს - შლიუზებს (Gateway).

თავი 5

მონაცემთა გადამცემა-მიღების ალგორითმების სარეალიზაციო ქსელის ფიზიკური დონის საკაბელო სისტემები და კადრის სტრუქტურები

5.1. ზოგადი ცნობები სიგნალების ფიზიკური გადაცემის შესახებ კომპიუტერული ქსელის საკომუნიკაციო არხებით

ნებისმიერი ტიპისა და დანიშნულების ქსელის ყველა კვანძი მონაცემთა პაკეტების მანძილზე გადაცემა – მიღებისათვის, ცხადია, ერთმანეთთან დაკავშირებული უნდა იყოს რაღაც ფიზიკური გარემოთი. გამონაკლისი არც კომპიუტერული ქსელი გახლავთ. გამომთვლელ ქსელებში ჩართული კომპიუტერებიც (როგორც კლიენტური, ასევე სერვერული დანიშნულების) ერთმანეთს მონაცემებს გადასცემენ გადამცემი ფიზიკური გარემოთი.

გადამცემი "გარემოს" ტერმინი იხმარება საკომუნიკაციო ქსელში მიმღებ და გადამცემ მოწყობილობებს შორის ინფორმაციის (შეტყობინებების) ფიზიკურად ამსახველი (მატარებელი) სიგნალების აღწერის, მათი გავრცელების მეთოდებისა და საშუალებების დახასიათებისათვის. ნებისმიერი სახის (შინაარსის მქონე) პაკეტი შეიძლება წარმოდგენილი იქნეს სხვადასხვა ფიზიკური ბუნების: ელექტრული, რადიოსიხშირული

ან ოპტიკური სიგნალების სახით. მათი ფიზიკური გავრცელება (გადაადგილება – ელექტრონული ტრანსპორტირება) წარმოებს ასევე შესაბამისი ფიზიკური ხაზებით, რომლებიც ქმნიან ერთ ან მრავალ არხებს (კავშირგაბმულობაში ამის გამო შესაბამისად განასხვავებენ ერთარხიან ან მრავალარხიან გადამცემ სისტემებს).

მრავალი წლის განმავლობაში ინფორმაციის გადამცემ გარემოდ ელექტრონულ კავშირგაბმულობაში ტრადიციულად წარმოადგენდა (და წარმოადგენს ახლაც) საკაბელო სისტემები. ოდნავ მოგვიანებით ფართო გავრცელება ჰპოვა სხვა სახის გადამცემმა გარემოებებმა, სადაც გამოყენებულია რადიოსიხშირული და სინათლის ელექტრო-მაგნიტური ბუნების მქონე ტალღები. ყველაზე მისაღებ ფიზიკურ გარემოდ კომპიუტერული ქსელებისათვის დასაწყისში (და ამჟამად მეტ-ნაკლები ინტენსიურობით) მიიჩნევდნენ კოაქსიალურ და არაკოაქსილურ კაბელებს დამცავი ბადით (ეკრანით) ან მის გარეშე. ეს უკანასკნელი ფაქტიურად წარმოადგენს ჩვეულებრივ გასაჭიმ სატელეფონო სპილენძის წყვილებს. ამგვარი საკაბელო სისტემები თავისი ფიზიკური მახასიათებლების მიხედვით იყოფა კატეგორიებად, რომლებიც დარეგისტრირებული და აღწერილი არიან სტანდარტიზაციის სათანადო დოკუმენტებში.

გარკვეულ სტანდარტულ მოთხოვნებს ექვემდებარება, აგრეთვე, ბოლო წლებში შექმნილი სრულიად ახალი ტექნოლოგიებით დამზადებული ოპტიკურ-ბოჭკოვანი გადამცემი ხაზებიც, რომლებიც უზრუნველყოფენ ქსელის კვანძებს შორის მაღალსი-

ჩქარიან კავშირს ზემოთნახსენები სინათლის ტალღების დახმარებით.

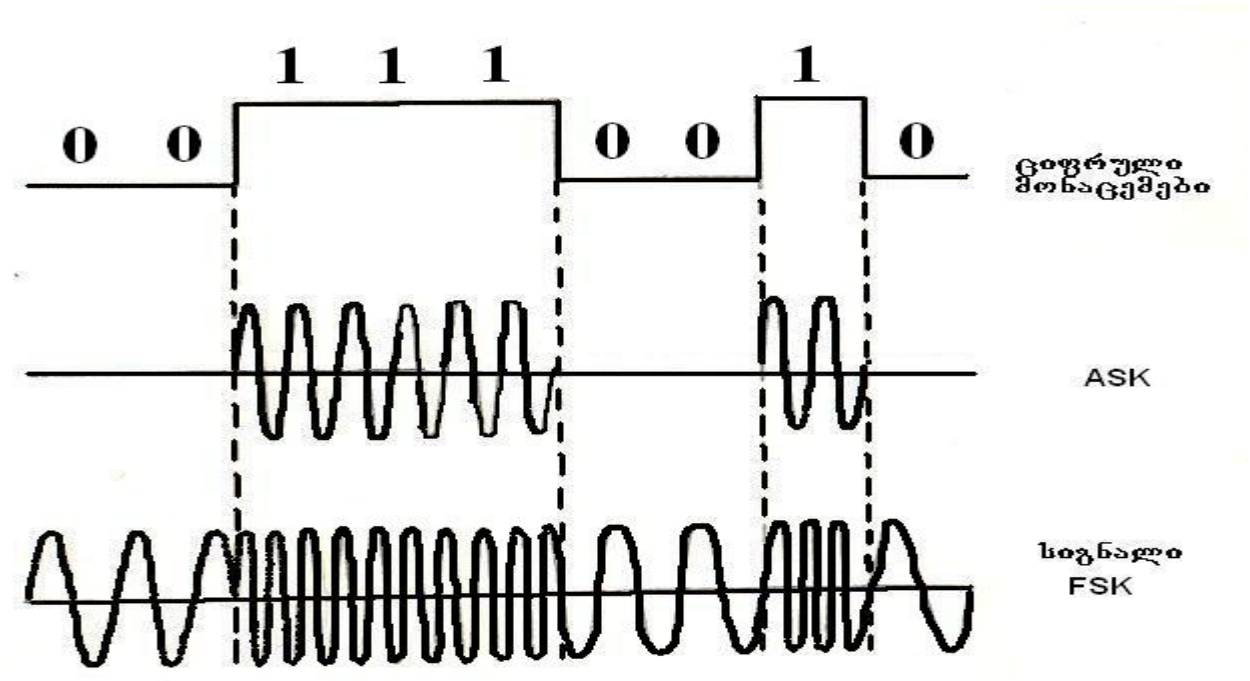
ზოგადად თუ ვიმსჯელებთ, სიგნალების (ნებისმიერი ფიზიკური ბუნების) ფიზიკური გადაცემა და მათი მიღება ყველა სახის საკომუნიკაციო არხებით არც თუ ისე ადვილი საქმეა. მათთან დაკავშირებული პრობლემატური საკითხების გადაწყვეტითაა დაკავებული ძირითადად კავშირგაბმულობის სამსახური, რომლის კვლევის ძირითად მიმართულებას წარმოადგენს სიგნალების კოდირების, გადაცემა-მიღების სიჩქარის გაზრდის მეთოდებისა და საშუალებების დამუშავება, სიგნალების გადამცემი და მიმღები მოწყობილობების მუშაობის სინქრონიზაციის პრობლემების გადაწყვეტა, კავშირის ხაზების (არხების) გამტარუნარიანობის ამაღლება და ა.შ.

განასხვავებენ ანალოგური და დისკრეტული (ციფრული) ბუნების კავშირის ხაზებს, სადაც ინფორმაციის მატარებლად (წარმტანებად) გამოყენებულია მოდულირებული და არამოდულირებული ელექტრონული სიხშირის სიგნალები. ანალოგური ბუნების (რომლის ძირითად მახასიათებელს წარმოადგენს ამპლიტუდა) სიგნალები ტრადიციულად გამოიყენება სატელეფონო კავშირგაბმულობაში, ხოლო კომპიუტერული ქსელებისათვის უპირატესობას სიგნალების წარმოსადგენად და მანძილზე გადასაცემად ძირითადად ციფრულ ფორმას ანიჭებენ.

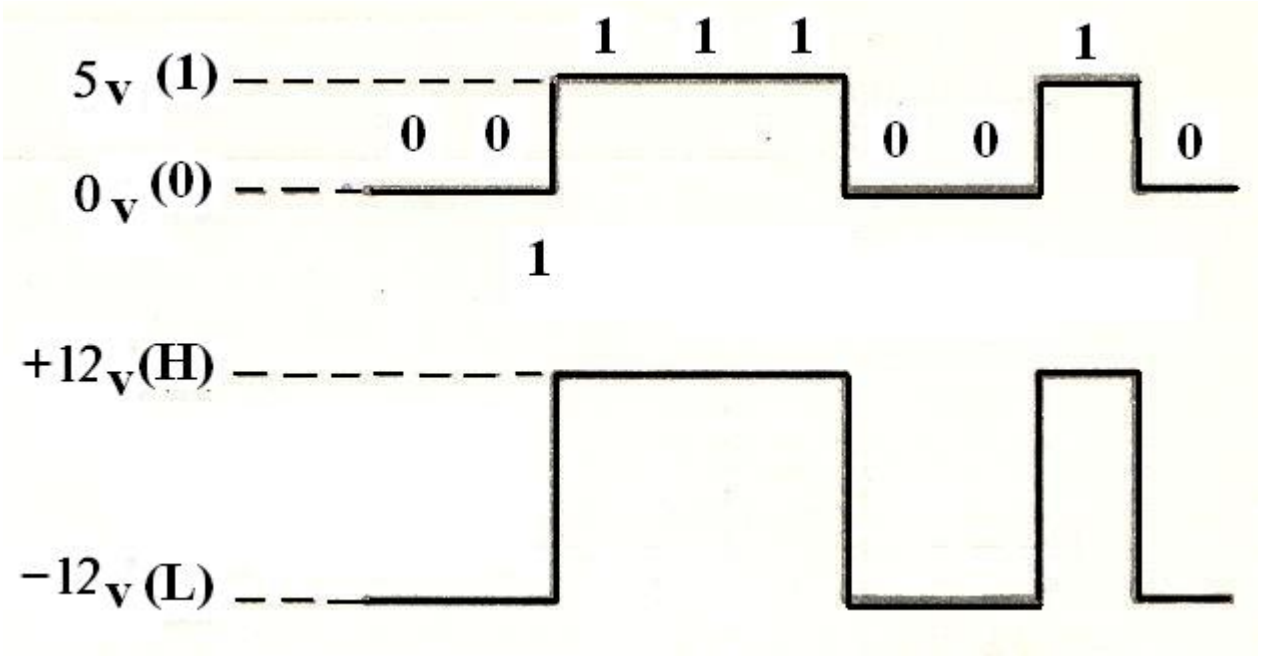
ციფრული ფორმით ელექტრონული შეტყობინებები ფიზიკურად წარმოიდგინება გადამცემ ხაზებში ძაბვების (პოტენციალების) მაღალი (1) და დაბალი (0) დონეების მიხედვით (ხოლო ოპტიკური საშუალებებით მონაცემთა გადაცემის დროს კი –

ოპტიკური სინათლის არსებობით (1) და არარსებობით (0) კავშირის ფიზიკურ ხაზებში). ნებისმიერი შინაარსის მქონე მონაცემები საკომუნიკაციო არხებში გადაიცემა დისკრეტული სიგნალების (1,0) თანამიმდევრობის სახით, რომელთა გარკვეულ სიმრავლეს (შემოფარგლულს დაწყებისა და დამთავრების მაუწყებელი ნიშნებით (ჭდეებით)) პოპულარულ ენაზე ქსელურ ტექნიკაში მოიხსენიებენ როგორც მონაცემთა კადრებს.

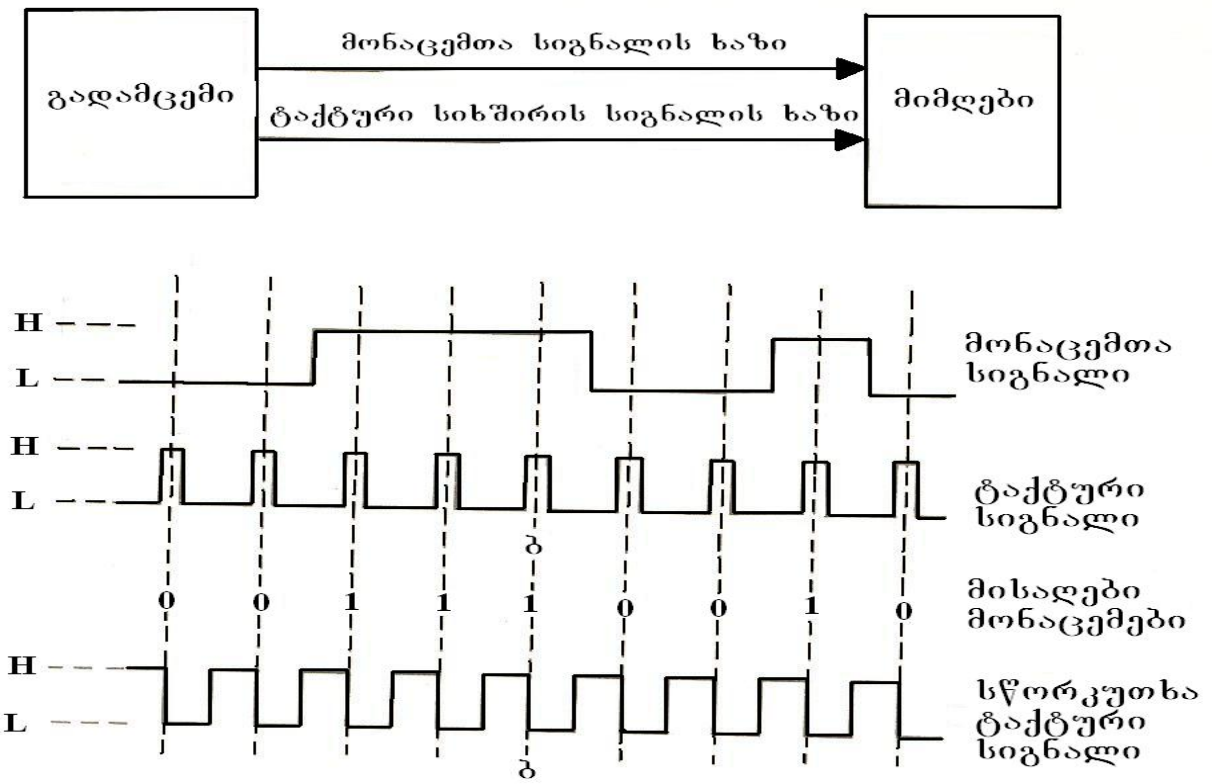
ზემოთ ნახსენები ძაბვების დონეები (1,0), ასევე სინათლის ტალღების არსებობა-არარსებობა (1,0) ცნობილია ორობითი კოდის სახელწოდებით, ხოლო ინფორმაციის წარმოდგენას (1,0) სიგნალების სახით, უწოდებენ ამ ინფორმაციის ციფრულ კოდირებას. კოდირების პრობლემურ საკითხებს შეისწავლის მეცნიერების ერთ-ერთი მიმართულება, რომელსაც იმპულსური ტექნიკა ეწოდება. მონაცემების ანალოგური და ციფრული კოდირების სახეებს ასახავს შესაბამისად ნახ. 5.1 და ნახ. 5.2. ხოლო დისკრეტული სიგნალების კავშირის ხაზებში სინქრონული და ასინქრონული გადაცემის მეთოდების არსი კი ნაჩვენებია შესაბამისად ნახ. 5.3 და ნახ. 5.4-ზე.



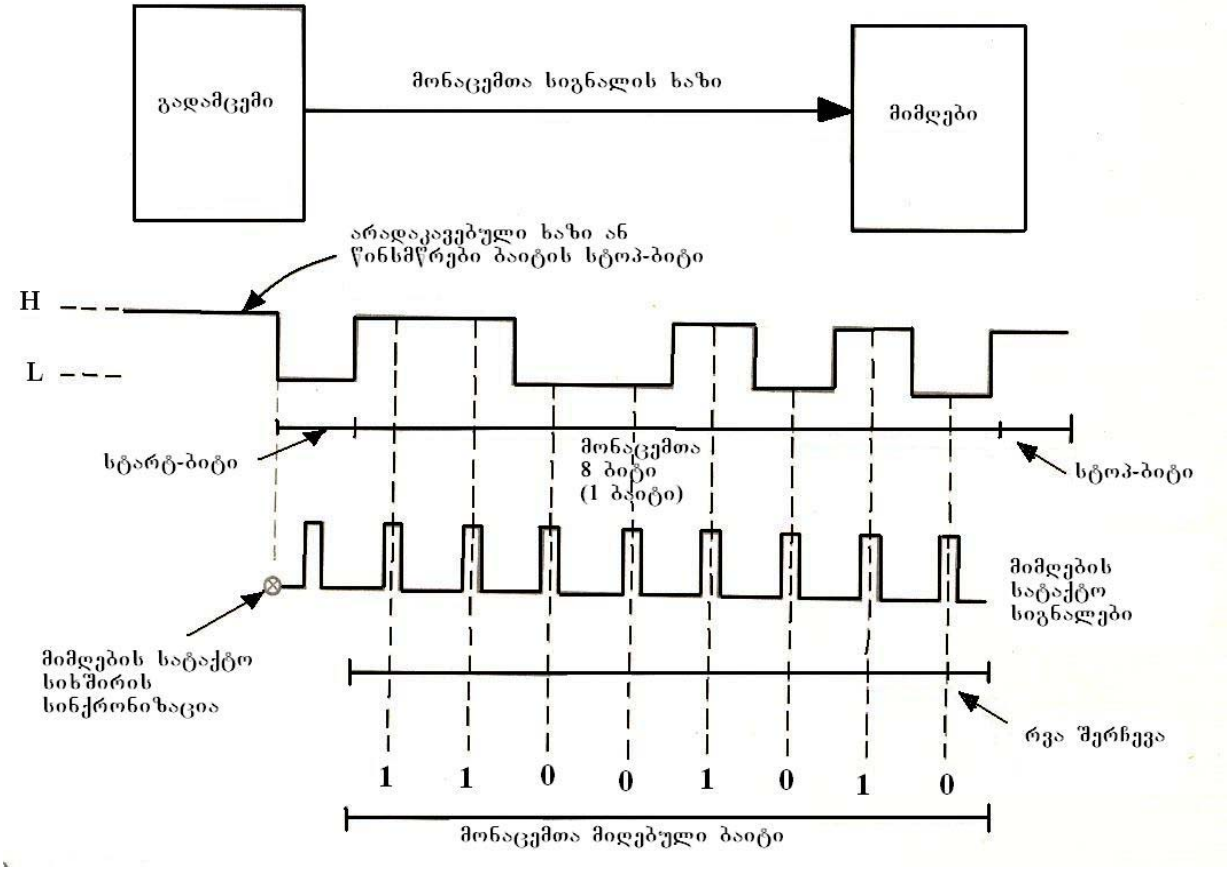
ნახ. 5.1. ციფრული მონაცემების ანალოგური კოდირება



ნახ. 5.2. ციფრული მონაცემების ციფრული კოდირება



ნახ. 5.3. კავშირის ხაზებში სიგნალების სინქრონული გადაცემა



ნახ. 5.4. კავშირის ხაზებში სიგნალების ასინქრონული გადაცემა

კოდირებული ინფორმაციის გადასაცემად ანალოგურ სიგნალებთან მუშაობის დროს გამოიყენება სინუსოიდალური ფორმის ანალოგური წარმტანი სიგნალი (ნახ. 5.1). ციფრულ სიგნალებთან მუშაობის დროს ისევე, როგორც სხვა შემთხვევებში გამოიყენება ორ დონიანი დისკრეტული სიგნალი.

ანალოგური სიგნალების გამოყენების უპირატესობა გამოიხატება იმაში, რომ ისინი ნაკლებად მგრძნობიარე არიან დამახინჯებების მიმართ, რომელიც განპირობებულია გადამცემ გარემოებში სიგნალების მილევადობით. ამასთან მილევადობას განიცდის ანალოგური სიგნალის მხოლოდ ამპლიტუდა, ხოლო სიგნალის ფორმა არ იცვლება. ამიტომ საწყისი სიგნალის აღდგენა პრობლემას არ წარმოადგენს, რომელიც ძლიერდება გამაძლიერებლების მქონე გადამცემ შუალედურ მოწყობილობებში (რეპიტერებში) ან უშუალოდ მიმღებ მოწყობილობებში.

თუ ინფორმაციის გადაცემისათვის გამოიყენება მხოლოდ ანალოგური სიგნალები, საჭიროა მონაცემების გადამცემი და მიმღები მოწყობილობები აღჭურვილი იქნენ სპეციალური მოწყობილობებით – სიგნალების მოდულიატორ-დემოდულიატორებით (მოდემებით). ამგვარად, თუ ინფორმაციის მატარებლად გამოიყენება ანალოგური სიგნალები, მაშინ როგორც აუცილებელი პირობა ციფრული მონაცემები უნდა გარდაიქმნას ანალოგურ ფორმაში. განასხვავებენ ანალოგური სიგნალების მოდულაციის ორ ძირითად სახეს: ამპლიტუდურ და ფაზურ მოდულაციებს. პირველ შემთხვევაში ანალოგურ წარმტან სიგნალს გააჩნია მუდმივი სიხშირე და ცვალებადი დონე (ამპლიტუდა), ხოლო ფაზური მოდულაციის დროს კი წარმტანი

სიგნალი წარმოიდგინება ორი სიხშირით, რომელთაგან ერთი f_1 გამოიყენება ლოგიკური “1”-ის ასახვისთვის, ხოლო მეორე f_2 – ლოგიკური “0”-ის წარმოსადგენად.

ხშირ შემთხვევებში ძალზე მოსახერხებელია წარმტანი სიგნალების წარმოდგენა არა ამპლიტუდებით და ფაზებით, არამედ უფრო მარტივად–სიგნალების დადებითი და უარყოფითი პოტენციალებით (პოლარობით). მაგალითისათვის ციფრული მონაცემების ამგვარი ციფრული კოდირება ნაჩვენებია ნახ. 5.2-ზე.

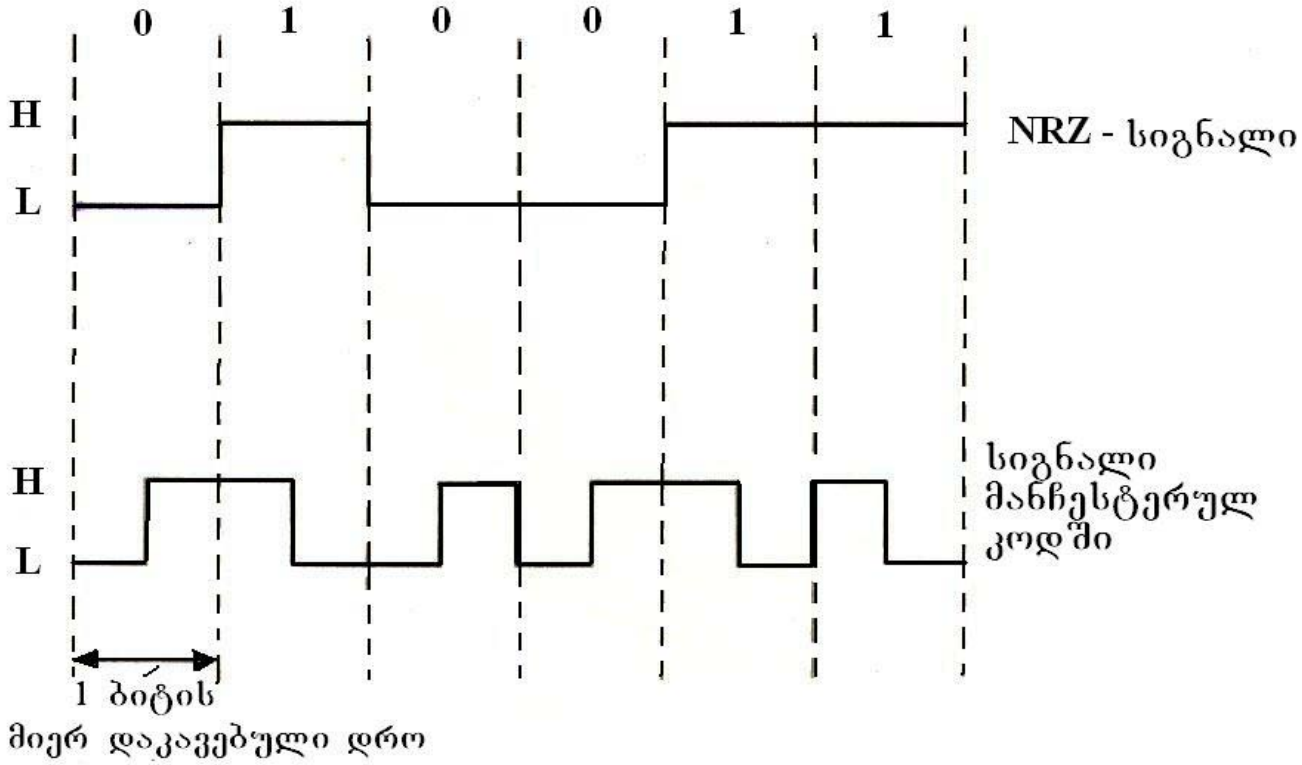
ციფრული სიგნალების (1-იანების და 0-ბის) გადაცემისას არც თუ ადვილია იმის გაგება თუ სად იწყება და სად მთავრდება გადამცემ და მიმღებ კვანძებში გადაცემული და მიღებული სიგნალების ურთიერთ შესაბამისობა. ანუ სხვა სიტყვებით რომ ვთქვათ, საჭიროა მოხდეს კვანძიდან გადაცემული და მიმღებ კვანძში მიღებული სიგნალების სინქრონიზაცია. აქ დღის წესრიგში დგება სიგნალების იმპულსების გადაცემა-მიღებისათვის დროითი ფაქტორების გათვალისწინება. აქედან გამომდინარე განასხვავებენ სიგნალების სინქრონულ (ნახ. 5.3) და ასინქრონულ (ნახ. 5.4) გადაცემებს. პირველ შემთხვევაში (სინქრონული გადაცემისას) გადამცემმა მოწყობილობამ მონაცემთა სიგნალების გარდა უნდა გადასცეს ტაქტური სიხშირის სიგნალებიც, რომლის მიხედვითაც მიმღები იღებს გადაცემული სიგნალების (წყაროდან) სწორად მიღების გარანტიას, ანუ ასევე სხვა სიტყვებით რომ ვთქვათ, სინქრონიზაციის სიგნალები (იმპულსები) ხელს უწყობს ინფორმაციის კორექტულად (სწორად) გადაცემა-მიღებას შესაბამისად გადამ-

ცემში და მიმღებში (კავშირგაბმულობის ტერმინი რომ ვიხმაროთ – მიმღებ-გადამცემ ტრაქტში).

სინქრონიზაციის პრობლემა ადვილი გადასაწყვეტია თუ კი გვექნება ცალკე ხაზი გადამცემ და მიმღებ მოწყობილობებს შორის, მაგრამ ასეთი მიდგომა ეკონომიკური დანახარჯების თვალსაზრისით არამომგებიანია, ამიტომ გადამცემ და მიმღებ მოწყობილობებს შორის სიგნალების სინქრონიზაციისათვის დამატებითი ხაზის გამოყოფის გარეშე გამოიყენება მონაცემთა გადაცემის ორი მეთოდი: ასინქრონული გადაცემა და გადაცემა ე.წ. ავტოგაწყობით.

ასინქრონული გადაცემის დროს (ნახ. 5.4) გადასაცემი ნაკადის ბიტებს (“1”, “0”–ების ერთობლიობას) ყოფენ ფიქსირებული სიგრძის ბლოკებად (ჩვეულებრივ შემთხვევაში ბაიტებად. 1 ბიტი = 8 ბიტს). ამ დროს როგორც გადამცემი, ასევე მიმღები მოწყობილობა აღჭურვილია ტაქტური იმპულსების შიგა გენერატორებით, რომლებიც მუშაობენ ერთ სიხშირეზე. ვინაიდან ამ სიხშირის დაცვა ტექნიკურად მკაცრად ვერ ხერხდება გადამცემი და მიმღები ტრაქტის გენერატორებით, ამიტომ საჭირო ხდება მათი გაწყობა (ხელით ადრეულ პერიოდში, ან ავტომატურად გაწყობა ამჟამად) ერთნაირ სიხშირეზე თითეული ბლოკის (ბაიტის) გადაცემის წინ. ასეთ შემთხვევებში მიმღები მოწყობილობის ტაქტური გენერატორის სინქრონიზაცია მიიღწევა იმის წყალობით, რომ გადასაცემი თითეული ბაიტის (ბლოკის) წინ მას გადამცემიდან ეგზავნება დამატებითი ერთი ბიტი, რომელიც ცნობილია start-bit (“სტარტ–ბიტი”) სახელწოდებით, და ერთი დამატებითი ბიტი,

რომელსაც უწოდებენ stop-bit (“სტოპ–ბიტს”), ამასთან “სტარტ–ბიტი” ყოველთვის ტოლია 0-ის, ხოლო “სტოპ–ბიტი” კი –1-ის. თუ მონაცემების გადაცემა არ სწარმოებს, გადამცემი ხაზი იმყოფება 1-ის მდგომარეობაში, რომელსაც უწოდებენ ხაზის “არდაკავების მდგომარეობას”. გენერატორების ამგვარ ავტომატურ გაწყობას ხელს უწყობს მეთოდი, რომელიც ტექნიკურ ლიტერატურაში ცნობილია ციფრული სიგნალის “მანჩესტერული კოდირებით” (ნახ. 5.5).



ნახ. 5.5. მანჩესტერული კოდირება (ავტოგაწყობით)

ნახ.5.5-დან როგორც ჩანს, მანჩესტერული კოდირების დროს გადასვლები დონეებს შორის სწარმოებს არა მარტო მონაცემთა თითეული ბიტის შუაში, არამედ თვით ბიტებს შორისაც იმ

დროს, როცა ორ მიმდევრობით ბიტს გააჩნია ერთნაირი მნიშვნელობა.

თითეული გადაცემული კადრი ქსელში უნდა შეიცავდეს (ფიქსირებული სიგრძის საკონტროლო ბიტების თანამიმდევრობას, რომელიც ლიტერატურაში ცნობილია "პრეამბულის" სახელწოდებით. პრეამბულას ხშირად უწოდებენ "მზადყოფნის ბიტებს", რომლებიც უზრუნველყოფენ გადასაცემი და მისაღები სიგნალების სინქრონიზაციას. მაგალითად, შეიძლება კადრში გამოყენებული იქნეს პრეამბულის ველი, რომელიც შედგება ერთი ბაიტისაგან. ე.ი. რვა ბიტისაგან: 11111110. ამ შემთხვევაში ბაიტის პირველი შვიდი ბიტი გამოიყენება საწყისი სინქრონიზაციისათვის, ხოლო ბოლო ბიტი (ჩვენს მაგალითში ნაჩვენებ ბაიტში 0-იანი) აცნობებს მიმღებს, რომ პრეამბულა დამთა-ვრდა და მას მოჰყვება უკვე მონაცემთა ბიტები.

კომპიუტერული ქსელებისათვის როგორც ზემოთ აღვნიშნეთ, პრობლემატურია ორი ძირითადი საკითხი, რომლებიც ეხება ქსელის სადგურებს შორის ფიზიკური კავშირის ხაზებში მონაცემთა გადაცემის სიჩქარესა და გადამცემი არხების გამტარუნარიანობას.

გადაცემის სიჩქარის ქვეშ იგულისხმება დისკრეტული სიგნალების (1,0) რაოდენობა (რომელთა ერთობლიობითაც, როგორც აღვნიშნეთ, წარმოიდგინება ნებისმიერი მონაცემები), რომლებიც გადაადგილდება კავშირის ხაზის ერთი წერტილიდან მეორეში (ე.ი. გარკვეულ მანძილზე) დროის რაიმე ერთეულში (ჩვეულებრივად მიღებულია წამი).

გამტარუნარიანობის ქვეშ კი იგულისხმება არხის ხაზის (მაგალითად, კაბელის) ფიზიკური უნარი დროის ერთეულში გაატაროს ზემოთხსენებული სიგნალების რაც შეიძლება მეტი რაოდენობა. ამ უნარს კავშირგაბმულობაში აფასებენ სიდიდით, რომელსაც სიგნალების გატარების სიხშირის ზოლს უწოდებენ. კომპიუტერული ქსელებისათვის მისაღებია ისეთი კავშირის (საკომუნიკაციო) ხაზები, რომლებსაც გააჩნიათ გატარების სიხშირის ფართო ზოლი. როგორც ზემოთ აღვნიშნეთ, ასეთებია ქსელის საკაბელო სისტემები (ძირითადად კოაქსიალური და ოპტიკურ-ბოჭკოვანი კაბელები), თუმცა არც თუ იშვიათად გამოიყენება ჩვეულებრივი სატელეფონო ხაზებიც (გადაცემის შედარებით დაბალი სიჩქარეებისათვის).

რაც შეეხება ჩვენს მიერ ზემოთ ნახსენებ რადიო-სიხშირულ ტალღებს, ისინიც (განსაკუთრებით ბოლო წლებში) საკმაოდ ფართოდ ინერგება კომპიუტერული ქსელების ბოლო ტექნოლოგიებში. მათი გამოყენება მიზანშეწონილია გლობალური ქსელებისათვის, კერძოდ კი თანამგზავრული კავშირებისათვის (პატარა ზომის ლოკალური ქსელების ორგანიზაციისათვის რადიოსიხშირული ტალღები (ე.წ. უგამტარო ქსელებში) ტექნიკურის გარდა, ეკონომიკური მოსაზრებიდან გამომდინარეც, ჯერ-ჯერობით ნაკლებ ეფექტურია (საჭიროა სპეციალური ძვირადღირებული რადიოტალღების მიმღებ-გადამცემები). აქედან გამომდინარე წარმოდგენილი სახელმძღვანელოს აღნიშნულ თავში ძირითადად ყურადღებას გავამახვილებთ კოაქსიალურ და ოპტიკურ-ბოჭკოვან კაბელებზე, რომლებიც უზრუნველყოფენ სიგნალების გადაცემის საკმაოდ მაღალ სიჩქარეებს. წვრილი

კაბელები, მათ შორის სატელეფონო ხაზებიც საკმაოდ ხშირად გამოიყენება ოჯახში, ან მცირე ზომის ქსელის პირობებში ინტერნეტის სატელეფონო ხაზებით მისაღებად (მოდემების დახმარებით). მათი გამოყენება უფრო მიზანშეწონილია ქსელებში ხმის ტრაფიკის სარეალიზაციოდ (როგორც ცნობილია, სატელეფონო ხაზებში ხმა გადაიცემა ანალოგური ფორმით).

იბადება კანონიერი კითხვები რამდენი უნდა იყოს ქსელის გადამცემ არხებში გამოყენებული კავშირის ხაზების რაოდენობა? რომელთა საშუალებითაც თითოეული კომპიუტერი მიუერთდება ქსელს? ხომ არ გამიწვევს ეს კაბელების ზომებისა (პირველ რიგში სიგრძეების) და მათი ღირებულების გაზრდას? რა თქმა უნდა ეს პრობლემა ტექნიკურად გადაუჭრელი დარჩებოდა, თუ კავშირის ხაზებში კომპიუტერებს შორის გამოყენებული იქნებოდა მონაცემების მატარებელი ბიტების პარალელური გადაცემა (როგორც ეს ხდება კომპიტერის შიგნით გადაცემები კვანძებს შორის) ცხადია, იგი გამოიწვევდა გამტარების უსასრულოდ დიდი რაოდენობით გამოყენების საჭიროებას. აქაც გამოიძებნა გამოსავალი. კომპიუტერის შიგნით ელემენტებსა და კვანძებს შორის (ძირითადად არითმეტიკულ მოწყობილობებში და ოპერატიულ მეხსიერებაში) ბიტების პარალელური გადაცემებისგან განსხვავებით (რომლის საშუალებას იძლევა ინტეგრალური ტექნოლოგია), კომპიუტერებს შორის ქსელის საკომუნიკაციო არხებში გამიყენება ინფორმაციის ბიტების მიხედვით გადაცემა, ანუ უფრო ზუსტად, მონაცემების გადაცემა კაბელში ბიტების თანამიმდევრობით. ეს

უკანასკნელი კი მოითხოვს გამტარების მხოლოდ ერთ წყვილს. თუმცა თანამედროვე დაჩქარებული გადაცემების მეთოდების გამოყენების დროს და მაღალსიჩქარიან გიგაბიტიან გადაცემებში კოაქსიალურ კაბელებში (ასევე ოპტიკურ-ბოჭკოვან კაბელებშიც) გამიყენება რამოდენიმე წყვილი (ე.წ. ტვინაქსიალური კაბელები), რომელთა სპეციფიკაციებზე გვექნება საუბარი აღნიშნული თავის მომდევნო პარაგრაფში.

აქვე შეიძლება დაიბადოს მეორე კითხვაც: ხომ არ გამოწვევს ქსელის საკომუნიკაციო კავშირის ხაზებში ბიტების მიმდევრობითი გადაცემა დროით პრობლემებს მონაცემთა მიღება გადაცემაში? აქაც მოიძებნა გამოსავალი, რომელთაგან აღვნიშნავთ სიგნალების გადაცემის ორ ტექნიკურ გადაწყვეტას (მიდგომას).

პირველი მიდგომა ეს არის ერთი და იმავე გამტარში სიგნალების სხვადასხვა სიხშირით გადაცემა, რომელიც წარმოქმნის მრავალარხიანობას. მეორე მიდგომა კი, როგორც ზემოთ იქნა აღნიშნული, ეს არის სიგნალების გადამცემებისა და მიმღებების ურთიერთ სინქრონიზაცია, რაც ნიშნავს იმას, რომ შეიძლება გადაცემული სიგნალები იყოს მრავალი (ერთ გამტარში), მაგრამ არხის ბოლოს ესა თუ ის მიმღები მიიღებს მხოლოდ იმ სიგნალებს, რომლებსაც გადასცემს ის გადამცემი მოწყობილობა, რომელიც სინქრონიზირებულია მიმღებ კონკრეტულ მოწყობილობასთან.

კომპიუტერულ ქსელებში მონაცემების ურთიერთ გაცვლის პროცედურებს აწარმოებენ სპეციალური აპარატურულ-პროგრა-

მული საშუალებებით, რომლებსაც ქსელური ადაპტერები ეწოდება.

5.2. მონაცემთა მიმღებ-გადამცემი კომპიუტერული ქსელების ფიზიკური დონის საკაბელო სისტემები

მონაცემთა გადამცემა-მიღება კომპიუტერული ქსელებში სწარმოებს საერთაშორისო სტანდარტით მიღებული შვიდდონიანი OSI-ეტალონური მოდელის ყველაზე დაბალ, პირველ დონეზე, რომელშიც უმეტეს შემთხვევაში იგულისხმება ფიზიკურად გაყვანილი საკაბელო სისტემები, აღჭურვილი საინფორმაციო სიგნალების გადამცემი და მიმღები მოწყობილობებით. ხატოვან გამოთქმას თუ ვიხმართ, საკაბელო სისტემა წარმოადგენს ნებისმიერი ტიპისა და დანიშნულების კომპიუტერული ქსელის სასიცოცხლო არტერიას. იგი (საკაბელო სისტემა) ქმნის ქსელში საკომუნიკაციო დამაკავშირებელ გარემოს, რომლითაც ელექტრონულად გადაადგილდებიან (ტრანსპორტირდებიან) მონაცემთა პაკეტები წყარო-კომპიუტერიდან მიმღები-კომპიუტერისაკენ გამგზავნი კომპიუტერის მიერ გაგზავნილ პაკეტში მიმღები კვანძის მისამართის მითითებით. კომპიუტერულ ქსელში საკაბელო სისტემა ქსელში ჩართული კომპონენტების მიმართ კონფიგურირებული უნდა იყოს კორექტულად პაკეტების ეფექტურად გადაცემა-მიღების მოსაზრებიდან გამომდინარე, რაც ნიშნავს პაკეტების ჩაბარებას (გადამცემი კვანძის მიერ დანიშნულების ადგილას – მიმღებ

კომპიუტერამდე) მინიმალური დროის ინტერვალში, რომლითაც ფასდება ქსელის სწრაფქმედება, ინფორმაციის გადაცემის მაქსიმალური საიმედოობით (იგულისხმება უპირველეს ყოვლისა შეცდომების გარეშე). კომპიუტერული ქსელის არასწორად კონფიგურირების დროს ეს მოთხოვნები არ სრულდება, ანდა სრულდება არადამაკმაყოფილებლად. ჯერ ერთი ქსელის მუშა სადგურები იმუშავებენ არაეფექტურად და მეორეც – რაც შეეხება ქსელის დატვირთვის (შესაბამისად მისი წარმადობის შეფასების) გაზომვას, იგი გადაიქცევა უაზრო საქმიანობად, ვინაიდან ან ტრაფიკი არ გვექნება საერთოდ (გავიხსენოთ, რომ ტრაფიკის ქვეშ ვგულისხმობთ საკაბელო სისტემის დატვირთვის დონეს პაკეტების საინფორმაციო (ან სამომსახურეო) შინაარსის ამსახველი სიგნალებით), ან თუ მაინც გვექნება რაიმე სტატისტიკა ქსელის დატვირთვის შესახებ, იგი იქნება საკმაოდ არასწორი.

ამგვარად, საკაბელო სისტემა ფიზიკურად აკავშირებს ქსელის მთავარი კომპონენტების განუყოფელ წყვილს პაკეტების გამგზავნ და მიმღებ კომპიუტერებს, რომლებსაც ხშირად მოიხსენიებენ როგორც ჰოსტის კომპიუტერებს, რომლებიც ურთიერთქმედებენ ერთმანეთთან კავშირის სეანსის განმავლობაში.

აღნიშნულ თავში საკაბელო სისტემები მიმოვიხილოთ მათი Ethernet-ის ქსელში გამოყენების მიზანშეწონილობებიდან გამომდინარე. ამ მხრივ არჩევანი ძალზე მრავალფეროვანია და მოიცავს სულ მცირე 200 დასახელების სპეციფიკაციას. ისინი ერთმანეთისაგან განსხვავდებიან როგორც ფიზიკური მახასიათე-

ბლებით (მათ შორის გეომეტრიული პარამეტრებით, როგორიცაა კაბელის სიგრძე, სიგანე მასში გამავალი სპილენძის გამტარის დიამეტრი, გამტანუნარიანობა, კონსტრუქციული თავისებურება, დამცავი ეკრანის არსებობა – არარსებობა), ასევე მათი საშუალებით გადაცემული სიგნალების ფიზიკური ბუნებით. ფიზიკურ ბუნებაში იგულისხმება, მაგალითად, კოაქსიალურ კაბელში გამავალი სიგნალის ელექტრონული სახე, ხოლო ოპტიკურ-ბოჭკოვან კაბელში – გამავალი სიგნალის ოპტიკური სახე. ამ და ასევე სხვა კონსტრუქციული და დამზადების ტექნოლოგიური პარამეტრების შესაბამისად, განსხვავებები არსებობს მათ ღირებულებაშიც. აქვე შევნიშნოთ, რომ კაბელების დამზადების ტექნოლოგიების ღირებულებიდან გამომდინარე ჯერ-ჯერობით ოპტიკურ–ბოჭკოვანი კაბელები შედარებით კვლავ ძვირადღირებულია ვიდრე დანარჩენი სხვა სახის კაბელები. ჩვენ ძირითადად ყურადღება გავამახვილოთ, როგორც ზემოთ აღვნიშნეთ, Ethernet –კომპიუტერული ქსელების საკაბელო სისტემებზე.

Ethernet 802.3 სტანდარტი მოიცავს სხვადასხვა ტიპის კაბელების აღწერას. ისინი გამოსადეგი არიან ისეთი ქსელების ფიზიკური რეალიზაციისათვის, რომლებიც მუშაობენ ქსელში შეღწევის CSMA/CD მეთოდით (აღნიშნული შემოკლება გაშიფრული გვქონდა ზემოთ განხილულ პარაგრაფებში).

ისტორიულად Ethernet-ის პირველი ქსელები შექმნილი იყვნენ კოაქსიალურ კაბელებზე (დამცავი ეკრანით). შემდგომში განსაზღვრულ იქნა ქსელის ფიზიკური დონის სხვა სპეციფიკა-

ციებიც, ორიენტირებული ძირითადად Ethernet-ის სტანდარტისათვის. პარამეტრები ძირითადად რჩებოდა ერთი და იგივე 10 მბიტი/წმ-იანი სიჩქარის Ethernet-ის ტექნოლოგიის ფიზიკური გარემოს ნებისმიერი სპეციფიკაციისათვის.

ამჟამად არსებობს საკაბელო მეურნეობაში ძალზე დიდი არჩევანი. დღეს-დღეობით მაინც ფართო ექსპლუატაციაში რჩება Ethernet – ტექნოლოგიის ისეთი სპეციფიკაციები, რომლებიც მოიცავენ მონაცემთა გადამცემ შემდეგ გარემოებს (კაბელებს):

— 10 Base 5. იგი წარმოადგენს კოაქსიალურ კაბელს, რომლის დიამეტრია 0,5 დიუმი და გააჩნია ტალღური წინაღობა 50 ომი. აღნიშნული ტიპი ცნობილია, როგორც "სქელი" ინტერნეტ-კაბელი;

— 10 Base 2. ამ სპეციფიკაციის კაბელიც კოაქსიალური ტიპისაა (დამცავი "მოწნული" ეკრანით, დიამეტრია 0,25 დიუმი. კაბელის ტალღური წინაღობაა იგივე, რაც 10 Base 5-ში – 50 ომი);

— 10 Base T – კაბელი, რომელიც კონსტრუქციულად შესრულებულია არაეკრანირე-ბულ გასაჭიმ წყვილზე. კაბელის ამგვარი ტიპი ხშირად გამოიყენება კონცენტრატორზე აგებული ვარსკვლავისმაგვარი ტოპოლოგიის ასაგებად.

— 10 Base F (ინდექსით, რომელიც იწყება ასო F –ით (F – Fiber), ნიშნავს ოპტიკურს).

ამგვარი სპეციფიკაციები წარმოადგენენ ოპტიკურ-ბოჭკოვან კაბელებს. ისინი ქმნიან 10 მეგაბიტი/წმ სიჩქარის ქსელს (ციფრი 10 ამ შემთხვევაში მიუთითებს კაბელის 10 მეგაბიტი/წმ

გამტარუნარიანობას), ანალოგიურად 10 Base T –სტანდარტი-სა. არსებობს ამ სპეციპიკაციების რამოდენიმე ვარიანტი, მაგალითად:

—— FOIRL (მოქმედების მანძილი 1 კმ-მდე);

—— 10 Base FL (მოქმედების მანძილი 2 კმ-მდე);

—— 10 Base FB (მოქმედების მანძილი ასევე 2 კმ-მდე).

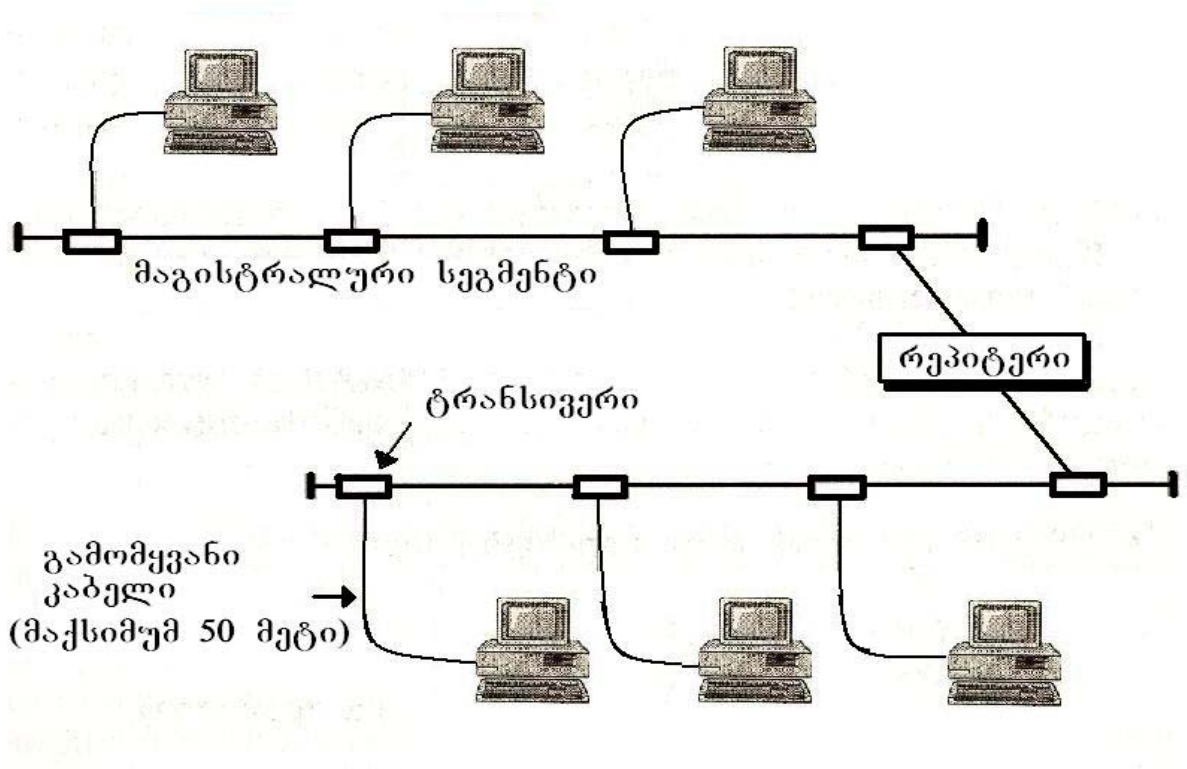
მოკლედ დავახასიათოდ თვითეული მათგანი, მათი გეომეტრიული სიგრძეებისა და მათზე მიერთებული მუშა სადგურების დასაშვები რაოდენობის მიხედვით.

სპეციფიკაცია 10 Base 5

“სქელი” კოაქსიალური კაბელი გამოიყენება ქსელებში (რეაზებული 10 Base 5 სპეციფიკაციის პარამეტრების დაცვით), ძირითადი მაგისტრალებისა და ამ მაგისტრალებიდან განშტოებებზე მუშა სადგურების (მომხმარებელთა პერსონალური კომპიუტერების) მისაერთებლად. მაგალითის სახით ასეთი გაყვანილობის საკაბელო სისტემა ნაჩვენებია ნახ. 5.7-ზე.

მიუხედავად გაყვანილობაში გარკვეული სიძნელეებისა (10Base 5 კაბელი საკმაოდ უხეშია), ასეთი საკაბელო სისტემა საშუალებას იძლევა შეიქმნას საკმაო სიგრძის ქსელის სეგმენტები. ქვემოთ ჩამოთვლილია 10Base 5 სპეციფიკაციის ძირითადი შეზღუდვებია:

—— სეგმენტიდან გამომყვანების რაოდენობა (ფაქტიურად ასეთი ტიპის კაბელიდან განშტოებების რიცხვი) – 100;



ნახ. 5.7. საკაბელო სისტემა მსხვილ კოაქსიალებზე 10 Base 5

— კვანძების დაყოფა არაუმეტეს 5 სეგმენტისა და 4 რეპიტერის;
— სეგმენტის მაქსიმალური სიგრძე (გადაბმის გარეშე) – 500 მეტრი;
— ქსელის საერთო სიგრძე – 2500 მეტრი;
— ტრასივერებს შორის მინიმალური მანძილი – 2,5 მეტრი;
— ტრანსივერული კაბელის მაქსიმალური სიგრძე – 50 მეტრი;

ასეთი ტიპის კაბელს სადგური უნდა მიუერთდეს მიმღებ–გადამცემების – ტრანსივერის დახმარებით. ტრანსივერი ყენდება უშუალოდ კაბელზე და იკვებება კომპიუტერული ქსელური ადაპტერებიდან. თანამედროვე ტექნოლოგია საშუალებას იძლევა ტრანსივერი მიერთებული იქნეს კაბელზე, როგორც გახვრეტის მეთოდით, რომელიც უზრუნველყოფს უშუალო ფიზიკურ კონტაქტს, ასევე უკონტაქტო მეთოდითაც.

ტრანსივერი ასრულებს შემდეგ ფუნქციებს:

— მონაცემთა მიღებასა და გადაცემას კაბელიდან კაბელზე;

— კაბელზე კოლიზიის განსაზღვრას (აღმოჩენას);

— ელექტრულ განმხოლოებას (განცალკევებას) კაბელსა და ადაპტერის დანარჩენ ნაწილებს შორის;

— კაბელის დაცვას ადაპტერის არაკორექტული მუშაობისგან;

სტანდარტი 10 Base 5 იძლევა შესაძლებლობას ქსელში გამოყენებული იქნეს სპეციალური მოწყობილობა – გამმეორებელი (repeator). გამმეორებელი, ე.ი. რეპიტერი (ნახ. 5.7) გამოიყენება ერთ ქსელად კაბელის რამოდენიმე სეგმენტის გასაერთიანებლად, ზრდის რა ამით ქსელის საერთო სიგრძეს (ქსელის გეომეტრიულ ზომას).

გამმეორებელი იღებს სიგნალებს კაბელის ერთი სეგმენტიდან და ბიტების მიხედვით სინქრონულად იმეორებს, ე.ი. აწარმოებს მათ გადაცემებს სხვა სეგმენტში, ამასთან ერთად ახდენს ასევე იმპულსების სინქრონიზაციას. იგი შედგება ორი (ან რამოდენიმე) ტრანსივერისაგან, რომლებიც მიუერთდება კაბელის სეგმენტებს, ასევე გამმეორებლის ბლოკს თავის ტაქტურ გენერატორთან ერთად. თითოეული გამმეორებელი მიუერთდება სეგმენტს ერთი თავისი ტრანსივერით. 10Base 5 კაბელით წარმოქმნილ სეგმენტებზე შესაძლებელია, მაგალითად, 99 პერსონალური კომპიუტერის მიერთება. ასეთი კაბელით აგებულ ქსელში განაპირა (ჰოსტის) კვანძების მაქსიმალური რიცხვი შეიძლება იყოს 99 x 3 = 297 კვანძი.

10Base 5 სტანდარტის კაბელის დადებითი მხარეებია:

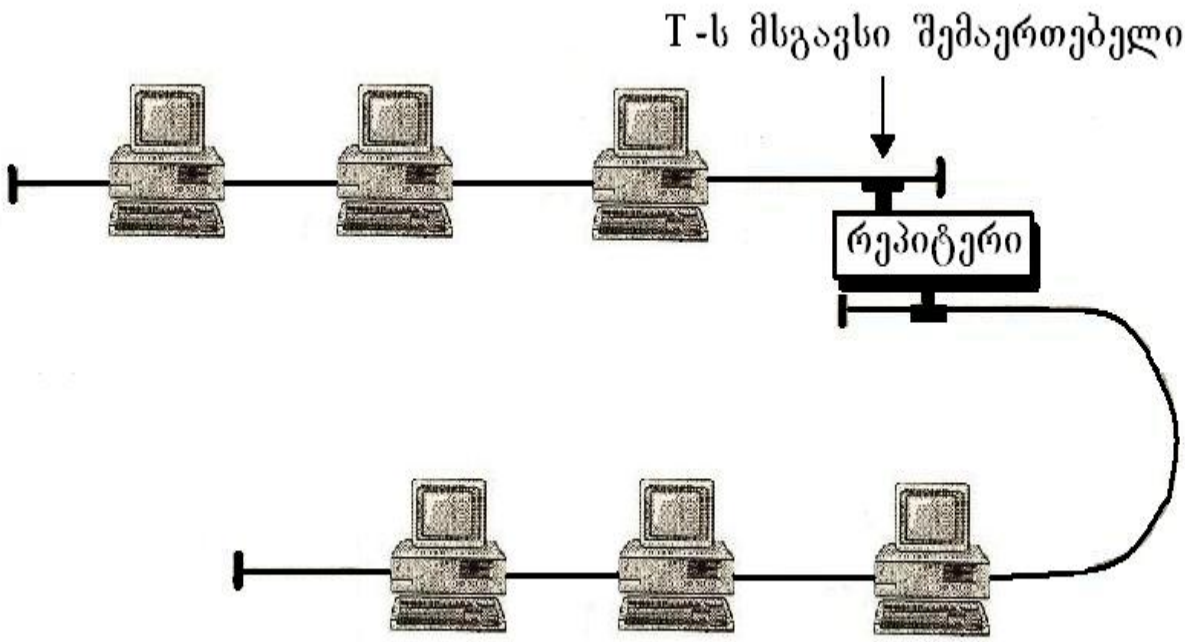
— გარე ზემოქმედებებისაგან კაბელის კარგი დაცვის უნარიანობა (კარგი მდგრადობა გარედან მოქმედი ხელისშემშლელების მიმართ) ;
— საკმაოდ დიდი მანძილი კვანძებს შორის;
— მარტივი, ადვილად გადაადგილების შესაძლებლობა მუშა სადგურებისა კაბელის სიგრძის საზღვრებში.

10Base 5 სტანდარტის კაბელის ნაკლოვანებებია:

— კაბელის საკმაოდ მაღალი ღირებულება;
— გაყვანილობის სირთულე კაბელის სიხისტის (არამოქნილობის) გამო;
— კაბელის გასაყვანად სპეციალური ინსტრუმენტების საჭიროება;
— ჩერდება მთელი ქსელი კაბელის დაზიანების ან ცუდი შეერთების გამო.

სპეციფიკაცია 10 Base 2

ქსელებში, რომლებიც რეალიზებულია 10Base 2 სპეციფიკაციის შესაბამისად, გამოიყენება წვრილი კოაქსიალური კაბელი (ნახ. 5.8). ასეთ ქსელებს ხშირად უწოდებენ **Chipearnet** ქსელებს. ამ სპეციფიკაციის თანახმად დაუშვებელია მუშა სადგურებისაკენ გამომყვანების გამოყენება. ამის მაგივრად სადგურები მიუერთდება უშუალოდ ძირითად მაგისტრალს T – მსგავსი შემაერთებლებით (იხ. ნახ. 5.8).



ნახ. 5.8 საკაბელო სისტემა 10Base 2 წვრილ კოაქსიალურ კაბელზე

ქვემოთ ჩამოთვლილია 10Base2 სპეციფიკაციის ძირითადი შეზღუდვები:

— განშტოებების მაქსიმალური რიცხვი – 30 ;

— კვანძების დაყოფა არა უმეტეს – 5 სეგმენტად და 4 რეპიტერად ;

— სეგმენტის მაქსიმალური სიგრძე – 185 მეტრი ;

— ქსელის სართო სიგრძე – 925 მეტრი ;

— ტრანსივერებს შორის მინიმალური მანძილი – 0.5 მეტრი.

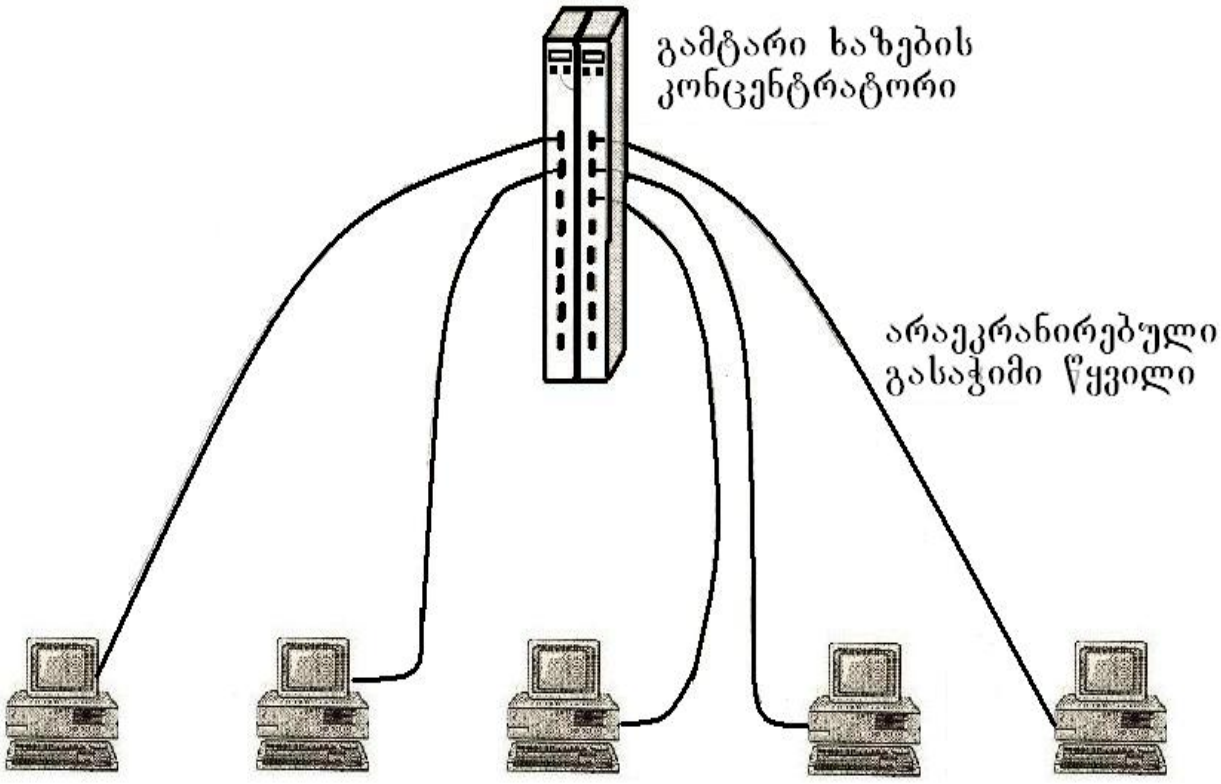
წვრილი კოაქსიალური კაბელის 10Base2 ღირებულება უფრო იაფია, ვიდრე სქელის (ამის გამოა, რომ ასეთ კაბელს უწოდებენ **Chipear** - უფრო იაფი). სამაგიეროდ "წვრილი" 10Base2 –ს "სქელ" 10Base5 – თან გააჩნია უფრო დაბალი მაჩვენებელი ხელისშემშლელების მიმართ მდგრადობის მხრივ, დაბალი

მექანიკური სიმტკიცე და სიგნალების გატარების უფრო ვიწრო ზოლი. ასეთი ტიპის კაბელის დაზიანება შესამჩნევი ხდება მაშინვე (ქსელი წყვეტს მუშაობას). მწყობრიდან გამოსული კაბელის მონაკვეთის მოსაძებნად საჭიროა სპეციალური ხელსაწყო – კაბელის ტესტერი.

სპეციფიკაცია 10 Base T

სპეციფიკაცია 10BaseT 802.3 სტანდარტს დაუმატეს 1991 წლის ბოლოს. იგი წარმატებით მუშაობს ქსელში შეღწევის CSMA CD მეთოდთან "ვარსკვლავის" ტიპის ტოპოლოგიით. გაყვანილობისათვის გამოიყენება გამტარების არაეკრანირებული გასაჭიმი წყვილი, ე.ი. ასეთი ტიპის კაბელი ძალზე წააგავს ჩვეულებრივი სატელეფონო გამტარების წყვილს. ასეთი ტიპის კაბელების გამოყენება სადგურების (მომხმარებელთა კომპიუტერების) შესაერთებლად ქსელის კონცეტრატორთან ნაჩვენე-ბია ნახ. 5.9-ზე.

10BaseT-ს სპეციფიკაცია მოდულურობის თვისებებითა და თავისი სიიაფით ამჟამად ძალზე პოპულარულია Ethernet – ქსელების აგების დროს. თუ გავაანალიზებთ 10Base2 და 10Base5, მათ შორის მეტად მნიშვნელოვანი განსხვავებებია. 10BaseT სპეციფიკაციის თანახმად კაბელი ქმნის სეგმენტს, რომელიც აერთებს მუშა სადგურსა და კონცენტრატორს, ამიტომ თითოეულ სეგმენტთან შეიძლება მიუერთდეს მხოლოდ ორი მოწყობილობა (სადგური და ხაზების გაერთიანების მოწყობი-ლობა – კონცენტრატორი).



ნახ.5.9. საკაბელო სისტემა არაეკრანირებულ გასაჭიმ 10 Base T წყვილზე

ქვემოთ ჩამოთვლილია 10 Base T-ს ძირითადი შეზღუდვები:

— კვანძების მაქსიმალური რაოდენობა ერთ სეგმენტზე – 2;
— ერთ მიმდევრობაში კონცეტრატორების რიცხვი არაუმეტეს 4;
— კვანძების დაყოფა არა უმეტეს 5 სეგმენტისა და 4 რეპიტერის;
— კონცეტრატორსა და მუშა სადგურს შორის მაქსიმალური მანძილი – 100 მეტრი;

10Bas T კაბელით აგებულ ქსელზე ჩართული სადგურების რაოდენობა შეადგენს 1024 ზღვრულ მნიშვნელობას. ეს ნიშნავს იმას, რომ ამისათვის საჭიროა შეიქმნას ქსელში კონცეტრა-

ტორების ორდონიანი იერარქია და დაბალ დონეზე კონცენტრატორებს გააჩნდეს პორტების საერთო რაოდენობა 1024.

10BaseT კაბელზე აგებული ქსელის მაქსიმალური სიგრძე შეადგენს 2500 მეტრს, რაც იგულისხმება ის, რომ ასეთი მაქსიმალური მანძილია დასაშვები ქსელის ნებისმიერ ორ ბოლო კვანძს შორის (ე.ი. ნებისმიერ ორ ჰოსტს შორის).

10 Base F სერიის სპეციფიკაციები

10 მეგაბიტიანი სიჩქარის მონაცემთა გადამცემი Ethernet – ქსელის საკაბელო სისტემად შესაძლებელია ასევე გამოყენებული იქნეს კაბელები რომლებიც დამზადებულია ოპტიკურ ბოჭკოზე. სპეციფიკაციებში, როგორც ზემოთ შევნიშნეთ, ასეთი ტიპის კაბელების ციფრული მიმანიშნებელი საერთო ასოა F (ინგლისური სიტყვიდან – Fiber). ერთი კილომეტრის სიგრძის ასეთი კაბელის გატარების ზოლი შეადგენს 500–800 მგჰც-ს. უფრო მაღალსიჩქარიან ქსელებში გამოიყენება შედარებით უფრო ძვირადღირებული ერთ–მოდიანი ან მრავალმოდიანი ოპტიკური ბოჭკო, რომლის გატარების ზოლი (ოპტიკური ფორმით წარმოდგენილი სიგნალებისთვის) შეადგენს რამოდენიმე გიგაჰერცს. ასეთი ტიპის კაბელები მოითხოვენ გამოყენებული იქნეს ტრანსივერების სპეციალური ტიპი (მუშა სადგურების სეგმენტების მისაერთებლად).

Ethernet ქსელი, აგებული ოპტიკურ კაბელზე მოითხოვს იმავე ელემენტების გამოყენებას, რასაც მოითხოვს 10BaseT ტიპის კაბელზე აგებული ქსელი. ეს ელემენტებია ქსელური ადაპტერე-

ბი (ოღონდ მორგებული ოპტიკურ-ბოჭკოვან კაბელთან სამუშაოდ), მრავალპორტიანი გამმეორებლები (ე.ი. რეპიტერები მრავალი შესასვლელ – გამოსასვლელებით და ა.შ.).

ისევე როგორც გასაჭიმი წყვილის შემთხვევაში, ადაპტერის გამმეორებელთან შესაერთებლად გამოიყენება ორი ოპტო-ბოჭკო. ერთი აერთებს ადაპტერის გამოსასვლელს გამმეორებლის შესასვლელთან (Tx – Rx), ხოლო მეორე ადაპტერის შესასვველს გამმეორებლის გამოსასვლელთან (Rx – Tx).

სტანდარტი FOIRL (Foirl – Fiber-Optic inter-repeator link) წარმოადგენს Ethernet 802.3 კომიტეტის პირველ სტანდარტს ოპტიკური ბოჭკოს გამოსაყენებლად. იგი გარანტირებულად უზრუნველყოფს ოპტიკურ ბოჭკოვანი კავშირის სიგრძეს (გამმეორებლებს შორის) ერთ კმ–მდე ქსელის 2500 მეტრამდე საერთო სიგრძის დროს, ასეთი ტიპის კაბელების გამოყენებისას ქსელის ნებისმიერ კაბელებს შორის გამმეორებლის მაქსიმალური რიცხვია 4.

სტანდარტი 10BaseFL წარმოადგენს FOIRL სტანდარტის უმნიშვნელო გაუმჯობესებას. გადამცემების სიმძლავრის გაზრდისას შესაძლებელია კვანძსა და კონცეტრატორს შორის მანძილი გაიზარდოს 2000 მეტრამდე. დანარჩენი პარამეტრები იგივე აქვს, რაც სტანდარტ FOIRL – ს.

სტანდარტი 10BaseFB განკუთვნილია მხოლოდ გამმეორებლების შესაერთებლად. ბოლო კვანძებს არ შეუძლიათ გამოიყენონ ეს სტანდარტი კონცენტრატორის პორტებთან მისაერთებლად. ქსელის კვანძებს შორის შესაძლებელია დაყენდეს 5-მდე

გამმეორებელი ერთი სეგმენტის 2000 მეტრამდე მაქსიმალური სიგრძის დროს, რაც ზრდის ქსელის მაქსიმალურ სიგრძეს 2740 მეტრამდე.

საკაბელო სისტემების მაღალსიჩქარიანი სპეციფიკაციები

ჩვენს მიერ ზემოთ ნახსენები საკაბელო სისტემები განხილული იყო ძირითადად 10 მბიტი/წმ სიჩქარის კაბელების მოთხოვნებიდან გამომდინარე. ამჟამად, კორპორაციულ ქსელებში ფართოდ ინერგება კლიენტ-სერვერული მონაცემების ურთიერთგაცვლის უფრო მაღალი სიჩქარის მქონე ტექნოლო-გიებიც, რომლებიც ცნობილია Fast Ethernet (100 მბიტი/წმ) და Gigabit Ethernet (1000 მბიტი/წმ) სახელწოდებით. აღნიშნული ტექნოლოგიები წარმოადგენს ყველა Ethernet-ტექნოლოგიების ლოგიკურ განვითარებას.

მაღალსიჩქარიან ქსელურ ტექნოლოგიებზე გადასვლა განპირობებულია ძირითადად ორი მიზეზით. პირველი ეს არის ქსელის მომხმარებელთა რაოდენობის არნახული ზრდა და მეორე – კორპორაციული მაღალი მოთხოვნები საკუთრივ საკაბელო სისტემების გამტანუნარიანობის ამაღლებაზე, გამომდინარე მის წინაშე არსებული სპეციფიკური ამოცანებიდან. ეს ამოცანები საჭიროებენ მონაცემების კვანძებს შორის ურთიერთგაცვლებს გაცილებით მეტი სიჩქარით, ვიდრე ამას უზრუნველყოფდა ზემოთ განხილული 10 მბიტ/წმ სიჩქარის გატარების ზოლის მქონე საკაბელო სისტემები.

100 მბიტი/წმ სიჩქარიანი გადაცემის საჭიროება გაჩნდა ჯერ კიდევ წინა საუკუნის 90-იან წლებში. მას ადასტურებს საერთაშორისო საკვლევო კომპანიის International Data Corporation (IDC) მიერ გამოქვეყნებული მონაცემები, რომლთა მიხედვითაც ჯერ კიდევ 1997 წელს 118 მილიონი ქსელთან მიერთებული მომხმარებელთა პერსონალური კომპიუტერები, მუშა სადგურები და სერვერები მოითხოვდნენ მაღალ სიჩქარიან ტექნოლოგიებზე გადასვლას. ამ პერიოდისათვის ფართოდ დაინერგა ისეთი მაღალ სიჩქარიანი ქსელური ტექნოლოგიები, როგორიც იყო FDDI და 100G-AnyLAN. თუმცა ამ კუთხით ქსელურ სპეციალისტებს მოუხდათ გარკვეული ტექნიკური სიძნელეების გადალახვა. პირველ რიგში ეს იყო ქსელის სეგმენტების გამოყენების შეზღუდვები მონაცემთა გადაცემა-მიღების მაღალი სიჩქარეების დროს. ქსელში შეღწევის CSMA/CD მეთოდის გამოყენებისას სიჩქარეთა გაზრდა იწვევდა კოლიზიების რაოდენობის გაზრდასაც და ამასთან ერთად ქსელის ჰოსტის კვანძებს ამ მეთოდის შესაბამისი პროტოკოლებით ასევე სწრაფად უნდა გამოეცნოთ ისინი და მოეხდინათ კოლიზიების შედეგად დამახინჯებული კადრების განმეორებითი, ხელახალი გადაცემების ეფექტური ორგანიზაცია. დღეისათვის არსებული სტანდარტებით საჭიროა, რომ კადრის გადაცემის დრო ყოველთვის უნდა იყოს მეტი Ethernet – სეგმენტით სიგნალის ორმაგი გარბენის დროის ხანგრძლივობაზე. ეს უკანასკნელი ქსელის სეგმენტების მიმართ წარმოქმნის გარკვეულ შეზღუდვებს მათი მაქსიმალური გეომეტრიული

ზომების (მაქსიმალურად დასაშვები სიგრძეების) მიმართ. სიგნალების გავრცელების დრო შეზღუდულია სინათლის გავრცელების სიჩქარით (ოპტიკურ-ბოჭკოვან კაბელში). მაგალითად Ethernet-ის სეგმენტის მაქსიმალური სიგრძე 10 მბიტი/წმ ბიტური სიჩქარის დროს შეადგენს დაახლოებით 2500 მეტრს. თუ ამ ბიტურ სიჩქარეს გავზრდით 10-ჯერ (ე.ი. გადავალთ Fast Ethernet ტექნოლოგიაზე 100 მბიტ/წმ სიჩქარით) და შევინარჩუნებთ კადრის მინიმალურ ზომას 64 ბაიტს (მაქსიმა-\lური კი Ethernet-ტექნოლოგიებით კადრის ზომა დღეისათვის არსებული სტანდარტით გათვალისწინებულია 1518 ბაიტი), სეგმენტის მაქსიმალური სიგრძე უნდა შემცირდეს შესაბამისად 10-ჯერ, ე.ი. არ უნდა აღემატებოდეს 250 მეტრს. ხოლო ბიტური სიჩქარის კიდევ შემდგომი გაზრდა კი კვლავ 10-ჯერ (1000 მბიტი/წმ – Gigabit Ethernet ტექნოლოგიის დროს) მოითხოვს, რომ სეგმენტის სიგრძე კვლავ შემცირდეს შესაბამისად 10-ჯერ. ასე რომ მონაცემთა 1000 მბიტ/წმ სიჩქარეების გამოყენების დროს სეგმენტის მაქსიმალური დასაშვები სიგრძე არ უნდა აღემატებოდეს 25 მეტრს. აღნიშნული პრობლემების დასაძლევად შეიქმნა (1992 წელს) არაფორმალური Fast Ethernet Alliance, სადაც შევიდნენ Ethernet-ტექნოლოგიების ისეთი ლიდერი კომპანიები, როგორიცაა SynOptics 3Com, Hewlett-Packcard, AT&T და სხვები. მათ შეიმუშავეს როგორც ქსელური ადაპტერების მიკროსქემები, გათვლილი მონაცემთა გადაცემის მაღალ-სიჩქარიან ტექნოლოგიებზე, ასევე კავშირის ხაზებში მონაცემთა სიგნალების

კოდირების ახალი მეთოდებიც (მაგალითად 4B/5B, 8B/6T და ა.შ.) და შეიმუშავეს სრულდუპლექსიანი კომუტირების ვარიანტების მქონე პროტოკოლების ახალი ვერსიები. ახალი ტექნოლოგიების სტანდარტიზაციის საერთაშორისო კვლევითმა IEEE ინსტიტუტმა Fast Ethernet-ისათვის დაარეგისტრირა (EIA/TIA 568 A სპეციფიკაციით) მაღალსიჩქარიანი საკაბელო სისტემები:

—— 100Base – TX (ორწყვილიანი კაბელი UTP Category 5), მათ შორის ეკრანირებული SPT Type 1);

—— 100 Base – T4 (ორწყვილიანი კაბელი UTP Category 3, 4 და 5);

—— 100 Base – FX (მრავალმოდიანი ოპტიკურ-ბოჭკოვანი კაბელი).

სტანდარტიზაციის საერთაშორისო ინსტიტუტმა დაარეგისტრირა, აგრეთვე საკაბელო სისტემის ახალი სპეციფიკაციები 1000 მბიტ/წმ სიჩქარეებისათვის Gigabit Ethernet ტექნოლოგიებისათვის. ისინი შემუშავებული იქნა მრავალმოდიანი ოპტიკურ-ბოჭკოვანი კაბელებისათვის სტანდარტი IEEE 802.3z კომიტეტის მიერ, რომელმაც განსაზღვრა ორი სპეციფიკაცია:

—— 1000 Base – SX;

—— 1000 Base – LX.

პირველ შემთხვევაში გამოიყენება 850 нm სიგრძის ტალღა (S –აღნიშნავს Short Wavelength – მოკლე ტალღა), ხოლო მეორეში-1300 нm (L-მომდინარეობს სიტყვიდან Long Wavelength – გრძელი ტალღა).

შემუშავებული იქნა კაბელი (IEEE 802.3ab კომიტეტის მიერ) გასაჭიმი წყვილისათვის 1000Base–T, რომელმაც გაზარდა სეგმენტის სიგრძე 100 მეტრამდე. ხოლო სპეციფიკაცია 1000Base – LH (LH-სიტყვებიდან Long Haul- გრძელი მანძილი) სპეციალურად შემუშავებული იქნა Gigabit Ethernet – სიჩქარიანი კაბელის სეგმენტების სხვადასხვა სიგრძეებისათვის (1310 mkm ტალღის სიგრძის მქონე კაბელის დიაპაზონი 1-49 კმ-მდე, ხოლო 1550 mkm ტალღის სიგრძის მქონე კაბელის დიაპაზონი მდებარეობს 50-100 კმ-ის საზღვრებში). ამ უკანასკნელ სპეციფიკაციებს (1000Base – LH) მხარს უჭერს (ე.ი. მათთან მუშაობს) ქსელური მოწყობილობები, რომელთა საფუძველზე შესაძლებელი გახდა მეგაპოლისის (MAN) მასშტაბის Ethernet–ქსელების აგება და მათი წარმატებით ექსპლუატაცია.

აღნიშნული პარაგრაფის დასასრულს შევნიშნოთ, რომ რაც წლები გადის მოწინავე ტექნოლოგიების დანერგვით კომპიუტერული ქსელის საკაბელო მეურნეობა ძალზე მრავალფეროვანი ხდება (შესაბამისი კომიტეტების მიერ ამჟამად დარეგისტრირებულია 2000-ზე მეტი დასახელების კაბელები და მათი ნომენკლატურა თანდათან იზრდება).

5.3. მონაცემთა მიღება-გადაცემისათვის ქსელში გამოყენებული კადრის სტრუქტურები

ისევე როგორც წინა პარაგრაფში განხილული ქსელის საკაბელო სისტემები, მონაცემთა გადაცემა–მიღებისათვის გამოყენებული კადრის სტრუქტურებიც ექვემდებარებიან გარკვეულ სტანდარტულ მოთხოვნებს, რომლებიც დარეგისტრირებული არიან ასევე სტანდარტიზაციის საერთაშორისო კომიტეტებში (მათ შორის ISO და IEEE – ორგანიზაციებში). მაგალითად, Ethernet – ტექნოლოგიის სტანდარტი, რომელიც აღწერილია IEEE 802.3 დოკუმენტში, შეიცავს ასეთი ტიპის ქსელებისათვის განკუთვნილი კადრების ფორმატის (კადრების სტრუქტურების) აღწერას. აღნიშნულ დოკუმენტში დაფიქსირებულია Ethernet ქსელებისათვის პრაქტიკაში გამოსაყენებლად რეკომინდირებული 4 სხვადასხვა ფორმატის (ტიპის) კადრის სტრუქტურა. კადრის ზოგიერთი ფორმატი წარმოიქმნა მაგალითად: Novell-კომპანიის ძალისხმევის შედეგად პროტოკოლების თავისი სტეკის მუშობის დასაჩქარებლად Ethernet ქსელებში. აღნიშნულ პარაგრაფში ძირითადი ყურადღება გავამახვილოთ ასეთი კადრების ფორმატებზე, ხოლო ამ პარაგრაფის ბოლო ნაწილში აღვნიშნოთ, თუ რა ფორმატის კადრებს იყენებს Ethernet- სალტური ტოპოლოგიების გარდა სხვა ტოპოლოგიის (მაგალი-თად რგოლური ტოპოლოგიის–Token King) ქსელები.

იბადება კითხვა. რა გავლენას ახდენს კადრის ფორმატებში სტრუქტურების სხვადასხვაობა? პასუხი მარტივია. უპირველეს ყოვლისა კადრის ფორმატებში განსხვავებები იწვევს ქსელში გამოყენებული აპარატურის მუშობაში გარკვეული სახის შეუთავსებლობას, ასევე სხვადასხვა პროგრამული უზრუნველყოფის (იგულისხმება ქსელური პროგრამული უზრუნველყოფა) არაშეთანხმებულ მუშობას. თუმცა აქვე უნდა აღინიშნოს ისიც, რომ დღეს-დღეობით ყველა ქსელურ ადაპტერს, მათ დრაივერებს, ხიდ/კომუტატორებს და მარშუტიზატორებს უკვე შეუძლიათ იმუშაონ Ethernet–ტექნოლოგიებში ამჟამად პრაქტიკაში გამოყენებული კადრების ყველა ფორმატებთან, ვინაიდან კადრის ტიპის გამოცნობა სწარმოებს ავტომატურად თანამედროვე ქსელური ოპერაციული სისტემების მიერ.

ნებისმიერი ტოპოლოგიის ქსელურ სტრუქტურებში კადრების დანიშნულება ყველგან ერთნაირია. იმისათვის რომ ქსელის სადგურმა (მაგალითად, ქსელთან მიერთებულმა მომხმარებლის კომპიუტერმა) თავისი მონაცემების გადასაცემად მიმართოს საკომუნიკაციო გარემოს (არხულ დონეზე), ყველა მონაცემი ფორმირებული უნდა იყოს კადრებად. კადრები უზრუნველყოფენ ჰოსტის სადგურების (გადამცემი-მიმღები სადგურების წყვილის) სინქრონიზაციას, კადრებზე უნდა აისახოს მონაცემების გამგზავნისა და მიმღების მისამართები, ასევე ამ მონაცემებით უნდა უზრუნველყოს ზედა დონის პროტოკოლი, (OSI-შვიდდონიანი ეტალონური მოდელის მიხედვით), რომელიც იმუშავებს კონკრეტულ კადრთან, მაგალითად, IPX ან SPX პროტოკოლი

(Netware ოპერაციულ გარემოში), ან ქსელური IP- პროტოკოლი Windows NT (Microsoft-ის გარემოში).

აღნიშნულ პარაგრაფში განვიხილოთ Ethernet-ის ტექნოლოგიებში ამჟამად გამოყენებული ყველა 4 ტიპის (ფორმატის) კადრის სტრუქტურები. აქვე აღვნიშნოთ, რომ სხვადასხვა ლიტერატურაში კადრის ერთი და იგივე ტიპს შეიძლება ჰქონდეს სხვადასხვა სახელწოდებები, ამიტომ ქვემოთ ჩამოვთვალოთ (ხოლო შემდეგ დავახასიათოდ თვითეული მათგანი) დღეისათვის ფართოდ გავრცელებული სახელწოდებებით ცნობილი კადრის ტიპები:

— კადრი Ethernet 802.3 (გვხვდება ამ კადრის სხვა აღნიშვნებიც, მაგალითად,
802.3/ LLC, 802.3/802.2 ან Novell 802.2);

— კადრი Raw 802.3 (ან კადრი Novell 802.3);

— კადრი Ethernet-DIX (ან კადრი Ethernet II);

— კადრი Ethernet-SNAP.

სანამ უშუალოდ დავახასიათებთ ზემოთჩამოთვლილი კადრების ტიპებს, აღვნიშნოთ ისიც, რომ ყველა მათგანს გააჩნია როგორც საერთო, ისე განმასხვავებე-ლი ნიშნები (ძირითადი და დამატებითი ველები). შენიშვნის სახით ხაზი გავუსვათ იმასაც, რომ მაგალითად, 802.3/LLC კადრის სათაური წარმოადგენს IEEE 802.3 და 802.2 სტანდარტებით განსაზღვრული კადრების სათაურების ველების გაერთიანების შედეგს.

აღვნიშნოთ ასევე ისიც, რომ ზემოთ მითითებულ კადრებში მიმღების მისამართის უფროსი ბაიტის პირველი ბიტი

მანიშნებელია იმისა, ეს მისამართი წარმოადგენს ინივიდუალურს თუ ჯგუფურს. თუ იგი ტოლია 0-ის, მაშინ კადრი დამისამართებულია ინდივიდუალურ მისამართზე (unicast), ხოლო, თუ მისი (პირველი ბიტის) მნიშვნელობაა 1, მაშინ ეს ჯგუფური მისამართია (multicast). ჯგუფური მისამართი შეიძლება ეკუთვნოდეს ქსელის ყველა კვანძებს ან ქსელის გარკვეულ ჯგუფს. ამასთან თუ მისამართი შეიცავს ყველა ერთიანებს, ე.ი. გააჩნია თექვსმეტობითი წარმოდგენა OxFF-FF-FF-FF-FF-FF, მაშინ იგი განკუთვნილია ქსელის ყველა სადგურისადმი და ეწოდება ფართოსამაუწყებლო მისამართი (broadcast). დანარჩენ შემთხვევებში ჯგუფური მისამართი დაკავშირებულია მხოლოდ იმ კვანძებთან, რომლებიც კონფიგურირებულია (მაგალითად, ხელით), როგორც ჯგუფის წევრები, და რომლის (ჯგუფის) ნომერი მითითებულია ჯგუფურ მისამართში. კადრის სათაურში მისამართის უფროსი ბაიტის მეორე ბიტი განსაზღვრავს მისამართის დანიშვნის ხერხს-ცენტრალურია თუ ლოკალური. თუ ეს ბიტი ტოლია 0-ის (რაც ყოველთვის წარმოადგენს ამ სიდიდეს თითქმის ყველა სტანდარტულ Ethernet – აპარატურაში), მაშინ მისამართი დანიშნულია ცენტრალიზებულად IEEE სტანდარტიზაციის კომიტეტის დახმარებით.

Raw 802.3 კადრს ხშირად მოიხსენიებენ, როგორც Novell 802.3 კადრად. Ethernet DIX კადრს უწოდებენ ასევე Ethernet-ის კადრს. მას გააჩნია სტრუქტურა, რომელიც ემთხვევა Raw 802.3 კადრის სტრუქტურას. თუმცა 2-ბიტიანი ველი კადრის სიგრძე (L) Raw

802.3 კადრის, Ethernet DIX კადრში ეს ველი მიუთითებს იმაზე, თუ პროტოკოლის რა ტიპია გამოყენებული მასში.

კადრს Ethernet SNAP (SNAP-SubNetwork Access Protocol), ხშირად უწოდებენ როგორც ქვექსელებში შეღწევის პროტოკოლს.

ქვემოთ მივუთითოთ Ethernet კადრის ტიპები, რომლებიც მხარს უჭერენ ქსელური დონის პოპულარული პროტოკოლების რეალიზაციას (ე.ი. რომლებსაც შეუძლიათ მუშაობა ქსელური დონის პროტოკოლებთან):

კადრის ტიპი	ქსელური პროტოკოლები
Ethernet 802.3	IPX/SPX
Ethernet II	IPX, TCP/IP, Apple Talk, Phase I
Ethernet 802.2	IPX/SPX, FTAM
Ethernet SNAP	IPX/SPX, TCP/IP, Apple Talk, Phase II

აღნიშნულ პარაგრაფში გამოვიყენოთ კადრის ტიპების სახელწოდებები, რომლებიც შემოღებული აქვს Novell-ის ფირმას (ეს სახელწოდებები გამოიყენება ფაილებში AVTO EXEC.NCF ან NET.CFG.

NETX.COM ან VLM.EXE გამოყენების დროს კადრის ტიპები, რომლებიც დასაშვებია მუშა სადგურების დრაივერებისათვის გამოსაყენებლად და რომლებიც უზრუნველყოფენ ODI ღია (გახსნილი) არხის ინტერფეისს, აღწერილია ფაილში NET.CFG.

ფაილ–სერვერზე კადრის ტიპი განისაზღვრება სერვერის კონსოლიდან, რომელსაც უპასუხებს იგი მასზე (კადრის ტიპზე) მოთხოვნისთანავე, ან ფაილში AVTO EXEC.NCF.

რახან Novell-ის ფირმაზე გავამახვილებთ ყურადღებას (მის ქსელებში, როგორც ცნობილია, გამოყენებულია ოპერაციული სისტემა NetWare), აღვნიშნოთ ისიც, რომ ODI ღია არხების ინტერფეისი, NetWare ოპერაციულ სისტემის სხვადასხვა ვერსიებში NetWare 3.x-ის ზემოთ, იყენებს (უფრო სწორად შეუძლია გამოიყენოს) სხვადასხვა ტიპის პროტოკოლები და ზემოთ ჩამოთვლილი კადრების ტიპები ერთი და იგივე ინტერფეისული პლატით. ხოლო ვერსიებში, რომლებიც NetWare 2.x და უფრო მის დაბლაა, იმ დრაივერებში სადაც არ სწარმოებს ODI-სა და გარე მარშუტიზატორების (BRIDGE.EXE და ROUTER.EXE) მხარდაჭერა, შესაძლებელია გამოყენებული იქნეს მხოლოდ Ethernet 802.3 და Ethernet II–ის ტიპის კადრები. მათი განსაზღვრა შესაძლე-ბელია ECONFIG-უტილიტით.

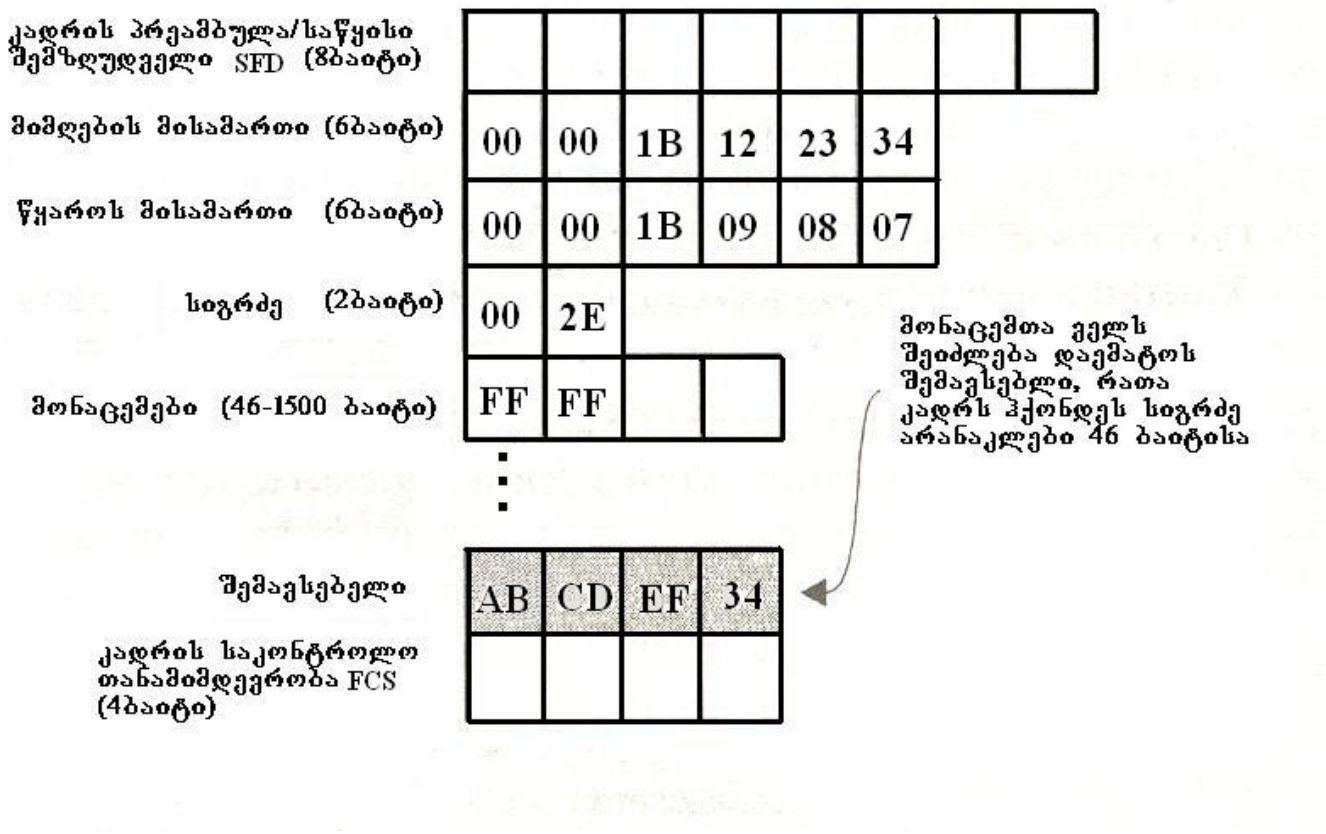
Ethernet 802.3 სტანდარტის კადრის სტრუქტურა

კადრის ამ ტიპს ქსელურ ლიტერატურაში ხშირად უწოდებენ “ნედლ” 802.3 სტანდარტს.

მხარდამჭერი პროტოკოლები. Ethernet 802.3 ტიპის კადრი, როგორც ზემოთ იქნა აღნიშნული, შეესაბამება მხოლოდ

IPX/SPX პროტოკოლს (ე.ი. ეს კადრი ძირითადად მუშაობს მხოლოდ ამ ტიპის პროტოკოლთან).

Ethernet 802.3 ტიპის კადრის სტრუქტურა. იგი ნაჩვენებია ნახ.5.10-ზე (ნახ.5.10-ზე და შემდეგ ნახაზებზეც თითო უჯრა შეესაბამება 1 ბაიტს).



ნახ.5.10. Ethernet 802.3 ტიპის კადრის სტრუქტურა

როგორც ნახ.5.10-დან ჩანს, Ethernet 802.3 კადრის სტრუქტურა შედგება შემდეგი ველებისაგან:

პრეამბულა და კადრის საწყისი შემზღუდველი SFD. პრეამბულა წარმოადგენს 7-ბაიტიან ველს, რომელიც გამოიყენება მიმღები სადგურების სინქრონიზაციისათვის. ეს ველი შეიცავს რიგ-რიგობით ერთმანეთის მიმდევარ ერთიანებსა

და ნოლებს 1010101010..., კადრის საწყისი შემზღუდველ SFD-ს გააჩნია 1 ბაიტის სიგრძე და მჭიდროდ მოჰყვება პრეამბულას, ე.ი. იგი უჩვენებს (მიუთითებს), რომ მის შემდეგ იწყება მონაცემები. ეს ველი ასევე შეიცავს ერთმანეთის თანამიმდევრობით მიყოლებულ ერთიანებსა და ნოლებს (101010... კრებულს), თუმცა იმ განსხვავებით, რომ იგი მთავრდება ორი თანამიმდევრობით მიყოლებული ერთიანებით, რომლებიც გვიჩვენებენ, რომ მათ შემდეგ მოსდევს კადრის დასაწყისი (ე.ი მიუთითებს კადრის დაწყებას).

მიმღების მისამართი. იგი წარმოადგენს 6-ბაიტიან ველს, რომელიც შეიცავს ლოკალური სადგურის მისამართს (აპარატურულ ან კვანძის მისამართს), რომელზეც დამისამართებულია მონაცემთა პაკეტები. როგორც ზემოთ ჩვენ უკვე აღვნიშნეთ, ფართოსამაუწყებლო მისამართი კოდირდება მნიშვნელობით FF-FF-FF-FF-FF-FF.

წყაროს (გამგზავნის) მისამართი. ასევე წარმოადგენს 6-ბაიტიან ველს, იგი შეიცავს ლოკალური სეგმენტის სადგურის კვანძის მისამართს, რომელიც აგზავნის მონაცემთა პაკეტს. წყაროს მისამართი შეიძლება იყოს აპარატურული (ან საკვანძო) მისამართი უშუალოდ სადგურის, სერვერის ან მარშუტიზატორის. ამ ველში არ შეიძლება ჩაწერილი იქნეს ფართოსამაუწყებლო მისამართი (FF-FF-FF-FF-FF-FF).

სიგრძე. წარმოადგენს 2-ბიტიან ველს, რომელშიც ჩაწერილია ზედა დონის მონაცემების სიგრძე, განლაგებული

კადრის მონაცემების ველში. Ethernet 802.3 ტიპის კადრის სიგრძე არ უნდა აღემატებოდეს 1500 (ათობითი რიცხვია) ბაიტს.

მონაცემთა ველი. იგი იწყება IPX- სათაურიდან, რომელიც მიღებულია NetWare ოპერაციულ სისტემაში. მონაცემთა ველის სიგრძე მდებარეობს 46-დან 1500 ბაიტამდე საზღვრებში (ამ სისტემისათვის), ხოლო Windows NT-თვის (Microsoft-ის ფირმის 1518 ბაიტამდე).

შემავსებელი. იმისათვის, რომ კადრს ჰქონდეს მინიმალური სიგრძე (Ethernet-სტანდარტისათვის ტოლია 64 ბაიტს), ველის სიგრძე უნდა იყოს არანაკლები 46 ბაიტის. მონაცემთა 46-ბაიტიანი ველი 18-ბაიტიანი კადრის ველთან ერთად შეადგენს ზუსტად კადრის მინიმალურ სიგრძეს – 64 ბაიტს (პრეამბულისა და საწყისი შემზღუდველის სიგრძე კადრის სიგრძის განსაზღვრის დროს მხედველობაში არ მიიღება). იმ შემთხვევაში, თუ მონაცემთა სიგრძე, რომლებიც უნდა გადაიცნენ კადრით, ნაკლებია 46 ბაიტის, მონაცემთა ველი ასეთ კადრში უნდა შეივსოს შემავსებლით (ნახ.5.10) ისე, რომ კადრი შეცავდეს მონაცემთა არა ნაკლებ 46 ბაიტს.

კადრის საკონტროლო თანამიმდევრობა. შეცდომების საკონტროლო ველი ჩაშენებულია ყველა კადრში იმისათვის, რომ მიმღებმა სადგურმა დაამუშაოს მხოლოდ კორექტული (სწორად ფორმირებული) კადრი და სხვებზე დრო არ დახარჯოს. საკონტროლო FCS თანამიმდევრობა შეიცავს 4-ბაიტიან თანამიმდევრობას ციკლური ჭარბი კოდის დახმარებით. საკონტროლო თანამიმდევრობას აფორმირებს მხოლოდ გადამცემი სადგური

თითოეული პაკეტის გადაცემის წინ. მიმღები სადგური გამოითვლის (ასევე პაკეტის დამუშავების წინ) საკონტროლო თანამიმდევრობას მიღებული მონაცემებისათვის და ახდენს მის შედარებას წყარო–სადგურის მიერ გაგზავნილ საკონტროლო თანამიმდევრობასთან. თუ კომბინაციები ერთმანეთს დაემთხვა, ითვლება რომ კადრი კორექტულია და მიმღები სადგური დაიწყებს მის დამუშავებას. ფიზიკურად ველის შემოწმებას, რომელიც განსაზღვრავს კადრის კორექტულობის (ან არა კორექტულობის) ფაქტს, აწარმოებს Ethernet-ის მიკროპროცე-სორული კრებული. მონაცემთა თითეული პაკეტისათვის, რომელსაც გააჩნია არაკორექტული საკონტროლო თანამიმდევ-რობა სრულდება ასევე (მიმღები სადგურის მიერ) კადრის გათანაბრებაზე შემოწმება.

საკონტროლო თანამიმდევრობა გამოითვლება იმის და მიხედვით, თუ როგორი შემცველობა გააჩნიათ ზემოთნახსენებ შემდეგ ველებს: “მიმღების მისამართს”, “წყაროს მისამართს”, “სიგრძეს” და “შემავსებელს” (იხილე კადრის სტრუქტურა ნახ.5.10-ზე).

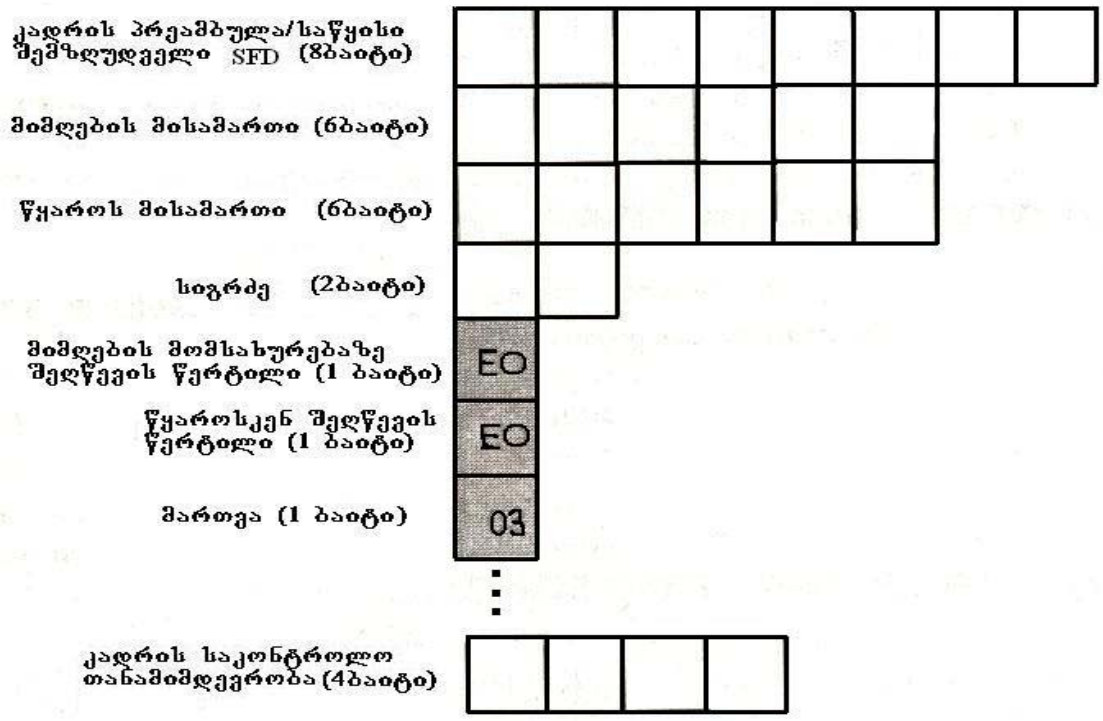
Ethernet 802.2 სტანდარტის კადრის სტრუქტურა

Ethernet 802.2 ტიპის კადრები აკმაყოფილებენ IEEE სტანდარტულ მოთხოვნებს, ვინაიდან ისინი შეიცავენ 802.2 და 802.3 სტანდარტულ ველებს. კადრის იმ ველებს, რომლებსაც

შეიცავენ მხოლოდ 802.2 სტანდარტის კადრები, ხშირად უწოდებენ ქსელის ლოგიკური რგოლის მართვის დონის ველებს.

მხარდამჭერი პროტოკოლები. Ethernet 802.2 შეესაბამება IPX/SPX- პროტოკოლს, რომელიც მიღებულია NetWare-ში და FTAM-პროტოკოლს (File Transfer, Access and Management Protocol – ფაილების გადაცემის, შეღწევის და მართვის პროტოკოლს).

Ethernet 802.2 ტიპის კადრის სტრუქტურა. ნაჩვენებია ნახ.5.11-ზე.



ნახ. 5.11. Ethernet 802.2 ტიპის კადრის სტრუქტურა

როგორც ამ ნახაზიდან ჩანს, IPX/SPX- პროტოკოლი (Noveel-ის პროტოკოლი) იყენებს ყოველთვის მართვის ერთბაიტიან ველს 0x03 შემცველობით.

ნახ. 5.10 და ნახ. 5.11-დან ჩანს, რომ Ethernet 802.3 და Ethernet 802.2 სტრუქტურის კადრებს შორის საერთო (მსგავს) ველებს წარმოადგენენ:

— კადრის პრეამბულა/საწყისი შემზღუდველი SFD (8 ბაიტი)
— მიმღების მისამართი (6 ბაიტი)
— წყაროს მისამართი (6 ბაიტი)
— სიგრძე (2 ბაიტი)
— მონაცემები და შემავსებელი (46-1500 ბაიტი) (ნახ. 5.11-ზე ეს ველები ნაჩვენები არ არის)
— კადრის საკონტროლო თანამიმდევრობა FCS (4 ბაიტი)

მიმღების მომსახურებაზე შეღწევის წერტილი DSAP. ეს ერთ-ბაიტიანი ველი მიუთითებს ზედა (ქსელური) დონის პაკეტის მიმღების პროტოკოლის ტიპზე. პაკეტები, რომლებიც მუშავდება IPX/SPX პროტოკოლის შესაბამისად, მიმღების მომსახურებაზე შეღწევის წერტილის ველში DSAP შეიცავს რიცხვს 0xE0 (აღნიშნულ სახელმძღვანელოში, თექვსმეტობით ფორმაში წარმოდგენილი რიცხვები შეიძლება დაწყებული იქნენ “0x”-დან).

წყაროს (პაკეტების გამგზავნის) მომსახურებაზე შეღწევის წერტილი SSAP. ისევე როგორც DSAP-ველში, ამ ერთ-ბაიტიან ველში მიეთითება ზედა (ქსელური) დონის პროტოკოლის ტიპი. IPX/SPX პროტოკოლის მიხედვით დამუშავებული პაკეტები წყაროს მომსახურებაზე შეღწევის წერტილის ველში შეიცავენ რიცხვს 0xE0.

მართვა. Netware-ოპერაციულ გარემოში IPX/SPX პროტოკოლის გამოყენების დროს მართვის ველი შეიცავს რიცხვს **0x03**, რომელიც Ethernet 802.2 სტანდარტში აღნიშნავს არარიცხვით ფორმატს. ეს არარიცხვითი ფორმატი მიანიშნებს იმაზე, რომ ლოგიკური რგოლის მართვის დონე უზრუნველყოფს მომსახურებას წინასწარი ლოგიკური შეერთების დამყარების გარეშე.

კადრის სრული სიგრძე Ethernet 802.2 სტანდარტში. კადრის სრული სიგრძის განსაზღვრის დროს მხედველობაში არ მიიღება პრეამბულისა და კადრის საწყისი შემზღუდველის სიგრძეები. ზემოთმოყვანილი ინფორმაციის თანახმად კადრის მინიმალური და მაქსიმალური სიგრძეები განისაზღვრება კადრის ყველა სხვა ველების სიგრძეების ჯამით:

მიღების მისამართი	6 ბაიტი
წყაროს მისამართი	6 ბაიტი
სიგრძე	2 ბაიტი
მონაცემები და შემავსებელი	46-1500 ბაიტი

მათ შორის ლოგიკური მართვის რგოლის დონის:

მიმღების მომსახურებაზე შეღწევის წერტილი DSAP	1 ბაიტი
წყაროს მომსახურებაზე შეღწევის წერტილი SSAP	1 ბაიტი
მართვა	1 ბაიტი
საკონტროლო თანამიმდევრობა FCS	4 ბაიტი
კადრის მინიმალური სიგრძე	64 ბაიტი
კადრის მაქსიმალური სიგრძე	1518 ბაიტი

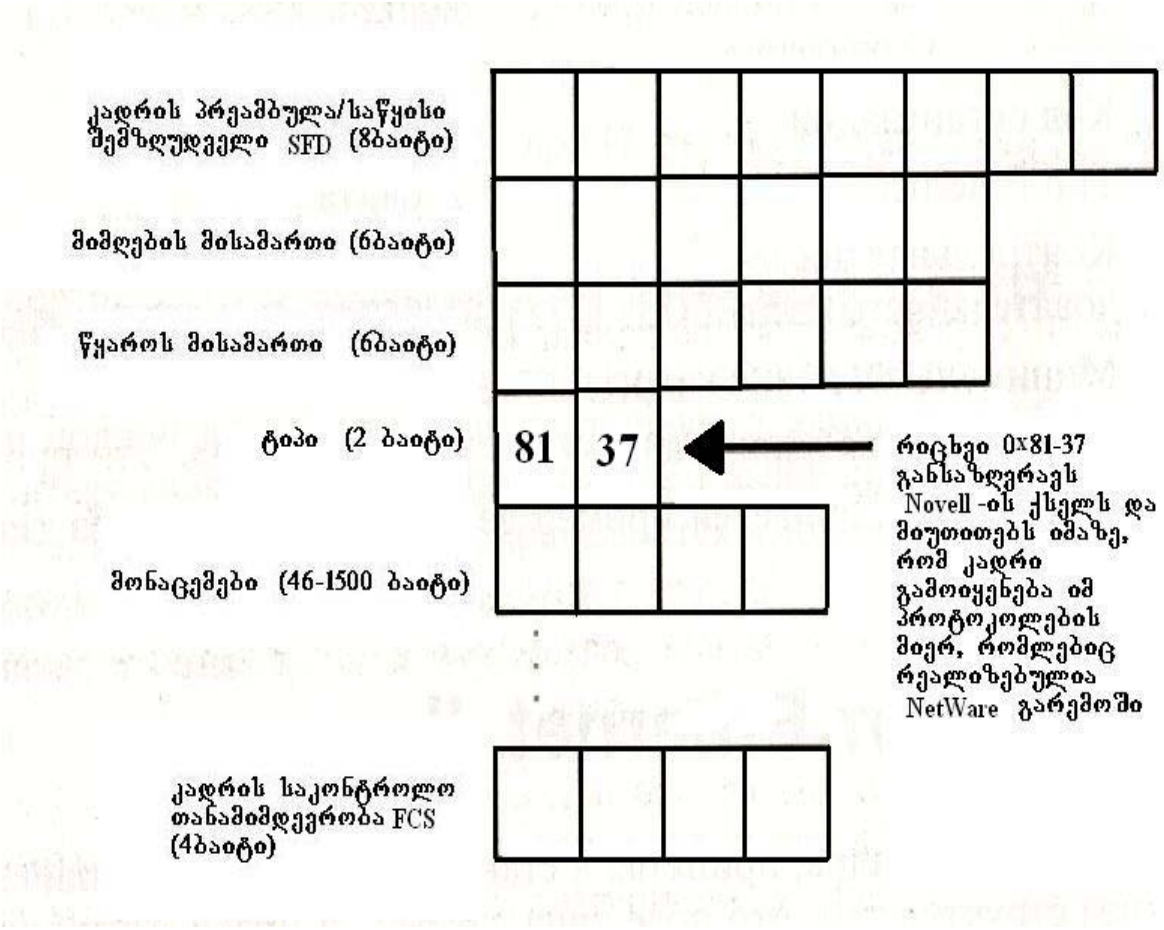
კადრის Ethernet II სტანდარტი

კადრის სტრუქტურა, რომელიც მიღებულია Ethernet II სტანდარტში, განსხვავდება ზემოთ აღწერილი სტრუქტურისაგან იმით, რომ კადრის ტიპის ველი მოსდევს წყაროს ველს. იმ კადრებში კი, რომლებიც ფორმირებულია Ethernet 802.3, Ethernet 802.2 და Ethernet SNAP სტანდარტებით, წყაროს ველის შემდეგ განლაგებულია სიგრძის მაჩვენებელი ველი.

მხარდამჭერი პროტოკოლები. Ethernet II ტიპის კადრი შეიძლება გამოყენებული იქნეს IPX/SPX, TCP/IP და Apple Talk Phase I პროტოკოლებთან.

Ethernet II ტიპის კადრის სტრუქტურა. ასეთი ტიპის კადრის სტრუქტურა ადრე აღწერილი სტრუქტურებისაგან განსხვავდება ორი განსაკუთრებულობით, კერძოდ პრეამბულისა და კადრის საწყისი შემზღუდველის ველითა და ტიპის ველით. Ethernet II ტიპის კადრის სტრუქტურა ნაჩვენებია ნახ. 5.12-ზე.

პრეამბულა. ისევე, როგორც კადრის სხვა სტანდარტების პრეამბულის 7-ბაიტიანი ველი, Ethernet II ტიპის კადრის პრეამბულის 8-ბაიტიანი ველიც შეიცავს ერთმანეთთან რიგრიგობით მიმდევარ ერთიანებისა და ნოლების სიმრავლეს, თუმცა, როგორც ზემოთ აღვნიშნეთ, ერთბაიტიანი საწყისი შემზღუდველი (10101011) ითვლება, როგორც პრეამბულის ნაწილი.



ნახ. 5.12. Ethernet II ტიპის კადრის სტრუქტურა

ტიპის ველი. კადრების ყველა ზემოთ აღწერილი ტიპებისაგან განსხვავებით Ethernet II კადრები სიგრძის ველის მაგივრად შეიცავენ ტიპის ველს.

ქვემოთ მოყვანილია ტიპის ველის მნიშვნელობების ჩამონათვალი, რომლებიც იდენტიფიცირებენ ამ ტიპის კადრის (Ethernet II) გამომყენებელი სხვადასხვა პროტოკოლები:

აღვნიშნოთ, რომ ეს სია სრულად ემთხვევა მნიშვნელობების ანალოგიურ სიებს, რომლებიც Ethernet ტიპის ველშია Ethernet SNAP ტიპის კადრებისათვის.

IP (Internet Protocol)	0x0800
ARP (Address Resolution Protocol)	0x0806
Reverse ARP	0x8035
Apple Talk	0x809B
Apple Talk ARP	0x80F3
Netware IPX/SPX	0x8137

კადრის სრული სიგრძე Ethernet II სტანდარტში. კადრის სრული სიგრძის განსაზღვრის დროს პრეამბულის სიგრძე მხედველობაში არ მიიღება. ზემოთ მოყვანილი ინფორმაციის თანახმად, კადრის მინიმალური და მაქსიმალური სიგრძეები განისაზღვრება კადრის ყველა სხვა ველების სიგრძეების შეკრებით:

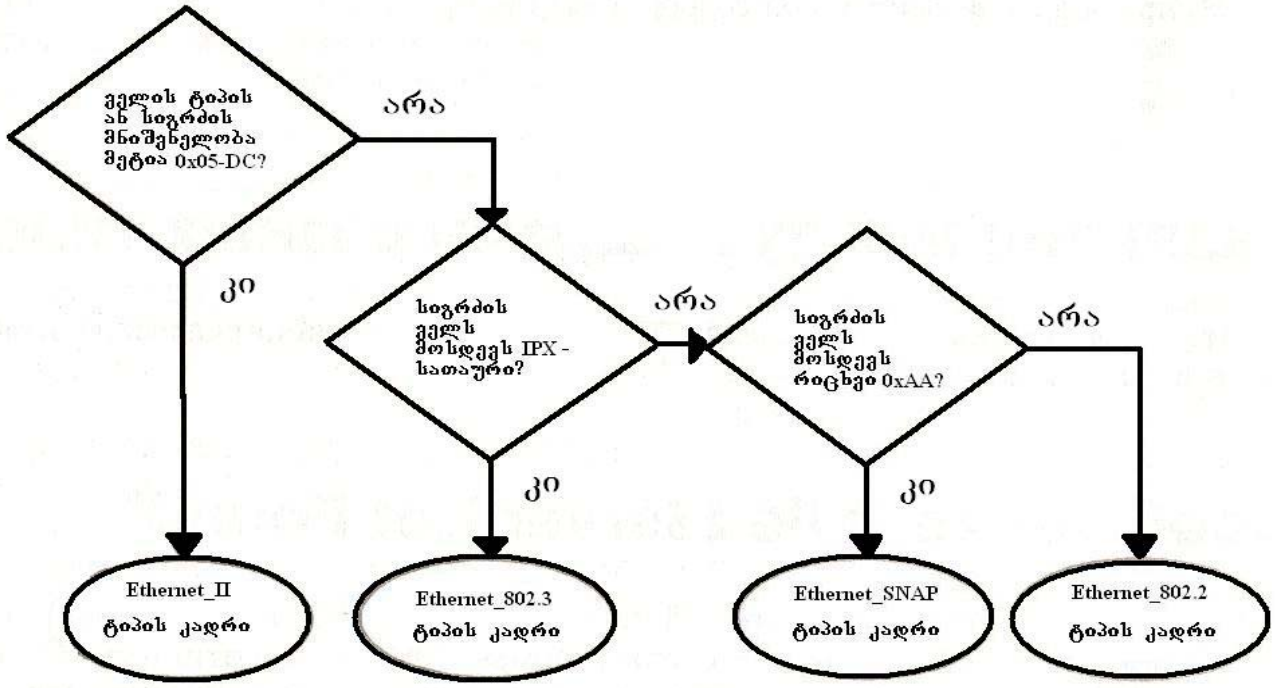
მიმღების მისამართი	6 ბაიტი
წყაროს მისამართი	6 ბაიტი
ტიპი	2 ბაიტი
მონაცემები და შემავსებელი	46-1500 ბაიტი
კადრის საკონტროლო თანამიმდევრობა FCS	4 ბაიტი
კადრის მინიმალური სიგრძე	64 ბაიტი
კადრის მაქსიმალური სიგრძე	1518 ბაიტი

Ethernet 802 ტიპის კადრებიდან Ethernet II ტიპის კადრებზე გადასასვლელად შეიძლება გამოყენებული იქნეს მეთოდი გარკვეული წესების დაცვით.

სხვადასხვა პროტოკოლები და კადრების ტიპები. Netware-ოპერაციულ სისტემაში (ვერსია 3.x-ის), რომელიც მხარს უჭერს ღია არხის ODI ინტერფეისს, შესაძლებელია გამოყენებული იქნეს სერვერისა და მუშა სადგურების კადრებისა და დრაივერების სხვადასხვა ტიპები. თუმცა ამასთან ერთად ისიც უნდა შევნიშნოთ, რომ სერვერ–მუშა სადგურის ნებისმიერ წყვილის ურთიერთდასაკავშირებლად გამოყენებული უნდა იქნეს ერთი და იმავე ტიპის კადრები. მაგალითად, Netware 3.x ვერსიაში, თუ რომელიმე სერვერი იყენებს Ethernet 802.3 ტიპის კადრებს, მაშინ იმ მუშა სადგურებმა (მომხმარებლის პერსონა-

ლურმა კომპიუტერებმა), რომლებსაც სურთ ამ სერვერთან დაკავშირება, უნდა გამოიყენონ ამავე ტიპის კადრები.

განსხვავებები სხვადასხვა ტიპის კადრებს შორის. ნახ. 5.13-ზე ნაჩვენებია მონაცემთა პაკეტში კადრების ტიპის განმსაზღვრელ-ალგორითმის მარტივი ბლოკ-სქემა.



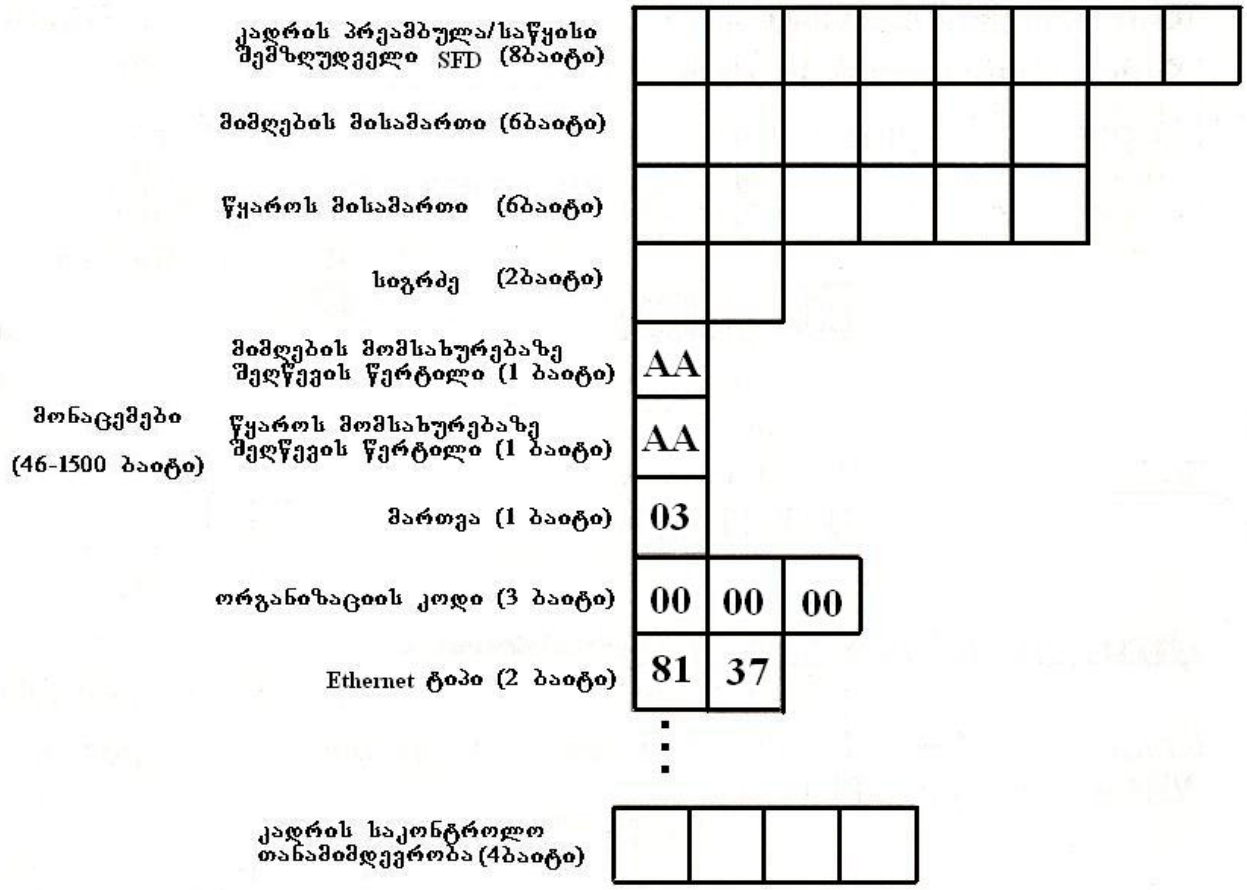
ნახ. 5.13 კადრის ტიპის განმსაზღვრელი ალგორითმის ბლოკ-სქემა.

კადრის Ethernet-SNAP სტანდარტი

SNAP მომდინარეობს ინგლისურ-ენოვანი შემოკლებიდან Sub-Network Access Protocol და შემოღებულია ქვექსელებში შელწევის პროტოკოლის აღსანიშნავად. Ethernet-SNAP ტიპის კადრის სტრუქტურა წარმოადგენს იმ კადრის სტრუქტურის განვითარებას, რომელიც მიღებულია სტანდარტში Ethernet 802.2.

მხარდამჭერი პროტოკოლები. Ethernet-SNAP ტიპის კადრები შეიძლება გამოყენებული იქნენ IPX/SPX, TCP/IP და Apple Talk Phase II პროტოკოლებთან.

Ethernet – SNAP ტიპის კადრის სტუქტურა. აღნიშნული ტიპის კადრის სტუქტურა ნაჩვენებია ნახ. 15.14-ზე.



ნახ. 5.14. Ethernet – SNAP ტიპის კადრის სტუქტურა

ამ ნახაზიდან ადვილი შესამჩნევია, რომ Ethernet – SNAP და Ethernet 802.2 სტანდარტების კადრების შორის საერთო (ერთანაირ) ველებს წარმოადგენენ:

— პრეამბულა / კადრის საწყისი შემზღუდავი SFD (8 ბაიტი);

— მიმღების მისამართი (6 ბაიტი);

— წყაროს მისამართი (6 ბაიტი);
— სიგრძე (2 ბაიტი);
— მონაცემები და შემავსებელი (46 – 1500 ბაიტი);

ლოგიკური რგოლის მართვის დონის ველებია:

— მიმღების მომსახურებაზე შეღწევის წერტილი DSAP (1 ბაიტი);
— წყაროს მომსხურებაზე შეღწევის წერტილი SSAP (1 ბაიტი)
— მართვის (1 ბაიტი);
— კადრის საკონტროლო თანმიმდევრობა FCS (4 ბაიტი)

მიმღების, წყაროს მომსახურებებზე შეღწევისა და მართვის ველები. DSAP და SSAP ველები Ethernet – SNAP კადრებში ყოველთვის შეიცავენ რიცხვს 0xAA. ეს რიცხვი მიუთითებს იმაზე, რომ კადრს გააჩნია Ethernet – SNAP ტიპის ფორმატი.

მართვის ველს Ethernet – SNAP ტიპის კადრებში ყოველთვის აქვს 1 ბაიტი ზომა (სიგრძე) და შეიცავს რიცხვს 0x03 (არარიცხვითი ფორმატია). როგორც ნახ. 5.14-დან ჩანს, მას მოჰყვება ორგანიზაციის კოდისა და Ethernet ტიპის აღმნიშვნელი ველები.

ორგანიზაციის კოდი. ეს კოდი აღწერს ქსელის ორგანიზაციის ტიპს, რომელსაც უწესებს მისი მომდევნო Ethernet ტიპის ველი. IPX/SPX ტიპის პროტოკოლის გამოყენების დროს NetWare ოპერაციულ გარემოში ორგანიზაციის კოდის ველი შეიცავს რიცხვს 0x00 – 00 – 00.

Ethernet ტიპი. Ethernet ტიპის ველი გამოიყენება უფრო ზედა დონის პროტოკოლის აღწერისათვის. მაგალითად, NetWare

– გარემოში Ethernet - ქსელებისათვის ამ ველის მნიშვნელობა ტოლია 0x81 – 37.

ქვემოთ მოყვანილია ამ მნიშვნელობების ჩამონათვალი, რომლებიც გააჩნიათ Ethernet ტიპის ველებს სხვადასხვა ქსელურ პროტოკოლებთან სამუშაოდ:

IP (Internet Protocol)	0x0800
ARP (Address Resolution Protocol	0x0806
Reverse	0x8035
Apple Talk	0x809B
Apple Talk	ARP 0x80F3
Net Ware	IPX/SPX 0x8137

კადრის სრული სიგრძე Ethernet – SNAP სტანდარტში. ამ კადრის სრული სიგრძის განსაზღვრის დროს ასევე არ გაითვალისწინება პრეამბულისა და კადრის საწყისი შემზღუდველის ველების სიგრძეები.

ზემოდ მოყვანილი ინფორმაციის თანახმად კადრის მინიმალური და მაქსიმალური სიგრძეები განისაზღვრება კადრის ყველა სხვა ველების სიგრძეების შკრებით:

მიმღების მისამართი	6 ბაიტი
წყაროს მისამართი	6 ბაიტი
სიგრძე	2 ბაიტი
მონაცემები და შემავსებელი	46 – 1500 ბაიტი

მონაცემებთა ველი შეიცავს:

მიმღების მომსახურებაზე შეღწევის წერტილი DSAP	1 ბაიტი
წყაროს მომსახურებაზე შეღწევის წერტილი SSAP	1 ბაიბი
მართვა	1 ბაიტი
ორგანიზაციის კოდი	3 ბაიტი
Ethernet ტიპი	2 ბაიტი
კადრის საკონტროლო თანამიმდევრობა FCS	4 ბაიტი
კადრის მინიმალური ისგრძე	64 ბაიტი
კადრის მაქსიმალური სიგრძე	1518 ბაიტი

Token Ring კადრის 802.5 სტანდარტი. Token Ring 802.5 სტანდარტის კლასის ფორმატები ძირითადად გამოიყენება რგოლური სტრუქტურის მქონე კომპიუტერულ ქსელებში. ამგვარი სტრუქტურის ქსელები შეიქმნა გასული საუკუნის 70-იანი წლებში, რომლის აპარატურულ და პროგრამულ უზრუნველყოფას ახორციელებს IBM – კორპორაცია. ასეთი ტიპის ქსელები ორიენტირებულია მომხმარებელთა დეტერმინირებულ შეღწევაზე და აქედან გამომდინარე იგი იყენებს ორგვარი ფორმატის კადრებს:

— ქსელურ გარემოში შეღწევის მმართველი კადრები;

— მონაცემთა კადრები.

პირველი მათგანი გამოიყენება რგოლისა და რგოლში ჩართული ცალკეული სადგურების მართვისათვის, ხოლო მეორე შეიცავს მხოლოდ მომხმარებლის მიერ გადაცემულ მონაცემებს. ამ კადრების გარდა რგოლში შეიძლება წარმოიქმნენ ორი ბიტური კომბინაციები: მარკერები და წყაროსა და მიმღები

კომპიუტერების შეერთების ავარიული დასრულების მაუწყებელი თანმიმდევრობები. ჯერ განვიხილოთ ეს ორივე ბიტური კომბინაციები, ხოლო შემდეგ კადრის ორი ძირითადი სტუქტურა.

Token Ring-ს სპეციალური ბიტური კომბინაციები. ორი ბიტური კომბინაცია, რომლებსაც იყენებს რგოლური სტრუქტურის ქსელები, არ წარმოადგენენ კადრებს ამ სიტყვის სრული გაგებით (თუმცა მათ ცალკე ველების სახით შეიცავენ კადრები), არამედ მხოლოდ მოგვაგონებენ მათ. ამ განსაკუთრებულ კომბინაციებს წარმოადგენენ მარკერები და ავარიული დასრულების თანმიმდევრობები.

მარკერები. როგორც მათი სახელწოდებიდან ჩანს, ისინი წარმოადგენენ Token Ring – ის ძალზე მნიშვნელოვან შემადგენელი ნაწილს. მარკერი შედგება სამი 8-თანრიგიანი (1 ბაიტიანი) პაკეტებისაგან:

საწყისი შემზღუდველი SDEL (1 ბაიტი)
შეღწევის მართვის ველი AC (1 ბაიტი)
ბოლო შემზღუდველი EDEL (1 ბაიტი)

ყველა ეს სამივე ველი, როგორც ზემოთ აღვნიშნეთ, შედიან Token Ring კადრების შემადგენლობაში. მას შემდეგ, როდესაც სადგური დაიჭერს თავისუფალ მარკერს, მას დაემატება დამატებითი ველები, რომლის შედეგად ეს თავისუფალი მარკერი გარდაიქმნება კადრად. მარკერის (ხშირად უწოდებენ მმართველ კადრს) რგოლში ბრუნვის (სადგურებს შორის ცირკულაციის) დროის ხანგრძლიობა მიუთითებს რგოლის

გადატვირთულ რეჟიმზე (ქსელის ადმინისტრატორი ასეთ გახანგრძლივებულ დროს აღმოაჩენს პროტოკოლების ანალიზატორის დამხარებით. მაგალითად, ასეთ ანალიზატორს, რომელიც მუშაობს NetWare–ოპერაციულ გარემოში, წარმოადგენს NCC LANalyzer).

ავარიული დასრულების თანმიმდევრობა. ეს თანმიმდევრობა შედგება საწყისი შემზღუდველის SDEL ველისაგან და ბოლო შემზღვუდველის EDEL ველისაგან და შეიცავენ თითო-თითო ბაიტს:

საწყისი შემზღუდველი SDEL (1 ბაიტი)

ბოლო შემზღუდველი EDEL (1 ბაიტი)

ავარიული დამთავრების თანმიმდევრობა (რომელიც ძალზე იშვიათად გამოიყენება რგოლის სადგურების მიერ) მიუთითებს სადგურის ისეთ კომბინაციას, რომლის დროსაც წყარო-კომპიუტერს არ შეუძლია კორექტულად (შეცდომის გარეშე) გადასცეს მონაცემები. ასეთ თანამიმდევრობას ადაპტერები გადასცემენ ორ შემთხვევაში:

— მაშინ, როდესაც კადრის გადაცემის დროს თავის მუშაობაში ადაპტერმა აღმოაჩინა სერიოზული შეცდომა, რომელიც საჭიროებს გადაცემის პროცესის ავარიული დამთავრებას;

— მაშინ, როდესაც ჰოსტ-კომპიუტერი აიძულებს ადაპტერს ავარიულად დაამთავროს კადრის (ან კადრების) მიმდინარე გადაცემა. ასეთი მოთხოვნა, როგორც წესი, ჩვეულებრივ მომდინარეობს უფრო მაღალი დონის პროტოკოლებიდან ან გამოყენებითი პროგრამებიდან.

როდესაც ადაპტერი გადასცემს ავარიული დამთავრების თანმიმდევრობას, ამ დროს იგი არ ამთავრებს თავისუფალი მარკერის გადაცემის (მარკერული შეღწევის) პროტოკოლის მუშაობას. იგი მხოლოდ წყვეტს გადაცემას და რგოლში სწარმოებს მარკერის ან კადრის უეცარი დაკარგვა (გაქრობა). შედეგად რგოლის შეცდომების მონიტორს ეგზავნება ორი შეტყობინება არამდგრადი შეცდომის შესახებ. ამ დროს მონიტორი აწარმოებს რგოლის გაწმენდასა და შემდეგ ატყობინებს მარკერის შეცდომის შესახებ, უჩვენებს რა ამით მარკერის ან კადრის დაკარგვას.

Token Ring კადრის სახეები. არსებობს Token Ring კადრების ორი სახე (კადრის ორი სტუქტურა):

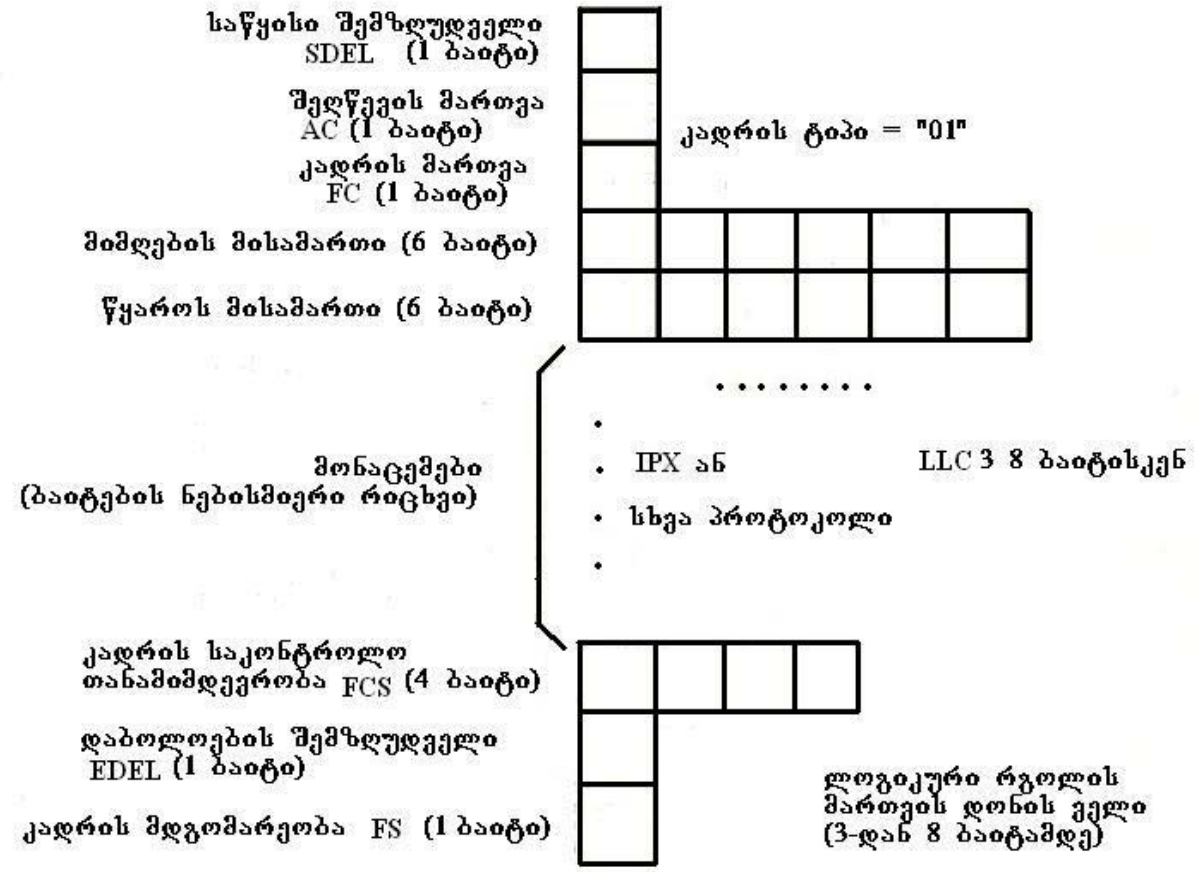
— მონაცემთა კადრის სტუქტურა;

— რგოლურ ქსელური გარემოში შეღწევის მართვის კადრის სტრუქტურა.

მონაცემთა კადრების დახმარებით წარმოებს მომხმარებელთა მონაცემების გადაცემა, რომელიც წარმოადგენს Token Ring ქსელების ძირითად ფუნქციას.

მონაცემთა კადრები შეიცავენ მომხმარებელთა მონაცემებს ლოგიკური რგოლის მართვის დონის მონაცემთა პროტოკოლური ბლოკის შიგნით.

მონაცემთა კადრის სტრუქტურა ნაჩვენებია ნახ. 5.15-ზე.



ნახ. 5.15 Token Ring კადრის სტრუქტურა

Ethernet – ქსელებისაგან განსხვავებით ODI – ღია არხის ინტერფეისთან მუშაობის დროს Token Ring ქსელებში გამოიყენება მხოლოდ ორი ფორმატის კადრები, რომელთაგან ერთი გამოიყენება ლოგიკური რგოლის სტანდარტული მართვისათვის, ხოლო მეორე – ლოგიკური რგოლის მართვისათვის ქვექსელში შეღწევის პროტოკოლის ჩარჩოებში. ამ ფორმატებს ეწოდება:

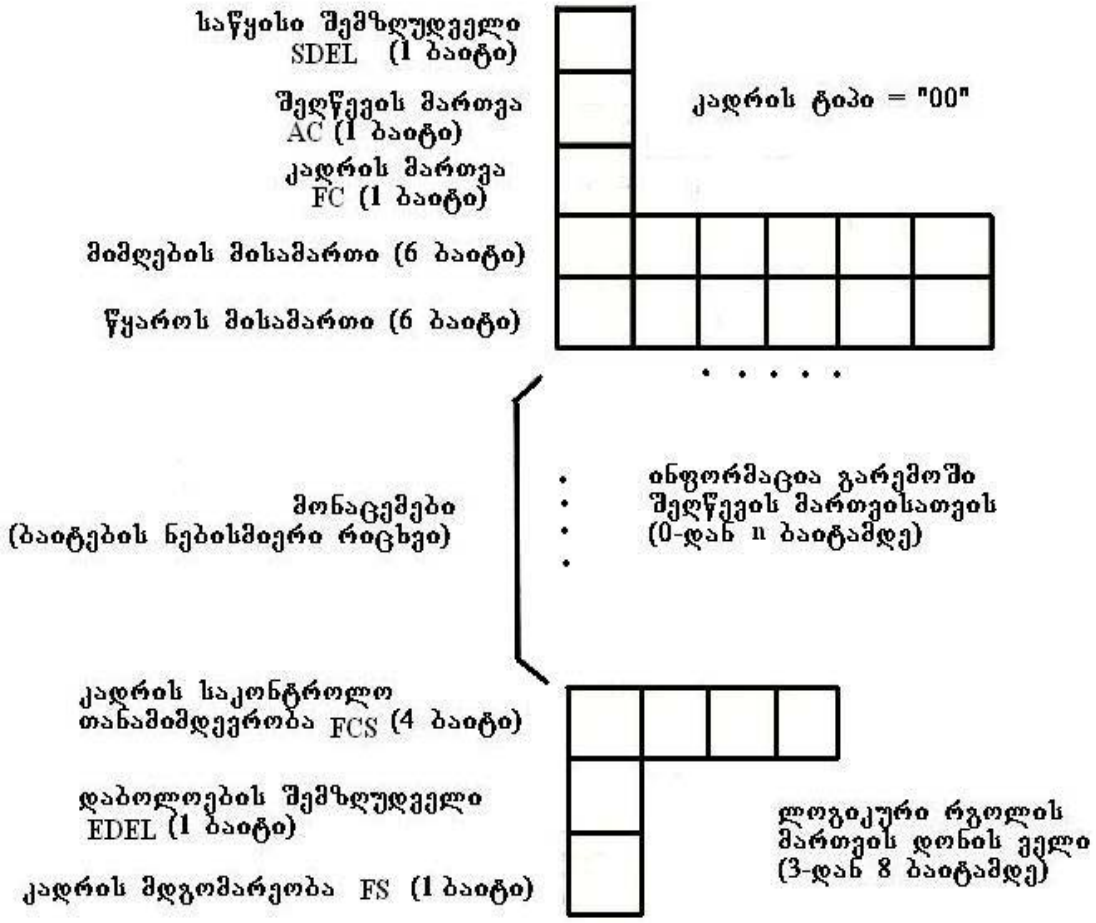
__ Token Ring ლოგიკური რგოლის მართვის საინფორმაციო – მმართველი ფორმატი;

__ Token Ring SNAP – ლოგიკური რგოლის მართვის ფორმატი ქვექსელში შეღწევის პროტოკოლის ჩარჩოებში.

რგოლურ გარემოში შეღწევის მართვის კადრი გამოიყენება მმართველი ინფორმაციის (მარკერის) გადასაცემად რგოლში ჩართულ სადგურებს შორის. სახელდობრ, ამგვარი კადრები იძლევიან საშუალებას ბოლომდე მივიყვანოთ პროცესები, რომელებიც მსგავსია რგოლის გამოკითხვის, შეჯიბრი მონიტორის დასაუფლებლად ან საავარიო სიგნალიზაციისათვის. რგოლურ გარემოში შეღწევის კადრები შეიცავენ ისეთ ინფორმაციას, რომელიც საჭიროა მხოლოდ Token Ring – ქვექსელების მართვისათვის. ამგვარი კადრები ცირკულირებენ სადგურებს შორის მხოლოდ ერთ რგოლში და არ გადაეცემიან ისინი სხვა რგოლებს ხიდებით ან მარშრუტიზატორებით.

რგოლურ გარემოში შეღწევის მართვის კადრის სტრუქტურა ნაჩვენებია ნახ. 5.16-ზე.

როგორც ნახ. 5.15 და ნახ. 5.16-დან ჩანს, Token Ring – ქსელში გამოყენებულ ორივე კადრს აქვს თითქმის ერთნაირი ფორმატი. ისინი ერთმანეთისაგან განსხვავდება მხოლოდ ინფორმაციებით, რომლებიც ჩაწერილი არიან მონაცემთა ველში. ზემოთ ნაჩვენებ სტრუქტურებში, თითოეულ ველს გააჩნია საკუთარი ინდიკატორები, რომლებითაც შეიძლება გამოვარჩიოთ კადრები სხვა ველებისაგან.



ნახ. 5.16 Token Ring რგოლის მართვის კადრის სტრუქტურა

Token Ring ქსელი წარმოადგენს უწყვეტი სინქრო–სიგნალის მქონე ჩაკეტილ რგოლს, ამიტომ რგოლში ჩართული ყველა სადგური მუდმივადაა დასინქრონიზებული ერთმანეთთან. აუცილებელია მეთოდის დაცვა, რომლის მიხედვითაც გამოიცნობა მარკერის ან/და მონაცემთა კადრების დაწყება და დამთავრება (მათი ინდიკატორებია შესაბამისად SDEL 1 ბაიტის სიგრძის და EDEL ასევე 1 ბაიტის სიგრძის). ასევე თითო-თითო ბაიტებისაგან შედგება შემდეგი ველებიც, რომელთა დანიშნულებაა:

– **შეღწევის მართვა AC.** მისი დანიშნულებაა უჩვენოს მიმდინარე ველები წარმოადგენენ თუ არა კადრის ან მარკერის ველებს; მიუთითონ მარკერის ან კადრის პრიორიტეტი და უზრუნველყონ სადგურის რგოლში არსებობა პრიორიტეტის მარკერის შესანახად; მიუთითონ აქტიურ მონიტორს თუ რამდენჯერ შემოუარა კადრმა რგოლს ამა თუ იმ კადრმა ან მარკერმა (ერთხელ თუ მრავალჯერ). ამისათვის მას გააჩნია ინდიკატორები და მონიტორების (მუშა სადგურების) რაოდენობის მთვლელები;
– **კადრის მართვა FC.** მისი დანიშნულებაა აუწყოს სადგურებს რგოლის გასუფთავება, მარკერის მოთხოვნები, საავარიო სიგნალიზაცია და ა.შ. მაგალითად, თუ ამ ველში რომელშიც კადრი კოდირებულია 00-ით, ეს ნიშნავს რომ იგი წარმოადგენს მმართველ კადრს (მარკერს), ხოლო თუ კოდირებულია 01-ით – მონაცემთა კადრს.
– **კადრის მდგომარეობის ველი FS.** მისი თითოეული თანრიგი (ეს ველიც, როგორც აღვნიშნეთ 1 ბაიტიანია (8 თანრიგიანია)) და შეიცავს სხვადასხვა ინდიკატორებს, რომელთა შორის არის გამოცნობილი მისამართის ინდიკატორი ARI და კადრის კოდირების ინდიკატორები FCI. პირველი მათგანი (ARI) მიუთითებს ფაქტს: თუ რომელი სადგური გამოიცნობს მიმღების მისამართის ველში საკუთარ მისამართს. ამ დროს კადრის რეტრანსლაციისას რგოლის გარშემო კადრი ანიჭებს ამ ინდიკატორს 1-ის მნიშვნელობას. FCI ინდიკატორი ასრულებს იმავე ფუნქციას, რაც ARI – ინდიკატორი, ოღონდ მიუთითებს აქვს თუ არა

მიმღებ სადგურს ბუფერი (თუ აქვს–იღებს მნიშვნელობას 1, ხოლო არქონის შემთხვევაში – 0), რომელიც საკმარისია კადრის კოპირებისათვის.

ნახ. 5.15 და ნახ. 5.16 სტრუქტურებში შემცველ ველებს, როგორიცაა მიმღების ველი (6 ბაიტი), წყაროს ველი (6 ბაიტი) და კადრის საკონტროლო FCS (4 ბაიტი), გააჩნიათ იგივე დანიშნულება, რაც Ethernet – კადრებს. თითეული მათგანში 48 თანრიგია (6 ბაიტი), რომელთაგან ბოლო სამი ბაიტის მნიშვნელო-ბას უნიშნავს მწარმოებელი (ადაპტერების) ფირმა, ხოლო პირველი სამი ბაიტის მნიშვნელობას ანიჭებს მისამართების სტანდარტიზაციის კომიტეტი IEEE. მისამართი, რომლის მნიშვნელობაა 0xFF - FF - FF - FF - FF – FF, გამოიყენება ფართოსამაუწყებლო მისამართის აღსანიშნავად (წყარო კომპიუტერიდან ყველა მიმღებ კომპიუტერებისაკენ კადრების გასაცემად). თუმცა არის განსხვავებებიც (Ethernet – ქსელებისაგან განსხვავებით). Token Ring – ქსელებში რეალიზებულია ფართოსამაუწყებლო მისამართების ორი სახე:

– სტანდარტული, უნივერსალური ფართოსამაუწყებლო 0xFF - FF - FF - FF - FF – FF, რომელიც გამოიყენება პაკეტების ფართოსამაუწყებლოდ დასაგზავნად ხიდების გავლით სხვა რგოლში მყოფი მომხმარებლებისაკენ;
– ფართოსამაუწყებლო მისამართი, 0xCO - 00 – FF – FF – FF – FF, რომელიც განკუთვნილია პაკეტების ფართოსამაუწყებლოდ დასაგზავნად მხოლოდ ერთი რგოლის შიგნით მყოფი მომხმარებელთა კომპიუტერებისაკენ (მუშა სადგურები-

საკენ). ამგვარი მისამართის კადრები არ გადაეცემა სხვა რგოლის მუშა სადგურებს.

რაც შეეხება წყაროს (პაკეტების გამგზავნი კომპიუტერის) მისამართს, იგი უნიკალურია და ეკუთვნის მხოლოდ კონკრეტულ სადგურს, საიდანაც იგზავნება პაკეტები (ეს ნიშნავს იმას, რომ არ არსებობენ კადრები, სადაც ნახავთ ფართოსამაუწყებლოდ დამისამართებულ წყარო – კომპიუტერს). და ბოლოს, Token Ring – ქსელებისათვის მიღებული სტანდარტის მიხედვით მარკერის შეკავების დრო აქტიური სადგურის (აქტიური მონიტორის) მიერ, რომლის განმავლობაში მან უნდა გადასცეს მონაცემები, შეადგენს 10 მწმ-ს. ეს ნიშნავს იმას, რომ თუ წყარო-კომპიუტერმა 10 მწმ-ის განმვალობაში არ გადასცა მიმღები კომპიუტერისაკენ თავისი მონაცემები, მაშინ ამ მარკერის "დაჭერა" შეუძლიათ რგოლში ჩართულ სხვა კომპიუტერებს.

თავი 6
მონაცემთა გადაცემა – მიღების ალგორითმები კომპიუტერულ ქსელებში

6.1. მონაცემთა პაკეტების გადაცემის ალგორითმი **Ethernet**-ქსელებისათვის

სალტური ტოპოლოგიის Internet-ის კომპიუტერული ქსელები, რომლებიც მუშაობენ მუშა სადგურებიდან (მომხმარებელთა პერსონალური კომპიუტერებიდან) ქსელში შეღწევის CSMA/CD მეთოდით, (როგორც ადრეც აღვნიშნეთ, ეს მეთოდი მდგომარეობს სიმრავლითი შეღწევის პირობის რეალიზაციაში წარმტანის მოსმენითა და კოლიზიების აღმოჩენით - CSMA/CD-Carrier Sense Multiple Access with Collision Detection), სალტური ტოპოლოგიის ქსელები იყენებენ საერთო საკაბელო სისტემას.

აღნიშნულ პარაგრაფში უფრო დაწვრილებით გავეცნოთ მონაცემთა გადაცემა – მიღების ალგორითმს ამ მეთოდის მიხედვით და ბიჯების მიხედვით ჩამოვაყალიბოთ მონაცემთა ჯერ გადაცემა და მერე მათი მიღება ქსელით. აღნიშნულ მეთოდს აქვს როგორც დადებითი, ასევე უარყოფითი მხარეები. დადებით მხარედ ითვლება ის, რომ შესაძლებელია სალტეს მიუერთდეს საკმაოდ დიდი რაოდენობის კომპიუტერები, ხოლო უარყოფითია ის, რომ მონაცემთა გადაცემები ქსელის სადგურების მიერ არაა დაზღვეული პაკეტების კოლიზიებისაგან

(სხვადასხვა კომპიუტერებიდან ერთდროუ-ლად გამოგზავნილი პაკეტების ერთმანეთთან შეჯახებისა და დაზიანებისაგან). აქედან გამომდინარე ამ მეთოდზე დაფუძვნებული ალგორითმის რეალიზაციის დროს პირველ რიგში დიდი ყურადღება უნდა გავამახვილოთ რამოდენიმე წესზე, რომლებიც მაქსიმალურად აგვარიდებენ თავს სხვადასხვა კომპიუტერებიდან (მუშა სადგურებიდან) მონაცემთა პაკეტების ერთდროულად გადაცემებს. თუ რამოდენიმე სადგური დროის რაღაც მომენტში დაიწყებს ერთდროულად გადაცემებს უნდა არსებობდეს რაიმე წესი იმის განსაზღვრისა, რომ პაკეტები ხვდებიან ერთმანეთთან კოლიზიაში (კონფლიქტში). და, თუ მაინც მოხვდნენ კოლიზიაში ასეთ შემთხვევებში მონაცემები უნდა გადაიცეს განმეორებით.

CSMA/CD პროტოკოლის მუშაობას თუ შევაფასებთ გადატანითი აზრით, იგი მსგავსია საერთო სარგებლობის სატელეფონო ხაზის, როცა შემთხვევით ერთდროულად ხდება რამოდენიმე ადამიანის ლაპარაკის დამთხვევა. თუ ისინი იწყებენ ერთად საუბარს, მივიღებთ რაღაც გაურკვეველ ხმაურს, ხოლო თუ კი თითეული მათგანი დაელოდება თავის რიგს, მაშინ შევძლებთ გავიგოთ თითოეული მათგანის საუბარი. მსგავს სიტუაციასთან გვაქვს საქმე მონაცემთა პაკეტების საერთო სალტით გადაცემის დროსაც.

კომპიუტერულ ქსელებში მონაცემთა პაკეტების გადაცემის დროს CSMA/CD-პროტოკოლის თანახმად, ალგორითმი ითვალი-

სწინებს 5 ბიჯის შესრულებას მუშა სადგურების, ე.ი. მომხმარებელთა პერსონალური კომპიუტერების მხრიდან. ისინი მდგომარეობენ შემდეგში:

ბიჯი 1 - ქსელის მოსმენა გადაცემის დაწყების წინ;

ბიჯი 2 - შეყოვნება (დალოდება), თუ კი ქსელის არხი დაკავებულია;

ბიჯი 3 - გადაცემის დაწყება და კოლიზიების მოსმენა;

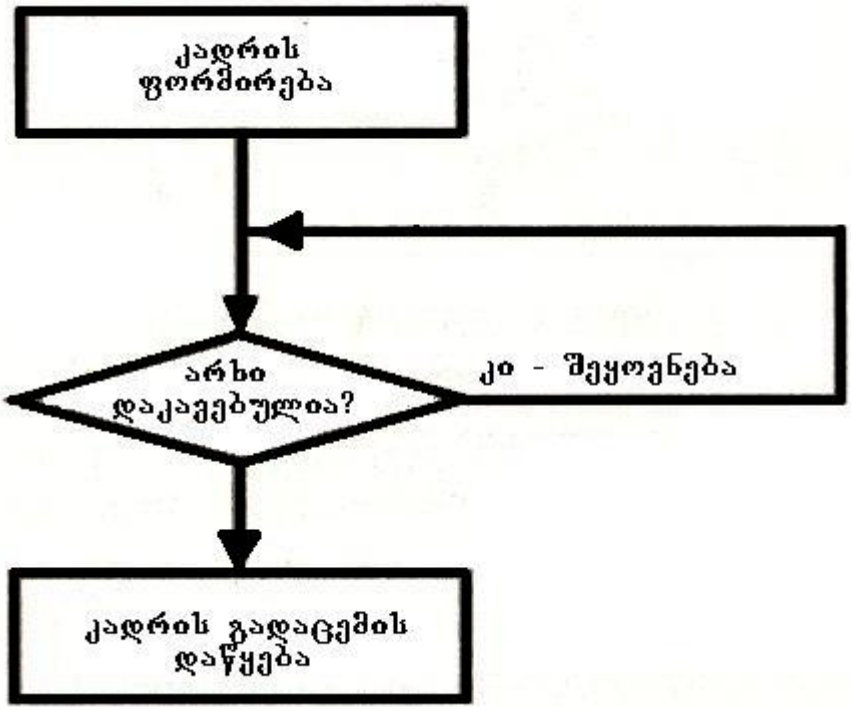
ბიჯი 4 - კოლიზიების წარმოქმნის დროს კვლავ ლოდინი განმეორებითი გადაცემების წინ;

ბიჯი 5 - განმეორებითი გადაცემა ან მუშაობის შეწყვეტა პაკეტების განუწყვეტლივ კოლიზიებში მოხვედრის დროს.

ცალკეული ქვეპარაგრაფების სახით განვიხილოთ მოკლედ თითოეული მათგანი. ხოლო გადაცემის თითეული საფეხური (ბიჯი) წარმოვადგინოთ შესაბამისი ბლოკ-სქემების ფრაგმენტების სახით. ბოლოს ამ ფრაგმენტების გაერთიანებით მოვახდინოთ მონაცემთა პაკეტების გადაცემის სრული ალგორითმის ფორმირება.

6.1.1. ქსელის მოსმენა გადაცემის დაწყებამდე (ბიჯი 1)

ქსელში ჩართული სადგურები (უფრო ზუსტად ქსელის სალტეზე მიერთებული პერსონალური კომპიუტერები) უთვალთვალებენ, ხომ არ წარმოიქმნა სეგმენტში სიგნალი "წარმტანის არსებობა" (ნახ. 6.1).



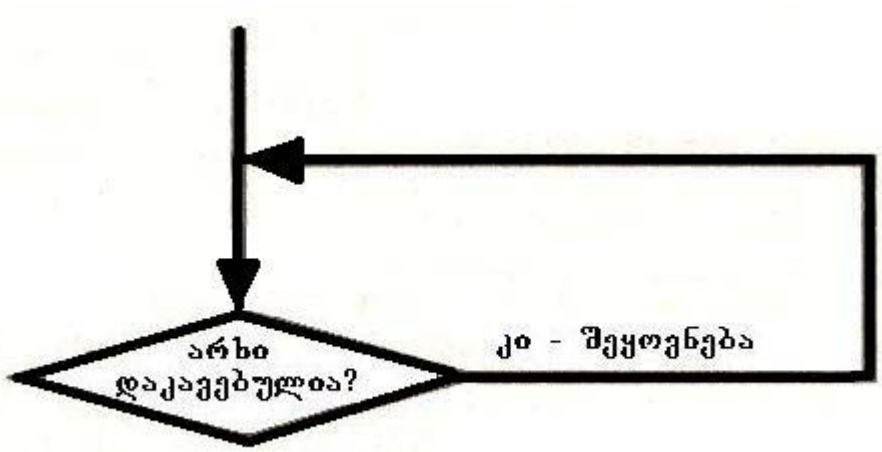
ნახ. 6.1. სადგურები თვალყურს ადევნებენ ქსელის არხის აქტივობას

სიგნალის "წარმტანის არსებობა" ქსელის კაბელში გადამცემი კომპიუტერის (წყარო-კომპიუტერის) მხრიდან ჩვეულებრივ გამოი-

ცნობა მასში (კაბელში) არსებული ძაბვის რაღაც დონის მიხედვით და უჩვენებს იმას, რომ არხი დაკავებულია. თუ ალგორითმის ამ ბიჯზე გადამცემმა სადგურმა ვერ აღმოაჩინა ამგვარი სიგნალის არსებობა, ეს მოწმობს იმაზე, რომ არხი ამ მომენტისთვის თავისუფალია და იგი იწყებს თავისი მონაცემების გადაცემას. თუ არხი დაკავებულია ვიღაცის მიერ და მაინც იგი დაიწყებს გადაცემას, ამ დროს კაბელში წარმოიქმნება "წარმტანის არსებობა" - სიგნალის (ძაბვის) დასშვებზე მაღალი დონე (ამ ფაქტს აფიქსირებს ქსელის პროტოკოლის ანალიზატორი). ეს მიუთითებს იმაზე, რომ ამ მომენტისათვის არხში წარმოიქმნა კოლიზია, შექმნილი სხვა სადგურის (სადგურების) მიერ გადაცემულ პაკეტის (ან პაკეტების) შეჯახებით იმავე მომენტში.

6.1.2. შეყოვნება (ლოდინი), თუ არხი დაკავებულია

თუ წყარო-კომპიუტერმა აღმოაჩინა, რომ არხი დაკავებულია ("წარმტანის არსებობა" სიგნალის სტანდარტული დონით), ან და თუ თავისი პაკეტის გადაცემის დროს ქსელის კაბელში უეცრად (მყისიერად) მოიმატა ძაბვის დონემ, მან უნდა მოიცადოს რაღაც დროით, რათა თავიდან იქნეს აცილებული კოლიზიური მოვლენა (ხოლო თუ კოლიზია მაინც მოხდა, იგი ასევე უნდა დაელოდოს "წარმტანის არსებობას"- სიგნალის მისაღებ სტანდარტულ დონემდე შემცირებას (ნახ. 6.2.)



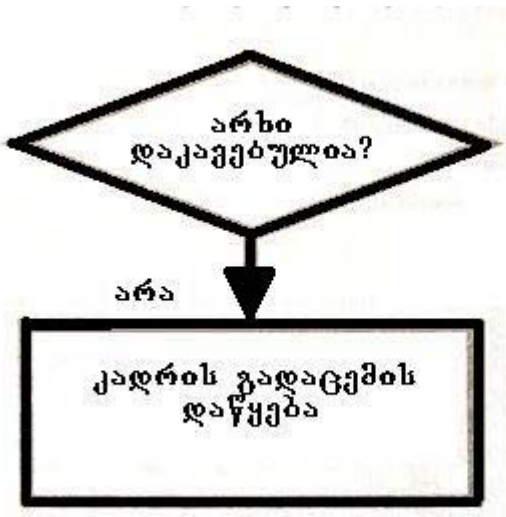
ნახ. 6.2. შეყოვნება თუ არხი დაკავებულია (ან კაბელში წარმიქმნა ძაბვის დასაშვებზე მაღალი დონე)

მუშა სადგურის კორექტულად მომუშავე ინტერფეისული რუქა (ინტერფეისული მოწყობლობა) არ დაიწყებს მაშინვე გდაცემას, თუ კი მისთვის ცნობილი გახდა, რომ არხი დაკავებულია (ჩვენს ანალოგიას თუ გავიხსენებთ, სატელეფონო საუბრისას, თუ ისმის სხვისი ლაპარაკი, უნდა მოვიცადოთ, სანამ იგი არ შეწყვეტს, რის შემდეგაც შეგვიძლია ჩვენ დავიწყოთ ლაპარაკი).

ამგვარად, ძალზე დიდი მნიშვნელობა აქვს ლოდინის რეჟიმის დაცვას. ლოდინის დრო ეწოდება ინტერვალს, რომლის განმავლობაში სადგურმა უნდა მოუცადოს არხის გამონთავისუფლებას, რის შემდეგაც იგი ეცდება თავისი გადაცემის (ან განმეორებითი გადაცემის) დაწყებას.

6.1.3 გადაცემის დაწყება და კოლიზიების (კონფლიქტების) მოსმენა (ბიჯი 3)

თუ არხი თავისუფალია (ე.ი. არხში არის "წარმტანის არსებობის" - სიგნალის ნებადართული დონე) არა უმეტეს 9,6 მწმ-ისა (ეს დრო განსაზღვრულია სტანდარტით Ethernet-ქსელებისათვის), სადგურს შეუძლია დაიწყოს მონაცემების გადაცემა (ნახ.6.3).



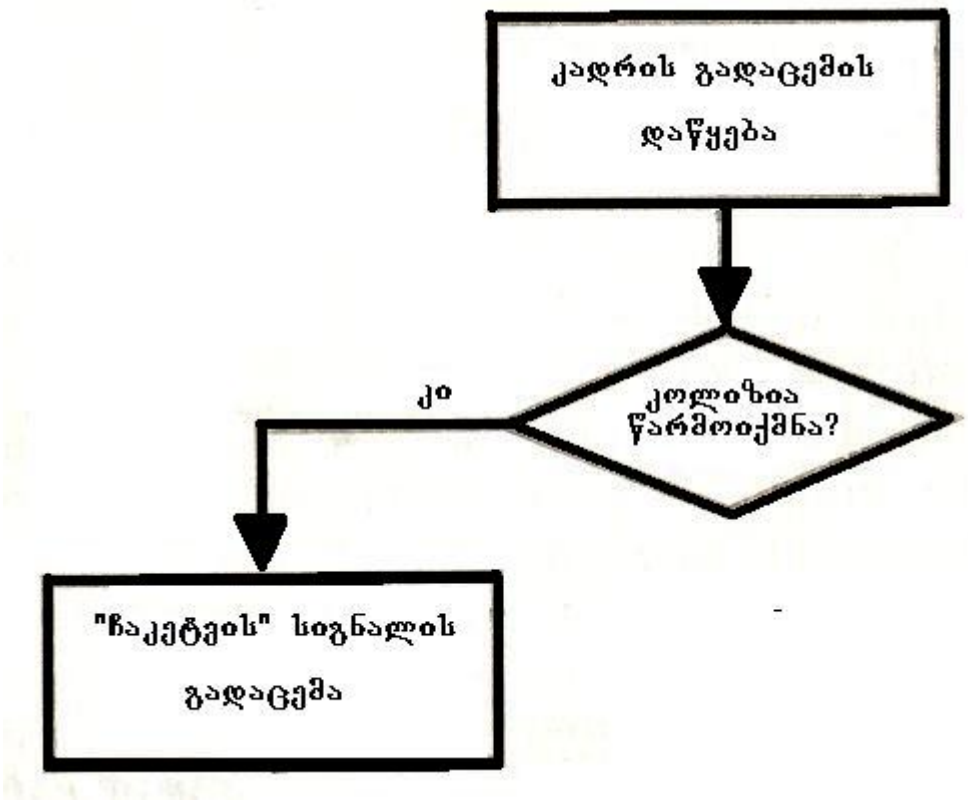
ნახ. 6.3. თუ არხი თავისუფალია, სადგურს შეუძლია გადაცემების დაწყება

სადგური თავის მონაცემთა პაკეტებს ამ შემთხვევაში საკაბელო სისტემაში გადასცემს ორივე მიმართულებით (გავიხსენოთ ქსელის სალტური სტრუქტურა). კვლავ გავიმეოროთ: თუ კი ამ დროს კიდევ ერთი სადგური დაიწყებს პაკეტის (პაკეტების) გადაცემას, არხში წარმოიქმნება კოლიზია. პაკეტები რომლებიც მოხვდებიან

კოლიზიაში (კონფლიქტში), გარდაიქმნებიან უაზრო (უშინაარსო) ფრაგმენტებში. ამიტომ თავისი პაკეტის გადაცემის დროსაც წყარო-კომპიუტერი აგრძელებს არხის სეგმენტის მოსმენას, რათა აღმოაჩინოს, ხომ არ მოხდა კოლიზია? კოლიზიის გამოცნობა როგორც წინა § 6.1.2-ში აღვნიშნეთ, სწარმოებს ქსელის კაბელში ამაღლებული ძაბვის დონით. თუ ეს დონე მკვეთრად გაზრდილია, ეს ნიშნავს რომ, დროის იმავე მომენტში ერთდროულ გადაცემას აწარმოებს ორი ან რამოდენიმე ტრანსივერი (ტრანსივერიებს წარმოადგენს ელექტრონული მოწყობილობები, რომლებიც აწარმოებენ ქსელურ გარემოში მონაცემთა კადრების ფიზიკურ გადაცემებსა და მიღებებს).

შესაძლებელია ისეთი შემთხვევაც, როცა სხვა სადგურები ვერ ამჩნევენ კოლიზიებს და განაგრძობენ თავიანთი კადრების გადაცემებს, რის გამოც მათ მიერ გადაცემული პაკეტები ყოველთვის მოხვდებიან კოლიზიაში "ჩვენი" მუშა სადგურის მიერ გადაცემულ პაკეტებთან (ეს შესაძლებელია მოხდეს, მაგალითად ისეთ შემთხვევებში, როცა სხვა კომპიუტერის (მუშა სადგურის) ადაპტერი დაზიანებულია, რომელიც განუწყვეტლივ "ანაგვიანებს" არხს თავისი პაკეტებით. ასეთ შემთხვევას ქსელური ლიტერატურის ტერმინოლოგიით კადრების "შტორმს", ანუ "ქარიშხალს" უწოდებენ). იმისთვის, რომ თავიდან იქნეს აცილებული ასეთი სიტუაცია, კოლიზიაში მოხვედრილი სადგურები იწყებენ ტრაფიკის "ჩაკეტვის" სიგნალის გადაცემას, რათა აუწყონ სეგმენტის სხვა მუშა

სადგურებს, რომ ხაზი დაკავებულია (რათა მათ ამ მომენტში აღარ დაიწყონ თავიანთი პაკეტების გადაცემა. იხილე ნახ. 6.4.).



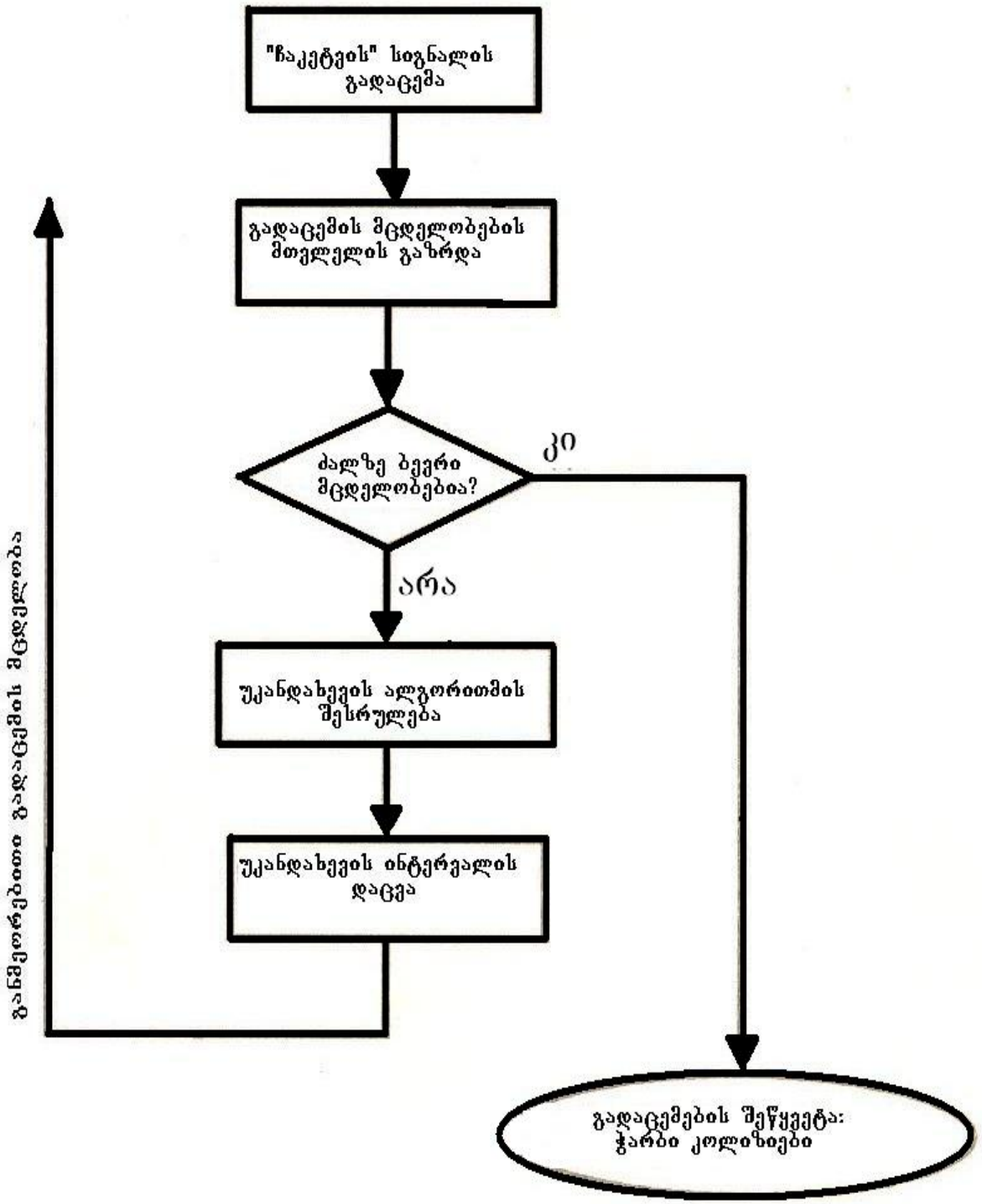
ნახ. 6.4. კოლიზიების წარმოქმნის დროს მასში მოხვედრილი სადგურები იწყებენ ტრაფიკის "ჩაკეტვის" სიგნალის გადაცემას

ტრაფიკის "ჩაკეტვის" სიგნალი განისაზღვრება, როგორც არანაკლები 32-ბიტის შეტყობინება, რომელიც არ ემთხვევა წინა შეტყობინების საკონტროლო თანმიმდევრობას. ის სადგურები, რომლებიც მოხვდნენ კოლიზიაში ზრდიან 1-ით მთვლელებს (გადაცემათა მცდელობის რიცხვის (რაოდენობის) მთვლელებს).

6.1.4. ლოდინი განმეორებითი გდაცემის წინ (ბიჯი 4)

თუ პაკეტების გადამცემი მუშა სადგური (წყარო-კომპიუტერი) დაიწყებს მონაცემთა განმეორებით გადაცემას მაშინვე (კოლიზიის აღმოჩენის შემდეგ), მაშინ კვლავ წარმოიქმნება კოლიზია. ამიტომ საჭიროა დროის ინტერვალების რანჟირება (რანჟირება ზოგადი გაგებით ნიშნავს დროის რაღაც მომენტის გამოყოფას მოწყობილობის მიერ რაღაც მოქმედების შესასრულებლად), რომლის განმავლობაში სადგურებმა უდა მოიცადონ, სანამ დაიწყებდნენ ისინი გადაცემის ახალ მცდელობას.

იმისათვის, რომ სადგურმა შეირჩიოს მომენტი თავის პაკეტის განმეორებით გადაცემისათვის მან უნდა იმოქმედოს ე.წ. "უკანდახევის" (ანუ იძულებითი შეფერხების) ალგორითმით (ნახ. 6.5), რომელიც უზრუნველყოფს მზადყოფნის სხვადასხვა დროებს განმეორებითი გადაცემისათვის.



ნახ. 6.5. სადგურები იწყებენ “უკანდახევის” ალგორითმს განმეორებითი გადაცემის მცდელობის დაწყებისათვის

თუ სადგურები გადაცემის დაწყების ახალი მცდელობის დროით მომენტებს შეარჩევენ შემთხვევით, ალბათობა იმისა, რომ

ორი ან რამოდენიმე სადგური დაიწყებენ ერთდროულად ახალ გადაცემებს, მნიშვნელოვნად მცირდება (თუ ჩვენ გავიხსენებთ გადატანითი მნიშვნელობით სატელეფონო საუბარს, ორი ადამიანის (აბონენტის) ერთდროული საუბრის დროს წარმოიქმნება გაუგებარი ხმაური. მაშინ ორივე მოსაუბრე უნდა გაჩუმდეს და შემდეგ ერთმა მათგანმა უნდა განაახლოს ლაპარაკი (ბუნებრივია შემთხვევით, ვინც დაასწრებს პირველი), ხოლო მეორე უსმენს).

6.1.5. განმეორებითი გადაცემა ან მუშაობის შეწყვეტა (ბიჯი 5)

თუ ქსელის სეგმენტი (რომელზედაც მიერთებულია რომელიმე სადგური, ე.ი. მომხმარებლის პერსონალური კომპიუტერი) დაკავებულია, მაშინ ეს სადგური ვერ შეძლებს გადასცეს თავისი მონაცემები ისე, რომ არ წარმოიქმნას კოლიზია. მუშა სადგურს (წყარო-კომპიუტერს) შეუძლია დაიწყოს თავისი მონაცემების გადაცემის მცდელობები 16-ჯერ (ეს რიცხვი ასევე განსაზღვრულია სტანდატით Ethernet-ქსელებისათვის), შემდეგ იგი წყვეტს გადაცემების ამ მცდელობებს. ასეთ შემთხვევებში სერვერებს გამოჰყავთ თავიანთ მონიტორზე (ეკრანზე) სერვერზე გადაცემების შეწყვეტის რიცხვი (გადაცემების მცდელობათა რაოდენობა) სპეციალური უტილიტის - MONITOR დახმარებით განყოფილებაში "ლოკალური გამომთვლელი ქსელის დრაივერის სტატისტიკური მონაცემები" სტრიქონზე, რომლის სათაურია Excess Collisions Cont

(ჭარბი კოლიზიების მთვლელი). თუ სადგური იმეორებს თავისი მონაცემების გადაცემის მცდელობას და ახალ კოლიზიაში მოხვედრილი პაკეტის ინდიკატორი არაფერს გვიჩვენებს, მაშინ მონაცემთა გადაცემა ამ სადგურის მიერ ითვლება წარმატებით დასრულებული, ხოლო თუ წყარო-სადგური წარუმატებლად შეასრულებს გადაცემის დაწყების ყველა 16 თანმიმდევრულ მცდელობას, მაშინ პაკეტი არ ითვლება გადაცემულად და ხდება გადაცემის ალგორითმის მუშაობის შეწყვეტა (და მიზეზების აღმოფხვრაში კვალიფიციური სპეციალისტების ჩართვა).

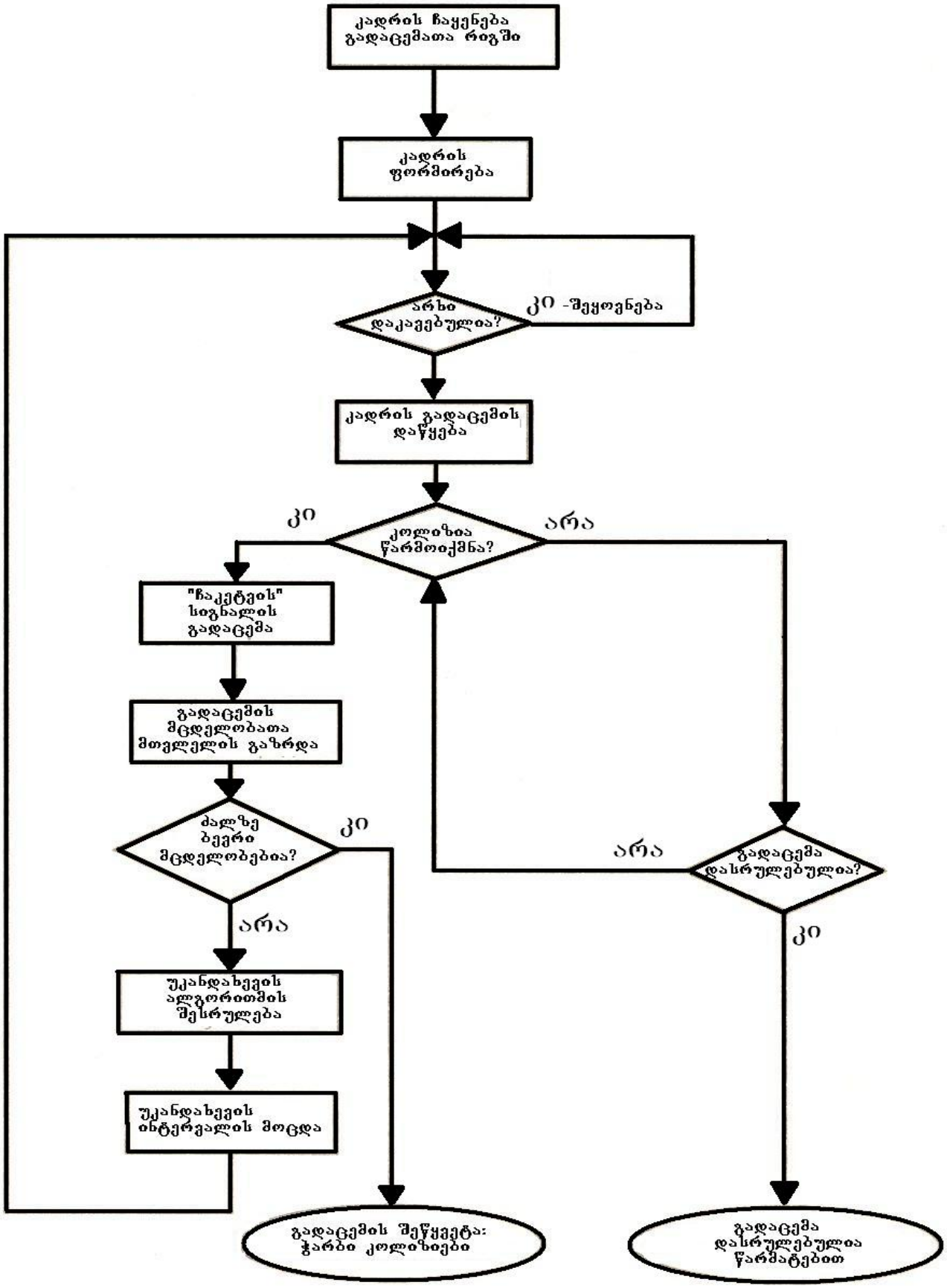
რათა დარწმუნდეს, რომ კოლიზიების აღმომჩენი ფუნქცია მუშაობს კორექტულად (სწორად), თითოეული წარმატებული გადაცემის შემდეგ წყარო-სადგურს შეუძლია ჩაატაროს SQR-ტესტი (ე.წ. სიგნალის ხარისხის შეცდომათა აღმოჩენის ტესტი). SQR-ტესტი სრულდება, თუ ტრანსივერის SQE-ფუნქცია გააქტიურებულია. ამ დროს ყველა რეპიტერმა უნდა ჩააყენონ SQE-ფუნქცია პასიურ მდგომარეობაში (მოახდინონ დეაქტივიზაცია). ამით აქტიური რეპიტერები თვლიან, რომ კოლიზიები იქმნება და ქმნიან ქსელში ტრაფიკის ჩაკეტვას.

6.1.6. მონაცემთა გადაცემის ალგორითმის ფრაგმენტების შეერთება

ყველა ზემოთ განხილული 1-5 ბიჯების გაერთიანება ქმნის მონაცემთა გადაცემის სრულ ალგორითმს. ამგვარად, კავშირის არხში გადამცემი სადგურის (წყარო-კომპიუტერის) შეღწევის ზემოთ განხილული პროცედურების (ალგორითმის ბიჯების) რეალიზაცია, გვაძლევს საშუალებას განვსაზღვროთ თუ რაოდენ ეფექტურია მონაცემთა პაკეტების გადამცემი სადგურის შეღწევა არხში, ასევე ასრულებს თუ არა ყველა სადგური თავის ფუნქციებს CSMA/CD - პროტოკოლის ქსელში შეღწევის წესების დასაცავად.

მონაცემთა გადაცემის ალგორითმის სრული ბლოკ-სქემა წარმოდგენილია ნახ.6.6-ზე.

ეს ალგორითმი აერთიანებს ყველა ბიჯს, რომლებიც უნდა შეასრულოს წყარო-სადგურმა თავისი გადაცემების დროს (კერძოდ, როდესაც ისინი მუშაობენ ქსელში შეღწევის CSMA/CD - პროტოკოლით).



ნახ. 6.6. მონაცემთა გადაცემის გაერთიანებული ალგორითმის ბლოკ-სქემა

6.2. მონაცემთა პაკეტების მიღების ალგორითმი Ethernet-ქსელებისათვის

განვიხილოთ მონაცემთა პაკეტების მიღების ალგორითმი წყარო-კომპიუტერიდან მიმღები კომპიუტერის მიერ ქსელში შეღწევის იმავე CSMA/CD - მეთოდით, რომლის შესახებაც საუბარი გვქონდა წინა 6.1. პარაგრაფში.

როგორც ადრე შევნიშნეთ, თუ რომელიმე სადგური გასცემს მონაცემთა პაკეტებს, მაშინ იგი მათ ავრცელებს ქსელის სეგმენტის ორივე მხარეს, რომელზედაც მიერთებულია მიმღები კომპიუტერები (მუშა სადგურები). ეს უკანასკნელნი მიღების დროს ფუნქციონირებენ მონაცემთა მიღების ალგორითმის მიხედვით, რომელიც შედგება შემდეგი 4 ბიჯისაგან:

ბიჯი 1 - მონაცემთა შემოსული პაკეტების დათვალიერება და ფრაგმენტების აღმოჩენა მიმღები კომპიუტერის მიერ;

ბიჯი 2 - მიმღების მისამართის შემოწმება;

ბიჯი 3 - მონაცემთა პაკეტის მთლიანობის შემოწმება, თუ პაკეტი დანიშნულებისამებრ მიიღო ქსელის მიმღებმა კომპუტერმა;

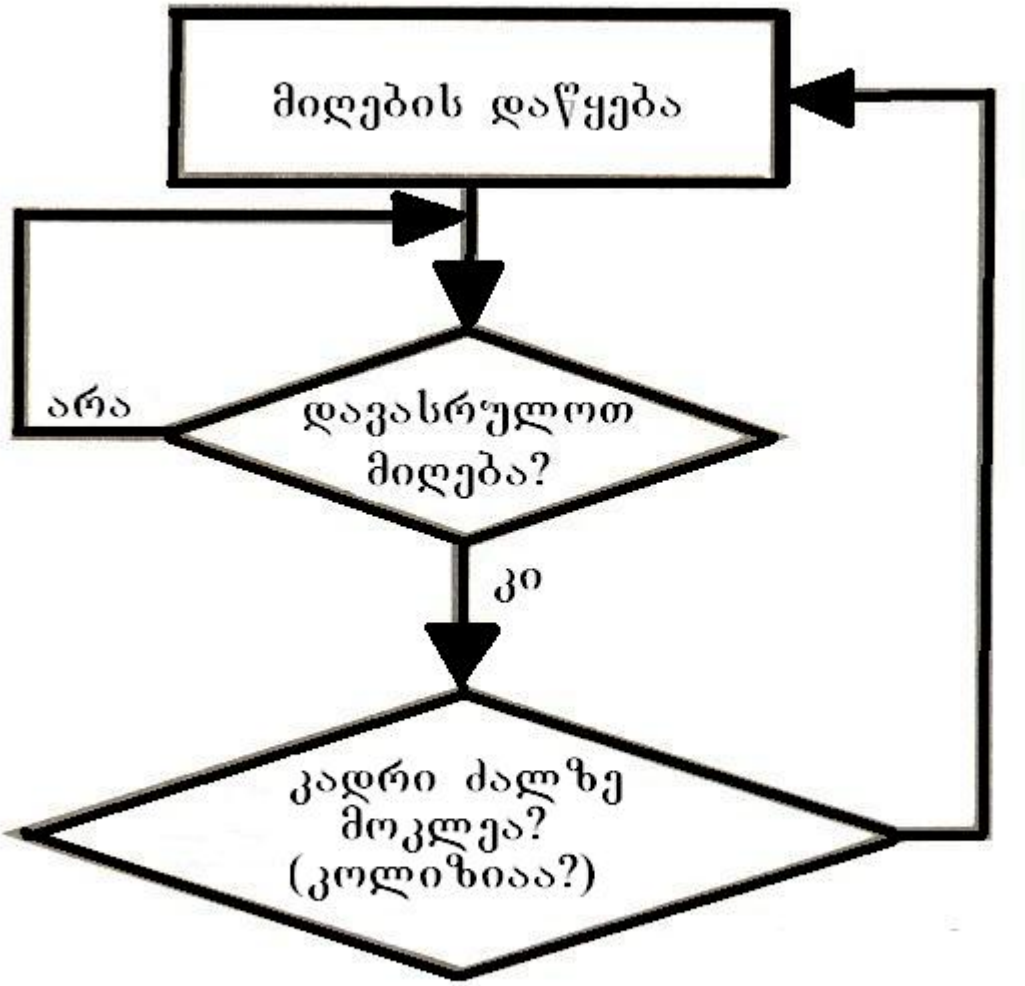
ბიჯი 4 - პაკეტის დამუშავება მიმღებ კომპიუტერში.

როგორც წინა, მონაცემთა გადაცემის ალგორითმის დროს, ამ შემთხვევაშიც მოკლედ განვიხილოთ მონაცემთა მიღების

ალგორითმის თითეული ბიჯი ძირითადი პროცედურებისა და შესაბამისი ბლოკ-სქემების ფრაგმენტების სახით. აღნიშნული პარაგრაფის დასასრულს კი ვაჩვენოთ მონაცემთა პაკეტების მიღების სრული ალგორითმის ბლოკ–სქემა ხსენებული ფრაგმენტების გაერთიანებით.

6.2.1. ქსელის სეგმენტში შემოსული პაკეტების დათვალიერება და ფრაგმენტების აღმოჩენა (ბიჯი 1)

კომპიუტერულ ქსელში ყველა სადგური, რომლებიც მიერთებული არიან ერთ სეგმენტზე, ათვალიერებენ მონაცემთა თითოეულ პაკეტს, რომლებიც კი მიეწოდება მათ არხით (იგულისხმება კომპიუტერული ქსელის ფიზიკური დონის არხი), იმის მიუხედავად ეს პაკეტი რომელ სადგურზე არის დამისამართებული (თუ მოვიყვანთ წინა პარაგრაფში ნაჩვენებ ტელეფონით საუბრის ანალოგს, ეს პროცედურა მოგვაგონებს საერთო სარგებლობის სატელეფონიო ხაზში მიმდინარე პროცესს. სპეციალური მოწყობილობით შესაძლებელია მოისმინოთ აბონენტთა ის საუბრებიც, რომლებიც თქვენ არ გეხებათ). როგორც ნახ.6.7-ზე არის ნაჩვენები, მიმღები სადგური ამოწმებს მონაცემთა პაკეტს რათა დარწმუნდეს, რომ მას გააჩნია დასაშვები სიგრძე (სტანდარტით უნდა იყოს არანაკლები 64 ბაიტისა) და არ წარმოადგენს ფრაგმენტს, რომელიც წარმოქმნილია კოლიზიების შედეგად.

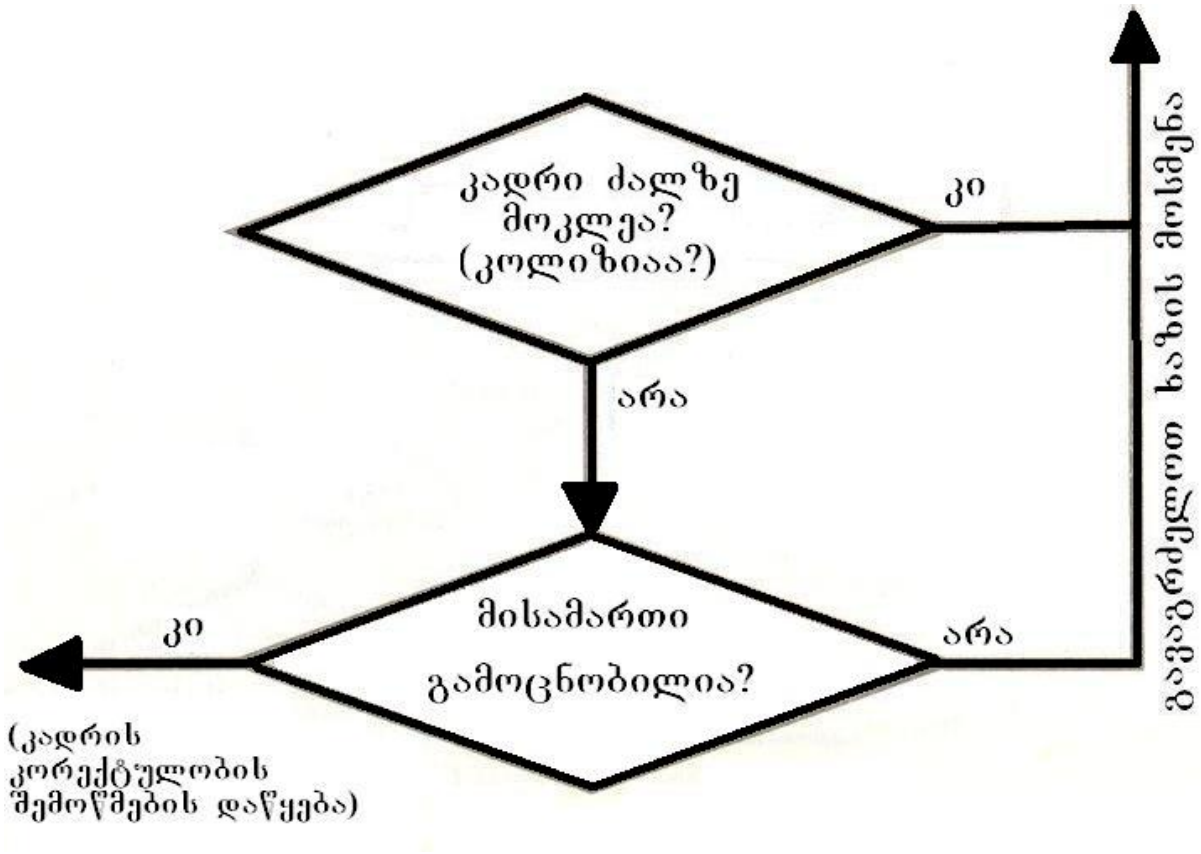


ნახ. 6.7. პაკეტების დათვალიერების დროს მიმღები სადგური ეძებს ფრაგმენტებს

6.2.2. მიმღების მისამართის შემოწმება (ბიჯი 2)

დარწმუნდება რა იმაში, რომ მონაცემთა პაკეტი არ წარმოადგენს ფრაგმენტს (ე.ი. არ არის დამახინჯებული და მისი სიგრძეც დასაშვებ ფარგლებშია), მიმღები სადგური ამოწმებს მიღებული პაკეტის მისამართს (ე.ი. ახდენს თავისი მისამართის (ხშირად უწოდებენ MAC – ფიზიკურ მისამართს) შედარებას

მიღებული პაკეტის კადრების სამისამართო ველში ნაჩვენებ მიმღების მისამართთან), რათა მიიღოს გადაწყვეტილება ეს პაკეტი დაამუშაოს თუ არა (ნახ.6.8).



ნახ. 6.8. სადგური ამოწმებს მიმღების მისამართს

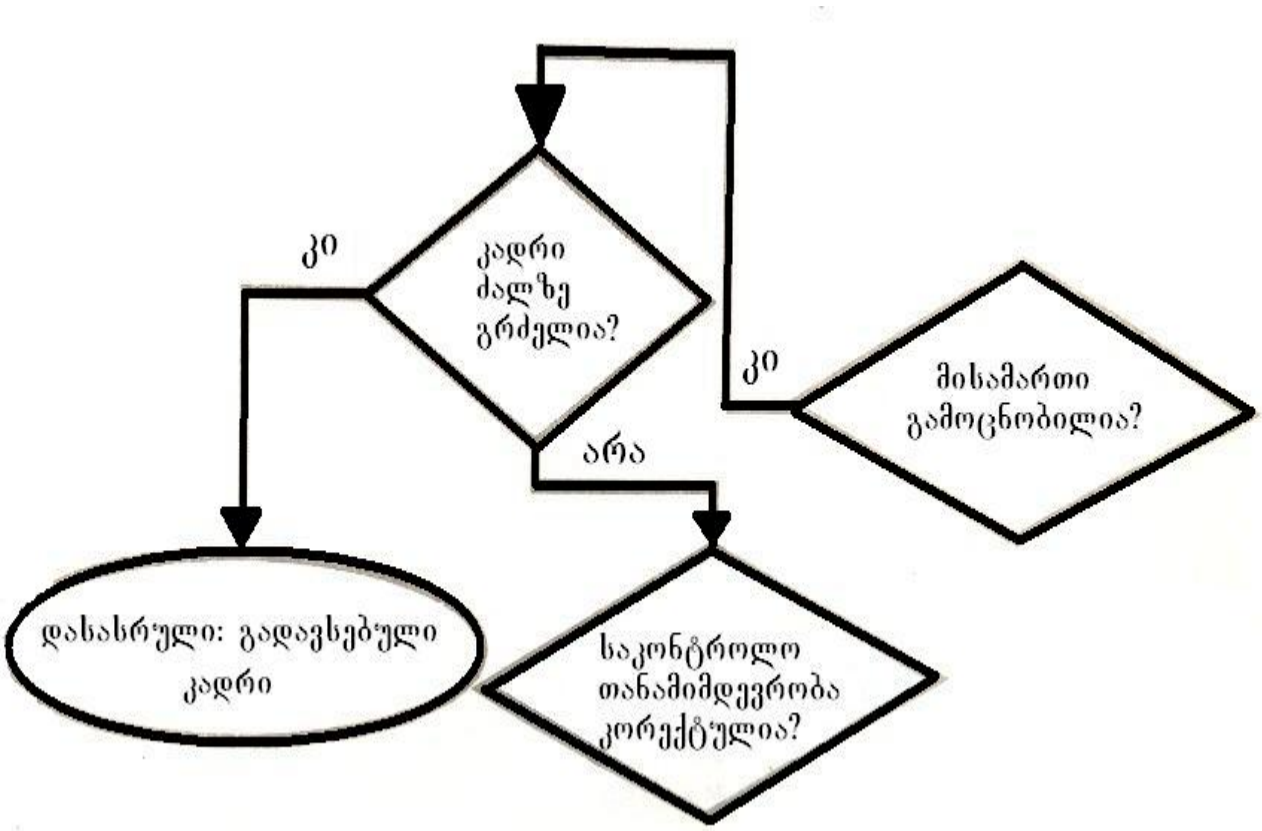
თუ შემოსული პაკეტი დამისამართებულია მიმღებ სადგურზე, ან წარმოადგენს იგი ფართოსამაუწყებლო დანიშნულების შეტყობინებას, ანდა გააჩნია მას (პაკეტს) ჯგუფური მისამართი, მიმღები სადგური გადადის ალგორითმის მომდევნო ბიჯის შესრულებაზე.

ფართოსამაუწყებლოს, როგორც ადრეც აღვნიშნეთ, წარმოადგენს შეტყობინება (პაკეტი), რომელიც დამისამართებულია ყველა სადგურზე, რომლებიც კი მიერთებული არიან ქსელთან (ასეთ შეტყობინებას წარმოადგენს, მაგალითად, შეტყობინება ყველა სადგურის მიმართ რათა აუწყოს მათ წყარო-კომპიუტერმა ქსელური მომსახურების რაიმე სახე). ჯგუფური მისამართების მქონე შეტყობინება დამისამართებულია მუშა სადგურების გარკვეულ რაოდენობაზე (კონკრეტულ ჯგუფზე), რომელიც კი მიერთებულია ამ ქსელთან (ასეთს წარმოადგენს მაგალითად, შეტყობინება DEC – მარშრუტიზატორებისათვის).

6.2.3. მონაცემთა პაკეტის მთლიანობის შემოწმება (ბიჯი 3)

ამ მომენტისათვის პაკეტის მიღების ალგორითმის მე-2 ბიჯის შესრულების შემდეგ მიმღებმა სადგურმა უკვე იცის, რომ მონაცემთა პაკეტი არ წარმოადგენს ფრაგმენტს და დამისამართებულია უშუალოდ მასზე, თუმცა ჯერ არ იცის, კორექტულადა (სწორადაა) თუ არა იგი ფორმირებული. ასეთ დროს მიმღებ სადგურებს შეუძლიათ მაინც წაიკითხონ მონაცემთა პაკეტები, დამახინჯებულნი არხით გადაცემების დროს, ან არაკორექტულად არიან ისინი ფორმირებული წყარო-კომპიუტერის მიერ.

იმისათვის, რომ მიმღებმა სადგურმა უქმად არ დახარჯოს დრო დამახინჯებული პაკეტების დამუშავებაზე, მან უნდა მოახდინოს მათი რამოდენიმე პარამეტრზე შემოწმება (ნახ.6.9).



ნახ.6.9. პაკეტების მთლიანობაზე შემოწმება

უპირველეს ყოვლისა მიმღებმა სადგურმა უნდა შეამოწმოს მიღებული პაკეტის სიგრძე. თუ კადრი გრძელია 1518 ბაიტზე (როგორც ადრეც შევნიშნეთ, ასეთი რაოდენობა განსაზღვრულია, სტანდარტით Ethernet – ქსელებისათვის), იგი ითვლება გადავსებულად. გადავსებული კადრები შეიძლება წარმოიქმნენ ქსელური დრაივერის უწესრიგობის გამო.

მიმღებმა სადგურმა ასევე უნდა დაადგინოს, ხომ არ შეიცვალა (მოცემულ პაკეტში მისი საკაბელო სისტემაში გავლის დროს) თანრიგების მნიშვნელობები 1 დან 0-ზე, ან პირიქით, რაც ასევე ამახინჯებს პაკეტის მონაცემებს. თუ პაკეტი არ არის გადავსებული მიმღები სადგური ამოწმებს პაკეტს,

რათა განსაზღვროს ემთხვევა თუ არა მისი შიანარსი იმას, რაც გადმოსცა გამომგზავნმა წყარო-კომპიუტერმა. ამ შემოწმებას ეწოდება კადრის საკონტროლო თანამიმდევრობის შემოწმება (იხილეთ ოთხბაიტიანი ველები Ethernet – ის ქსელებში გამოყენებული კადრების სტრუქტურებში). იგი ხორციელდება ჭარბი ციკლური კოდის დახმარებით. თუ აღმოჩნდება, რომ საკონტროლო თანამიმდევრობა კორექტულია, მაშინ მიმღები სადგური ამოწმებს პაკეტის გათანაბრებას. ეს ნიშნავს იმას, რომ ყველა პაკეტი უნდა შიეცავდეს ბაიტების სრულ რიცხვს (1 ბაიტი = 8 ბიტს) და უნდა მთავრდებოდეს 8–ბიტიან საზღვარზე. ის პაკეტები, რომლებიც არ მთავრდებიან ბაიტის საზღვარზე, ითვლებიან არაკორექტულად გათანაბრებულები. პაკეტს არ უნდა ქონდეს სიგრძე, მაგალითად, 72 ბაიტი და 3 ბიტი ასეთ შემთხვევაში პაკეტის სიგრძე უნდა იყოს ან 72 ან 73 ბაიტი.

თუ კადრის საკონტროლო თანამიმდევრობა არაკორექტულია, მაგრამ იგი (კადრი) შეიცავს ბაიტების სრულ რიცხვს (ე.ი. კორექტულადაა გათანაბრებული), ასეთ შემთხ-ვევაში ითვლება რომ ადგილი აქვს შეცდომას საკონტროლო თანამიმდევრობაში. ამგვარად პაკეტის შემოწმებისას მიმღები სადგური არკვევს:

- წარმოადგენს თუ არა პაკეტი ფრაგმენტს?
- ხომ არ არის ძალზე დიდი (გრძელი) მისი სიგრძე?
- ხომ არა არის მისი საკონტროლო თანამიმდევრობა შეცდომის შემცველი?
- კორექტულად (სწორად) არის თუ არა იგი გათანაბრებული?.

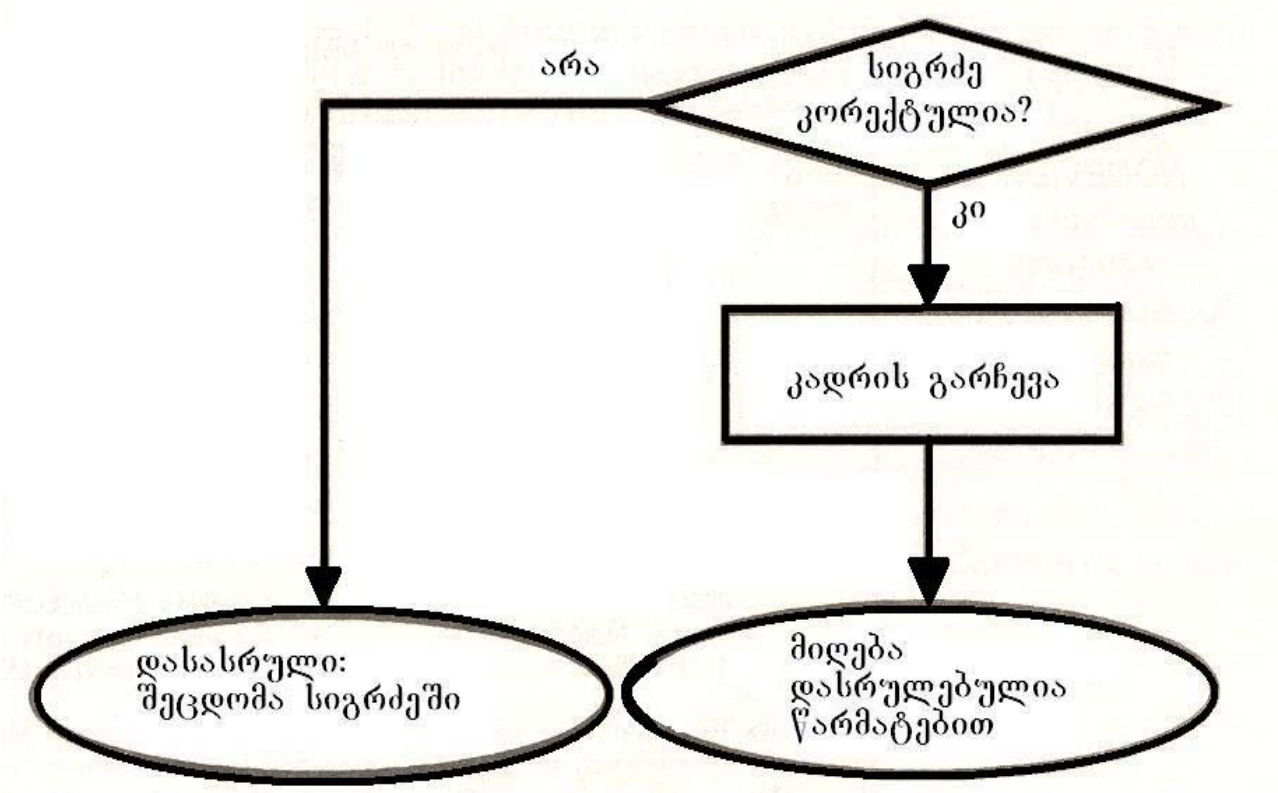
მხოლოდ ასეთი შემოწმების გავლის შემდეგ (ე.ი. თუ შემოწმებისას დარღვევები არ აღმოჩნდება მიმღები სადგური მოახდენს ბოლო შემოწმებას: ხომ არა არის კადრი ძალზე მოკლე? თუ კადრი მოკლეა 64 ბაიტზე (გავიხსენოთ რომ ეს რაოდენობაც სტანდარტითაა განსაზღვრული Ethernet – ქსელებისათვის) და ამასთან იგი კორექტულადაა ფორმირებული (ე.ი. ყველა წინა შემოწმებების შედეგი დადებითია), ითვლება, რომ კადრი არასაკმარისადაა დატვირთული (ასეთ კადრებს ქსელურ ლიტერატურაში ხატოვნად "კარლიკ-კადრებს" უწოდებენ და ის უნდა შეივსოს ნოლებით). არასაკმარისად დატვითული კადრები შეიძლება წარმოიქმნას ქსელური დრაივერის მტყუნების დროს.

ამგვარად, ყველა ზემოთხსენებული შემოწმების გავლისას საბოლოოდ დგინდება პაკეტების სიგრძე და მისი შინაარსის ფორმირება (ამ შემთხვევაში "შინაარსის" ფორმირების კორექტულბაში იგულისხმება მისი გაფორმების გარეგნული სახე და არა თვით შინაარსი მისი პირდაპირი გაგებით). თუ ყველა შემოწმება გაიარა წარმატებით, მიმღები სადგური შეუდგება ალგორითმის ბოლო ბიჯის - მის (პაკეტის) დამუშავებას, ე.ი. იგი გადაეცემა უფრო მაღალი დონის პროტოკოლს და მას ამუშავებს მიზნობრივი დანიშნულების ესა თუ ის პროგრამული დამატება, რომელიც ფუნქციონირებს კომპიუტერული ქსელის გამოყენებით დონეზე (OSI-მოდელის მოდელის მე-7 დონეზე), წინააღმდეგ შემთხვევაში იგი (მიმღები სადგური) არ გადასცემს მაღალი დონის პროტოკოლს მანამდე, სანამ შემოწმების ყველა პირობა არ დაკმაყოფილდება.

ამგვარად ზემოთხსენებული შემოწმებების პროცედურების გავლის შემდეგ სრულდება ალგორითმის ბოლო საფეხური (ბოლო ბიჯი).

6.2.4. პაკეტის დამუშავება (ბიჯი 4)

როგორც წინა ქვეპარაგრაფ 6.2.3-ში აღვნიშნეთ, პაკეტი, რომელმაც წარმატებით გაიარა ყველა შემოწმება მიღების ალგორითმის მიხედვით (ნახ. 6.10), ითვლება როგორც კორექტული, სწორად ფორმირებული და გააჩნია დასაშვები სიგრძე.

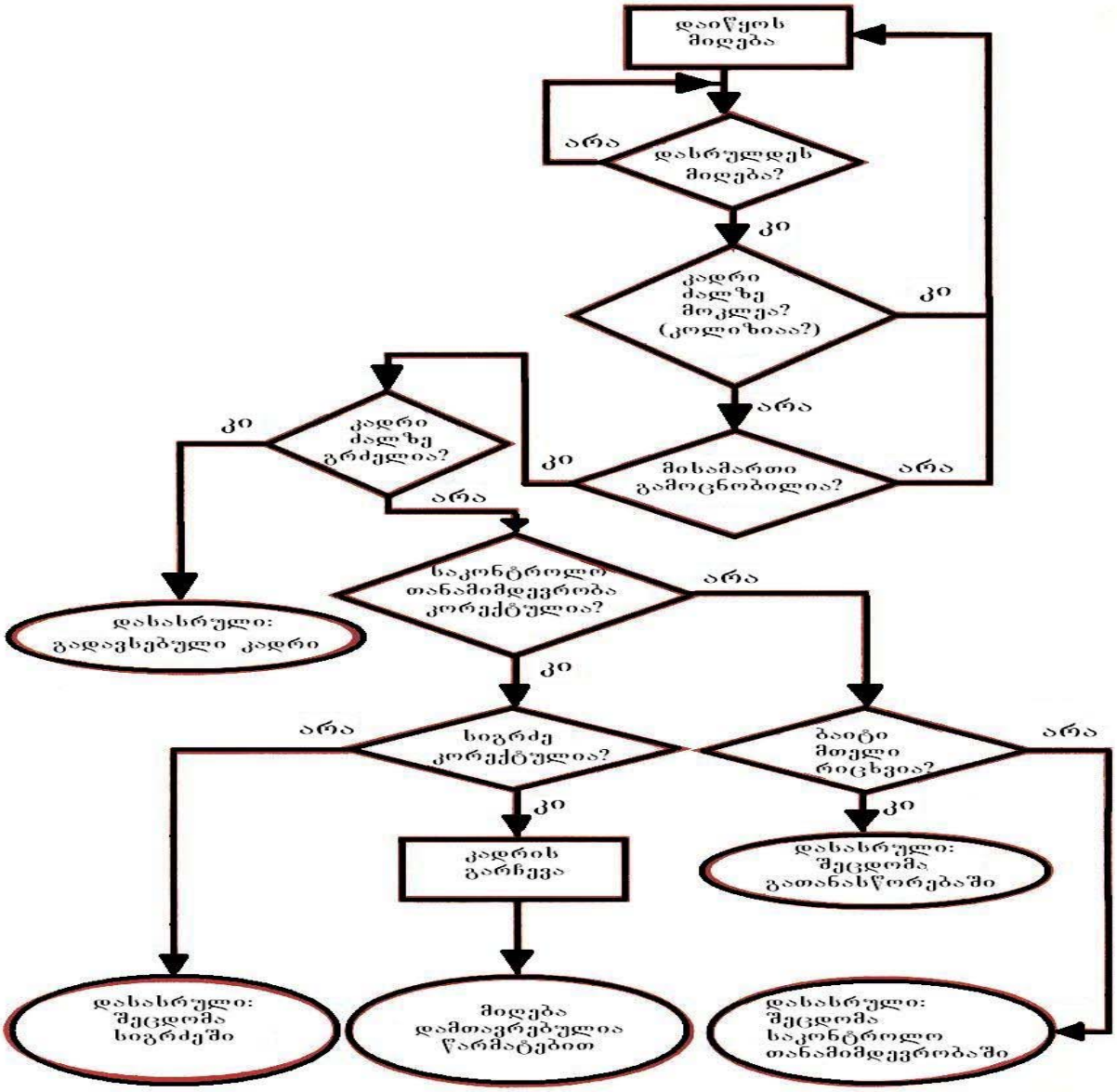


ნახ. 6.10. შემოწმების შემდეგ პაკეტი გადაეცემა დამუშავებაზე

თუ წარმოიქმნა ისეთი შემთხვევა, როდესაც მიმღებ - სადგურს (მომხმარებლის მიმღებ კომპიუტერს) არ შეუძლია კორექტულად მიიღოს პაკეტი, გამოგზავნილი წყარო-კომპიუტერიდან, მაშინ აუცილებელია ჩატარდეს უფრო დაწვრილებითი გამოკვლევა რათა დადგინდეს ხელისშემშლელი ფაქტორები. მაგალითად, ასეთი ფაქტორები შეიძლება იყვნენ სადგურში ჩატვირთული კადრის არასწორი ტიპი, შეცდომა პაკეტის სათაურში (მაგალითად, IPX\SPX – სათაურში) და სხვა.

6.2.5. მონაცემთა მიღების ალგორითმის სრული სახე

ზემოთ განხილული ყველა საფეხურის (ბიჯების) გაერთიანება გვაძლევს კომპიუტერულ ქსელებში მონაცემთა პაკეტების მიღების სრულ სახეს. მიღების ალგორითმის ბლოკ-სქემა, რომელიც წრმოდგენილია ნახ. 6.11-ზე, ასახავს ყველა იმ საჭირო პროცედურას, რომელიც აუცილებელია მონაცემთა პაკეტების კორექტულად მიღებისა და მისი შემდგომი დამუშავებისათვის ქსელის მიმღები სადგურების მიერ.



ნახ. 6.11. მონაცემთა პაკეტის მიღების ალგორითმის ბლოკ-სქემა

აღნიშნული თავის დასასრულს მოკლედ აღვნიშნოთ თუ რა საშუალებითაა შესაძლებელი წინა პარაგრაფებში (§6.1 და §6.2) განხილული ალგორითმების შემოწმება.

6.3. კომპიუტერულ ქსელში სადგურების შესაძლებლობების შემოწმების საშუალებები მონაცემთა პაკეტების გადაცემა - მიღებაზე

კომპიუტერულ ქსელში თუ მუშა სადგურები (მომხმარებელთა პერსონალური კომპიუტერები) ჩართული არიან სწორად, გააჩნიათ გამართულად მომუშავე რუქები და ტრანსივერები და იცავენ CSMA\CD - სპეციფიკაციის მიერ დადგენილი ალგორითმების ყველა წესს, მაშინ შესაძლებლობა ეძლევათ გადასცენ და მიიღონ კორექტულად ფორმირებული მონაცემთა პაკეტები.

იმ შემთხვევაში, როდესაც ქსელის მომხმარებელი უკმაყოფილოა ქსელის სეგმენტში სათანადო ხარისხის კავშირის არ არსებობით, შესაძლებელია შემოწმდეს ქსელთან მიერთებულია სადგურების უნარი სწორად გადასცენ და მიიღონ მონაცემთა პაკეტები (ე.ი. რეალიზება მოახდინონ პაკეტების გადაცემა-მიღების ალგორითმების). ამ მიზნით გამოიყენება ქსელის პროტოკოლების ანალიზატორი.

ამჟამად არსებობს ანალიზატორების მრავალნაირი სახეობა, რომლებიც ერთმანეთისგან განსხვავდებიან მათი ტექნიკური შესაძლებლობებითა (რომლებიც აისახება შესაბამისი ღირებულებითაც) და იმ ოპერაციული სისტემებით, რომელთა დახმარებითაც ისინი აწარმოებენ საკონტროლო-სადიაგნოსტიკო პროცედურებს. შესაბამისად არსებობს მრავალი ფირმა, რომელიც დაკავებულია აღნიშნული ანალიზატორების როგორც პროგრამული საშუალებების უზრუნველყოფით, ასევე აწარმოებენ (და

გამოაქვთ ქსელურ ბაზარზე გასაყიდად) მათ სარეალიზაციო აპარატურასაც.

მაგალითის სახით აღვნიშნოთ რომ NCC LANalyzer ანალიზაორის (მწარმოებელი ფირმა Network communication corporation) გამოყენებითი პროგრამა NODEVIEW (დამუშავებული Novell ფირმის მიერ) ამოწმებს კავშირის ხარისხს ქსელის იმ სადგურებს შორის, რომლებშიც ჩატვირთულია IPX - პროტოკოლი (ეს ანალიზატორი ფუნქციონირებს Netware - ოპერაციულ გარემოში). ამავე ფირმის სხვა გამოყენებითი პროგრამით, მაგალითად, SERVERVU, შეიძლება შემოწმდეს კავშირის ხარისხი ფაილ-სერვერებთან.

გამოყენებითი პროგრამა NODEVIEW, რომელიც ინსტალირებულია (გაწყობილია) ზემოთ ნახსენებ NCC LANalyzer – ანალიზატორში, შემოწმებისას გადასცემს ქსელში ფართოსამაუწყებლო შეტყობინებას სადიაგნოსტიკო პაკეტის სახით, რომელიც ცნობილია "პინგ-პონგის" სახელწოდებით. ამ შეტყობინებას შემოწმების პროცედურის დროს უნდა უპასუხონ ყველა იმ სადგურებმა რომლებშიც ჩატვირთულია პროტოკო-ლი Diagnostic responder - პროტოკოლი. მოპასუხე სადგურების სია გამოიყვანება სადგურის (მომხმარებლის კომპიუტერის) ეკრანზე MONITOR - უტილიტის დახმარებით (უტილიტის ქვეშ იგულისხმება მცირე ზომის და კონკტერული დანიშნულების მმართველი პროგრამა), რომლებიც აცნობებენ თავიანთ შესძლებლობებს მონაცემთა პაკეტების კორექტულად გადაცემა-მიღების ოპერაციების რეალიზაციებზე. თუ რომელიმე სადგური არ

რეაგირებს "პინგ-პონგის" ტესტზე, ანალიზატორი მიუთითებს კონკრეტულ უწესრიგობაზე. მაგალითად, იგი შეიძლება იყოს სადგური, კონფიგურირებული არასწორად, ანდა სხვა უწესივრობები, რომელთა მიზეითაც არასწორად სრულდება სადგურებში პაკეტების გადაცემისა და მიღების ფუნქციები. სადიაგნოსტიკო ტესტით მოწმდება ჩვენს მიერ ზემონახსენები ისეთი უწესივრობები, როგორიცაა, მაგალითად, კორექტულად გამოიყენება კადრის ტიპი თუ არა, ამასთან ანალიზატორი მიუთითებს იმასაც, რომ საჭიროა შეიცვალოს კადრების ტიპი ამა თუ იმ სადგურში, რომელიც განსაზღვრულია, მაგალითად, NET.CFG - ფაილში. შეიძლება უჩვენოს ის უწესივრობები, რომლებიც ეხება პროტოკოლებს შორის განსხვავებულო-ბას, უწესივრობას ინტერფეისულ რუქებში, ტრანსივერებში, საკაბელო სისტემების შემაერთებლებში და ა.შ., რის შემდეგაც ქსელის სპეციალისტები (რომელთა შორის აქტიური როლი აკისრიათ ქსელის ადმინისტრატორებს) აღმოფხვრიან ხსენებულ უწესივრობებს ან საჭიროების შემთხვევაში მიმართავენ ქსელური აპარატის დამამზადებელ ფირმებს.

თავი 7

კომპიუტერული ქსელის მონიტორინგის და მართვის ალგორითმები

7.1. ზოგადი განმარტებები კომპიუტერული ქსელის მონიტორინგისა და მართვის შესახებ

ნებისმიერი ტიპისა და დანიშნულების კომპიუტერული ქსელის ფუნქციონირების ნორმალური რეჟიმის დასაცავად, იგი საჭიროებს მუდმივი კონტროლის განხორციელებას მონაცემთა პაკეტების გადაცემა–მიღების ალგორითმების (განხილული წინა მე-6 თავში) ეფექტური რეალიზაციების მიზნით. ამისათვის საჭიროა მთელი რიგი ღონისძიებების ჩატარება ქსელის მუშა მდგომარეობაში მუდმივად მზადყოფნის შესანარჩუნებლად.

მონაცემების გადაცემა–მიღებაზე კონტროლი – ეს არის აუცილებელი პირველი ნაბიჯი, რომელიც უნდა შესრულდეს ქსელის მართვის დროს. ამ ფუნქციის მნიშვნელობიდან გამომდინარე მას (კონტროლს) ხშირად გამოყოფენ ქსელის მართვის სისტემის სხვა ფუნქციებიდან და ახორციელებენ სპეციალური მეთოდებითა და საშუალებებით.

კონტროლის მეთოდებისა (ამ მეთოდებზე დაფუძნებული საკონტროლო პროცედურების ალგორითმების) და საშუალებების ეფექტური გამოყენებით პირველ რიგში დაინტერესებული

არიან ქსელის ადმინისტრატორები, რომლებიც პასუხს აგებენ მათ დაქვემდებარებაში მყოფი ქსელური სისტემის გამართულ მუშაობაზე. მათ ხელთ არსებული საკონტროლო საშუალებები ეხმარებიან ქსელის ადმინისტრატორებს დროულად გამოავლინონ ქსელის პრობლემური მონაკვეთები (ქსელის სეგმენტები) და ამ მონაკვეთებში ჩართულ მოწყობილობებში უწესრიგობები. მათი დროებითი ამორთვა (პრობლემური მონაკვეთების) ან ქსელის რეკონფიგურაცია საჭიროების შემთხვევაში შესაძლებელია როგორც ავტომატურად, ასევე ხელით.

ქსელის მუშაობის კონტროლის მართვის მთლიან პროცესს ყოფენ ორ ეტაპად: მონიტორინგისა და ანალიზის პროცესად.

მონიტორინგის ქვეშ იგულისხმება კომპიუტერულ ქსელში თვალყურის დევნა მასში მიმდინარე ქსელურ პროცესებზე და მათი სარეალიზაციო აპარატურის მუშაობის რეჟიმებზე. ქსელის მონიტორინგი შედარებით უფრო მარტივ პროცედურას წარმოადგენს ქსელის ანალიზის პროცედურასთან შედარებით. მასში შედის ქსელის მუშაობის შესახებ პირველადი მონაცემების შეგროვება, როგორიცაა მაგალითად: სტატისტიკა ქსელში მოძრავი კადრებისა და პაკეტების რაოდენობის შესახებ, რომლებიც სარგებლობენ (ან უნდა ისარგებლონ) სხვადასხვა პრიორიტეტებით; ქსელში ცირკულირებული მმართველი მარკერების მოძრაობა ქსელის სადგურებს შორის; სხვადასხვა უტილიტების შესრულების კონტროლის და სხვა. ონიტორინგით დგინდება პორტების მიმდინარე მდგომარეობა კონცენტრატორებში, კომუტატორებში, მარშრუტიზატორებში და ა.შ.

ქსელის მონიტორინგის შემდეგ სრულდება მისი ქსელის ანალიზატორის მიერ მოპოვებული (შეგროვებული) სტატისტიკური მონაცემების ანალიზის ეტაპი. ანალიზი, როგორც ზემოთ შევნიშნეთ, უფრო რთული პროცედურაა, რომლის ქვეშ იგულისხმება უფრო რთული და ინტელექტუალური პროცესი. მისი მიზანია გაირკვეს ქსელში შექმნილი არასახარბიელო მდგომარეობის მიზეზი (ამა თუ იმ პროცესის მიმდინარეობის შესახებ). ანალიზის დროს სწარმოებს მონიტორინგის სხვადასხვა ეტაპებზე მიღებული ინფორმაციის (მონაცემების) შედარება საბაზო მონაცემებთან, რომლებიც უნდა შესაბამებოდნენ მონაცემებს, მიღებულს ქსელის მუშაობის ნორმალურ რეჟიმში, რათა შემუშავდეს (ადმინისტრატორის ან ქსელის სხვა სპეციალისტების მხრიდან) ღონისძიებები ქსელის მუშაობის შენელების ან არასაიმედოდ ფუნქციონირების შესაძლო მიზეზების აღსაკვეთად.

7.2. მონიტორინგის ალგორითმები

კომპიუტერული ქსელის მონიტორინგის ამოცანები მრავალნაირია. მათი გადაწყვეტა ხდება როგორც პროგრამული საშუალებებით, ასევე სპეციალური აპარატურის დახმარებით, გამზომი ხელსაწყოებით, ტესტერებით. მონიტორინგის ამოცანები წყდება როგორც ავტონომიურად მომუშავე ქსელური ანალიზატორებით, ასევე მონიტორინგის საკომუნიკაციო მოწყობილობებში ჩაშენებული (ჩადგმული) საშუალებებით. მონიტორინგი ხორციელდება ქსელის მართვის სისტემის ე.წ. აგენტებით.

მონიტორინგის პროცედურებში, განსაკუთრებით კი ანალიზის ამოცანების გადაწყვეტაში, დიდ როლს თამაშობს ადამიანის აქტიური მონაწილეობა (როგორც შევნიშნეთ, პირველ რიგში ქსელის ადმინისტრატორის), თუმცა ბოლო პერიოდში მისი (ადამიანის) შრომის გასაადვილებლად გამოიყენება საკმაოდ რთული პროგრამული საშუალებები, რომლებშიც შეთავსებულია როგორც მონიტორინგის, ისე ანალიზის ფუნქციები ქსელის ნორმალური ფუნქციონირების დიაგნოსტიკის მიზნით. ასეთ უახლოეს ავტომატიზირებულ სადიაგნოსტიკო საშუალებას წარმოადგენს ექსპერტული სისტემები, რომლებშიც აკუმულირებულია ქსელის მრავალი სპეციალისტის პრაქტიკული გამოცდილება.

კომპიუტერული ქსელის მონიტორინგის ალგორითმები მოიცავენ შემდეგ ძირითად ეტაპებს:

1. ქსელის ყველაზე აქტიური კლიენტ/სერვერების განსაზღვრა;
2. სადგურების გამოვლენა, რომლებიც ყველაზე მეტად ტვირთავენ ქსელის გატარების ზოლს;
3. იმ სადგურების გამოვლენა, რომლებიც იწვევენ შეცდომების წარმოქმნას ქსელში;
4. ინფორმაციის შეგროვება სახელწოდებების შესახებ.

განვიხილოთ მოკლედ ზემოთ ჩამოთვლილი პროცედურების არსი.

1. ქსელის ყველაზე აქტიური კლიენტ/სერვერების განსაზღვრა

ქსელის სერვერსა და რომელიმე მუშა სადგურს შორის ტრაფიკის ფილტრაციის გზით განსაზღვრავენ იმ კლიენტს,

რომელიც ყველაზე ხშირად ურთიერთმოქმედებს სერვერთან. ეს ამოცანა წყდება ორ ეტაპად:

– სწარმოებს ქსელური სერვისის სრული ტრაფიკის რეგისტრაცია;

– სწარმოებს სადგურების სახელწოდებათა დახარისხება გადაცემული პაკეტების საერთო რაოდენობის მიხედვით.

თუ ავიღებთ, მაგალითად, ქსელს, რომელიც მუშაობს 16 მომხმარებელთან და ერთ სერვერთან, ამ სერვერის მისამართი შეიძლება გამოყენებული იქნეს ტრაფიკის ფილტრაციის დროს ყველაზე უფრო აქტიური მომხმარებლების გამოსავლინებლად. ტრაფიკის ფილტრაცია, სერვერის სრული ტრაფიკის რეგისტრაცია, ყველაზე აქტიური სადგურების სახელწოდებების დახარისხება და ა.შ. შესაძლებელია მაგალითად, LANalyzer for Windows ანალიზატორების დახმარებით (Novell – ის ფირმის).

2. სადგურების გამოვლენა, რომლებიც ყველაზე მეტად ტვირთავენ ქსელის გატარების ზოლს

ქსელის ანალიზატორების დახმარებით ძალზე ძლიერ დატვირთულ საკაბელო სისტემებში განსაზღვრავენ რომელი მომხმარებლები ყველაზე ძალიან ტვირთავენ ქსელის გატარების ზოლს და, თუ ეს შესაძლებელია, ქსელის ადმინისტრატორს დანიშნულების ადგილებისაკენ გადასაგზავნად გადაჰყავს მათი პაკეტები სხვა, ქსელის უფრო ნაკლებად დატვირთულ სეგმენტებში, რათა გაუმკვლავდეს ქსელში ძლიერ დატვირთვებს. იმ კლიენტების გამოსავლინებლად, რომლებიც ყველაზე ინტენსიურად ტვირთავენ ქსელის გატარების ზოლს, თქვენ (როგორც

ქსელის ადმინისტრატორმა) უნდა განახორციელოთ მონიტორინგის ალგორითმის შემდეგი ბიჯები:

- გააძევეთ (გაანულეთ) მუშა სადგურების ყველა ფილტრი;
- დაახარისხეთ ინფორმაცია (მაგალითად, იმავე LANalyzer for Windows ანალიზატორის გამოყენების დროს ინფორმაციის დახარისხება შეგიძლიათ Station Monitor-ის ეკრანზე Kbytes Out - სვეტით).

3. სადგურების გამოვლენა, რომლებიც იწვევენ შეცდომების წარმოქმნას ქსელში

იმავე ქსელური ანალიზატორის LANalyzer for Windows გამოყენებისას, Station Monitor-ის ეკრანზე არის ასევე სვეტი – Errors (შეცდომები). ამ სვეტში დაფიქსირებული შეცდომები ეკუთვნის იმ სადგურებს, რომლებიც ატყობინებენ ანალიზატორს მათ ამ შეცდომების შესახებ.

Station Monitor-ის ეკრანზე Errors-სვეტით ინფორმაციის დახარისხება საშუალებას გვაძლევს გავარკვიოთ რომელი სადგურის მიზეზითაა წარმოქმნილი ქსელში შეცდომების უმეტესი ნაწილი. დაიჭერს რა (ანალიზატორი) ზოგიერთ პაკეტებს, რომლებსაც აგზავნის ესა თუ ის სადგური, განსაზღვრავენ სადგურის მიერ გენერირებული შეცდომების ტიპს.

ვინაიდან ერთი სადგურის მიერ გადაცემული საკონტროლო თანამიმდევრობის შეცდომები მიუთითებენ ამ სადგურის ქსელური ინტერფეისული პლატის უწესივრობაზე, იგი უნდა შეიცვალოს ახლით და ხელახლა ჩატარდეს მონიტორინგი ქსელში

შეცდომების წარმოქმნაზე. თუ საკონტროლო თანამიმდევრობის შეცდომები ქსელის ანალიზატორში მიეწოდა რამოდენიმე მუშა სადგურიდან, უნდა ვივარაუდოთ, რომ ალბათ მოხდა რაღაც უწესივრობა კაბელში ან სეგმენტში, სადაც იმყოფება ეს სადგურები.

ამგვარად, გამოვლენა (განსაზღვრა) იმ აქტიური მუშა სადგურებისა და იმ სადგურებისაც, რომლებიც წარმოქმნიან ქსელში შეცდომებს, სწარმოებს არაკორექტული პაკეტების რაოდენობის მიხედვით, რომლებსაც გადასცემენ ისინი სერვერს (იღებენ სერვერიდან), რათა დაადგინონ რა ხარისხით იკავებენ ისინი ქსელის გატარების ზოლს.

ქვემოთ განვიხილოთ სახელწოდების შესახებ ინფორმაციის შემგროვებელი საშუალებები, რომლებიც გამოყენებული იქნება ქსელის სადგურებს შორის ურთიერთქმედების ინტერპრეტაციის გასამარტივებლად.

4. სადგურის სახელწოდებების შესახებ ინფორმაციის შეგროვება

თუ ვიმსჯელებთ Novell – ის იმავე ანალიზატორების მიხედვით, NCC LANalyzer და LANalyzer for Windows ანალიზატორების ეკრანზე გამოტანილი ინფორმაციები საშუალებას იძლევიან ჩატარდეს ქსელის სეგმენტებზე მიერთებული მუშა სადგურებისა და სერვერების მონიტორინგი. ანალიზატორების ეკრანებზე ხშირად სადგურის კვანძის 6-ბაიტიანი მისამართის მაგიერ ნაჩვენებია სახელწოდება. ზოგიერთ ეკრანზე წარმოდგენილია აგრეთვე სერვერების სახელწოდებებიც. ეს სახელები ინახება სახელწოდებების ფაილში და მისი გააქტიურების დროს

წარმოიქმნება შესაძლებლობა ეკრანზე გამოყვანის დროს ფიზიკური მისამართები შეიცვალოს იდენტიფიკატორებით (მაგალითად, სარეგისტრაციო სახელწოდებით ან სერვერების სახელწოდებით). ვინაიდან ეკრანის გაანალიზება, რომელიც გავსებულია კვანძების მისამართებით, საკმაოდ ძნელია, სახელწოდებების მიხედვით მონაცემთა თავმოყრა (შეგროვება) აადვილებს ქსელური ურთიერთმქმედების პროცესების ინტერპრეტაციას.

თუ განვიხილავთ ზოგადად გამომთვლელი ქსელების როგორც მონიტორინგის, ისე მათი ანალიზის ამოცანებს, ისინი საჭიროებენ ადამიანის უფრო აქტიურ მონაწილეობას (უმეტესწილად ქსელის ადმინისტრატორის უშუალო მონაწილეობას). ისინი იყენებენ ისეთ რთულ საშუალებსაც, როგორიცაა სხვადასხვა შესაძლებლო-ბების მქონე აპარატურულ-პროგრამული ანალიზატორები, ექსპერტული სისტემები და სხვა ინტელექტუალური საშუალებები, რომლებშიც აკუმულირებულია (თავმოყრილია) მრავალი ქსელური სპეციალისტის პრაქტიკული გამოცდილება.

7.3. კომპიუტერული ქსელის მართვის პროგრამული საშუალებები და ძირითადი ალგორითმები

ჩვენს მიერ ზემოთ განხილული მონიტორინგის, ასევე ქსელის მართვის პროცესები წარმოებს სხვადასხვა პროტოკოლების დახმარებით. ამჟამად მათ შორის ყველაზე პოპულარულია ქსელის მართვის პროტოკოლი SNMP.

პროტოკოლი SNMP (Simple Network Management Protocol – ქსელის მართვის მარტივი პროტოკოლი) განკუთვნილია ქსელის მმართველ სადგურებთან სამუშაოდ. იგი საშუალებას აძლევს მმართველ სადგურებს შეკრიბონ (შეაგროვონ) ინფორმაცია კონტროლირებად ქსელში "საქმის მდგომარეობის" შესახებ. ეს პროტოკოლი იძლევა საშუალებას მართოს სხვადასხვა ზომისა და დანიშნუ-ლების, როგორიცაა მაგალითად, კომერციული საქმეების საწარმოებლად განკუთვნილი, საუნივერსიტეტო (კამპუსების), საკვლევი გაერთიანებების (კორპორაციული დანიშნულების) და ა.შ. ქსელები.

SNMP წარმოადგენს გამოყენებითი დონის პროტოკოლს ქსელურ მოწყობილობებს შორის მმართველი ინფორმაციის ურთიერთ გაცვლის გასაადვილებლად. ხელმძღვანელობენ რა SNMP – პროტოკოლის მიერ წარმოდგენილი ინფორმაციით, ქსელის ადმინისტრატორებს შეუძლიათ უფრო ოპერატიულად და მარტივად მართონ მათ დაქვემდებარებაში მყოფი ქსელის საერთო წარმადობა, აღმოაჩინონ და გადაჭრან წარმოქმნილი მრავალი ქსელური პრობლემა.

SNMP - პროტოკოლის, როგორც კომპიუტერული ქსელის მართვის ძირითადი პროგრამული საშუალების შექმნაში დიდი წვლილი მიუძღვის ჩატარებულ სამუშა-ოებს შემდეგი სამი ძირითადი მიმართულებით:

1. High-level Entity Management Sustem(HEMS);
2. Simple Gateway Monitoring Protokol(SGMP);
3. CMIP over TCP (CMOT).

განვიხილოთ მოკლედ თითოეული მათგანი:

– HEMS წარმოადგენს ქსელის ობიექტების მართვის მაღალი დონის სისტემას (პროტოკოლს). მასში აღწერილია ქსელების მართვის პრინციპები და მექანიზმები (მათ შორის არასტანდარტული მახასიათებლების მქონე ქსელების), ისეთები, როგორიცაა ობიექტების მონაცემების საინფორმაციო ბაზების მართვა, შეღწევის მექანიზმები, საანგარიშო (ქსელის პარამეტრების) ინფორმაციების აგება, მოთხოვნების აგების ენა RPC–ს მექანიზმების გამოყენებით (RPC - Remote Procedure Call-დაშორებული პროცედურების გამოძახება). სამწუხაროდ, ამჟამად HEMS უკვე აღარ გამოიყენება, ვინაიდან არსებობს უფრო გაუმჯობესებული მეთოდები, ვიდრე ამ სისტემაშია აღწერილი.

– SGMP - მარტივი როუტერის (მარშრუტიზატორის) მართვის პროტოკოლის თავდაპირველი დანიშნულება იყო მხოლოდ ქსელური ინსტრუმენტების მართვა. აღნიშნული სამუშაო ჩაატარა ქსელურ ინჟინერთა ერთმა ჯგუფმა სწრაფქმედი Internet-ის მართვის პრობლემების გადასაწყვეტად (მათ დაამუშავეს პროტოკოლი, რომელიც განკუთვნილი იყო Internet-ის როუტერების მართვისათვის). ამჟამად SGMP პროტოკოლს იყენებენ Internet-ქსელის მრავალ რეგიონალურ შტოებში.

– “CMIP TCP-ს ზემოთ” – ეს პროტოკოლი, რომელიც ბაზირდება OSI – სტანდარტზე, აწარმოებს CMIP-ის (CMPI – Common Management Information Protocol – საერთო მართვის ინფორმაციის პროტოკოლი) გამოყენების პროპაგანდას და იგი (CMIP) განკუთვნილია TCP-გაერთიანებული ქსელების მართვის გასაადვილებლად.

სამუშაოები ყველა ზემოთ ჩამოთვლილი სამი მიმართულებით ჩატარებული იქნა IAB-ის ხელმძღვანელობით (IAB - Internet Activities Broad). ამ მიმართულებით სამუშაო-ბის საწარმოებლდ შექმნილი იყო ორი მუშა ჯგუფი. პირველი მათგანი დაკავებული იყო MIB-ის (MIB – Management Information Base) დამუშავებით. ე.ი. ეს ჯგუფი ამუშავებდა სპეციფიკაციებსა და მართვის საინფორმაციო ბაზის ელემენტებს. ამ სამუშაოებიდან ცალკე გამოიკვეთა SMI-ის შექმნა (SMI – Structure for management Information-ობიექტების მართვის სტრუქტურები). მეორე ჯგუფი მუშაობდა ქსელის მართვის პროტოკოლის გაუმჯობესებული ვარიანტების შემუშავებაზე და შექმნეს კიდეც გაუმჯობესებული ვერსია SGMP, რომელსაც მოგვიანებით ეწოდა ჩვენს მიერ დასაწყისში ნახსენები ქსელის მართვის SNMP-პროტოკოლი

SNMP, როგორც აღვნიშნეთ, წარმოადგენს ქსელის მართვის შედარებით მარტივ პროტოკოლს, თუმცა მისი მახასიათებლები საკმაოდ ძლიერია რათა გადაწყვიტოს მრავალი პრობლემა (მათ შორის საკმაოდ ძნელი), რომლებიც წარმოიქმნებიან კომპიუტერული ქსელის მართვის დროს.

ამჟამად SNMP-პროტოკოლის შესაძლებლობების გაფართოებაზე კვლავ მიმდინარეობს სამუშაოები. მრავალი მომწოდებელი ამუშავებს და გამოაქვს გასაყიდად (ქსელური პროდუქტების ბაზარზე) მართვის გამოყენებითი სხვადასხვა პროგრამები, რომლებიც დაფუძნებულია SNMP-ს აგების ფუძემდებლურ პრინციპებზე (ეს პრინცი-პები განხილულია ამავე თავის მომდევნო §7.3.1-ში)

ქსელის მართვის SNMP-არის “მოთხოვნა-პასუხის” ტიპის პროტოკოლი, ე.ი. მისმა აგენტებმა უნდა გასცენ პასუხები მენეჯერის თითოეულ შეკითხვაზე. ამგვარად, ამ პროტოკოლის განსაკუთრებულობა მდგომარეობს იმაში, რომ იგი ძალიან მარტივია და მოიცავს მხოლოდ რამოდენიმე (კერძოდ 5) ბრძანებას, რომლებსაც ხშირად მოიხსენიებენ, როგორც SNMP-პრიმიტივებს. Am ბრძანებების რეალიზაციებზეა აგებული SNMP-პროტოკოლით ქსელის მართვის ძირითადი ალგორითმები.

განვიხილოთ თითეული მათგანი (ეს ბრძანებები):

– ბრძანება Get-request მენეჯერის მიერ გამოიყენება ქსელის რაიმე ობიექტის (მისი სახელწოდების მიხედვით) მნიშვნელობის მისაღებად აგენტიდან.

– ბრძანება GetNext-request, რომელსაც იყენებს მენეჯერი შემდეგი ობიექტის მნიშვნელობის გამოსაყოფად (ამ ობიექტის სახელწოდების მითითების გარეშე) ობიექტების ცხრილის თანამიმდევრობით დათვალიერების დროს.

– ბრძანება Get-response, რომლის დახმარებით SNMP-აძლევს მენეჯერს პასუხს Get-request ან GetNext-request ბრძანებებზე.

– ბრძანება Set გამოიყენება მენეჯერის მიერ რაიმე ობიექტის მნიშვნელობის გასაზომად. Set – ის დახმარებით სწარმოებს საკუთრივ მოწყობილობის მართვა. აგენტს უნდა ესმოდეს ობიექტის მნიშვნელობის აზრი, რომელიც გამოიყენება ქსელის მოწყობილობის მართვისათვის და ამ მნიშვნელობის საფუძველზე უნდა მოახდინოს რეალური მართვითი ზემოქმედება, მაგალითად გამორთოს პორტი ან

ეს პორტი მიაკუთვნოს რომელიმე VLAN–ს (ვირტუალურ ლოკალურ ქსელს) და ა.შ. ბრძანება Set შეიძლება გამოიყენებული იქნეს ასევე იმ პირობის წაყენებისათვის, რომლის შესრულების დროს SNMP-აგენტმა უნდა გაუგზავნოს მენეჯერს შესაბამისი შეტყობინება. შეიძლება განსაზღვრული იქნეს, თუ რა რეაქცია ექნება ისეთ მოვლენას, როგორიცაა აგენტის ინიციალიზაცია, აგენტის რესტარტი (ხელახლა გაშვება), კავშირის გაწყვეტა, ან კავშირის აღდგენა, არასწორი აუტენტიფიკაცია და უახლოესი მარშრუტიზატორის (როუტერის) დაკარგვა. თუ ადგილი აქვს ამ მოვლენებიდან ერთ-ერთს მაინც, მაშინ აგენტი მოახდენს წყვეტას (სხვა სიტყვებით, მოახდენს წყვეტის ინიციალიზაციას).

– ბრძანება Trap გამოიყენება აგენტის მიერ, რათა აცნობოს მენეჯერს განსაკუთრებული სიტუაციის ქსელში წარმოქმნის შესახებ.

7.3.1. ქსელის მართვის სისტემის აგების ძირითადი პრინციპები, რომლებიც საფუძვლად უდევს მართვის ალგორითმების რეალიზაციებს

კომპიუტერული ქსელის მართვის ძირითადი სისტემა, როგორც წინა პარაგრაფში იყო აღნიშნული, აგებულია SNMP-პროტოკოლზე. ეს სისტემა მთლიანობაში წარმოადგენს ქსელის მმართველი სადგურებისა და ქსელების ელემენტების-სამართავი ობიექტების კომპლექსს. მმართველი სადგურები ასრულებენ

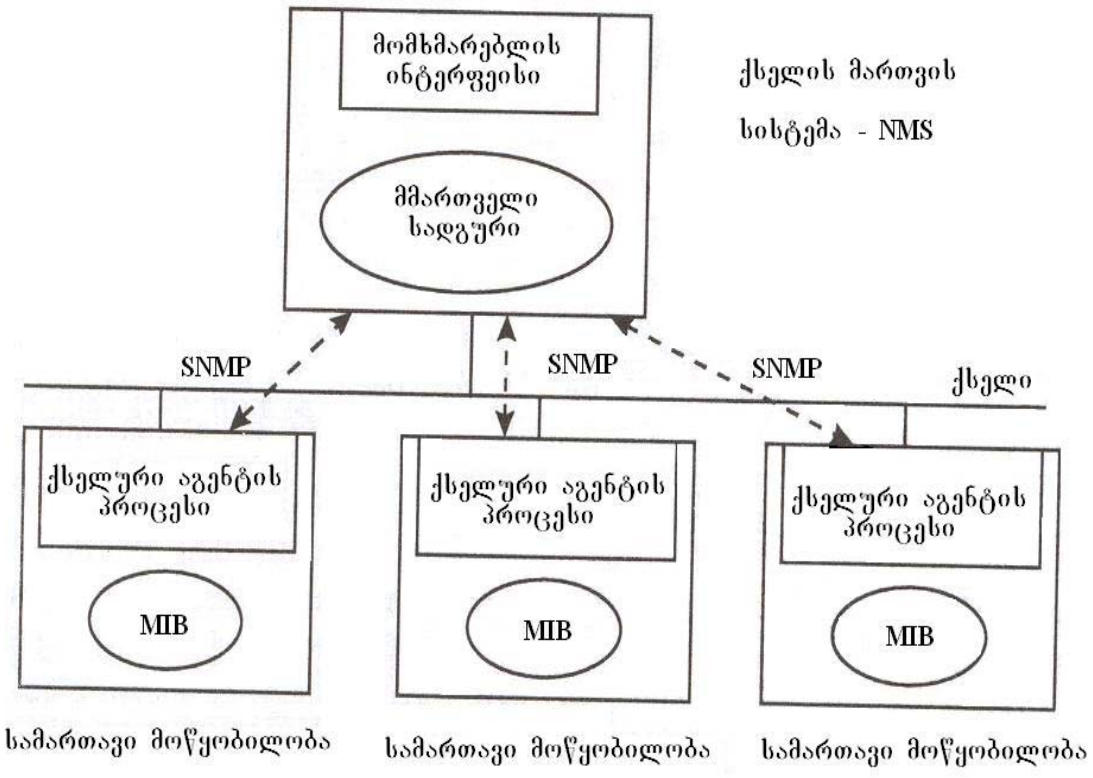
სხვადასხვა პროგრამულ დამატებებს, რომლებიც ქსელის სამართავ ობიექტებთან საინფორმაციო კონტაქტებს ამყარებენ SNMP-აგენტებთან ქსელური ელემენტების მართვის მიზნით. ქსელური ელემენტების ქვეშ იგულისხმება ისეთი ობიექტები, როგორებიც არიან ჰოსტის კომპიუტერები, რაბები ("შლიუზები"), სატერმინალო სერვერები და სხვა, რომლებზედაც მმართველი ზემოქმედება სრულდება ქსელური აგენტების მოდულებით – სამართავი ობიექტებიდან მოწოდებული ინფორმაციებით. ამგვარად აგენტები აგროვებენ ინფორმაციას სამართავი ობიექტების შესახებ, რომლებშიც ისინი მუშაობენ. სამართავ ობიექტებზე განთავსებული აგენტები თავიანთი ლოკალური ცვლადებით, წარმოადგენენ ქსელის მართვის ერთიანი საინფორმაციო ბაზის შემადგენელ ელემენტებს - MIB.

SNMP-პროტოკოლი, როგორც ზემოთ აღვნიშნეთ, გამოიყენება ქსელის მმართველ სადგურებსა და ელემენტებს შორის მმართველი და საკონტროლო ინფორმაციის ურთიერთ გაცვლისათვის. მის გარდა SNMP-პროტოკოლის დახმარებით ლოკალური ინფორმაცია ხელმისაწვდომი ხდება ქსელის მართვის მთლიანი სისტემისათვის – NMS (NMS – Network Management System) და მონაცემთა ბაზის მართვის სისტემებისათვის – MIB.

ზემოთხსენებულის გარდა სამართავ ობიექტს შეიძლება წარმოადგენდეს ნებისმიერი ტიპის კვანძი, რომელიც კი იმყოფება ქსელში: ეს შეიძლება იყოს ჰოსტის სადგური, კავშირის სამომსახურეო მოწყობილობა, პრინტერი, როუტერი, ხიდი, კონცენტრატორი და ა.შ. ამათგან ზოგიერთ სისტემას შეიძლება გააჩნდეს მართვის შეზღუდული შესაძლებლობა

პროგრამული უზრუნველყოფით (ასევე შეზღუდული შესაძლებლობით). მაგალითად, მათ (სისტემებს) შეიძლება ჰქონდეთ პროცესორები შედარებით დაბალი სწრაფქმედებით ანდა გააჩნდეთ მეხსიერების შეზღუდული მოცულობა. მართვის პროგრამები ამიტომ ისეთნაირად უნდა იქნეს აგებული, რომ საკმარისი იყოს მათი წარმადობა მართვის საწარმოებლად (უფრო ზუსტად მინიმიზირებული იქნეს თავისი წარმადობა ზემოქმედებისათვის სამართავი ობიექტის მუშაობაზე), რათა მართვის მთელი სიმძიმე გადატანილი იქნეს ქსელის მმართველ სადგურებზე.

ნახ. 7.1-ზე ნაჩვენებია კომპიუტერული ქსელის მართვის სისტემის (NMS) მუშაობის ზოგადი ბლოკ-სქემა, რომელიც საფუძვლად უდევს ძირითად ალგორითმებს.



ნახ. 7.1. ქსელის მართვის სისტემა (NMS)

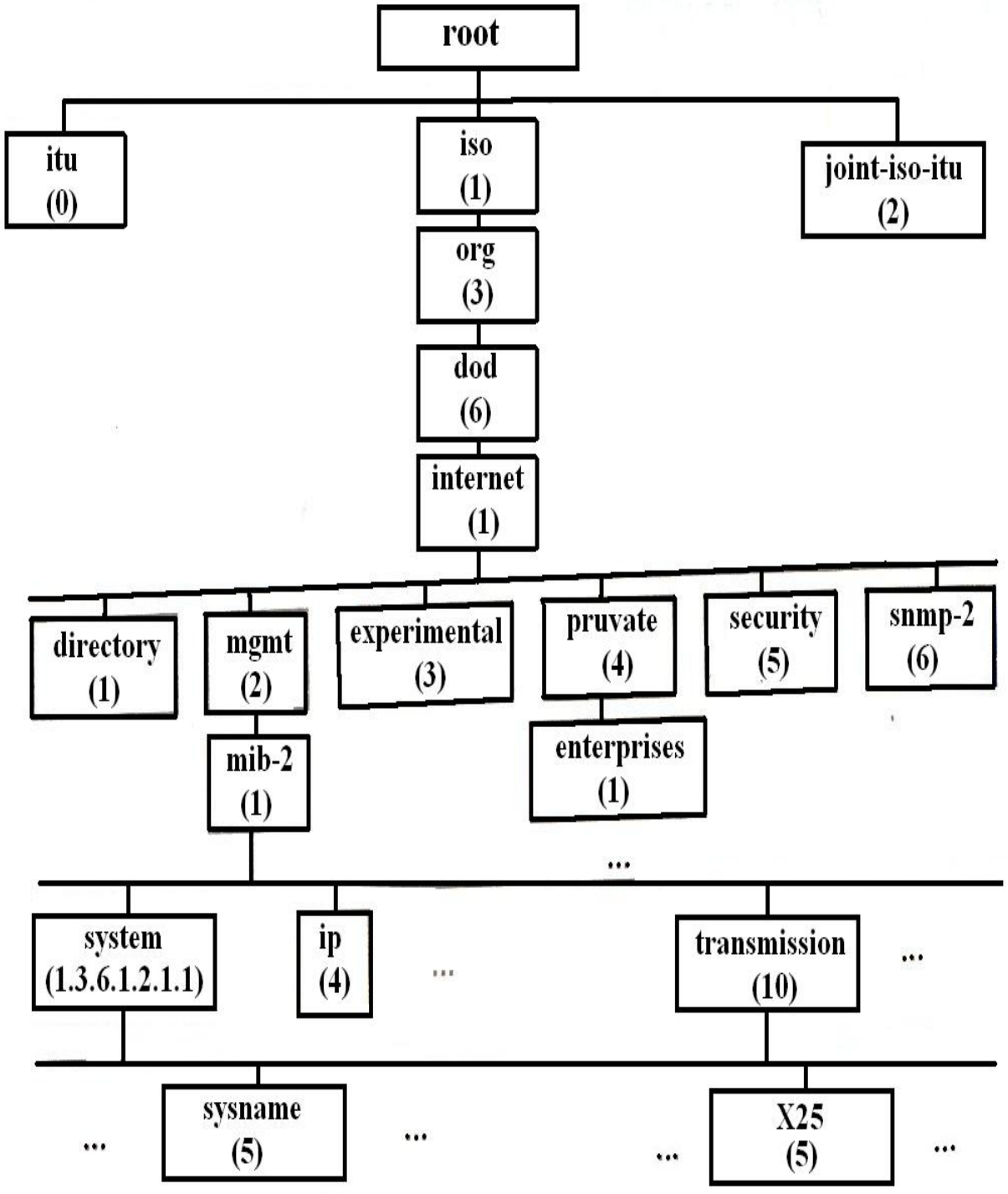
NMS- ის მმართველი სადგურები მუშაობენ საკმაოდ მძლავრ კომპიუტერებზე, რომლებსაც გააჩნიათ სწრაფქმედი ცენტრალური პროცესორები, მეხსიერების საკმარისი მოცულობა და მაღალი წარმადობის პერიფერია. NMS – სადგურებზე მუშაობენ ქსელის მართვის გამოყენებითი პროგრამები, რომლებიც ამუშავებენ და წარუდგენენ მომხმარებლებს ინფორმაციას როგორც მთლიანი ქსელის შესახებ, ისე მართვის ცალკეული ობიექტების შესახებ.

7.3.2. სახელწოდებათა გლობალური "ხის" აგების არსი და მისი მნიშვნელობა ქსელის მართვაში

კომპიუტერული ქსელის (ამჯერად ზოგადად იგულისხმება საერთო-სახალხო გლობალური ქსელი) ყველა სამართავი ობიექტები განლაგებულია ობიექტების ერთიან ვირტუალურ "ხეზე" – მართვის საინფორმაციო ბაზაში – MIB, რომლის "ფოთლებს" წარმოადგენს ცალკეული საიფორმაციო ელემენტები. ვირტუალური "ხის" აგების არსი (სხვა სიტყვებით, აგების სინტაქსისი) განსაზღვრულია სპეციალიზაციით ASN.1 (Abstract Syntax Notation One-სპეციალიზაცია სინტაქსისა ნომერი 1).

ვირტუალური "ხის" აგების არსი მდგომარეობს იმაში, რომ "ხის" შემცველ თითოეულ ობიექტს გააჩნია თავისი სახელწოდება, რომლიც ასახავს ამ ობიექტის ფუნქციას. მას (ობიექტს) გააჩნია თავისი ამოსაცნობი იდენტიფიკატორი. ეს იდენტიფიკატორი წარმოადგენს მთელი რიცხვების თანამიმდევრობას,

რომელიც მიუთითებს გზას ობიექტისაკენ, დაწყებული “ხის” ფესვიდან (ხის აგების ერთ-ერთი ფრაგმენტი მაგალითის სახით ნაჩვენებია ნახ.7.2-ზე). თვით “ხის ფესვს” იდენტიფიკატორი არ გააჩნია.



ნახ. 7.2. სახელწოდებათა გლობალური “ხის” აგების ფრაგმენტი

ფესვიდან (root) პირველ დონეს, როგორც ნახ. 7.2 – დან ჩანს, შეადგენენ itu - ობიექტები. და joint-iso-itu- ობიექტები (2) იგი ახდენს ქვეხის (0) ადმინისტრირებას. ISO–ადმინისტრირებს “ხეს” რომელიც ეშვება კვანძებიდან (1) და (2). ძირითად “ხის” მეორე დონეზე განლაგებულია ორგანიზაციული კვანძი – org (3), რომელიც ეკუთვნის ISO ქვეხეს. ეს კვანძი განსაზღვრულია “ხის” გასაგრძელებლად სხვა ორგანიზაციებზე პასუხისმგებლობის დელეგირებისათვის. ერთ-ერთ ასეთ მესამე დონის ორგანიზაციებს წარმოადგენს dood (6) (აშშ-ს თავდაცვის სამინისტრო), რომელსაც, მართვის იერარქიის თანახმად, ეკუთვნის Internet (1)–ქსელი, რომელიც განლაგებულია ობიექტების მართვის გლობალური ხის მეოთხე დონეზე.

ამგვარად, მართვის ალგორითმის სარეალეზაციოდ, იმ იერარქიის თანახმად Internet ობიექტების იდენტიფიკატორები იწყება კოდიდან 1.3.6.1. ნახ. 7.2-ზე ასევე ჩანს, რომ უშუალოდ Internet(1) კვანძის ქვეშ განლაგებულია 6 კვანძი: derectory (1) (ცნობარი); mgmt(2) (მართვა); experimental (3) (ექსპერიმენტალური); private (4) (კერძო); security (5) (უსაფრთხოება) და snmp (6) (მართვის კვანძი SNMP პროტოკოლით).

ამ 6 კვანძიდან, მაგალითად, კვანძს private(4) ამჟამად გააჩნია მხოლოდ ერთი ქვეხე-exterprises (1) (საწარმო). “ხის” “შტო”, exterprises (1) შედგება 1000-ზე მეტი კვანძისაგან, რომლებსაც იკავებენ ქსელური აღჭურვილობის სხვადასხვა მომწოდებლები. მათ შორისაა, აგრეთვე, პროგრამული უზრუნველყოფის დამამუშავებლები, სახელმწიფო დაწესებულებები,

უნივერსიტეტები და ა.შ. სხვა ორგანიზაციები. ამ კვანძებიდან თითოეული საშუალებას აძლევს ორგანიზაციებს თვითონ განსაზღვრონ ქსელური პროდუქტებისა და სტრუქტურების იდენტიფიკატორები, რომლებიც კი საჭიროა ამ პროდუქტების მართვისათვის. მაგალითად, თუ მითითებულია კვანძი 348 (1.3.6.1.4.1.348), ეს კვანძი აღნიშნავს Procter&Gamble, ხოლო კვანძი 743 (1.3.6.1.4.1.743)- ცენტრალურ სადაზვერვო სამმართველოს. ე.ი. იდენტიფიკატორების თანამიმდევრობა ...1.348 და ...1.743 მიუთითებს "ხის" შემცველ ორგანიზაციებზე (ბუნებრივია, ამ მაგალითში ნაჩვენებია აშშ-ის ორგანიზაციები).

ნახ. 7.2-ზე ნაჩვენებ "ხეზე" კვანძი mgmt (2) შეიცავს ცვლად ქსელურ მართვას. მაგალითად სისტემური ჯგუფი ip (4), mib-2 (1)-შტოს "ხის" mgmt (2), რომლის იდენტიფიკატორია 1.3.6.1.2.1.4 იძლევა ინფორმაციას, რომელიც საჭიროა მუშა კომპიუტერებისა და მარშრუტიზატორების სამართავად (როგორც ადრეც შევნიშნეთ, ამ ინფორმაციას აწვდიან შესაბამისი SNMP-აგენტები).

გლობალური "ხე" MIB ქსელური ტექნიკის განვითარებასთან ერთად თანდათან ფართოვდება (ე.ი. მისი "შტოები" მრავლდება სხვადასხვა ექსპერიმენტალური პროდუქტების მიხედვით). მაგალითად, პროგრამული უზრუნველყოფის მომწოდებლებს შეუძლიათ დააფიქსირონ (იდენტიფიკატორი) თავიანთი საკუთარი "შტოები" თავიანთი ნაწარმისათვის (ამ შემთხვევაში თავიანთი პროგრამული პროდუქტებისათვის). ამჟამად, სტანდა-

რტიზაციის მიზნით მთელი სამუშაოები მიმდინარეობს ექსპერიმენტალურ "შტოზე".

ქსელის მართვის ალგორითმების რეალიზაციების მიზნით სახელწოდებათა გლობალური "ხის" ამოცანას წარმოადგენს უზრუნველყოს სტანდარტული მეთოდი, რათა დაეკონტაქტონ SNMP-აგენტებს და მათგან მიიღონ პარამეტრების (ცვლადების) მნიშვნელობები შესაბამისი სამართავი ობიექტების შესახებ.

ამგვარად, იმისათვის, რომ ვაწარმოოთ ქსელის მართვა რომელიმე პრობლემური ობიექტის (ქსელური კომპონენტის) პარამეტრების დასარეგულირებლად, საჭიროა ვიცოდეთ ამ სამართავი ობიექტის IP-მისამართი და ადგილმდებარეობა სახელწოდებით გლობალურ "ხეზე" ამ ობიექტის იდენტიფიკატორით (რა თქმა უნდა თუ ეს ობიექტი არსებობს საერთოდ სახელწოდებათა "ხეზე"), რის შემდეგაც საშუალება გვეძლევა SNMP–აგენტებიდან მიღებული ინფორმაციების მიხედვით ვცვალოთ (ე.ი. ვმართოთ) მისი პარამეტრები.

სხვა სიტყვებით რომ ვთქვათ, ობიექტის მდებარეობა გლობალურ "ხეზე" იძლევა მის ფუნქციონალურობას, ხოლო IP-მისამართი იდენტიფიცირებს თვით ამ ობიექტს. ამასთან, თუ რომელიმე ობიექტი ასრულებს სხვადასხვა ფუნქციებს (ე.ი. მრავალფუ-ნქციონალური ობიექტია), მაშინ იგი უნდა მოიძებნოს "ხის" სხვადასხვა "შტოებზე".

SNMP - პროტოკოლით მართვის ალგორითმის სარეალიზაციოდ საჭიროა სახელწოდებათა "ხეზე" (და " შტოზე") მოიძებნოს კონკრეტული სამართავი ობიექტი და მოხდეს SMI-

სპეციფიკაციის მიხედვით მისი სრული აღწერა. ამისათვის საჭიროა განისაზღვროს:

1. გლობალური “ხის” “შტოს” (ან ”ფოთლის”) ტექსტური სახელწოდება, რომელსაც შეესაბამება სამართავი ობიექტი;
2. სამართავი ობიექტის ტიპი;
3. განისაზღვროს ობიექტი, რისთვისაც მის შესახებ აღწერა უნდა შეიცავდეს ობიექტის ტიპის სემანტიკას (ე.ი. დაზუსტდეს აზრი თუ რა ფუნქციას (მოქმედებას) ასრულებს ეს ობიექტი და რაში გამოიყენება);
4. შეღწევა (წვდომა), ეს პარამეტრი ახასიათებს სამართავ ობიექტთან შეღწევის ტიპს (ე.ი. უნდა დაზუსტდეს შეღწევის ტიპი: მხოლოდწაკითხვა (read-only). წაკითხვა–ჩაწერა (read-write), მხოლოდ ჩაწერა (write-only) და ა.შ.)
5. ობიექტის სტატუსი: აუცილებელი, არააუცილებელი ან მოძველებული.

მაგალითად, მართვის გლობალური “ხის” ობიექტის კონკრეტული აღწერა შეიძლება გამოიყურებოდეს შემდეგნაირად:

1. სახელწოდება: sysUpTime (System), იდენტიფიკატორი - 1.3.6.1.2.1.1.3.
2. ტიპი: Ticks.
3. განსაზღვრა: აღნიშნავს დროს (წამის მეასედ ნაწილს), რომელმაც გაიარა ქსელის მართვის ქვესისტემის ბოლო ინიციალიზაციიდან.
4. შეღწევა: read-only (მხოლოდ წაკითხვა)

5. სტატუსი: აუცილებელი (ე.ი. ობიექტი აუცილებლივ სახეზე უნდა იყოს სისტემაში).

შესაძლებელია სხვა მაგალითების მოყვანაც.

MIB - ბაზის ცვლადებთან შეღწევა სწარმოებს მათი იდენტიფიკატორებისა და ცვლადების მიხედვით, რომლებიც კონკრეტულად ასახავენ ობიექტში (ობიექტებში) ცვლადებს. სამართავი ობიექტის ფუნქციები მოიცემა ფორმატში “variable. parametrs”. თითოეულ სამართავ ობიექტს აქვს თავისი პარამეტრები, ხოლო მათი გადაცემის ხერხი კი (SNMP – აგენტებით) – საერთოა ყველა ობიექტებისათვის.

7.3.3. ქსელის მართვის SNMP- ოპერაციები

SNMP, როგორც აღვნიშნეთ, წარმოადგენს ქსელის გამოყენებითი დონის (OSI – ეტალონური მოდელის დონეების მიხედვით) პროტოკოლს, რომლის დახმარებით შეიძლება შემოწმდეს და შეიცვალოს MIB – ცვლადების მდგომარეობა, რაც ფაქტიურად ნიშნავს ქსელის მართვის ალგორითმის რეალიზაციას.

მმართველი შეტყობინებების ტრაფიკისა და მთლიანობაში ქსელურ სისტემაზე დატვირთვის შემცირების მიზნით SNMP-ოპერაციებისთვის საჭირო ინფორმაციების მმართველ და სამართავ ობიექტებს შორის გაცვლისათვის იყენებენ UDP – დეიტაგრამების პროტოკოლს. დეიტაგრამები წარმოადგენენ მიზნობრივი დანიშნულების მოკლე ტექსტურ შეტყობინებას (UDP – User Datagram Protocol – სამომხმარებლო დეიტაგრამე-ბის

პროტოკოლი). თუმცა ზოგიერთი სპეციალისტი ამტკიცებს, რომ არასაიმედო UDP – პროტოკოლით მუშაობა წარმოადგენს SNMP-პროტოკოლის ერთ-ერთ ნაკლს. მათი მტკიცებით SNMP – აგენტებთან მენეჯერებისაკენ ავარიული შეტყობინებების (trap-შეტყობინებების) დაკარგვა იწვევს ქსელის არახარისხიანად მართვას (რაც ვერ ვიტყვით §7.3-ის დასაწყისში ნახსენებ CMIP – პროტოკოლზე, რომელსაც არ გააჩნია ამგვარი უარყოფითი მხარეები). მიუხედავად ამისა SNMP ჯერ-ჯერობით კვლავ რჩება, როგორც ქსელის მართვის ერთ-ერთი ძირითადი პროტოკოლი.

თითეული SNMP – შეტყობინება გადაიცემა სხვებისგან დამოუკიდებლად, რაც ნიშნავს იმას, რომ UDP – დეიტაგრამებიც არ არიან დამოკიდებული სხვა შეტყობინებებზე და წარმოადგენენ SNMP – აგენტებთან ურთიერთქმედებებს ძირითად საშუალებას.

SNMP – პროტოკოლის ოპერაციათა უმრავლესობა იყოფა ორ ძირითად დანიშნულებად. იგი უნდა გამოიყენებული იყოს გარკვეული ინფორმაციის ან მიღების, ან ჩაწერის მიზნით. ამ ინფორმაციაზე მიმართვა წარმოებს პირდაპირ აგენტთან. SNMP – პროტოკოლით მართვაში დასაშვებია, რომ მოთხოვნის ნაწილი არ დამუშავდება, მაგალითად, რაიმე მოთხოვნილი პარამეტრის არ არსებობის გამო. ამ შემთხვევაში აგენტმა უნდა დაუბრუნოს მომთხოვნ სისტემას ცნობა (პასუხი) ამგვარი სახის ინფორმაციის სამართავი ობიექტიდან მმართველი ობიექტის მიერ მიღების შეუძლებლობის შესახებ.

SNMP – ზედა დონის პროტოკოლის შეტყობინებები შედგება შემდეგი ნაწილებისაგან:

- პროტოკოლის (SNMP-ს) ვერსიის იდენტიფიკატორი (Version);
- საქმიანობის სფეროს (თანამოაზრეების ერთმანეთთან შესაბამისობის) სახელ-წოდება (community name);
- მონაცემთა სტრუქტურა (data);
- აუტენტიფიკაციის პარამეტრები.

საქმიანობის სახელწოდება აწესებს შეღწევის გარემოს NMS – ცვლადებისათვის, რომლებსაც გამოიყენებს ეს სახელწოდება. საქმიანობის თანამოაზრეობა შინაარსით ნიშნავს იმ წესების კრებულს (ერთობლიობას), რომლებსაც ემორჩილება გარკვეულ ობიექტებთან მომუშავე SNMP – აგენტების გარკვეული ჯგუფი. შეტყობინების საინფორმაციო ნაწილი შეიცავს SNMP – ოპერაციას (get, set და ა.შ.) და მასთან (ოპერაციასთან) დაკავშირებულ ოპერანდებს, რომლებიც აღნიშნავენ მოცემულ SNMP- ტრანზაქციაში ჩართული ობიექტების რეალიზაციას (ტრანზაქცია ნიშნავს ამა თუ იმ საქმიანობის ოპერაციის განხორციელებას).

SNMP - პროტოკოლში განსაზღვრულია შემდეგი ოთხი ოპერაცია:

- Get (ამორჩევა) – აგენტიდან ამოარჩევს ობიექტის რომელიმე რეალიზაციას;
- Get-next (ამოირჩიე (მოიძიე) შემდეგი) – ამოირჩევს ობიექტის რომელიმე შემდეგ რეალიზაციას ცხრილიდან

ან ჩამონათვალიდან, რომლებსაც შეიცავს მოცემული აგენტი;

- Set (დაყენებები) – აყენებს ობიექტის რეალიზაციას რომელიმე აგენტის საზღვრებში;
- Trap (ხაფანგი) – გამოიყენება აგენტის მიერ შეცდომის რაიმე მოვლენის NMS ასინქრონული ინფორმირებისათვის.

SNMP - აგენტი მოთხოვნის შეტყობინების გადასაცემად სამართავი ობიექტიდან მმართველი ობიექტისაკენ მოქმედებს ალგორითმის მიხედვით, რომელიც ითვალისწინებს შემდეგ ოპერაციებს:

1. აიგოს მოთხოვნილი ობიექტის შასაბამისი PDU;
2. მოახდინოს კომპონირება (ფორმირება) მიზნობრივი ობიექტის, აღჭურვოს ჩასატარებელი საქმიანობა თავისი სახელწოდებით, გამგზავნისა და მიმღების სატრანსპორტო მისამართით და გადასცემს მას აუტენტიფიკაციის სერვისს;
3. აუტენტიფიკაციის სერვისმა დააბრუნოს ობიექტი ASN.1 – შეტყობინების სახით;
4. მიღებული ობიექტი დაყოს პაკეტებად და გადააგზავნოს ისინი დანიშნულების მისამართით.

პაკეტის გაშიფვრა – თითქმის ზუსტად შეესაბამება ზემოთმოყვანილი ალგორითმის უკუ ოპერაციებს. აქვე შენიშვნის სახით აღვნიშნოთ, რომ SNMP- დეიტაგრამების დამუშავების განსაკუთრებულობა მდგომარეობს იმაში, რომ თუ სამართავი ობიექტის აგენტებიდან შემოსული

პარამეტრები ერთმანეთთან შეუთანხმებულია (მაგალითად, არ ემთხვევა მათი სპეციფიკაციის ვერსიები), მაშინ ასეთი პაკეტები დაუყონებლივ ნადგურდება.

PDU – მოთხოვნის (და PDU-პასუხის) პაკეტი შედგება შემდეგი ობიექტებისაგან (ნაწილებისაგან):

– Request-ID – მოთხოვნის იდენტიფიკატორი. ეს გამოიყენება საპასუხო შეტყობინებების მისათითებლად მოცემულ მოთხოვნაზე;

– Error-Status - შეიცავს მოთხოვნის დამუშავების შეცდომის კოდს:

No Error – არ არის შეცდომა;

tooBig – ცვლადის ძალზე გრძელი მნიშვნე-ლობა;

noSuchName – არასწორადაა მოცემული სახელწოდება;

badValue – არასწორი იდენტიფიკატორი;

readOnly – დარღვეულია შეღწევის მეთოდი;

genEzz – და სხვა.

– Error-index- შეიცავს ობიექტის ინდექსს, რომელიც იწვევს შეცდომას;

– Variable bindings – მიბმის ცვლადები, რომლებიც შედგება SNMP PDU მონაცემებისაგან. ისინი ადგენენ კავშირს კონკრეტული ცვლადების დასაშვებ მნიშვნელობებსა და მათ მიმდინარე მნიშვნელობებს შორის. სია შედგება წყვილებისაგან: სახელწოდება – პარამეტრი.

PDU-Trap-სახის შეტყობინების (სხვა სახის შეტყობინებებისაგან განსხვავებით) ველების სტრუქტურა განსხვავდება

იმით, რომ შეიცავს იმ ობიექტის იდენტიფიკაციების უფრო დეტალურ აღწერას, რომელიც იწვევს დროებითი შეფერხების (ჩავარდნის ან დადგენილი პარამეტრებიდან მკვეთრი გადახვევის) სიტუაციას.

შეტყობინებების გაცვლების დროს, SNMP – აგენტები იყენებენ შეტყობი-ნებების გამგზავნისა და მიმღების აუტენტიფიკაციის მექანიზმებს. ეს მექანიზმები წარმოადგენენ წესების ერთობლიობას (კრებულს), რომლის მიხედვითაც ცალკეული თანამოაზრეების (საქმიანობის) მოდულები ახდენენ ერთმანეთის იდენტიფიცირებას. ამასთან ზოგიერთი SNMP რეალიზაციები იყენებენ მარტივ სქემებს, ხოლო ზოგიერთი – უფრო რთულ სქემებს დაცვის მაღალი ხარისხით.

მივიყვანოთ ალგორითმის ერთი მაგალითი, რომელიც ეხება რაიმე ჰოსტის მარშრუტიზაციის ცხრილის მდგომარეობის SNMP – შეტყობინებით გადაცემის მექანიზმის მუშაობას. დაუშვათ, მოცემულ ცხრილს აქვს შემდეგი სახე:

Destination	Next Hop	Metric
9.1.2.3	**99.0.0.3**	**3**
10.0.0.51	**89.1.1.42**	**5**

მაშინ მოთხოვნების (→) და პასუხების (←) თანამიმდევრობები შეიძლება გამოიყურებოდნენ შემდეგნაირად:

→GetRequest (ipRouterDest,ipRouteNextHop, ipRouteMetric)

←GetResponse ((ipRouteDest.9.1.2.3=”9.1.2.3”),
(ipRouteNextHop.9.1.2.3=”99.0.0.3”),
(ipRouteMetric1.9.1.2.3=3))

→GetNextRequest (ipRouterDest,9.1.2.3,
ipRouteNextHop.9.1.2.3,
ipRouteMetric1.9.1.2.3)

←GetResponse ((ipRouteDest.10.0.0.51=”10.0.0.51”),
(ipRouteNextHop.10.0.0.51=”89.1.1.42”),
(ipRouteMetric1.10.0.0.51=5))

თავი 8

კომპიუტერული ქსელის სადიაგნოსტიკო საშუალებები. უწესრიგობების აღმოჩენისა და მათი აღმოფხვრის ტექნოლოგიები

8.1. ქსელის სადიაგნოსტიკო საშუალებების დანიშნულება, მიზნები და ამოცანები

კომპიუტერული ქსელი იყენებს გამოთვლითი ტექნიკის როგორც აპარატურულ და პროგრამულ საშუალებებს, ასევე კავშირგაბმულობის ტექნიკურ საშუალებებსაც. მთლიანობაში იგი წარმოადგენს მეტად რთულ ტელესაკომუნიკაციო ორგანიზმს, რომლის მართვა, როგორც წინა თავში აღვნიშნეთ, საკმაოდ რთული და მრავალფუნქციური პროცესია. სხვა ქსელურ პროცესებს შორის დიაგნოსტიკა ერთ-ერთი მეტად საჭირო პროცედურაა და ამ მიზნისათვის ეფექტური საშუალებების გამოყენებას ძალზე დიდი მნიშვნელობა ენიჭება.

დიაგნოსტიკის ძირითადი მიზანია გამოავლინოს ის პირობები, რომლებიც წარმოქმნიან პრობლემებს, რათა ქსელის ადმინისტრატორმა ან სხვა მომსახურე პერსონალმა აღმოფხვრან ისინი და დროულად აღკვეთონ შეფერხებები ქსელის გამართულ მუშაობაში.

ამჟამად არსებობს ქსელური პრობლემების მრავალნაირი სახეობა და აქედან გამომდინარე ამ პრობლემების აღმოფხვრის სხვადასხვა აპარატურული და პროგრამ-მული საშუალებებიც.

ნებისმიერი სირთულის ქსელური პრობლემების აღმოფხვრას და მის ლოკალიზ-აციას საფუძვლად უდევს სადიაგნოსტიკო საშუალებებით მიღებილი მონაცემები. განასხვავებენ კომპიუტერული ქსელის დიაგნოსტირების ორგვარ მიდგომას (ფორმას): გეგმიურს და შერჩევითს: პირველი მათგანი სწარმოებს ქსელის ადმინისტრატორის მიერ ე.წ. წინასწარ შედგენილი ეტალონური გრაფიკის მიხედვით. მსხვილ კორპორაციაში ეტალონური შემოწმების გრაფიკი შემუშავდება და მტკიცდება ქსელის ადმინისტრატორის მიერ. იგი ითვალისწინებს ქსელის მახასიათებლების პერიოდულ შემოწმებას და მათ შედარებას იმ მახასიათებლებთან, რომლებიც უნდა გააჩნდეს ქსელს მისი მუშაობის ნორმალური რეჟიმის დროს. შემოწმების შედეგები სათანადო თარიღების აღნიშვნით ფორმდება შესაბამისი დოკუმენტაციებით და ფიქსირდება ე.წ. სადიაგნოსტიკო ჟურნალში, სადაც მიეთითება დარღვევებიც (ე.ი. წარმოქმნილი უწესივრობები, თუ კი ასეთი შეინიშნება ქსელის გეგმიური დიაგნოსტიკის დროს).

დიაგნოსტიკის მეორე ფორმა – შერჩევითი სწარმოებს ქსელის მიმდინარე მუშაობაში წარმოქმნილი შეფერხებების დროს (ქსელურ ლიტერატურაში მათ მოიხსენიებენ როგორც ქსელის “შეცდომებს” ან “მტკივნეულ ადგილებს”). აღნიშნული დარღვევებიც, როგორც წესი, ფიქსირდება სათანადო სადიაგნოსტიკო ჟურნალში ქსელის ადმინისტრატორის მიერ.

ამგვარად, ქსელის დიაგნოსტიკის დროს დგინდება როგორც ცალკეული კომპიუტერების (მუშა სადგურების) კორექტული მუშაუნარიანობა, ისე ქსელის საერთო სურათი, რომელზედაც ასახულია პროტოკოლებისა და პროგრამული დამატებების ტრაფიკის ცვლილებებიც. ამ მიზანს ემსახურება უტილიტა – Perfomance Monitor, რომელიც საშუალებას იძლევა ნაპოვნი იქნეს პრაქტიკულად ყველა "მტკივნეული ადგილები". შეცდომების ფიქსაცია ტექსტური შეტყობინებების გარდა, სწარმოებს ასევე სხვადასხვა ფორმით, მაგალითად, გრაფიკების, დიაგრამების, ცხრილების და ა.შ. სახით.

ქსელის სადიაგნოსტიკო პროცესში მნიშვნელოვან როლს თამაშობს მომხმარებელთა გამოკითხვაც, რომლებიც მუშაობენ უშუალოდ ქსელის მუშა სადგურებთან. ასეთ შემთხვევაში ადმინისტრატორი ან ე.წ. ქსელის მხარდაჭერის ინჟინერი (ასეთი თანამდებობაც არსებობს მსხვილ კორპორაციულ ქსელებში) აძლევს მათ კითხვების სერიას, რათა დიაგნოსტირებისას გაარკვიოს შეფერხების მიზეზები. დიაგნოსტირების დროს, თუ ქსელის წინასწარმა დათვალიერებამ ვერ გამოავლინა პრობლემების მიზეზი, ადმინისტრატორმა ან მხარდაჭერის ინჟინერმა აზრობრივად უნდა დაყოს ქსელი მაქსიმალურად შესაძლო რაოდენობის სეგმენტებად, რათა უწესივრობების აღმოფხვრისას საქმე ჰქონდეს არა მთლიან ქსელთან, არამედ მის მცირე ნაწილთან. გამოაცალკევებს რა სეგმენტს, რომელშიც სავარაუდოა რომ იმალება პრობლემა, მათ მიერ რიგ-რიგობით მოწმდება (დიაგნოსტირდება) ამ ქსელური სეგმენტის კომპონენტები: ადაპტერები, კონცენტრატორები, კაბელები და შემაერთებლები.

მოწმდება კლიენტებისა და სერვერების მუშაობა, მათთან დამაკავშირებელი ქსელური კომპონენტები: განმეორებლები, ხიდები, მარშრუტიზატორები, კომუტატორები და შლიუზები (რაბები). მოწმდება ამ კომპონენტებზე მომუშავე პროტოკოლების კორექტული მუშაობაც.

ქსელის თანამედროვე პროტოკოლების უმრავლესობაში ჩაშენებულია სპეციალური სადიაგნოსტიკო საშუალებებიც, რომლებიც ავტომატურად გამოავლენენ შეცდომებს და აღადგენენ ნორმალურ მუშაუნარიანობას. ამ მექანიზმის – ჩაშენებული სადიაგნოსტიკო პროგრამების (უტილიტების) გაშვების საჭიროება მაშინვე გახდება შესამჩნევი, ვინაიდან ქსელის მუშაობა ძალზე შენელდება (ან უფრო უარესი – ავარიულად გამოირთვება შესაბამისი სეგმენტი ან მოწყობილობა), რომელიც იწვევს შეცდომებს.

კომპიუტერული ქსელის სადიაგნოსტიკო საშუალებები იყოფა ორ ძირითად ჯგუფად:

- აპარატურული სადიაგნოსტიკო მოწყობილობები (ხშირად უწოდებენ ქსელის აპარატურულ ანალიზატორებს);
- პროგრამული სადიაგნოსტიკო საშუალებები (ქსელის პროტოკოლების ანალიზა-ტორები).

მოკლედ შევეხოთ თითოეული მათგანის დანიშნულებას.

სპეციალურ აპარატურულ სადიაგნოსტიკო საშუალებებში შედის:

- ციფრული ვოლტმეტრები;
- რეფლექტომეტრები;
- კაბელის ტესტერები;

– ოსცილოგრაფები.

ციფრული ვოლტმეტრი – ეს არის უნიკალური ელექტრო საზომი ხელსაწყო. მცოდნე სპეციალისტის ხელში მას შეუძლია დაადგინოს, მაგალითად, თუ რა მოხდა ქსელის საკაბელო სისტემაში: მოხდა კაბელის გაწყვეტა, თუ მისი მოკლე ჩართვა.

რეფლექტომეტრი (TDR) – ეს არის სპეციალური მოწყობილობა ქსელის კაბელებში გაწყვეტების, მოკლე ჩართვების ან უხარისხოდ შეერთებული მონაკვეთების აღმოსაჩენად. ეს მოწყობილობა ვოლტმეტრისაგან განსხვავევით, კაბელში აგზავნის შემმოწმე-ბელ (სატესტო) იმპულსებს. თუ იმპულსის გავლის გზაზე გვხვდება უხარისხო მონაკვეთი რეფლექტომეტრი გაანალიზებს არეკლილ (დაზიანებული ადგილიდან უკან დაბრუნებულ) სიგნალს და იძლევა პასუხს, რომელიც მიუთითებს პრობლემების მიზეზზე. კარგ რეფლექტომეტრს შეუძლია დაადგინოს (ე.ი. მოახდინოს დაზიანების დიაგნოსტიკა) კაბელის გაწყვეტის ადგილი რამოდენიმე ათეული სანტიმეტრის სიზუსტით (ერთ მეტრამდე).

კაბელის სპეციალური ტესტერები – მიეკუთვნებიან სპეციალიზებულ სადიაგნოსტიკო მოწყობილობებს. მათ აქვთ გაფართოებული ფუნქციები, ვიდრე ზემოთ ნახსენებ ხელსაწყოებს. ისინი მუშაობენ ქსელის ფიზიკურ დონეზე, შეუძლიათ ასახონ ინფორმაცია ფიზიკური კაბელის მიმდინარე მდგომარეობის შესახებ, ასევე განსაზღვრონ:

– კადრების რაოდენობა;

– კოლიზიების სიჭარბე;

– ინფორმაცია გადატვირთების შესახებ;

– მაიაკის გაშვება (მაიაკი წარმოადგენს სიგნალს, რომელიც დიაგნოსტირების დროს იძლევა ნიშანს ამა თუ იმ სახის შეცდომების წარმოქმნისას).

აღნიშნული ხელსაწყოები ძალზე საჭიროა ქსელის დიაგნოსტირებისათვის. მათ შეუძლიათ დაათვალიერონ მთელი ქსელური ტრაფიკი (ტრაფიკის ქვეშ იგულისხმება ქსელის კაბელის პაკეტებით დატვირთვა მიმდინარე მომენტში, ე.ი. დატვირთვა მასში გამავალი კადრების ამსახველი (მატარებელი) სიგნალებით), გამოავლინონ შეცდომების ცალკეული სახეები. ისინი ინფორმირებენ, სახელდობრ, კაბელის რომელი სეგმენტი ან ქსელური ადაპტერის პლატა წარმოადგენს პრობლემის მიზეზს.

ოსცილოგრაფი – ეს არის ელექტრონული ხელსაწყო, რომელიც ეკრანზე ასახავს კაბელში გამავალი სიგნალის ფორმას. რეფლექტომეტრთან ერთად იგი საშუალებას იძლევა ასევე:

– მოძებნოს მოკლე ჩართვა ან კაბელის გაწყვეტა;

– ინახოს კაბელით გადაცემული სიგნალის ფორმა, რომლის საფუძველზეც შესაძლებელია მსჯელობა, აქვს თუ არა ადგილი ამ სიგნალის მილევადობას.

ქსელის მონიტორი – ეს არის აპარატურულ - პროგრამული მოწყობილობა, რომელიც დიაგნოსტირების მიზნით უთვალთვალებს ქსელის მთლიან ან მისი რომელიმე მითითებული ნაწილის ტრაფიკს (კაბელის დატვირთვის დონეს). იგი ამოწმებს პაკეტებს და აგროვებს ინფორმაციას მათი ტიპების, მათში შეცდომების შესახებ, ასევე კრებს (აგროვებს)

ინფორმაციებს ქსელის თითოეული კომპიუტერის მიერ მიღებული ან გადაცემული პაკეტების რაოდენობაზე (ამას აკეთებს, მაგალითად, HP Network Advisor - ი).

სპციალიზებული პროგრამული საშუალებები – პროტოკოლების ანალიზატორები

ქსელის მონიტორინგისა და დიაგნოსტიკის ამგვარ ანალიზატორებს ხშირად მოკლედ უწოდებენ პროტოკოლის ანალიზატორებს (Protocol Analyzers), ან უფრო ზოგადად ქსელის ანალიზატორებს (Network Analyzers), რომლებიც ახდენენ ქსელური ტრაფიკის ანალიზს მიმდინარე რეალურ დროში (ანუ კომპიუტერული ქსელის ფუნქციონირების დროს). ამასთან იგი ამოწმებს კადრების დაჭერას სადგურების მიერ, მათ არასასურველ გარდაქმნას (ე.ი. გამოიცნობენ ტრანსპორტირებისას კადრის ფორმების შეცვლას), არაკორექტულობას გადაცემისას და სხვა. ქსელის ადმინისტრატორებისა და მომსახურე ინჟინრების უმრავლესობა, რომლებიც პასუხს აგებენ, მაგალითად, მსხვილი ქსელის ნორმალურ ფუნქციონირებაზე, ძალზე დიდ იმედებს ამყარებენ დიაგნოსტირების ამ საკმაოდ მძლავრ ინსტრუმენტზე, იყენებენ რა მას ქსელის რომელიმე ინტერაქტიული მონიტორინგისათვის (ე.ი. ქსელის მუშაობის ამა თუ იმ პერიოდისათვის, ე.ი. დროის მონაკვეთში მის სეგმენტებში მიმდინარე მდგომარეობის გამოკითხვისათვის).

იმისათვის, რომ განისაზღვროს ქსელში წარმოქმნილი პრობლემის (ან პრობლემების) მიზეზი, პროტოკოლების ანალიზატორები საჭიროების შემთხვევაში იკვლევენ პაკეტების შემცველი კადრების სტანდარტული ფორმების კორექტულობას.

მათ შეუძლიათ აწარმოონ ქსელური ტრაფიკის სტატისტიკა, რათა ქსელის ადმინისტრატორებმა შეძლონ შექმნან თავიანთი ქსელური სისტემის ფუნქციონირების საერთო სურათი (განსაკუთრებით ქსელის დატვირთვის შესახებ) ან დაადგინონ მისი ცალკეული კომპონენტების "ქცევის" ხასიათი უწესივრო-ბების აღმოჩენის მიზნით.

ამგვარად, ანალიზატორების დახმარებით შესაძლებელია მოპოვებული იქნეს შემდეგი ინფორმაციები:

- ქსელის საკაბელო სისტემის დატვირთვის შესახებ;
- პროგრამული უზრუნველყოფის ქსელში მომუშავე ვერსიის შესახებ;
- ფაილების სერვერის (ან სერვერების) მუშაობის შესახებ;
- მუშა სადგურების ფუნქციონირების შესახებ;
- ინტერფეისული პლატების უწესივრობების შესახებ და ა.შ.

თანამედროვე პროტოკოლების ანალიზატორები, როგორც ვხედავთ, ხასიათდებიან მეტად გაფართოებული ფუნქციონალური შესაძლებლობებით. მაგალითად, ანალიზატორების უმრავლესობის ბოლო ვერსიებში ჩაშენებულია ჩვენს მიერ ზემოთ ნახსენები რეფლექტომეტრებიც კი.

ამგვარად, კვალიფიციურ მომხმარებელს ან გამოცდილ ქსელის ადმინისტრატორს პროტოკოლის ანალიზატორის დახმარებით ყოველთვის შეუძლიათ "შეხედონ შიგნიდან" ქსელის მოქმედებას (ქსელის "ყოფა-ქცვის" ხასიათს), რათა აღმოაჩინონ:

- ქსელში უწესივროდ მომუშავე კომპონენტები;

– ქსელის გაწყობისას (მათ შორის ქსელის სადგურებზე პროგრამების ინტეგრა-- ციისა) ან შეერთებისას დაშვებული შეცდომები;
– ტრაფიკის პულსაციები, ე.ი. ქსელის კაბელის დატვირთვის დონის ცვალებადობა (განსაკუთვრებით ქსელის მუშაობის პიკური დატვირთვის დროს);
– პრობლემები, დაკავშირებული პროტოკოლებთან (ან პროტოკოლებს შორის შეუსაბამოებები);
– პროგრამული დამატებები ზედა დონზე, რომლებიც ხვდებიან ერთმანეთთან კონფლიქტში;
– სერვისის უჩვეულო ტრაფიკი;

ვინაიდან პროტოკოლების ანალიზატორებს შეუძლიათ გამოავლინონ მრავალი პრობლემა ქსელის მიმდინარე მუშაობაში, მათ ხშირად იყენებენ შემდეგი მიზნებისათვის:

– განსაზღვრონ ქსელის ყველაზე აქტიური კომპიუტერები ან ისეთი კომპიუტერებიც, რომლებიც აგზავნიან ქსელით შეცდომების შემცველ პაკეტებს (ან მის ცალკეულ კადრებს, მათ შორის დიდი რაოდენობით). ასეთ შემთხვევებს უწოდებენ ქსელის ტრაფიკის დანაგვიანებას, ან არაკორექტული პაკეტების (ან კადრების) ”ქარიშხალს”;
– გარკვეული ტიპის პაკეტების იდენტიფიკაციის, მათი დათვალიერებისა და ფილტრაციისათვის;
– ქსელის წარმადობის შემოწმებისათვის მოცემული დროის განმავლობაში;
– სხვადასხვა ქსელურ კომპონენტებს შორის შეერთებებისა (დაკავშირებისა) და კაბელების შემოწმებისათვის (დიაგნოს-

ტიკის) ტესტური პაკეტების გენერაციისა და ქსელში მათი გატარების რეზულტატების (შედეგების) ანალიზის გზით;

– იმ პირობების შესამოწმებლად, რომლის დროსაც წარმოიქმნებიან შეცდომები.

თანამედროვე ანალიზატორები ერთმანეთისაგან განხვავდებიან თავიანთი ფუნქციონალური შესაძლებლობებით (მათ შორის შესაბამისი საბაზრო ღირებულებებითაც).

დღეისათვის ყველაზე პოპულარულ ანალიზატორებს მიეკუთვნება შემდეგი აპარატურულ-პროგრამული პროდუქტები. მათი დიდი რაოდენობის გამო განვიხლავთ მხოლოდ რამოდე-ნიმე მათგანს:

– Hewlett – Packard Network Advisor. Network Advisor – ანალიზატორი წარმოადგენს სადიაგნოსტიკო კომპიუტერს, რომელიც რელიზებულია 386 - პროცესორის ბაზაზე. მას აქვს ფერადი თხევად – კრისტალური ეკრანი, ლოკალურ ქსელთან ინტერფეისი (ქსელთან დამაკავშირებელი მოწყობილობა) და ხელოვნური ინტელექტის ჩაშენებული (ჩადგმული) მოდული, რომელსაც ჰქვია Fault Finder (შეცდომების მძებნელი).

– Network General Sniffer. Sniffer-i aris Network General ფირმის ანალიზატორების წარმომადგენელი. იგი საშუალებას იძლევა დაიჭიროს, დეკოდირდეს და ინტერპრეტირდეს კადრები 14–ზე მეტი პროტოკოლების: Apple Talk; Windows NT; Net ware; SNA; TCP/IP; VINES; X.25 და ა.შ.

Sniffer – ანალიზატორი ზომავს ქსელურ ტრაფიკს წამში კილობაიტების საერთო რაოდენობით ან წამში გამავალი კადრე-

ბის რაოდენობით. იგი გვაძლევს ინფორმაციას პროცენტებში ქსელის საერთო (ჯამური) გამტარუნარიანობებიდან. ამას გარდა Sniffer – ს შეუძლია აწარმოოს ლოკალური ქსელის ტრაფიკის სტატისტიკა, მოძებნოს ქსელში ვიწრო (მტკივნეული) ადგილები და სხვა.

– LANalyzer for windows (მწარმოებელი ფირმა Novell,Inc.) . ანალიზატორი LANalyzer for windows ასრულებს პრაქტიკულად იმავე ფუნქციებს, რაც Sniffer, ოღონდ მხოლოდ იმ ქსელებისათვის, რომლებიც მუშაობენ NetWare ოპერაციული სისტემის მართვით (კარგად მუშაობს IPX/SPX – პროტოკოლებთან). იგი წარმოადგენს არც თუ ისე ძვირ პროგრამულ პროდუქტს, რომელიც იყენებს მომხმარებლებისათვის (იგული-სხმება ქსელის ადმინისტრატორებიც) კარგად გასაგებ გრაფიკულ ინტერფეისს.
– NCC LANalyzer (მწარმოებელი ფირმა Network Communications Corporation – NCC). ეს ანალიზატორიც კარგად მუშაობს Netware ოპერაციულ სისტემაში (დამუშავებული Novell – ი ფირმის მიერ). ზემოთხსენებული LANanalyzer for Windows – ანალიზატორისაგან განსხვავებით, ანალიზატორი NCC LANanalyzer იყენებს C-worthy ინტერფეისს Netware სისტემისათვის და გამოჰყავს სადიაგნოსტიკო ინფორმაცია ტექსტურ რეჟიმში. იგი საშუალებას იძლევა გაანალიზოს და დაიჭიროს ტრაფიკი ქსელის იმ სეგმენტებზეც, რომლებიც განლაგებულია ქსელის ხიდის ან მარშრუტიზატორის მეორე ბოლოს ან WIDE AREA LINK. ამ სახის ანალიზატორებზე მომუშავე

Netware Management System უზრუნველყოფს კონსოლს (მონაცემების ამსახველ მონიტორს), რომელზედაც გამოჰყავს მონაცემები, შეკრებილი (მოგროვილი) ქსელის სხვადასხვა სეგმენტებიდან.

ამგვარად, ქსელის ადმისტრატორებს შეუძლიათ იყიდონ ზემოთ განხილული ანალიზატორები თუ სურთ გააფართოონ თავისი კომპიუტერი, აღჭურვონ ქსელის სადიაგნოსტიკო საშუალებებით (მათი შეძენა შესაძლებელია პლატების სახით, რომლებსაც აქვთ თავისი პროგრამული უზრუნველყოფა. ეს პლატები განკუთვნილია უშუალოდ ქსელის კომპიუტერში დასაყენებლად).

ზემოთ ჩამოთვლილების გარდა, როგორც ავღნიშნეთ ქსელურ ბაზარზე არსებობს საკმაოდ დიდი რაოდენობის ქსელური პროდუქტები ახალ-ახალი სადიაგნოსტიკო შესაძლებლობებით. არსებობენ ქსელის მხარდამჭერი ოპერატიული სამსახურებიც, გამოიცემა პერიოდული ნაბეჭდი მასალები და ინფორმაციის სხვა წყაროები, რომლებიც დაგეხმარებათ თქვენ (როგორც ქსელის ადმინისტრატორებს) პრობლემების გადაწყვეტის დროს. მათი შეძენა ძალზედ ადვილია, ხოლო უფრო გაცილებით ადვილია გააფორმოთ მათზე ხელმოწერა. მაგალითად, Microsoft technical information Network (TechNet) სთავაზობს მომხმარებელს ყოველმხრივ ინფორმაციას ქსელების მხარდასაჭერად (რა თქმა უნდა Microsoft–ის პროდუქტებზე ორიენტაციით).

ამას გარდა არსებობს ინტერნეტში მრავალი, ე.წ. განცხადებების ელექტრონული დაფა (BBC), რომელიც ეძღნება კომპიუტე-

რულ ქსელებს. მათი დახმარებით თქვენ შეგიძლიათ მიმართოთ გამოცდილ ქსელურ სპეციალისტებს დახმარებისათვის, განათავსებთ რა თქვენს კითხვებს ამ BBC –დაფაზე. ხოლო ყველაზე ამომწურავი ინფო-რმაცია Microsoft–ის ქსელურ პროდუქტზე თქვენ შეგიძლიათ მიიღოთ Microsoft Download Library (MSDL)–ში (ისე ცნობისათვის აღვნიშნოთ, რომ ეს სამსახური მუშაობს მხოლოდ დაგზავნის რეჟიმში. იგი არ იძლევა განაცხადების სახით ინფორმაციასა და შეკითხვებს).

ყოველივე ამის გარდა, არსებობს უამრავი წიგნი ამ სფეროში (თუმცა აქვე შევნიშნოთ, რომ ეს წიგნები საკმაოდ სწრაფად ძველდებიან ქსელური ტექნიკის განვითარების სწრაფი ტემპების გამო). შეგიძლიათ შეიძინოთ პერიოდული გამოცემებიც, რომელთაგან ამჟამად ყველაზე ცნობილია – LANMagazine (იგი გამოდის ყოველთვიურად). მის გარდა შეგიძლიათ გაეცნოთ Data communications ან PC Week. მრავალი გამოცემა შეგიძლიათ მოძებნოთ ინტერნეტშიც.

8.2 ქსელის პროტოკოლების ანალიზატორების ფუნქციების ზოგადი მიმოხილვა

კომპიუტერულ ქსელში თუ რომელიმე წყარო-სადგური გადასცემს სწორად (კორექტულად) ფორმირებულ კადრს და საკაბელო სისტემაში გავლისას ეს კადრი არ მახინჯდება, მაშინ მიმღებმა სადგურმა უნდა შენიშნოს ეს კორექტული კადრი და დაიწყოს კადრის შემცველი ინფორმაციის დამუშავება. სამწუხაროდ გვხვდება ისეთი შემთხვევები, როცა

რომელიმე სადგური (სადგურები) არ (ან ვერ) გადასცემს კორექტულად ფორმირებულ კადრებს. ამის მიზეზი შეიძლება იყოს მრავალნაირი. მაგალითად, დამახინჯებული სტრუქტურის მქონე კადრების გადაცემის მიზეზი შეიძლება იყოს (როგორც წინა თავში აღვნიშნეთ) უწესივრობები ტრანსივერებში, ქსელურ რუქებში, ქსელური მოწყობილობების დრაივერებში და ა.შ. ქსელური მოწყობილობების გარდა, ქსელის საკაბელო სისტემასაც თავის მხრივ შეუძლია დაამახინჯოს კადრები მასში სიგნალების გავლის დროს.

ქსელის მომხმარებლებისათვის (პირველ რიგში ქსელის ადმინისტრატორებისათვის) ძალზე მნიშვნელოვანია თუ როგორ სწარმოებს ანალიზატორების დახმარებით სხვადასხვა შეცდომებისა და უწესივრობების ძებნა მის არხულ დონეზე (ღია (გახსნილი) ქსელური სისტემების OSI –ეტალონური მოდელის მე-2-ე დონეზე).

აღნიშნულ პარაგრაფში სადიაგნოსტიკო მიზნებისათვის განვიხილოთ ქსელის პროტოკოლების ანალიზატორების (NCC LANalyzer და LANalyzer for Windows –ანალიზატორების მაგალითზე) ძირითადი ფუნქციები. ყურადღება გავამახვილოთ თუ როგორ სწარმოებს კადრების (განსაკუთრებით დამახინჯებული კადრების) თვალთვალი, ქსელში დაჭერა და მათი გამოკვლევა შეცდომების არსებობაზე. ამასთან ძირითადი ყურადღება გავამახვილოთ იმ კადრებზე რომლებიც არ აკმაყოფილებენ შესაბამის სტანდარტულ მოთხოვნებს. გავაანალიზებთ რა ამგვარი სახის შეცდომებს და მოვახდენთ მათ ინტერპრეტაციას, ჩვენ შეგვიძლია დავადგინოთ: სწორად მუშაობს თუ

არა ქსელის შემადგენელი ძირითდი კომპონენტები, ისეთები როგორიცაა პირველ რიგში ქსელის საკაბელო სისტემა, ქსელური ინტერფეისული რუქა, ქსელური დრაივერი თუ ტრანსივერი. ამასთან ანალიზატორების დახმარებით შეგვიძლია მოვახდინოთ ქსელის დიაგნოსტირება, კერძოდ, გამოვიკვლიოთ გადატვირთვის შემთხვევები და მათი გამომწვევი მიზეზები.

ქვემოთ ძალზე მოკლეთ, განვიხილოთ შეცდომების შემდეგი ტიპები:

– ლოკალური და დაშორებული კოლიზიები;
– შეცდომები საკონტროლო თანამიმდევრობები/გათანაბრებაში;
– შეცდომები კადრის სიგრძეში;
– მონაცემთა გაწელილი (დაგვიანებული) გადაცემა.

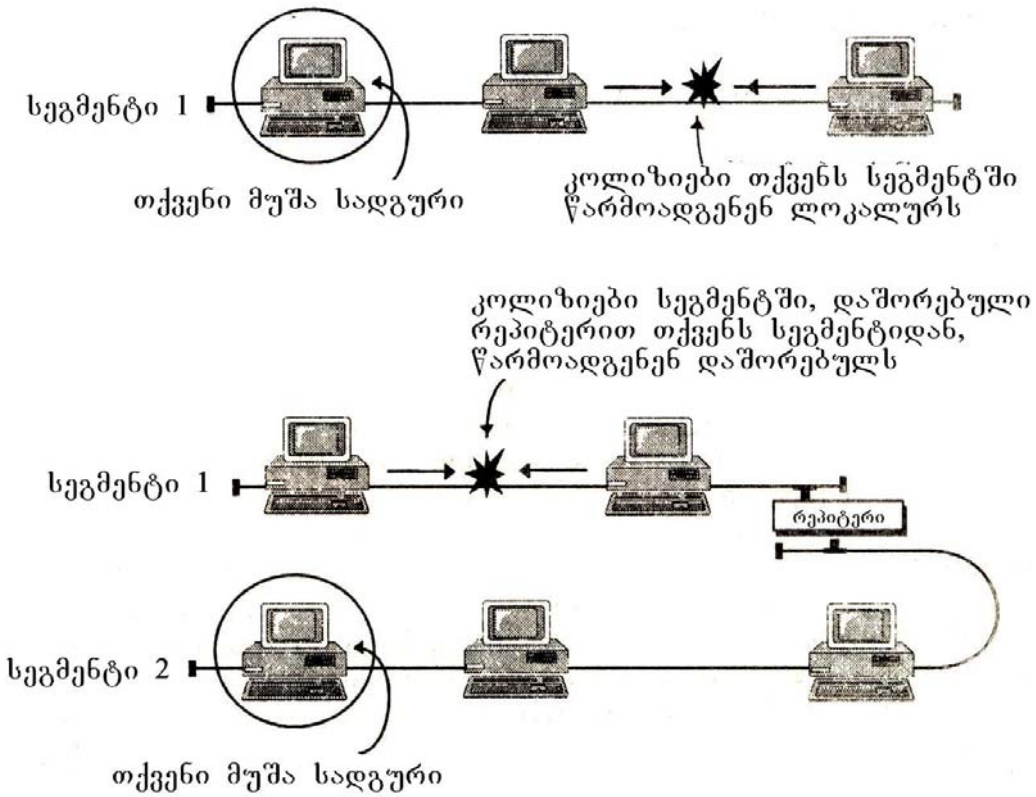
8.2.1. ლოკალურ და დაშორებულ კოლიზიებზე დაკვირვება

კომპიუტერულ ქსელებში (ქვექსელებში) მონაცემთა პაკეტების გადაცემისას, როგორც ადრეც შევნიშნეთ, თუმცა კოლიზიების წარმოქმნა წარმოადგენს CSMA/CD – პროტოკოლით მუშაობის თანმდევ მოვლენას, ამგვარი შემთხვევების გახშირება აქვეითებს ქსელის ერთ-ერთი ძირითადი პარამეტრის – წარმადობის მაჩვენებელს (წარმადობის ქვეშ ამ შემთხვევაში ზოგადად ვგულისხმობთ მომხმარებლის მხრიდან ქსელის დახმარებით შესრულებული ამოცანების რაოდენობას დროის ერთეულში). ნებისმიერ შემთხვევაში კოლიზიური მოვლენები უნდა აღმოიფხვრას. ამისათვის საჭიროა დადგინდეს მისი

გამომწვევი მიზეზები, რომლებიც მოითხოვენ ქსელის კომპონენტების დიაგნოსტიკას.

გავაანალიზებთ რა შესაბამის ინფორმაციას, შეიძლება გავარკვიოთ გამოწვეულია თუ არა კოლიზია ქსელის სეგმენტის გადატვირთვით, თუ იგი წარმოქმნილია ქსელის რომელიმე კომპონენტის უწესივრო მუშაობით. ორივე მიზეზის გასარკვევად ქსელის ადმინისტრატორმა უნდა მოახდინოს დაკვირვება და კონტროლი ქსელის მუშაობაზე. ქსელის ანალიზატორის დახმარებით დაადგინოს კოლიზიების კონკრეტული სახე, ე.ი. წარმოადგენს თუ არა ეს კოლიზიები ლოკალურს თუ დაშორებულს.

ლოკალურ კოლიზიას წარმოადგენს მოვლენა (გადაცემული პაკეტების ერთმანეთთან შეჯახება და დაზიანება), რომელიც წარმოიქმნება ერთი სეგმენტის ფარგლებში მყოფი მუშა სადგურიდან, ხოლო თუ კოლიზიები წარმოიქმნება სხვადასხვა სეგმენტზე მყოფი მომხმარებელთა კომპიუტერებიდან, მაგალითად ხვადასხვა სეგმენტზე მიერთებული მუშა სადგურებიდან, რომლებიც (სეგმენტები) ერთმანეთს უკავშირდება განმეორებლებით (რეპიტერებით) გადაცემული პაკეტების შეჯახებით, მაშინ ასეთ კოლიზიებს უწოდებენ დაშორებულ კოლიზიებს. ეს კარგად ჩანს ნახ. 8.1-ზე.



ნახ.8.1. ლოკალური და დაშორებული კოლიზიები

ასეთ ორგვარი სახის კოლიზიებს აქვთ განმასხვავებელი ნიშნები, რომლებსაც ქსელის ადმისტრატორი დაადგენს მათზე დაკვირვებით და ერთმანეთთან შეადარებს დაზიანებული კადრების პარამეტრებს, მაგალითად არიან თუ არა შეჯახებული კადრების (ე.ი. კოლიზიაში მოხვედრილი კადრების) სიგრძეები 64 ბაიტზე ნაკლები, ადგილი აქვთ თუ არა შეცდომებს მათ საკონტროლო თანამიმდევრობაში და ა.შ.

ქვემოთ კონკრეტულად დავახასიათოდ კოლიზიების ეს ორი ტიპი:

ა) ლოკალური კოლიზიები

კოლიზიებს, როგორც ზემოთ აღვნიშნეთ, ეწოდებათ ლოკალური, თუ ისინი წარმოიქმნებიან ლოკალურ სეგმენტზე. კადრის ფრაგმენტს, რომელიც წარმოიქმნება კოლიზიის შედეგად, აქვს 64 ბაიტზე ნაკლები სიგრძე და შეიცავს შეცდომის შემცველ საკონტროლო თანამიმდევრობას.

ლოკალურ კოლიზიას ავლენს კოლიზიების აღმომჩენი სქემა, რომელიც შედის ქსელური ინტერფეისული პლატის ან ტრანსივერის შემადგენლობაში. ამ სქემის დახმარებით აღმოჩნილი კოლიზია საშუალებას გვაძლევს გავარჩიოთ ლოკალური კოლიზიები დაშორებული კოლიზიებისაგან, რომლებსაც ვერ ავლენს მიმღები კომპიუტრების წყვილი, რომლებსაც უნდა მიეღოთ კოლიზიის გარეშე ეს კადრები (პაკეტები).

ბ) დაშორებული კოლიზიები

დაშორებული კოლიზიები, როგორც ავღნიშნეთ, წარმოიქმნება "იქითა მხარეს" რეპიტერიდან, რომელიც ჰყოფს ქსელის სეგმენტებს (იხ. ნახ. 8.1). სავარაუდოა, რომ წარმოიქმნა დაშორებული კოლიზია, თუ წინა შემთხვევისას (ლოკალური კოლიზიების) მსგავსად შეიქმნება მონაცემთა პაკეტები, რომელთა სიგრძე ნაკლებია 64 ბაიტის და ასევე შეიცავენ შეცდომას საკონტროლო თანამიმდევრობაში. განსხვავება იმაშია, რომ დამახინჯებული პაკეტები ვრცელდება ქსელში უფრო ფართო მასშტაბით, ვიდრე ლოკალური კოლიზიების დროს. ასეთ შემთხვევებში ხიდებისა და მარშრუტიზატორებისგან განსხვავებით რეპიტერები გადასცემენ კოლიზიის

შედეგად წარმოქმნილი პაკეტის ფრაგმენტებს (ე.ი. დამახინჯებულ კადრებს) მის მიერ (რეპიტერების მიერ) შეერთებულ ყველა სეგმენტს.

თუ ქსელის ადმინისტრატორი შენიშნავს დაშორებული კოლიზიების წარმოქმნის შემთხვევების ძალზე დიდ რაოდენობას, მან დაუყოვნებლივ უნდა მიიღოს სათანადო ზომები მათ აღსაკვეთად. ეს გამოიხატება იმაში, რომ უპირველეს ყოვლისა საჭიროა დაყენდეს დამატებითი ხიდი სეგმენტებს შორის, რათა მოახდინოს კოლიზიების გაფილტვრა. ამის შემდეგ საჭიროა ქსელის ადმინისტრატორი ეცადოს შეამციროს იმ სეგმენტის დატვირთვა, რომელიც წარმოქმნის ძალზე ხშირ კოლიზიებს. ამისათვის იგი ცვლის საკაბელო სისტემის კონფიგურაციას. ხელახალი სტრუქტურიზციის დროს თუ შეიმჩნევა კოლიზიების რაოდენობის თანდათანობით კლება, გამოკვლევის შედეგად ბოლოს და ბოლოს იგი დაადგენს იმ სეგმენტს, რომელშიც იმყოფება კონკრეტული კომპონენტი (ან კომპონენტები), რის მიზეზადაც ხდება კოლიზიების წარმოქმნა.

ამგვარად, ნებისმიერ შემთხვევაში საჭიროა ქსელის ადმინისტრატორმა დაადგინოს კოლიზიების წარმოქმნის მიზეზები.

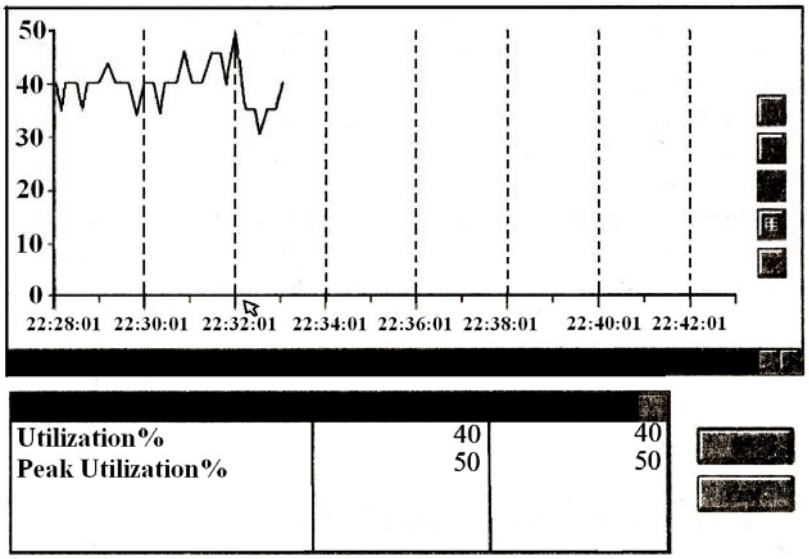
8.2.2. ხშირი ლოკალური და დაშორებული კოლიზიების მიზეზების განსაზღვრა

ბუნებრივია, წარმოიქმნება კითხვა: კოლიზიების რა რაოდენობა წარმოადგენს ძალზე დიდს, რომელიც გავლენას მოახდენს

ქსელის წარმადობაზე? თითოეულმა ქსელმა, რა თქმა უნდა, შეიძლება დაუშვას კოლიზიების გარკვეული რაოდენობა, სანამ წარმადობის დაქვეითება არ გახდება აშკარად შესამჩნევი. ითვლება, რომ კოლიზიები წარმოიქმნება ძალზე ხშირად, თუ ისინი ზემოქმედებენ თქვენს ქსელზე იმ ზომამდე, რომ მომხმარებლები უკვე "ჩივიან " ქსელის წარმადობის დაქვეითებაზე. ამ შემთხვევაში ქსელის ადმინისტრატორი ანალიზატორის დახმარებით ათვალიერებს მიმდინარე სტატისტიკურ მონაცემებს კოლიზიების წარმოქმნის რაოდენობის შესახებ. მისივე (ქსელის ანალიზატორის) დახმარებით ძალზე მნიშვნელოვანია გაეცნოს (ქსელის ადმინისტრატორი) ასევე ინფორმაციას ქსელის მიმდინარე დატვირთვის შესახებ. ასეთი ინფორმაცია ეხმარება ქსელის ადმინისტრატორს განსაზღვროს არის თუ არა ძალზე გახშირებული კოლიზიების წარმოქმნის მიზეზი სეგმენტის გადატვირთვა, თუ ეს გამოწვეულია რომელიმე კომპონენტის უწესივრო მუშაობით. კოლიზიების ძალზე მომატებული რიცხვის მიზეზები, ეს იქნება აპარატურაში უწესივრობა, თუ მიმდინარე მომენტისათვის ძალზე ინტენსიური ტრაფიკი, კოლიზიების რაოდენობის მკვეთრი გაზრდა სწრაფად და ადვილად გამოვლინდება ქსელის ანალიზატორის სტატისტიკური მონაცემებით, რომლებიც საშუალებას აძლევს ქსელის ადმინისტრატორს შეადაროს მიმდინარე მდგომარეობა კოლიზიების რაოდენობის შესახებ დაგროვილ მონაცემებთან.

ა) კოლიზიები, გამოწვეული გადატვირთული სეგმენტით

თუ ქსელის სეგმენტის დატვირთვა გაიზარდა ახალი კვანძების მიერთებით, ან ახალი გამოყენებითი პროგრამის ამოქმედებით და კოლიზიების რიცხვი მაღალია, სავარაუდოა, რომ კოლიზიები წარმოიქმნენ ქსელის სეგმენტზე ინტენსიური ტრაფიკის ზემოქმედებით. ეს შეიმჩნევა როგორც დატვირთვის დიაგრამაზე (როგორც აღვნიშნეთ, თუ დიაგნოსტირების დროს ვიყენებთ LANalyzer for Windows – ანალიზატორს, მას აქვს მომხმარებილისათვის კარგად გასაგები გრაფიკული ინტერფეისი) წარმოქმნილი პიკებით (მაგალითის სახით ეს ნაჩვენებია ნახ. 8.2-ზე, საიდანაც კარგად ჩანს, რომ



ნახ.8.2. გადატვირთული სეგმენტი

ქსელის სეგმენტზე 22.32.01 საათზე კოლიზიების რაოდენობამ მიაღწია 50), იგივე რაოდენობა შეიძლება გამოვლენილი იქნეს სტატისტიკის შედარებით და გამოვლენილი იქნეს ტექსტურ რეჟიმში ანალიზატორის მუშაობის დროს. ასეთი რეჟიმი გააჩნია ჩვენს მიერ წინა §8.1 პარაგრაფში ნახსენებ NCC LANalyzer ანალიზატორს (იმავე ნახ.8.2-ზე ნაჩვენებია ინფორმაცია კოლიზიების სტატისტიკის შესახებ, გამოხატული ანალიზატორის მიერ % – ში, საიდანაც ვიგებთ, რომ კოლიზიების რიცხვი მიმდინარე მომენტისათვის 40% – დან გაიზარდა 50% - მდე).

ერთ – ერთი შესაძლო გამოსავალს ამ სიტუაციიდან წარმოადგენს ქსელის საკაბელო სისტემის რეკონფიგურაცია (დატვირთვის გამოსავლინებლად) ხიდების ან/და მარშრუტიზატორების გამოყენებით (რეპიტერები, როგორც წესი, არ ფილტრავენ ტრაფიკს). ხიდები და მარშრუტიზატორები გაფილტრავენ დაშორებულ კოლიზიებს და შეინარჩუნებენ ლოკალური ტრაფიკის დონეს, დამისამართებულს ერთ სეგმენტზე.

ასეთ შემთხვევაში სადიაგნოსტიკო საშუალებებით (ჩვენს მიერ ნახსენები ანალიზატორებით) უწესივრობების აღმოჩენისა და აღმოფხვრის ტექნოლოგია მდგომარეობს იმაში, რომ, როცა ორი ან მეტი სეგმენტების შემაერთებელი ხიდი შენიშნავს მონაცემთა პაკეტს, იგი აფიქსირებს ამ პაკეტის გამომგზავნ – წყარო კომპიუტერის აპარატულ (ანუ ფიზიკურ) მისამართს, ასევე იწერს ინტერფეისის ნომერს, საიდანაც გამოგზავნილია ეს პაკეტი. ეს ინფორმაცია ინახება და გამოიყენება ხიდის მიერ იმ პაკეტების გამოსავლინებლად, რომლებიც განკუთვნილია სხვა

სეგმენტებისათვის და არ მოითხოვენ შემდგომ რეტრანსლაციას. ხიდები იყენებენ მხოლოდ მისამართს Ethernet – სათაურიდან (რომლებიც მითითებულია კადრებში) და არ ითვალისწინებენ ქსელურ ინფორმაციას ან მისამართს,რომელიც შეესაბამება IPX–პროტოკოლს.

მარშრუტიზატორები ახდენენ მხოლოდ იმ პაკეტების რეტრანსლაციას, რომლებიც იგზავნება სხვა ქსელური მისამართით. პაკეტები რომლებიც განკუთვნილია იმავე ლოკალური ქსელისათვის, იფილტრება მარშრუტიზატორის მიერ.

ანალიზატორების ეკრანზე ნაჩვენები იქნება ქსელის დატვირთვის შესახებ მონაცემები როგორც ხიდის დაყენებამდე, ისე მისი დაყენების შემდეგ (ფილტრაციის მიზნით).

დ) კოლიზიები, გამოწვეული ძალიან გრძელი სეგმენტებით

თუ ქსელის რომელიმე სეგმენტი (სეგმენტები) აღემატება სტანდარტით დასაშვებ მაქსიმალურ სიგრძეს, მაშინ კაბელის დაშორებულ მხარეს მყოფმა კვანძებმა შეიძლება ჩათვალონ, რომ არხი თავისუფალია და დაიწყებენ თავიანთი პაკეტის გადაცემას. ამ დროს სინამდვილეში არხში გადაცემულია უკვე სხვა პაკეტი, რომლის გავრცელება (გაადგილება) დიდ ხანგრძლივობას მოითხოვს. ასეთ შემთხვევაში შეიძლება მოხდეს ამ პაკეტების შეჯახება (კოლიზია). ამგვარად, ვინაიდან რომელიმე სადგურის მიერ გადაცემულმა პაკეტმა ჯერ ვერ მოასწრო გავრცელება საკაბელო სისტემაში, დაშორებულ მხარეს მყოფ კვანძებს (მუშა სადგურებს) შეუძლიათ დაიწყონ

პაკეტაბის გადაცემა, რაც გამოიწვევს კოლიზიებს. ცხადია, ამ შემთხვევაში ლოკალური კოლიზიები არ წარმოიქმნებიან ქსელის გადატვირთვის შედეგად და არც სეგმენტის დატვირთვა არ გაცდება დასაშვებ ნორმალურ დონეს. ასეთ შემთხვევაში წარმოდგენილი კოლიზიების აღსაკვეთად ქსელის ადმინისტრატორმა უნდა შეამოწმოს სეგმენტის სიგრძე, რათა დარწმუნდეს, იმაში, ხომ არ გადასცდა იგი დასაშვებ სიდიდეს.

ე) კოლიზიები, გამოწვეული დაშორებული სეგმენტის დატვირთვით

სეგმენტში დაშორებული კოლიზიების დიდი რაოდენობის წარმოქმნა მოწმობს იმაზე, რომ ეს კოლიზიები წარმოადგენენ ლოკალურს სხვა იმ სეგმენტისათვის, რომელიც მიერთებულია რეპიტერით. ქსელის ადმინისტრატორმა ამ შემთხვევაში უნდა გაარკვიოს მიზეზი, რომელიც იწვევს ლოკალურ კოლიზიებს მიერთებულ სეგმენტში. იმისათვის, რომ შეამციროს რაოდენობა დაშორებული კოლიზიებისა, რომლებიც გადადიან ლოკალურ სეგმენტში, ქსელის ადმინისტრატორმა რეპიტერი უნდა შეცვალოს ხიდით ან მარშრუტიზატორით. ეს ხიდი ან მარშრუტიზატორი გაფილტრავენ დაშორებულ კოლიზიებს და არ მისცემენ მათ საშუალებას გავრცელდნენ სხვა სეგმენტებზე.

ქსელს, რომლის სეგმენტი გაერთიანებულია რეპიტერებით, უნდა ჰქონდეს დაახლოებით თანაბარი ტრაფიკი (დატვირთვა პაკეტებით) სეგმენტებში, ვინაიდან მთელი ტრაფიკი “მეორდება” და არ იფილტრება. თუ არსებობს საფუძველი ვივარაუდოთ, რომ

რომელიმე სეგმენტში წარმოიქმნება უფრო მეტი კოლიზიები, ვიდრე სხვა სეგმენტებში, მათი მიზეზი შეიძლება იყოს აპარატურის ისეთი უწესივრობა, როგორიცაა რომელიმე ქსელური პლატის ან ტრანსივერის მტყუნება (მწყობრიდან გამოსვლა). ვინაიდან კოლიზიაში მოხვედრილი სადგურები, როგორც წესი, ალბათ შეეცდებიან დაიწყონ პაკეტების (ამჟამად უკვე დაზიანებული) განმეორებითი გადაცემები, ქსელის ადმინისტრატორი უნდა დააკვირდეს რამოდენიმე კოლიზიას და განსაზღვროს, შეიძლება თუ არა იმ სადგურის გამოვლენა, რომელიც მაშინვე იწყებს გადაცემას კოლიზიის შემდეგ. ამით დგინდება, რომ დიდი ალბათობაა იმისი, რომ ამ სადგურის აპარატურაა უწესივრო მდგომარეობაში, რაც ასევე იწვევს დაშორებული კოლიზიების წარმოქმნას. დაზიანებული აპარატურის დროული შეცვლა გამოასწორებს ამ პრობლემას.

8.2.3. დაგვიანებულ კოლიზიებზე და საკონტროლო თანამიმდევრობა/გათანაბრების შეცდომებზე დაკვირვება

დაგვიანებული კოლიზიები და შეცდომები კადრების საკონტროლო თანამიმდევრობა/გათანაბრებაში მოწმობენ საკაბელო სისტემაში ან ქსელის კომპონენტებში უწესივრობების არსებობას.

ა) დაგვიანებული კოლიზიები

დაგვიანებული კოლიზიები განისაზღვრება, როგორც წარმოქმნილი ისეთი პაკეტები, რომელთა სიგრძე აღემატება 64 ბაიტს და შეიცავენ საკონტროლო თანამიმდევრობა /გათანაბრებაში შეცდომებს. დაგვიანებული კოლიზიები დაითვლება მხოლოდ ლოკალური სეგმენტისათვის. თუ დაგვიანებული კოლიზიის პაკეტი გადაიცემა მარშრუტიზატორით, ითვლება, რომ იგი შეიცავს არასწორ საკონტროლო თანამიმდევრობას.

დაგვიანებული კოლიზიები არ არის ბუნებრივად დამახასიათებელი Ethernet- ქსელებისათვის. მიუხედავად ამისა დაგვიანებული კოლიზიების წარმოქმნა ნიშნავს იმას, რომ, თუმცა რომელიმე სადგური, რომელიც გადასცემდა საკმარისი სიგრძის (როგორც აღვნიშნეთ დასაშვები მინიმალური სიგრძეა 64 ბაიტი) მონაცემებს, იმავე მომენტში გადამცემ გარემოს შესაძლებელია დაეუფლა კიდევ სხვა სადგური, რომელიც ასევე ახდენდა თავისი მონაცემების გადაცემას, რის შედეგადაც წარმოიქმნა ამ სადგურის მიერ გადაცემული პაკეტების შორის კონფლიქტი.

ქსელის მუშაობის ნორმალურ რეჟიმში მუშაობისას ჩვენს მიერ ზემოთ (§6.1) განხილული მონაცემთა გადაცემის ალგორითმის მიხედვით ქსელში ჩართულმა ყველა სადგურმა უნდა გამოიცნოს არხში პაკეტების არსებობა. თუ ქსელის ყველა კვანძში სრულდება CSMA/CD–მეთოდით (ალგორითმით) გათვალისწინებული ქსელში შეღწევის წესი, დაგვიანებული კოლიზიები პრაქტიკულად არასდროს წარმოიქმნება.

ბ) შეცდომები საკონტროლო თანამიმდევრობა/გათანაბრებაში

პაკეტები, რომელთა საკონტროლო თანამიმდევრობის ველები არაკორექტულია (არასწორი მნიშვნელობისაა), ითვლება "შეცდომების" შემცველ პაკეტებად. გადასცემს რა კადრს ქსელურ გარემოში სადგური აერთებს კოდურ თანმიმდევრობას კადრის ბოლოში. ეს მნიშვნელობა წარმოადგენს მრავალწევრების გაყოფის ნაშთს, რომელიც გამოითვლება თითოეული წყარო–სადგურის კადრის შემცველობის მიხედვით. მიმღებმა სადგურმაც უნდა შეასრულოს მსგავსი გამოთვლა და შეადაროს მიღებული შედეგი (ნაშთი) საკონტროლო თანამიმდვრობის ველის შემცველობასთან. თუ ეს რიცხვები (ნაშთები) არ ემთხვევა ერთმანეთს, ითვლება, რომ კადრი შეიცავს შეცდომის მქონე (არაკორექტულ) საკონტროლო თანამიმდევრობას. ხოლო თუ კადრი არ მთავრდება 8 ბიტიან საზღვარზე, ითვლება, რომ იგი შეიცავს შეცდომას გათანაბრებაში. შეცდომის ეს ორივე ტიპი გაერთიანდება და განიხილება როგორც შეცდომა საკონტროლო თანამიმდევრობა/გათანაბრებაში.

ქვემოთ ნაჩვენებ ცხრილში შედარებულია დაგვიანებული კოლიზიები და შეცდომები საკონტროლო თანამიმდევრობა /გათანაბრებაში:

შეცდომის ტიპი	64 ბაიტზე ნაკლები სიგრძე	შეცდომა საკონტ. თანმიმდევრობაში	კოლიზიების აღმომ.წყ.გადთ
დაგვიანებული კოლიზია	არა	კი	კი
CRC/გათნაბრება	არა	კი	არა

CRC –შეცდომა საკონტროლო თანმიმდევრობაში.

8.2.4. დაგვიანებული კოლიზიებისა და საკონტროლო თანამიმდევრობა / გათანაბრებაში შეცდომების განსაზღვრა

დაშორებული კოლიზიები და შეცდომები საკონტროლო თანამიმდევრობა / გათანაბრებაში, როგორც ზემოთ აღვნიშნეთ, არ წარმოადგენს ბუნებრივ დამახასიათებელ თვისებას Ethernet–ისათვის. ამისათვის ამგვარი შეცდომები უნდა იქნეს გამოვლენილი და უნდა დავრწმუნდეთ იმაში, რომ ისინი გავლენას არ მოახდენენ ქსელის წარმადობაზე. არსებობს ორი ძირითდი მიზეზი ასეთი შეცდომების არსებობისა. ერთი მდგომარეობს საკაბელო სისტემის უწესივრობაში, ხოლო მეორე–ქსელის კომპონენტების უწესივრობაში.

ა) საკაბელო სიტემის უწესივრობები

არსებობს დიდი ალბათობა იმისა, რომ საკონტროლო თანამიმდევრობა/გათანაბრებაში შეცდომის წარმოქმნას იწვევდეს საკაბელო სისტემის ისეთი უწესივრობა, როგორიცაა მოკლე ჩართვა ან ხმაური, წარმოქმნილი კაბელზე ზემომქმედი რაიმე ელექტრომაგნიტური ველით.

კოლიზიების წარმოქმნის მიზეზი ხშირად ქსელის საკაბელო სისტემის არასწორი მონტაჟის ბრალიცაა (როდესაც ეს მონტაჟი არ შეესაბამება მიღებული სტანდრტის სპეციფიკაციას) ან ეს შეიძლება გამოწვეული იყოს ქსელში "ყრუ" კვანძების არსებობით (რომლებიც ცუდად უსმენენ წარმტან სიგნალებს). თუ ქსელში მატულობს დაგვიანებული კოლიზიების რიცხვი, ან საკონტროლო თანამიმდევრობა/გათანაბრებაში შეცდომების რაოდენობა, ქსელის ადმინისტრატორმა აუცილებლად უნდა შეამოწმოს საკაბელო სისტემაში შესაძლო შემდეგი დარღვევები:

– **ძალზე გრძელი სეგმენტი.** საკაბელო სისტემის ძალზე შორს (ერთ ბოლოს) მყოფი კვნძები (მუშა სადგურები) იწყებენ გადაცემას, არ იციან რა იმის შესახებ, რომ მეორე ბოლოს მყოფმა რომელიმე სადგურმა აიღო თავის თავზე (ხელში ჩაიგდო) გარემოს მართვა, რომელიც გადასცემს კადრის პირველ 64 ბაიტს.

– **კაბელის უწესივრობა.** მონაცემთა პაკეტი, რომლიც გადის მოკლედჩართულ ან დაზიანებულ კაბელში, მანამდე მახინჯდება, სანამ იგი მიაღწევდეს მიმღებ სადგურამდე.

– **სეგმენტი ცუდადაა დამიწებული.** უხარისხოდ დამიწებული სეგმენტი იწვევს მონაცემთა ნაკადის დამახინჯებას ფონური ან კაბელზე ზემოქმედი ხელშეშლებით.

–**კაბელის არასწორი დაბოლოება.** თუ კაბელის სეგმენტის ბოლოები დამონტაჟებულია არასწორად, სეგმენტის ბოლოებისაკენ (ორივე მხარეს) გამავალი სიგნალების ნაწილი შესაძლოა

შთაინთქას, ან მათმა დანარჩენმა ნაწილმა გამოიწვიოს "ხმაური" და კოლიზიები კაბელში არსებულ სიგნალებთან.

– ძალზე ახლოსაა განლაგებული კაბელიდან გამომყვანები. ერთ კაბელზე მიერთებულ მუშა სადგურებს შორის დაცული უნდა იყოს მათი განლაგების დასაშვები მინიმალური სიგრძე (ეს სიგრძე გათვალისწინებულია, აგრეთვე, სტანდარტის სპეციფიკაციებით და დამოკიდებულია გამოყენებული კაბელის ტიპზე), რათა არ მოხდეს სიგნალების არეკვლები და სადურების მიერ გადაცემული მონაცემების დამახინჯებები.

– კაბელის "დახმაურება". რადიოხელშეშლები და ელექტრომაგნიტური ველები, რომლებიც ზემოქმედებენ გაჭიმულ კაბელზე (მაგალითად, თუ კაბელის ახლოს მუშაობს რაიმე ელექტროძრავა, ან ისეთი დანადგარი (შესადუღი აპარატი), რომელიც აფრქვევს ნაპერწკლებს და წარმოქმნის ხელშემშლელი "ხმაურის" ველებს), ამხინჯებენ სიგნალებს და იწვევენ შეცდომებს საკონტროლო თანამიმდევრობა /გათანაბრებებში.

ბ) კომპონენტების უწესივრობები

ქსელში არსებული უწესივრო (დაზიანებული) კომპონენტები იწვევენ როგორც დაგვიანებული კოლიზიების წარმოქმნას, ასევე შეცდომებს საკონტროლო თანამიმდევრობა/გათანაბრებაში. ყველაზე ხშირად გავრცელებულ უწესივრობას ქსელში წარმოადგენს:

– ყრუ /ნახევრად ყრუ კვანძები. ისეთ უწესივრო სადგურს, რომელსაც დაკარგული აქვს შესაძლებლობა მოუსმინოს ხაზის აქტიურობას, ე.ი. კაბელში გამავალი სიგნალების მდგომარეობას, უწოდებენ ყრუ კვანძებს. თუ გაჩნდა ეჭვი იმისა, რომ

კვანძი (მუშა სადგური ანუ ქსელის მომხმარებლის პერონალური კომპიუტერი) გახდა "ყრუ" (ან "ნახევრად ყრუ"), საჭიროა ქსელური პლატის (ხშირად მოიხსენიებენ, როგორც ინტერფეისული რუქის) ან ტრანსივერის (მონაცემთა მიმღებ/გადამცემი მოწყობილობების) შეცვლა.

– რეპიტერის, ტრანსივერის ან კონტროლერის რუქის (პლატის) უწესივრობა.

ასეთ შემთხვევებში მათ შეუძლიათ დაამახინჯონ სიგნალი ქსელში და გადასცენ შეცდომების შემცველი სიგნალები ხაზში ან იგნორირება გაუკეთონ მონაცემთა შემოსულ (მიმღებ კვანძებში) პაკეტებს. უწესივრო კომპონენტი ასევე უნდა შეიცვალოს ახლით, ვინაიდან მათი შეკეთება (განსაკუთრებით პლატის, შესრულებული ინტეგრალური ტექნოლიგიით) პრაქტიკულად შეუძლებელია.

8.2.5. კადრის სიგრძის შეცდომებზე დაკვირვება

დღეისათვის მომქმედი სტანდარტის მიხედვით Ethernet–ის ტიპის კადრების სიგრძე (ასეთი კადრების სტრუქტურები განხილული გვქონდა მე–5 თავში) უნდა მდებარეობდეს 64–დან 1518–მდე ბაიტის დიაპაზონში (კადრის სათაურის სიგრძის და საკონტროლო თანამიმდევრობის ველების სიგრძის ჩათვლით). კადრებს, რომლებსაც გააჩნიათ 64 ბაიტზე ნაკლები, ან 1518 ბაიტზე მეტი სიგრძე (მიუხედავათ იმისა, რომ მათ შეიძლება ჰქონდეთ კორექტული საკონტროლო თანამიმდევრობა), უწოდებენ სიგრძეში შეცდომების შემცველ კადრებს.

ა) მოკლე კადრები

ასეთ კადრებს ლიტერატურაში (განსაკუთრებით რუსულ ენოვან ლიტერატურაში) უწოდებენ მოკლე, ანუ "კარლიკ-კადრებს" ("ლილიპუტ–კადრებს"). მათი სიგრძე ნაკლებია 64 ბაიტზე და შეიცავენ კორექტულ საკონტროლო თანამიმდევრობას.

ბ) გრძელი კადრები

კადრებს, რომელთა სიგრძე აღემატება აღემატება 1518 ბაიტს, მაგრამ შეიცავენ კორექტულ თანამიმდევრობას, უწოდებენ გრძელ კადრებს (ზოგჯერ მოიხსენებენ როგორც "გიგანტ კადრებს").

ორივე შემთხვევაში მდგომარეობის გამოსასწორებლად არსებობს შემდეგი გამოსავალი. პირველ შემთხვევაში (ა) კადრებს შეავსებენ "0"–ებით (დასაშვებმინიმალურ 64–ბაიტამდე), ხოლო მეორე შემთხვევაში (ბ) სწარმოებს კადრის დაყოფა ორ ან მეტ ნაწილებად, ამასთან თითოეულს უნდა გააჩნდეს არანაკლები დასაშვები 64 ბაიტის სიგრძე.

8.2.6. კადრის სიგრძის დარღვევის მიზეზების განსაზღვრა

კადრები, დარღვეული სიგრძეებით გამოწვეულია გადამცემი-სადგურის (წყარო–კომპიუტერის) მიზეზით. იმ კვანძის მოძებნა, რომელიც პასუხისმგებელია ასეთი კადრების გაგზავნაზე, სირთულეს არ წარმოადგენს, ვინაიდან კადრი ფორმირებულია კორექტულად, სათაური კი შეიცავს წყაროს მისამართსაც.

სიგრძის დარღვევას იწვევს უწესივრო ქსელური დრაივერები (ე.ი. პროგრამები), რომლებიც მუშაობენ წყარო-სადგურებზე. ქსელის ადმინისტრატორი ვალდებულია შეამოწმოს ძველი დრაივერი და შეცვალოს ახალი ვერსიით. თუ კი იგი (ქსელის ადმინისტრატორი) თვლის, რომ ვერსია არ არის მოძველებული, მაშინ შესაძლოა დამახინჯდა დრაივერის ფაილი. ასეთ შემთხვევაში მან უნდა გადატვირთოს დრაივერი საწყისი დისკიდან ან გადმოაკოპიროს სხვა სადგურიდან, რომელიც გადასცემს კორექტული სიგრძის კადრებს.

დარღვეული სიგრძის მქონე კადრების წარმოქმნის მიზეზი შეიძლება იყოს მარშრუტიზატორიც. თუ მარშრუტიზატორი აკავშირებს ერთმანეთს ორ სხვადასხვა ტიპიან ქსელებს, სადაც (რომელიმე მათგანში) არ სრულდება მოთხოვნები კადრის სიგრძეების შეზღუდვაზე, მაშინ იგი (მარშრუტიზატორი) გადასცემს კადრებს დარღვეული სიგრძით. მაგალითად, ATM გარემოდან Ethernet–ის გარემოში, მარშრუტიზატორმა 53 – ბაიტიან პაკეტებს (უფრო ზუსტად ამ პაკეტების კადრებს) უნდა დაუმატოს შემავსებელი (იხილე ასეთი ველები კადრების სტრუქტურებში, რომლებიც განხილულია მე-5 თავში), რათა პაკეტის სიგრძე გახდეს ტოლი არანაკლებ 64 ბაიტის. თუ მარშრუტიზატორი მუდამ გადასცემს სიგრძეში დარღვეულ კადრებს, მაშინ უნდა მიმართოს (ქსელის ადმინისტრატორმა) მის დამამზადებელ ფირმას.

8.2.7. მონაცემების დროში გაწელილ გადაცემებზე დაკვირვება

მონაცემთა გადაცემის დროში გაწელვას (ე.ი. პაკეტების "გაჭიანურებულ" გადაცემებს) იწვევს ისეთი პაკეტების არსებობა, რომლებსაც გააჩნიათ 1518 ბაიტზე მეტი სიგრძე და ამასთან ისინი შეიცავენ შეცდომებს საკონტროლო თანამიმდევრობაში. მონაცემთა დროში გაწელილი გადაცემა უკავშირდება ტრანსივერის უწესივრობას (ტრანსივერში იგულისხმება მონაცემთა პაკეტების მიმღებ–გადამცემი ფიზიკური მოწყობილობა (აპარატურა)). ამჟამად მომქმედი სტანდარტის სპეციფიკაციით (ინტერნეტ–ქსელებისათვის) ტრანსივრმა უნდა აწარმოოს გადაცემა არა უმეტეს 150 მბიტ/წამში. ეს დრო საკმარისია 1518 ბაიტის ერთჯერადი გადაცემისათვის. თუ ტრანსივერი არ წყვეტს გადაცემას 1518 ბაიტის გადაცემის შემდაგაც, ითვლება, რომ იგი "წელავს" (როგორც ვთქვით "აჭიანურებს") გადაცემის სტანდარტულ დროს. თუ ქსელის ადმინისტრატორი ეჭვობს, რომ ზოგიერთი ტრანსივერი "წელავს" გადაცემის დროს, მაშინ მან უნდა შეამოწმოს გადაცემის საინდიკაციო ნათურა, მდებარე ტრანსივერის გარეთა ნაწილზე, რათა დარწმუნდეს, რომ ტრანსივერი არასწორად გადასცემს მონაცემებს. ასეთ შემთხვევაში საჭიროა შეიცვალოს უწესივრო ტრანსივერი, რათა მან გავლენა არ მოახდინოს ქსელის წარმადობაზე.

8.3 სადიაგნოსტიკო პაკეტები. მათი დანიშნულება და ფორმირების მაგალითები

ლოკალურ კომპიუტერულ ქსელებში, როგორც ამ თავის დასაწყისში (§8.1) აღვნიშნეთ, ამჟამად გამოიყენება დიაგნოსტიკის სხვადასხვა მეთოდები და საშუალებები. მათ შორის საკმაო პოპულარობით სარგებლობს ჩვენს მიერ ზემოთ განხილული ფირმა Novell, Inc-ის მიერ წარმოებული ანალიზატორები (ასეთს წარმოადგენს LANalyzer for Windows, რომელსაც აქვს გრაფიკული ინტერფეისი), ასევე NCC LANalyzer (მწარმოებელი ფირმა Network Communication Corporation), რომელსაც დიაგნოსტიკის შედეგები გამოჰყავს C-Worthy ინტერფეისზე და ინფორმაციას კომპიუტერის ეკრანზე ასახავს ტექსტურ რეჟიმში. ორივე ზემოთხსენებული ანალიზატორი ეფექტურად მუშაობს Netware ოპერაციული სისტემის მართვით. ამასთან მათ გააჩნიათ ექსპერტული ჩაშენებული სისტემა, რომელიც ქსელის სადიაგნოსტიკო საქმიანობას წარმართავს "კითხვა-პასუხის" დიალოგურ რეჟიმში. ფირმა Novell, Inc-ის ანალიზატორის გაუმჯობესებული ვერსიაა Netware LANanalyzer Agent, რომელიც წარმოადგენს განაწილებულ პროგრამულ პროდუქტს.

Netware LANanalyzer Agent საშუალებას იძლევა გაანალიზებული და დაჭერილი იქნეს ტრაფიკი ქსელის იმ სეგმენტებზეც, რომლებიც განლაგებულია ქსელური ხიდის, მარშრუტიზატორის სხვა მხარეს (მეორე ბოლოს) ან WIDE AREA LINC.

აღნიშნულ პარაგრაფში სადიაგნოსტიკო პაკეტების შექმნა და მათი გამოყენების პროცედურები (ალგორითმები) განვიხილოთ ამ ანალიზატორების გამოყენების მაგალითზე, თუმცა, როგორც ავღნიშნეთ, არსებობს სხვა ანალიზატორებიც, მათ შორის Microsoft ფირმის, რომლებიც ხასიათდებიან სხვადასხვა სადიაგნოსტიკო შესაძლებლობებით (რაც აისახება კიდეც მათ გასაყიდ ფასზე. ცხადია გაფართოებული და სრულყოფილი ანალიზატორები უფრო ძვირადღირებულია, ვიდრე შეზღუდული ფუნქციონალური შესაძლებლობების მქონე ანალიზატორების საბაზრო ღირებულებები. ზოგადად თუ ვიმსჯელებთ, მათი ფასი დამოკიდებულია იმაზეც თუ რაოდენ ავტომატიზებულია სადიაგნოსტიკო პროცედურები, რეალიზაციის თვალსაზრისით როგორია მათში აპარატურისა და პროგრამული ნაწილის ხვედრითი წილი და ა.შ.).

ზემოთხსენებულ ანალიზატორებში, როგორც ადრეც შევნიშნეთ, სადიაგნოსტიკო პროცედურები წარმოებს Netware ოპერაციული სისტემის მართვით (იგულისხმება ანალიზატორები LANalyzer for Windows, NCC LANanalyzer და Netware LANanlyzer Agent).

ლოკალური კომპიუტერული ქსელების ანალიზისათვის ძალზე სასრგებლოს წარმოადგენს Diagnostic Responder - პროტოკოლის გამოყენება. ამ პროტოკოლს გააჩნია მონაცემების ქსელთაშორისო (ან ქვექსელებს შორის) გაცვლის შესაძლებლობა, მაგალითად, “პინგ-პონგის” ტიპის. ეს ნიშნავს იმას, რომ სადიაგნოსტიკო პაკეტების გაგზავნისას, დამისამართებულმა

კვანძებმა ამ პაკეტს უნდა გამოუგზავნოს პასუხი, რომელიც შეიცავს ქსელის სადიაგნოსტიკო მონაცემებს.

ძალზე საინტერესოა (და სასრგებლოა) გავეცნოთ მეთოდებს, და ამ მეთოდებზე დაფუძნებულ სადიაგნოსტიკო ალგორითმებს, რომლებიც გააჩნია Diagnostic Responder –პროტოკოლს: შეერთებების (ქსელის სადურების); შემოწმების; კონფიგურაციის შესახებ ინფორმაციის შეგროვების და ა.შ. სადგურების მდგომარეობების გამოკვლევის მიზნით. სადიაგნოსტიკო შეკითხვებისა (მოთხოვნებისა) და სადიაგნოსტიკო პასუხების დახმარებით, შესაძლებელია გავიგოთ ქსელის სხვადასხვა კომპონენტების (როგორიცაა დრაივერები, მარშრუტიზატორები, ფაილური სერვერები და ა.შ.) მიმდინარე მდგომარეობა. აღნიშნულ პარაგრაფში ასევე მოკლედ განვიხილოთ სადიაგნოსტიკო შეკითხვებისა და სადიაგნოსტიკო პასუხების შემცველი პაკეტების სტრუქტურა, ამას გარდა განვიხილოდ სადიაგნოსტიკო ტესტების შექმნის საკითხები (თუ როგორია სადიაგნოსტიკო ტექნოლოგია) IPX სათაურის გამოყენებით, რომელიც შეიცავს ზემოთხსენებულ სადიაგნოსტიკო შეკითხვებსა და სადიაგნოსტიკო პასუხებს.

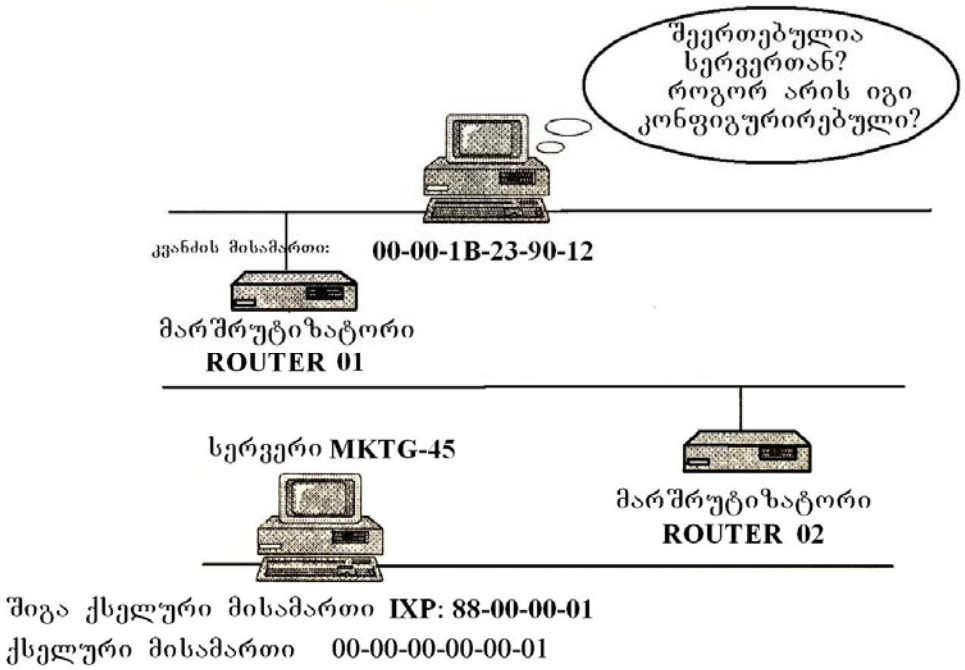
8.3.1. კლიენტ სერვერული შეერთებების ტესტირება ქსელში

კომპიუტერული ქსელის მუშა სადგურებზე IPX, COM ან IPXODI. COM ჩატვირთვისას პროტოკული – Diagnostic Reaponder-იც ჩაიტვირთება ავტომატურად. ქსელის ყველა სერვე-

რებს და კლიენტებს, რომელებშიც ჩატვირთულია Diagnostical Responder, თუ კი ისინი შეკითხვის (მოთხოვნის) დროს მიიღებენ სადიაგნოსტიკო პაკეტს (მისი სტრუქტურების შედგენის მაგალითები განხილული ამავე პარაგრაფის 8.3.4 ქვეპარაგრაფში) კონკრეტული კვანძის მისამართით ან OxFF-FF-FF-FF-FF-FF (ფართო-სამაუწყებლო დაგზავნა) მისამართით, მათ უნდა გაუგზავნონ სადიაგნოსტიკო პასუხი სადიაგნოსტიკო კითხვაში (მოთხოვნაში, ხშირად ასეთ შეკითხვებს უწოდებენ, როგორც სადიაგნოსტიკო განაცხადებს) მითითებულ პარამეტრებზე (ან ცალკეული ქსელური კომპონენტების მიმდინარე მდგომარეობაზე). ჩვენს შემთხვევაში (კომპონენტების შეერთების მდგომარეობაზე) სადიაგნოსტიკო პასუხის მიღებისას ნაჩვენები იქნება, რომ მითითებულ კვანძს შეუძლია წარმატებით მიიღოს და გადასცეს პაკეტები.

8.3.2. კონფიგურაციის შესახებ ინფორმაციის მიღება სადიაგნოსტიკო პაკეტით

ხშირად სადიაგნოსტიკო პასუხები კლიენტ–სერვერული შეერთებების მიმდინარე მდგომარეობასთან ერთად შეიცავენ, ინფორმაციას სერვერის ან კლიენტის კონფიგურაციის შესახებ. მის ერთ–ერთი კონკრეტული მაგალითი ნაჩვენებია ნახ.8.3-ზე.



ნახ.8.3. Diagnostic Responder-ი შეიძლება გამოიყენებული იყოს შეერთების ტესტირებისა და კონფიგურაციის შესახებ ინფორმაციის მისაღებად

მოახდენს რა რეაგირებას სადიაგნოსტიკო მოთხოვნაზე, სერვერი ან კლიენტი გაუგზავნის პასუხს (უფრო ზუსტად უპასუხებს სადიაგნოსტიკო შეკითხვის მიმცემ კვანძს) კონფიგურაციის შესახებ (Configuration Response), სადაც აღწერილი იქნება სადიაგნოსტიკო კითხვაში მითითებული კომპონენტები.

სერვერსა და კლიენტებს თავიანთ სადიაგნოსტიკო პასუხებში შეუძლიათ შეატყობინონ შემდეგი კომპონენტების არსებობა და მათი მდგომარეობა:

–IPX/SPX –პროტოკოლის;

–მარშრუტიზატორის დრაივერის;

–ფაილური სერვერ/მარშრუტიზატორის;

–ლოკალური ქსელის დრაივერის;

–გარსის.

კონკრეტულად თუ ვიმსჯელებთ სადიაგნოსტიკო პაკეტის დანიშნულებაზე კონფიგურაციის შესახებ, შეკითხვის (მოთხოვნის) მიმცემი კვანძი აფორმირებს და გამოყენებითი პროგრამით ან პროტოკოლების ანალიზატორით უგზავნის პაკეტს Configuration Request საჭირო სერვისის ან კლიენტის მისამართით. სადიაგნოსტიკო შეკითხვა კონფიგურაციის შესახებ წარმოადგენს პაკეტს, რომელიც შეიცავს კომპონენტების სიას, რომელთა შესახებაც პასუხები ფორმირებული უნდა იქნეს სერვერის ან კლიენტის მიერ სადიაგნოსტიკო პასუხში.

მაგალითის სახით ქვემოთ ნაჩვენებია კონფიგურაციის შესახებ მდგომარეობის ამსახველი სადიაგნოსტიკო პასუხის პაკეტში შემცველი კომპონენტების ჩამონათვალი (სია):

diagxxooxxxooxxxooxxIPX Diagnostic Support Protocol oxxoooxxoooxxooo
Major Version: 1
Minor Version: 0
SPX Diagnostic socket: 0x4003
Number of Components: 3
Component ID :0 (IPX/ SPX)
Component ID : 1 (Router driver)
Component ID: 6 (file server /router)
Number of Local Networks :2
Local Network Type : 1(non-dedcated File Server (virtual board))
Network Address 1: EE ED FA CE
Node address1 :00-00-00-00-00-01
Local Network Type:0 (lan Board)
Network Address 2: DE AD BE FF
Node Address 2:00-00-1b-16-24-1D

სადიაგნოსტიკო პაკეტები შეიძლება გამოყენებული იქნენ მარშრუტიზატორებით ორმაგი გარბენის დროის განსაზღვრი-

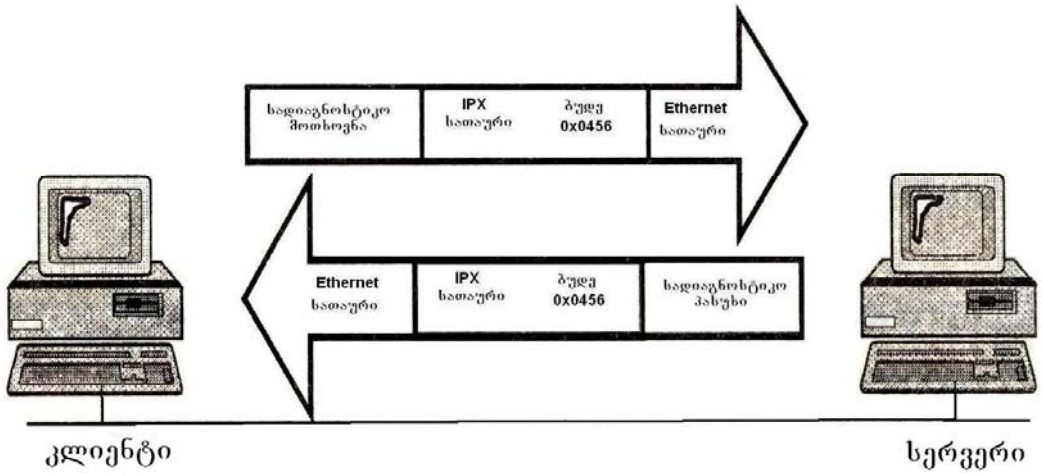
სათვისაც, თუმცა, მაგალითად, NCC LANalyzer შეიცავს გამოყენებით პროგრამას, რომელიც გადასცემს არხებით სადიაგნოსტიკო მოთხოვნის (Diagnostic Reqest) წინასწარ ფორმირებულ პაკეტს, ზოგიერთი შემთხვევაში კი უფრო სასურველია შეიქმნას სადიაგნოსტიკო მოთხოვნის საკუთარი კონკრეტული პაკეტი, რომელშიც თქვენი (როგორც ქსელის ადმინისტრატორის) ინტერესებიდან გამომდინარე უფრო დაკონკრატებული იქნება კითხვები, რომლებზედაც უპასუხებენ თქვენს მიერ დამისამართებული კვანძები (სერვერები ან კლიენტები).

8.3.3. სადიაგნოსტიკო მოთხოვნის პაკეტისა და სადიაგნოსტიკო პასუხი პაკეტის სტრუქტურები

განვიხილოთ თუ როგორი სტრუქტურები უნდა გააჩნდეს მოთხოვნა–პასუხის სადიაგნოსტიკო პაკეტებს, კვანძის მიერ დამისამართებული კლიენტებისა და სერვერებისაკენ. სადიაგნოსტიკო პაკეტების დაგზავნა–მიღების ტაქნოლოგიის მაგალითები მოვიყვანოთ Netware ოპერაციულ სისტემაში მომუშავე ზემოთ ნახსენები ანალიზატორებისათვის.

1. სადიაგნოსტიკო მოთხოვნების პაკეტების სტრუქტურა

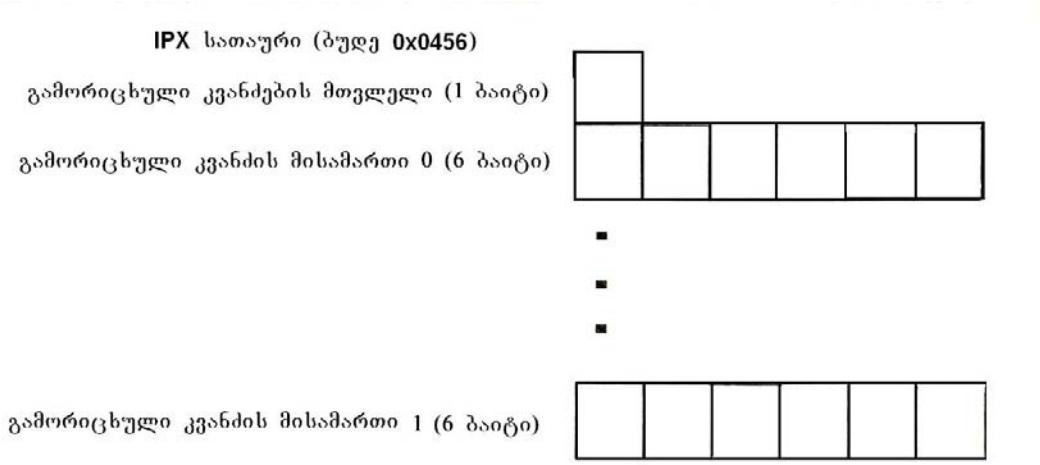
სადიაგნოსტიკო მოთხოვნის (შეკითხვის ანუ განაცხადებაზე პასუხის მისაღებად) პაკეტი განისაზღვრება 0x0456 მნიშვნელობით მიმღების IPX – სათაურის ბუდის ველში (ნახ.8.4).



ნახ. 8.4 სადიაგნოსტიკო პაკეტები იყენებენ ბუდის ნომერს 0x0456

IPX–სათაურს მოსდევს უშუალოდ სადიაგნოსტიკო ინფორმაცია. სადიაგნოსტიკო მოთხოვნის საინფორმაციო ნაწილი შეიძლება იყოს საკმაოდ მარტივი, თუ კი, მაგალითად, საჭიროა მივიღოთ მონაცემები ქსელის იმ სადგურებიდან, რომლებისკენაც დამისამართებულია მოთხოვნა. მეორე მხრივ იგი (საინფორმაციო ნაწილი) შეიძლება იყოს ძალზე მოცულობითიც, რომელიც საშუალებას მოგვცემს შეასრულოთ სადიაგნოსტიკო მოთხოვნის პაკეტის ფართოსამაუწყებლო დაგზავნა ან მიუთითოთ პაკეტში სადგურები, რომლებისგანაც არ ითხოვთ პასუხების მიღებას.

სადიაგნოსტიკო პაკეტის სტრუქტურა ნაჩვენებია ნახ.8.5-ზე.



ნახ.8.5 სდიაგნოსტიკო მოთხოვნის პაკეტის სტრუქტურა

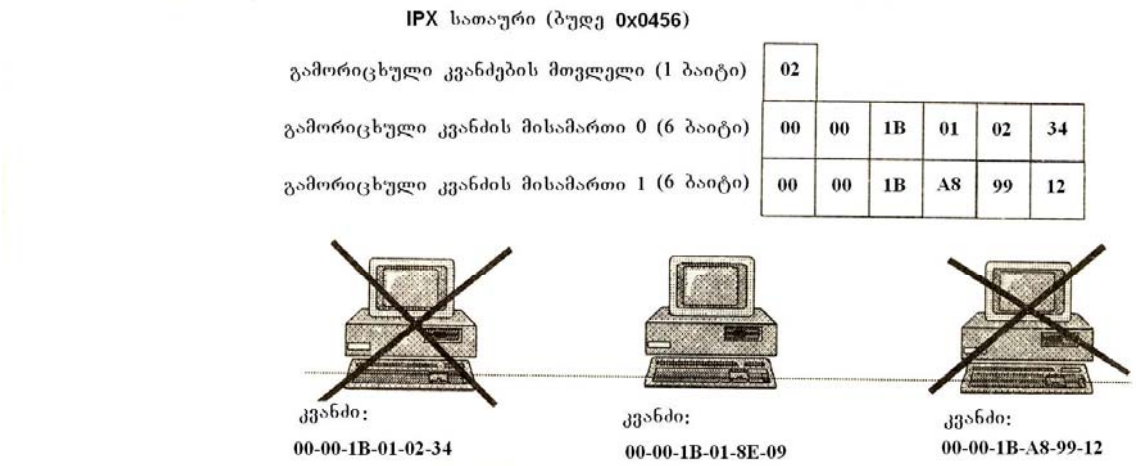
IP სათაურს, როგორც ნახ.8.5–დან ჩანს, მოსდევს გამორიცხული კვანძების მაჩვენებელი ველი და გამორიცხული კვანძების მისამართები. ქვემოთ განვმარტოთ მათი დანიშნულება.

გამორიცხული კვანძების მთვლელი. ეს მთვლელი განსაზღვრავს იმ სადგურების რიცხვს, რომლებისაგანაც არ არის საჭირო პასუხების გაცემა, ე.ი. ველი უჩვენებს სადგურების რაოდენობას, რომლებსაც სადიაგნოსტიკო მოთხოვნა უნდა დატოვონ უპასუხოდ. ამ ველის მნიშვნელობა 0 მიუთითებს იმაზე, რომ მოთხოვნას უნდა უპასუხონ ყველა სადგურებმა. მისი მაქსიმალური დასაშვები მნიშვნელობაა 80 (გამორიცხული სადგურების რიცხვი მდებარეობს საზღვრებში 0–დან 79–მდე).

გამორიცხული კვანძების მისამართები. თუ IPX სათურებში (იხ.ნახ.8.4) მითითებულია სადიაგნოსტიკო პაკეტების ფართო სამაუწყებლო დაგზავნა, მაშინ ამ მოთხოვნას უნდა უპასუხონ ყველა სადგურებმა. იმ შემთხვევაში თუ რომელიმე სერვერიდან

ან კლიენტიდან არ არის საჭირო პასუხის მიღება, მაშინ მისი მისამართი უნდა მოათავსოთ გამორიცხული კვანძის მისამართის ველში, როგორც ზემოთ აღვნიშნეთ, მოპასუხე სადგურიდან შეიძლება გამოირიცხოს 80–მდე სადგური.

ნახ.8.6–ზე მაგალითის სახით ნაჩვენებია სადიაგნოსტიკო მოთხოვნის პაკეტი, რომელშიც აღწერილია ორი გამორიცხული კვანძი (კვანძის გამორიცხვა გადახაზულია ჯვრით).



ნახ.8.6. კვანძის მისამართების სია განსაზღვრავს იმ სადგურებს, რომლებმაც არ უნდა უპასუხონ სადიაგნოსტიკო პაკეტს

ამგვარად, რეაგირებენ რა კვანძები (სერვერები ან კლიენტები) სადიაგნოსტიკო მოთხოვნის პაკეტზე, ისინი გადასცემენ მომთხოვნის კვანძებს სადიაგნოსტიკო პასუხის შემცველ პაკეტს. ამასთან ამ პაკეტით მათ უნდა უპასუხონ არა უგვიანეს 0,5 წმ-ის განმავლობაში, მას შემდეგ რა დროსაც მიიღებენ სადიაგნოსტიკო მოთხოვნას.

თუ საქმე გვაქვს დიდი ქსელის ტესტირებასთან, მოთხოვნა–პასუხის სადიგნოსტიკო პაკეტების ხშირმა ურთიერთ გაცვლებმა შეიძლება გავლენა მოახდინოს ქსელის საერთო წარმადობაზე, რის გამოც შესაძლოა შენელდეს ქსელში პასუხის მიღების დროითი ფაზები (მათ შორის იგულისხმება არა მარტო სადიაგნოსტიკო, არამედ ქსელის მომხმარებელთა სხვა გამოყენებითი საქმიანობის ამსახველი პაკეტების დაგვიანებაც).

2.სადიაგნოსტიკო პასუხის სტრუქტურა

თუ კვანძი იღებს პაკეტს, დამისამართებულს, სახელდობრ, მასზე ანდა პაკეტი ვრცელდება ფართოსამაუწყებლო დაგზავნით, რომელიც მიმღების ბუდის ველში შეიცავს 0x0456 მნიშვნელობას (იხ.ნახ.8.4), კვანძი იგებს, რომ მიიღო სადიაგნოსტიკო პაკეტი. გაანალიზებს რა ამ პაკეტს, სადგური (ან სერვერი, ან კლიენტი) იღებს გადაწყვეტილებას უნდა გასცეს თუ არა მასზე პასუხი. თუ ამ სადგურის კვანძის მისამართი არ არის მითითებული გამორიცხული სადგურების მისამართების სიაში, იგი მოახდენს რეაგირებას მიღებულ პაკეტზე თავის პასუხით, ე.ი. გაუგზავნის მოთხოვნის გამომგზავნ კვანძს სადიაგნოსტიკო პასუხის შემცველ პაკეტს.

სადიაგნოსტიკო პასუხის პაკეტის საინფორმაციო ნაწილი მოსდევს IPX-სათაურს და გადაეგზავნება მომთხოვნ-კვანძს ბუდიდან 0x0456.

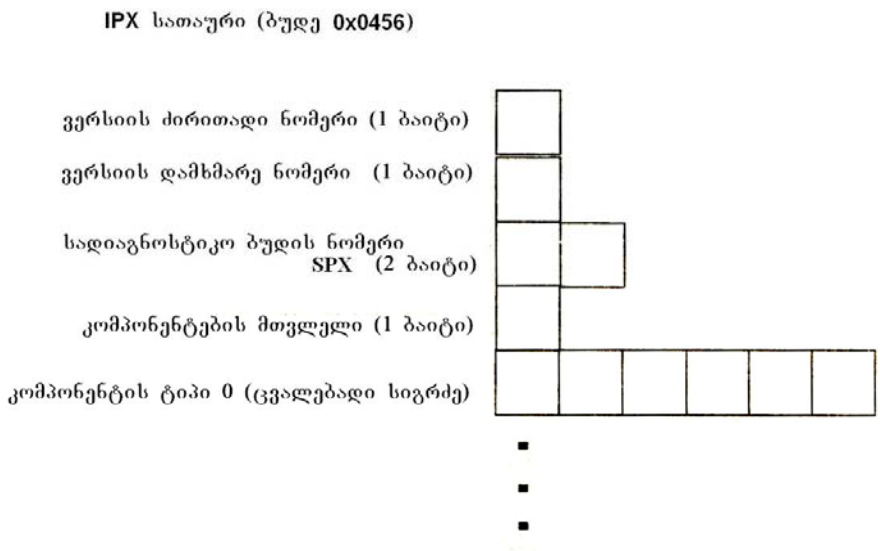
თუ ავიღებთ იმავე ანალიზატორის – LANalyzer for Windows-ის გამოყენების მაგალითს, ნაჩვენები ბუდის ამ მნიშვნელობას

სადიაგნოსტიკო პასუხის მიმღები კვანძი (სერვერი ან კლიენტი) აღიქვამს, როგორც შეტყობინებას კონფიგურაციის შესახებ. ეს კარგად ჩანს ქვემოთ მოყვანილი ჩამონათვალიდან (ეს სიაც ნაჩვენებია მაგალითის სადემონსტრაციოდ), რომელიც ქვემოთ მოგვყავს შემდეგი მაგალითის სახით:

ipx xxxxxxxxxInternetwork Packet Exchange xxxxxxxxx
Checksum : 0xFFFF
Length : 39
Hop Count : 0
Paket Type :17(NCP)
Network: DE Ad BE EF DE AD BE EF
Node : 00-00-1B- 32-E7-00 08-00-14-65-15-75
Socket : Configure 0x04006
diag xxxxxxxxxIPX Diagonostic Support Protocol xxxxxxxxx
Major Version :1
Minor Version :1
SPX Diagnostic Socket :0x4001
Number of Components :4
Component ID : 0(IPX/SPX)
Component ID : 2 (LAN DRAVER)
Component ID: 3(Shell)

იმისდა მიხედვით თუ რამდენი კომპონენტია, რომელთა შესახებაც პასუხობს კვანძი, სადიაგნოსტიკო პასუხის პაკეტის სიგრძე შეიძლება იყოს სხვადასხვა.

სადიაგნოსტიკო პასუხის პაკეტის სტრუქტურა ნაჩვენებია ნახ.8.7-ზე.



ნახ.8.7. სადიაგნოსტიკო პასუხის პაკეტის სტრუქტურა

მოკლედ დავახასიათოდ ამ სტრუქტურების ველების დანიშნულება.

ვერსიის ძირითადი /დამხმარე ნომრები. ამ ნომრების ველები აღწერენ Diagnostis Responder ვერსიას, რომელიც დაყენებულია პასუხის მომცემ სადგურზე. ამჟამად, გამოიყენება ვერსია 1.0 (ძირითადის ნომერია1 , ხოლო დამხმარის –0) ან ვერსია 1.1.

SPX სადიაგნოსტიკო ბუდის ნომერი. ამ ნომერის ველი შეიცავს ბუდეს,რომლის მიხედვითაც დამისამართდება ყველა სადიაგნოსტიკო SPX – პასუხები.

კომპონენტების მთვლელი. კომპონენტების მთვლელი ველი განსაზღვრავს იმ კომპონენტების რაოდენობას, რომელიც აღწერილია სადიაგნოსტიკო პასუხის პაკეტში.

კომპონენტის ტიპი. ეს ველი შეიცავს ინფორმაციას ერთ-ერთი კომპონენტის (ან აქტიური პროცესების) შესახებ სადიაგნოსტიკო პასუხის მომცემ კვანძში (სერვერში ან კლიენტში), ამასთან კომპონენტების სტრუქტურა შეიძლება იყოს

როგორც მარტივი, ისე რთული (გაფართოებული, თუ ეს შეეხება პროცესებს).

დავახასიათოდ მათი ველები, ე.ი. კომპონენტის მარტივი და გაფართოებული ველების სტრუქტურები, უფრო კონკრეტულად:

კომპონენტის მარტივი სტრუქტურა. კომპონენტის მარტივი სტრუქტურა შეიცავს ერთადერთ ერთბაიტიან ველს. მარტივი სტრუქტურები გამოიყენება შემდეგი ტიპის კომპონენტების იდენტიფიკაციისათვის:

კომპონენტის ტიპი	აღწერა
0	IPX/SPX
1	მარშრუტისატორის დრაივერები
2	ლოკალური ქსელის დრაივერები
3	გარსები
4	VAP

ზემოთ მოყვანილ მაგალითზე ნაჩვენები იყო სადიაგნოსტიკო პასუხის პაკეტი, რომელიც ატყობინებს სადიაგნოსტიკო მოთხოვნის (შეკითხვის მომცემ) კვანძს სამი მარტივი კომპონენტის შესახებ. ესენია IPX/SPX,ლოკალური დრაივერი (LAN Driver) და გარსი (Shell).

კომპონენტის გაფართოებული სტრუქტურა. ქვემოთ მოყვანილ მაგალითზე ნაჩვენებია (სადიაგნოსტიკო პასუხის პაკეტის მეორე მაგალითში) გაფართოებული კომპონენტი (იდენტიფიკატორით 6):

diag xxxxxxxxxIPX Diagnostic Support Protocol xxxxxxxxx
Major Version :1
Minor Version :0
SPX Diagnostic Socket: 0x4002
Number of Component :3
Component ID : 0 (IPX/SPX)
Component ID :1 (Bridge Driver)
Component ID : 6 (File Server / Bridge)
Number of local Networks :2
Local Network Type : 1 (Non-dedicated File Server (Virtual board))
Network Address 1: 44 ED EE E0
Node Address 1 :00-00-00-00-00-01
Local Network Type : 0 (LAN Board)
Network Address2: 44 ED 00 10
Node Address 2 : 00-00-1B-02-0F B9

კომპონენტის გაფართოებული სტრუქტურა შეიცავს ინფორმაციას ისეთ კომპონენტებზე, როგორიცაა მარშრუტიზატორები, ფაილ-სერვერები/მარშრუტიზატორები და არაგამოყოფელი IPX/SPX. როგორც მარტივი, ისე გაფართოებული სტრუქტურის შემცველი სადიაგნოსტიკო პასუხის პაკეტი შეიცავს გარკვეული რაოდენობის (შესაბამისად მეტ-ნაკლები) ბაიტებს მონაცემებისათვის, IPX/SPX – სათაურისათვის და საინფორმაციო ნაწილისათვის.

დავახასიათოდ ასევე მოკლედ სადიაგნოსტიკო პაკეტის გაფართოებული კომპონენტები, რომლებსაც უჩვენებს კომპონენტის ტიპის ამსახველი ველი (იხ. ნახ. 8.7-ზე).

გაფართოებული კომპონენტის იდენტიფიკატორი. ეს ველი ასევე განსაზღვრვს კომპონენტის იმ ტიპებს, რომლებიც ემატება სადიაგნოსტიკო პასუხის პაკეტს.

შესაძლებელია გაფართოებული კომპონენტების შემდეგი ტიპები:

გაფართოებული კომპონენტის ტიპი	აღწერა
5	მარშრუტიზატორი
6	ფაილური სერვერ/მარშრუტიზატორი
7	IPX/SPX

ლოკალური ქსელების რიცხვი. ეს ველი განსაზღვრევს იმ ლოკალური ქსელების რიცხვს, რომლებსაც ეს კომპონენტი სადიაგნოსტიკო პაკეტით (პაკეტებით) უგზავნის მონაცემებს მიმდინარე მომენტისათვის თავისი მდგომარეობის შესახებ. თითოეული ქსელისათვის, რომლებსაც აინტერესებთ ამ კომპონენტების მდგომარეობა, სადიაგნოსტიკო პასუხის პაკეტში მიეთითება ქსელის ტიპი, ქსელის მისამართი და კვანძის მისამართი.

ლოკალური ქსელის ტიპი. ლოკალური ქსელის ტიპის მაჩვენებელი ველი შეიცავს ნომერს, რომელიც აღწერს იმ ქსელის ტიპს, რომელსაც უგზავნის მონაცემებს კომპონენტი. დასაშვებია შემდეგი ტიპები:

ქსელის ტიპი	კომპონენტი
0	ლოკალური ქსელის ქსელური ინტერფეისის პლატა
1	გამოუყოფელი ფაილური სერვერი (ვირტუალური პლატა)
2	დანიშნულებაშეცვლილი დაშორებული ხაზი

მაგალითად, Netware 3 და 4 ვერსიებს ყოველთვის აქვთ ჩამოთვლილი გაფართოე-ბული კომპონენტებისათვის არაგამოყო-ფილი ფაილური სერვერი (ვირტუალური პლატა). ეს არის IPX შიგა ქსელი, რომლიც განსაზღვრულია სერვერის დაყენების დროს.

ქსელის მისამართი. ეს ველი შეიცავს კვანძის 6–ბაიტიან მისამართს, რომელიც მიკუთვნებული აქვს ქსელს ლოკალური ქსელის ტიპის მაჩვენებელ ველში.

კვანძის მისამართის ველი. ეს ველი შეიცავს ასევე კვანძის 6–ბაიტიან მისამართს, უმატებს (შეავსებს) რა ზემოთ ნაჩვენები ლოკალური ქსელის მისამართს. დაშორებულ ხაზებს აქვთ კვანძის მისამართი 0x00 00 00 00 00.

IPX შიგა ქსელებს (ვგულისხმობთ Netware 3 და4 ვერსიების მქონე ქსლებს) გააჩნიათ კვანძის მისამართი 0x00 00 00 00 01. ზემოთ ნაჩვენებ მაგალითში (კომპონენტის გაფართოებული კომპონენტის სადიაგნოსტიკო პასუხის მაგალითში) შევამჩნიოთ, რომ სერვერს აქვს შიგა IPX მისამართი 44–ED-EE-ED და ქსელური მისამართი 44-ED-00-10.

კომპონენტის ტიპის აღწერა. ქვემოთ ნაჩვენებია კომპონენტის ტიპის აღწერის მაგალითები, რომლებსაც შესაძლოა შეიცავდეს სადიაგნოსტიკო პასუხის პაკეტები.

კომპონენტის აღმნიშვნელი ნომერი	კომპონენტი	აღწერს პროცესებს
0	IPX/SPX	IPX/SPX–ში მიმდინარე ფაქტიური პროცესი ან გამოყოფილ Netware ფაილ–სერვერის მოდულში,გამოყოფილ მარშრუტიზატორში ან კლიეტში მიმდინარე პროცესები.
1	მარშრუტიზატორის დრაივერები	ლოკალური ქსელის პლატის დრაივერში მიმდინარე პროცესები, რომლებიც ასახავენ ფაილ–სერვერის ან მარშრუტიზატორის მიმდინარე მდგომარეობას, ამასთან "ლოკალური ქსელის დრაივერი" ნიშნავს კლიენტის ქსელური პლატის დრაივერს.
2	გარსები	პროცესი, რომლებიც მიმდინარეობს ემულაციის მოდულში ან მუშა სადგურზე DOS– ის გარსში
4	VAP	პროცესები ემულაციის მოდულში ან DOS–ის გარსში ან გარე მარშრუტიზატორში VAP–ის მხარდასაჭერად.
5	მარშრუტიზატორი	პროცესები სამარშრუტო კომპონენტში (გარე მარშრუტიზატორი)
6	ფაილ–სერვერ/მარშრუტ.	პროცესები, რომლებიც გვიჩვენებს ფაილ–სერვერ მარშრუტიზატორში მიმდინარე მდგომარეობას (შიგა მარშრუტიზატორში).
7	არაგამოყოფილი IPS/SPX	IPS/SPX პროცესები არაგამოყოფილ ფაილ–სერვერზე, გარე მარშრუტიზატორზე ან შიგა IPX ქსელში

8.4. სადიაგნოსტიკო ტესტების შედგენის ტექნოლოგიის მაგალითები

ამავე თავის დასაწყისში ვახსენეთ, რომ ანალიზატორის დახმარებით კომპიუტერული ქსელის კლიენტ–სერვერული შეერთების შესამოწმებლად ან ინფორმაციის შესაგროვებლად სერვერის ან კლიენტის კონფიგურაციის შესახებ, შეიძლება გამოყენებული იქნეს პროგრამათა კომპლექსი Diagnostic Responder.

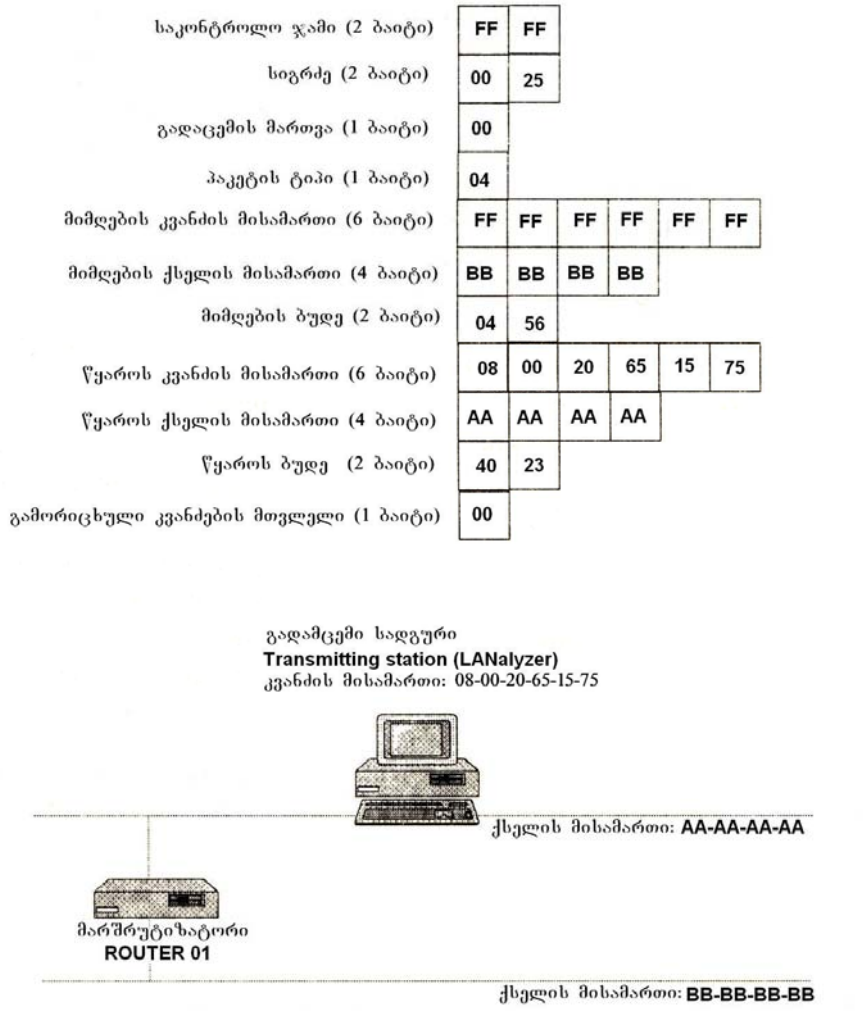
სადიაგნოსტიკო ტესტის შექმნის დროს დასაწყისში ჯერ უნდა განსაზღვროთ, რომელ ქსელს და რომელ კვანძს გინდათ გაუგზავნოთ სადიაგნოსტიკო შეკითხვა (მოთხოვნა) და რომელ კომპონენტიდან გსურთ მიიღოთ პასუხი. ეს ინფორმაცია (მისამართები) უნდა შეიტანოთ (მიუთითოთ) სადიაგნოსტიკო მოთხოვნის პაკეტის IPX–სათაურში.

ამგვარად, მიმღების (სადიაგნოსტიკო პასუხის პაკეტის მიმღები ქსელის) მისამართის ველში უნდა მიუთითოდ დაშორებული ან ლოკალური ქსელის მისამართი. ლოკალური ქსელის მისათითებლად შეიძლება გამოიყენოთ მისამართის მნიშვნელობა 0x00 00 00 00 00. კლიენტის ან სერვერის კვანძის მისამართი, რომელსაც უნდა გაუგზავნოთ სადიაგნოსტიკო მოთხოვნა, უნდა მოათავსოთ მიმღების (სადაც იმყოფება გამოსაკვლევი კომპონენტი) კვანძის მისამართის ველში. თუ მისამართის მნიშვნელობა ფართოსამაუწყებლოა, ე.ი. არის

OxFF-FF-FF-FF-FF-FF, მაშინ ამ მოთხოვნას უნდა უპასუხონ მითითებული ქსელის ყველა კვანძმა. თქვენი ქსელური მისამართი უნდა მოათავსოთ წყაროს (მოთხოვნის გამგზავნის) მისამართის ველში. თუ თქვენ გსურთ, რომ პასუხები გადაეცეს სხვა ქსელში, მისი მისამართი შეგიძლიათ მოათავსოთ საწყისი ქსელის მისამართის ველში. იმისათვის, რომ დაიჭიროთ ამა თუ იმ კონკრეტულ კვანძზე დამისამართებული სადიაგნოსტიკო პასუხის პაკეტები, ანალიზატორი (ჩვენს მაგალითში გამოყენებული LANalyzer) უნდა გააწყოთ (მომართოთ) მოთხოვნის ყველა პაკეტის ფილტრაციაზე, რომლებიც კი ეგზავნება კვანძის ამ მისამართზე.

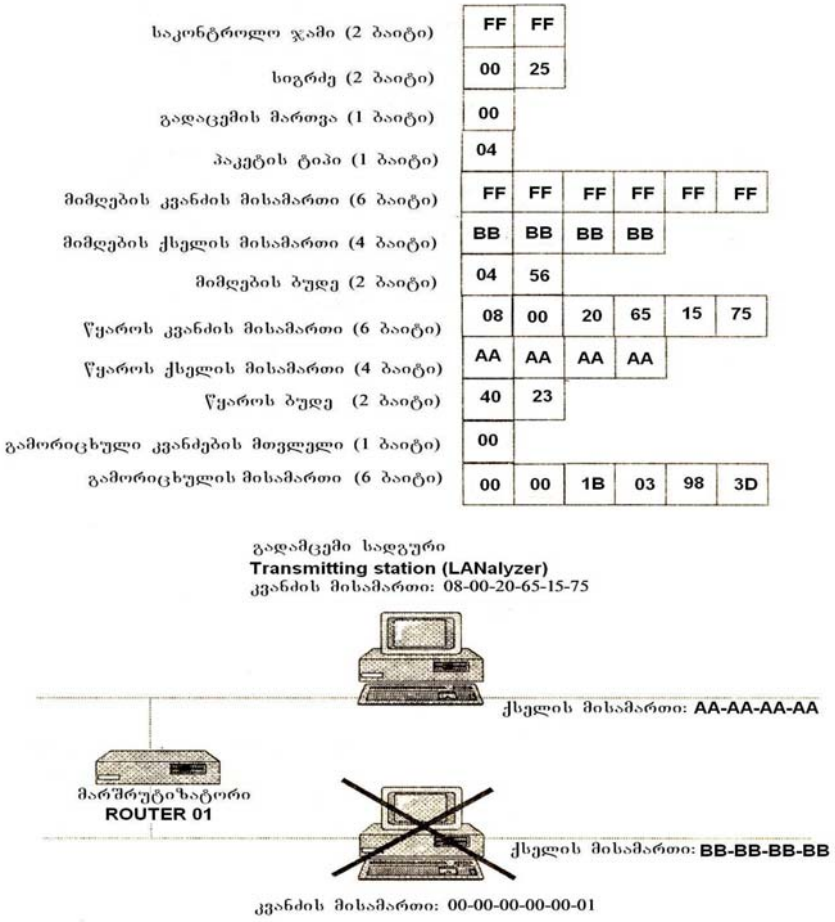
მაგალითად, ნახ.8.8–ზე ნაჩვენებია სადიაგნოსტიკო მოთხოვნის პაკეტი, რომელიც გადაეცემა ფართოსამაუწყებლოდ BB-BB-BB-BB ქსელის ყველა კვანძს.

IPX–სათაურის შემდეგ შეგიძლიათ უჩვენოთ ინფორმაცია, რომელიც ეკუთვნის მიმღებს. თუ თქვენ გსურთ მიიღოთ პასუხი ყველა მუშა სადგურიდან (რაზედაც მიუთითებს IPX სათაურის ფართოსამაუწყებლო მისამართი), მაშინ გამორიცხული კვანძების (რომლებმაც არ უნდა უპასუხონ სადიაგნოსტიკო მოთხოვნის პაკეტს) მთვლელის ველის მნიშვნელობა უნდა იყოს ნულოვანი (0x00), ხოლო თუ თქვენ გსურთ, რომ გიპასუხონ (ე.ი. გამოგიგზავნოთ სადიაგნოსტიკო პასუხების პაკეტები) სადგურის არა ყველა, არამედ მათმა გარკვეულმა ნაწილმა, მაშინ თქვენ გამორიცხული კვანძების მისამართების მთვლელში უნდა მიუთითოთ (ჩამოვთვალოთ) იმ კვანძების მისამართები, რომ –



ნახ.8.8 IPX–სათაური შეიცავს ინფორმაციას სადიაგნოსტიკო პაკეტის გაგზავნისა და მიმღების შესახებ

ლებმაც თქვენს მოთხოვნას არ უნდა უპასუხონ. ამასთან, მაგალითად, თქვენ შეგიძლიათ მიუთითოთ, რომ თქვენ გსურთ პასუხის მიღება მხოლოდ მუშა სადგურებიდან და არა სერვერებიდან. ეს ნაჩვენებია ნახ. 8.9-ზე ნაჩვენებ მაგალითზე, საიდანაც ჩანს, რომ სადიაგნოსტიკო მოთხოვნა ეგზავნება BB-BB-BB-BB ქსელის ყველა კვანძს, თუმცა IPX–სათაურის შემდეგ მითითებულია, რომ მუშა სადგურმა, რომლის მისამართია

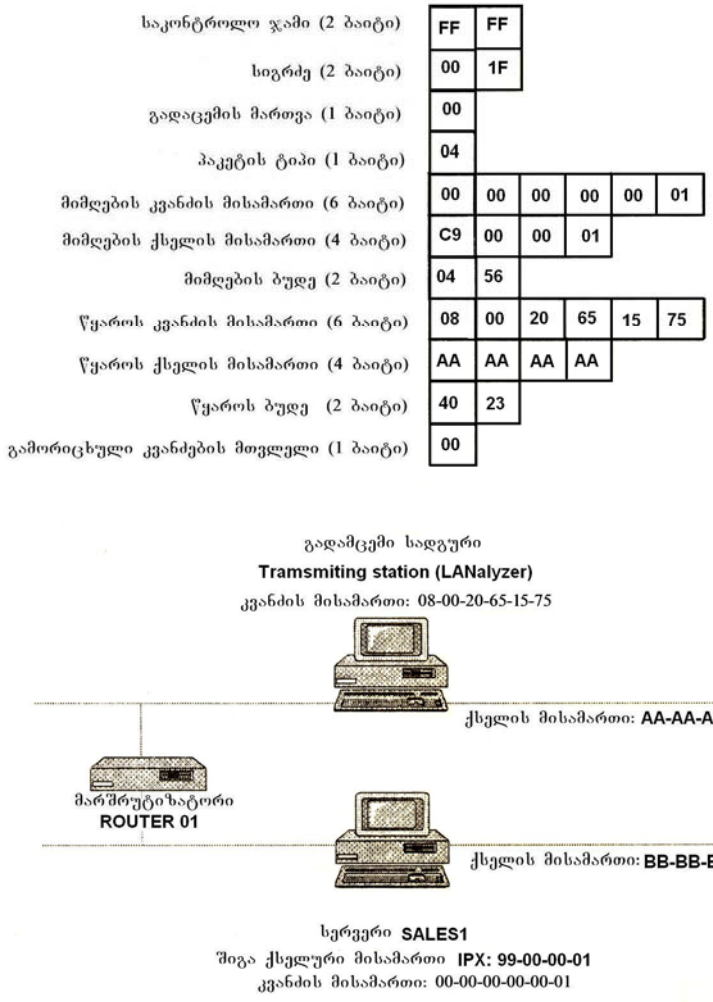


ნახ.8.9. გამორიცხული კვანძის ველში მითითებული კონკრეტული კვანძის მისამართი მიუთითებს იმაზე, რომ ამ კვანძმა არ უნდა უპაასუხოს სადიაგნოსტიკო მოთხოვნის პაკეტს

0x00-1B-03-98-3D, არ უნდა უპასუხოს ამ მოთხოვნას, ხოლო ამ ქსელის სხვა დანარჩენი კვანძები კი ვალდებულია გაუგზავნოს მომთხოვნ კვანძს (ე.ი. სადიაგნოსტიკო მოთხოვნის პაკეტის წყარო–სადგურს) პასუხები.

სადიაგნოსტიკო პაკეტების გადაცემა–მიღების პროცედურებით შეიძლება ასევე გაირკვეს შეერთებების (დაკავშირების) მდგომარეობები საჭირო კლიენტებსა და სერვერებს შორის.

მაგალითის სახით ნახ. 8.10–ზე ნაჩვენებია SALES1 სერვერთან შეერთების შემოწმების ტესტი (ამას უჩვენებს მიმღები ქსელისა და მიმღები კვანძის მისამართების ველებში შესაბამისი მისამართების არსებობა სადიაგნოსტიკო ტესტის გამგზავნის IPX–სათაურში.



ნახ. 8.10. შეერთების შემოწმება SALES1 სერვერთან

ვინაიდან ქსელის (რომელსაც აკონტროლებს ქსელის ადმინისტრატორი) ყველა სერვერზე ჩატვირთული Diagnostic Responder, მათ უნდა უპასუხონ მოთხოვნაზე (წყარო–სადგურის სადიაგნოსტიკო მოთხოვნის პაკეტზე). თუმცა, ვინაიდან Diagnostic Responder იყენებს IPX–პროტოკოლს, არ არის გარანტია იმისა, რომ სადიაგნოსტიკო მოთხოვნები მიაღწევს დაშორებული ქსელის კომპონენტებს. ამ შემთხვევაში შეიძლება მოთხოვნის პაკეტი დაეგზავნოს ყველა კვანძს, რათა დადგინდეს არის თუ არა შეღწევა (წვდომა) დაშორებულ ქსელში. თუ ყველა სადგური სერვერის გარდა პასუხობენ წარმატებით, შეიძლება დავასკვნათ, რომ ან ეს სერვერი არ მუშაობს, ან მასთან არ არის კავშირი (შეერთება).

ამგვარად, Diagnostic Responder შეიძლება იყოს ქსელში შეერთებების ტესტირების მეტად საჭირო და მნიშვნელოვანი ინსტრუმენტი. ამასთან, ვინაიდან პასუხები შეიძლება შეიცავდნენ ასევე ინფორმაციას სერვერებისა და კლიენტების კონფიგურაციების შესახებაც, იგი შეიძლება გამოყენებული იქნეს ინფორმაციის შესაგროვებლადაც. ამიტომაც არის, რომ ზოგიერთი მწარმოებელი Diagnostic Responder–ს იყენებს სხვადასხვა ქსელური მოწყობილობების ქსელში მათი არსებობის ფაქტის დასადგენადაც.

ჩვენ სადიაგნოსტიკო ტექნოლოგიების გასაცნობად მაგალითის სახით განვიხილეთ NCC LANalyzer–ანალიზატორის შესაძლებლობები სადიაგნოსტიკო მოთხოვნების პაკეტების გადასაცემად და პასუხების შემცველი პაკეტების ფილტრი-

სათვის. ამ მიზნებს ემსახურება ის, რომ ამ ტიპის ანალიზატორს გააჩნია ორი გამოყენებითი პროგრამა: NODEVIEW და ROUTVIEW. პირველი მათგანი შეიძლება გამოყენებული იქნეს ქსელის კვანძებთან შეერთებების შესამოწმებლად, ხოლო მეორე – იმ კვანძებისა და სერვერების შესამოწმებლად, რომლებიც იმყოფებიან მარშრუტიზატო-რის სხვა (დაშორებულ) მხარეს.

დასასრულს, კვლავ შევნიშნოთ, რომ ჩვენს მაგალითებში განხილული ანალიზატორების (LANalyzer for Windows და NCC LANalyzer) გარდა, ამჟამად წარმატებით გამოიყენება სხვადასხვა მწარმოებელი ფირმების მიერ დამუშავებული სადიაგნოსტიკო საშუალებებიც, რომლებიც ერთმანეთისაგან განსხვავდებიან, როგორც ავღნიშნეთ, სხვადასხვა ფუნქციონალური შესაძლე-ბლობებითა და მათი საბაზრო ღირებულებებითაც.

კომპიუტერული უზრუნველყოფა ნ. ნატროშვილის

იბეჭდება ავტორის მიერ წარმოდგენილი სახით

გადაეცა წარმოებას 28.05.2009. ხელმოწერილია დასაბეჭდად 12.06.2009. ქაღალდის ზომა 60X84 1/16. პირობითი ნაბეჭდი თაბახი 17. ტირაჟი 100 ეგზ.

საგამომცემლო სახლი „ტექნიკური უნივერსიტეტი“, თბილისი,
კოსტავას 77